J. Eur. Math. Soc. 11, 1057–1103

Jean Bourgain · Alex Gamburd

Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$: II

with an appendix by Jean Bourgain

Received October 8, 2008

Abstract. We prove that the Cayley graphs of $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ are expanders with respect to the projection of any fixed elements in $\mathrm{SL}_d(\mathbb{Z})$ generating a Zariski dense subgroup.

1. Introduction

The general setup considered in [7] and [8] and here is as follows.

Let $S = \{g_1, \dots, g_k\}$ be a subset of $\mathrm{SL}_d(\mathbb{Z})$ and $\Lambda = \langle S\rangle \subset \mathrm{SL}_d(\mathbb{Z})$ the subgroup generated by S. We assume Λ is Zariski dense in SL_d. According to the theorem of Matthews–Vaserstein–Weisfeiler [21], there is some integer $q_0 = q_0(S)$ such that $\pi_q(\Lambda) = \mathrm{SL}_d(q)$, assuming $(q, q_0) = 1$. Here π_q denotes the reduction mod q. It was conjectured in [19], [7], [8] that the Cayley graphs $\mathcal{G}(\mathrm{SL}_d(q), \pi_q(S))$ form an expander family, with expansion coefficient bounded below by a constant $c = c(S)$. For $d = 2$, we verified this conjecture in [5], [7], [8] provided q is assumed square free (in fact, for q prime, even stronger results are obtained in [5]). At the other end, there are moduli of the form $q = p^n$ where we fix p say and let $n \to \infty$. In [6] we established the conjecture for such moduli in the case $d = 2$. The main goal of this paper is to extend the method to the case $d > 2$ providing the first results towards the above conjecture in this setting. Our main result is the following:

Theorem 1.1. *Let $S = \{g_1, \dots, g_k\}$ be a finite subset of $\mathrm{SL}_d(\mathbb{Z})$ generating a subgroup Λ which is Zariski dense in SL_d. Let p be a sufficiently large prime. Then the Cayley graphs $\mathcal{G}(\mathrm{SL}_d(p^n), \pi_{p^n}(S))$ form an expander family as $n \to \infty$. The expansion coefficients are bounded below by a positive number $c(S, p) > 0$.*

As in [5, 6, 8], the proof, following the approach of Sarnak and Xue [25], is based on exploiting high multiplicity of nontrivial eigenvalues (the bound obtained in [6] is sufficient for our purposes), together with the sharp upper bound on the number of short closed geodesics. As in the preceding works, the starting point for the proof of the upper bound

J. Bourgain: School of Mathematics, IAS, Princeton, NJ 08540, USA;
e-mail: bourgain@math.ias.edu

A. Gamburd: Department of Mathematics, UCSC, Santa Cruz, CA 95064, USA, and Department of Mathematics, Northwestern University, Evanston, IL 60208-2730, USA;
e-mail: agamburd@ucsc.edu

is the appropriate sum-product estimate—in our case we need the extension of the sum-product estimate for $\mathbb{Z}/p^n\mathbb{Z}$ established in [3] to certain extension fields. This crucial ingredient, which is of independent interest, is obtained in the Appendix by the first author. As in [6], the proof relies on a "multi-scale" approach, reminiscent of the Solovay–Kitaev algorithm in quantum computation [11] (see [12, 13] for an $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ analogue, yielding uniform polylog diameter bounds). The "multi-scale" structure in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ is encapsulated in the identity

$$(I + QA)(I + QB) \equiv I + Q(A + B) \pmod{Q^2},$$

which allows for immediate exploitation of the sum structure. The exploitation of the product structure is based on producing a large set of commuting elements, diagonalized in the appropriate basis, and then proceeding by conjugation. To execute this argument we need to produce elements outside of proper subvarieties, which is accomplished by analyzing the random walk in $\mathrm{SL}_d(\mathbb{Z})$ based on the generating set S and using the theory of products of random matrices [2] and effective Bézout theorem [1]. As in the preceding works, the required upper bound is obtained from a measure convolution result which is established using noncommutative product-set estimates due to Tao [26, 27].

We now turn to some consequences of Theorem 1.1. Let us take the set S symmetric, i.e. $S = \{g_1, \dots, g_k, g_1^{-1}, \dots, g_k^{-1}\}$, to which we associate the probability measure

$$\nu = \frac{1}{|S|}\sum_{g\in S}\delta_g$$

on SL_d (δ_x denotes the Dirac measure at x). The theorem stated above has the following implication, whose proof is analogous to the proof of Proposition 3.2 in [8]:

Corollary 1.1. *Let S and ν be as above. Let $\mathfrak{S}$ be a nontrivial algebraic subvariety of $\mathrm{SL}_d(\mathbb{C})$. Then the convolution powers $\nu^{(\ell)}$ of ν satisfy*

$$\nu^{(\ell)}(\mathfrak{S}) < e^{-c\ell} \quad \text{for } \ell \to \infty \tag{1.1}$$

for some $c > 0$ (in fact c depends only on ν and the degree of $\mathfrak{S}$).

Assume now q a sufficiently large prime and G a proper subgroup of $\mathrm{SL}_d(q)$. From the work of Nori [22] on the strong approximation property, it follows that G satisfies a nontrivial algebraic equation $\bmod\, q$. We may then invoke Corollary 1.1 to obtain

Corollary 1.2. *Let again S and ν be as above and let q be a sufficiently large prime. Let G be a proper subgroup of $\mathrm{SL}_d(q)$. Denote $\pi_q[\nu]$ also by ν. There is an estimate*

$$\nu^{(\ell)}(G) < Cc^{-c\ell} \quad \text{for } \ell < \log q, \tag{1.2}$$

where the constants c, C only depend on S.

Corollary 1.2 is of significance to establish the conjecture mentioned at the beginning for other moduli q (besides q of the form $q = p^n$ with fixed p). Recalling the approach in

[5] (see also Section 2), the conjecture for $\mathrm{SL}_d(q)$ (q prime say) will result by combining Lemma 2.1 and Corollary 1.2 with a 'product theorem' in $\mathrm{SL}_d(q)$, of the form

$$|A \cdot A \cdot A| > |A|^{1+\varepsilon} \tag{1.3}$$

whenever $A \subset \mathrm{SL}_d(q)$ generates the full group and $|A| < |\mathrm{SL}_d(q)|^{1-\delta}$, with $\varepsilon = \varepsilon(\delta) > 0$.

Theorem 1.2. *Assume* (1.3) *holds in* $\mathrm{SL}_d(p)$. *Let* $S = \{g_1, \dots, g_k\}$ *be a finite subset of* $\mathrm{SL}_d(\mathbb{Z})$ *generating a subgroup* Λ *which is Zariski dense in* SL_d. *Then the family of Cayley graphs* $\mathcal{G}(\mathrm{SL}_d(p), \pi_p(S))$ *forms an expander family as* $p \to \infty$. *The expansion coefficients are bounded below by a positive number* $c(S) > 0$.

The product theorem (1.3) was recently proven by Helfgott [16] for $d = 3$ and consequently we have:

Theorem 1.3. *Let* $S = \{g_1, \dots, g_k\}$ *be a finite subset of* $\mathrm{SL}_3(\mathbb{Z})$ *generating a subgroup* Λ *which is Zariski dense in* SL_3. *Then the family of Cayley graphs* $\mathcal{G}(\mathrm{SL}_3(p), \pi_p(S))$ *forms an expander family as* $p \to \infty$. *The expansion coefficients are bounded below by a positive number* $c(S) > 0$.

The special moduli $q = p^n$ with fixed p turn out to be also of interest in relation to the work of D. Long, A. Lubotzky and A. Reid [18] on Heegaard genus and property τ for hyperbolic 3-manifolds. More precisely, let M be a finite volume hyperbolic 3-manifold. From the result for the $\mathrm{SL}_2(p^n)$ towers, one may then produce a nested cofinal family of finite sheeted covers with positive infimal Heegaard gradient. [18] also puts forward the conjecture that any finitely generated subgroup Γ of $\mathrm{GL}(n, \mathbb{C})$ with semisimple Zariski closure has a cofinal (nested) $\mathcal{L} = \{N_i\}$ of finite index normal subgroups for which Γ has property τ with respect to $\mathcal{L}$. It seems reasonable to believe that the moduli $q = p^n$ and the proof of our theorem may provide an approach to this last conjecture.

2. Measure convolution and approximate subgroups

Let ν be a finitely supported symmetric probability measure on $\mathrm{SL}_d(\mathbb{Z})$ whose support, supp ν, generates a Zariski dense subgroup. It is no restriction to assume this subgroup is free. We will also denote by ν the measure $\pi_q[\nu]$ on $\mathrm{SL}_d(\mathbb{Z}_q)$.

The following result is proven using the noncommutative Balog–Szemerédi–Gowers theorem due to Tao (see [26, 27]). The argument is analogous to the one in the proof of Proposition 2 in [5].

Lemma 2.1. *Let* G *be a finite group with* $N = |G|$. *Suppose* $\mu \in \mathcal{P}(G)$ *is a symmetric probability measure on* G *and assume*

$$\|\mu\|_\infty < N^{-\gamma} \quad \text{and} \quad \|\mu\|_2 > N^{-1/2+\gamma} \tag{2.1}$$

with $\gamma > 0$ *an arbitrary given constant. Assume further that*

$$\|\mu * \mu\|_2 > N^{-\varepsilon}\|\mu\|_2 \tag{2.2}$$

with $0 < \varepsilon < \varepsilon(\gamma)$. *Then there exists a subset* $H \subset G$ *with the following properties:*

$$H = H^{-1} \text{ and there exists a subset } X \subset G \text{ with } |X| < N^{\varepsilon'} \text{ such that}$$
$$H \cdot H \subset X \cdot H \text{ and } H \cdot H \subset H \cdot X, \tag{2.3}$$
$$\mu(x_0 H) > N^{-\varepsilon'} \quad \text{for some } x_0 \in G, \tag{2.4}$$
$$|H| < N^{1-\gamma}, \tag{2.5}$$

where $\varepsilon' \sim \varepsilon$.

Remark. In the terminology of [27], H satisfying (2.3) is called an '$N^{\varepsilon'}$-approximate subgroup' of G. In particular, H satisfies the product set estimates

$$|H^{(s)}| = |\underbrace{H \dots H}_{s\text{-fold}}| < q^{(s-1)\varepsilon'}|H| \quad \text{for } s \geq 1. \tag{2.6}$$

We let $G = \mathrm{SL}_d(\mathbb{Z}_q)$, $q = p^n$ with p fixed. Hence $\log N \sim n$. Our measure μ will be obtained as an ℓ-fold convolution $\mu = \nu^{(\ell)} = \nu * \cdots * \nu$, where $\ell \sim n$. Note that if $m \sim n$, then $\pi_{p^m}(H)$ is an approximate subgroup in $\mathrm{SL}_d(p^m)$.

Assume μ satisfies (2.1)–(2.2) and take $H \subset G$ satisfying (2.3)–(2.5). Fix $\ell_0 < \ell$ and write

$$N^{-\varepsilon'} \overset{(2.4)}{<} \mu(x_0 H) = \sum_{y \in G} \nu^{(\ell-\ell_0)}(y)\nu^{(\ell_0)}(y^{-1}x_0 H),$$

implying

$$\nu^{(\ell_0)}(x_1 H) > N^{-\varepsilon'} \quad \text{for some } x_1 \in G. \tag{2.7}$$

Hence, since H and ν are symmetric,

$$\begin{aligned}\nu^{(2\ell_0)}(H.H) &\geq \sum_{y \in x_1 H,\, z \in H^{-1}H} \nu^{(\ell_0)}(y)\nu^{(\ell_0)}(zy^{-1}) \geq \sum_{y \in x_1 H,\, w \in H} \nu^{(\ell_0)}(y)\nu^{(\ell_0)}(w^{-1}x_1^{-1}) \\ &= [\nu^{(\ell_0)}(x_1 H)]^2 \overset{(2.7)}{>} N^{-2\varepsilon'}. \end{aligned} \tag{2.8}$$

3. Preliminaries related to sum-product

The results in this section depend essentially on [3]. Fix $w \in \mathbb{Z}_+$. Denote by $\mathbb{Z}_q^w = \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q$ the w-fold product ring. For $q' \,|\, q$, let $\pi_{q'} : \mathbb{Z}_q^w \to \mathbb{Z}_{q'}^w$ be the quotient map. In what follows, $q = p^n$ with p a fixed prime and $n \to \infty$.

Proposition 3.1. *Given $\delta > 0$, there are $\varepsilon, \kappa > 0$ and positive integers $r, s < C(\delta)$ such that the following holds. Let $q_1 \mid q$ with $q_1 < q^\varepsilon$ (q_1 sufficiently large) and $A \subset \mathbb{Z}_q^w$ satisfy*

$$|\pi_{q_1}(A)| > q_1^\delta. \tag{3.1}$$

Then there are $q_2 \mid q$ and $q_3 \mid q_2$ and $\xi \in \mathbb{Z}_{q_2}^w$ such that

$$\log q_2 < C(\delta) \log q_1, \tag{3.2}$$

$$q_2 > q_1^\kappa q_3, \tag{3.3}$$

$$\pi_p(\xi) \neq 0, \tag{3.4}$$

$$\pi_{q_2}(rA^{(s)} - rA^{(s)}) \supset q_3 \xi \mathbb{Z}_{q_2}. \tag{3.5}$$

In (3.5), *$q_3\xi\mathbb{Z}_{q_2}$ is the subset $\{q_3 t\xi \mid 0 \le t \le q_2/q_3\}$ of $\mathbb{Z}_{q_2}^w$.*

The following proposition (Proposition 1.4 from [6]) yields the conclusion of Proposition 3.1 for $w = 1$.

Proposition 3.2. *Given $\delta > 0$, there is $\varepsilon > 0$ and positive integers $r, s < C(\delta)$ such that if q is as above, $q_1 \mid q$, $q_1 < q^\varepsilon$ and $A \subset \mathbb{Z}_q$ satisfies*

$$|\pi_{q_1}(A)| > q_1^\delta, \tag{3.6}$$

then

$$\pi_{q_2}(rA^{(s)} - rA^{(s)}) \supset q_3 \mathbb{Z}_{q_2}$$

for some divisors $q_2 \mid q$ and $q_3 \mid q_2$ with

$$\log q_2 < C(\delta) \log q_1, \qquad q_2 > q_1^{\delta/4} q_3.$$

Proof of Proposition 3.1. We proceed by induction on w, the case $w = 1$ following from Proposition 3.2. Assume the statement is valid for w and $A \subset \mathbb{Z}_q^{w+1}$ satisfies (3.6). Denote by P_I for $I \subset \{1, \dots, w+1\}$ the coordinate restriction. Rearranging the coordinates we may assume

$$|\pi_{q_1}(B)| > q_1^{\frac{w}{w+1}\delta} > q_1^{\delta/2},$$

where $B = P_{\{1,\dots,w\}}(A)$. From the induction hypothesis, we obtain $q_2 \mid q$, $q_3 \mid q$ and $\xi \in \mathbb{Z}_{q_2}^w$ such that

$$\log q_2 < C(\delta) \log q_1, \tag{3.7}$$

$$q_2 > q_1^\kappa q_3, \tag{3.8}$$

$$\pi_p(\xi) \neq 0, \tag{3.9}$$

$$\pi_{q_2}(rB^{(s)} - rB^{(s)}) \supset q_3 \xi \mathbb{Z}_{q_2} \tag{3.10}$$

with $r, s < C(\delta)$.

Setting $A_1 = rA^{(s)} - rA^{(s)}$, it follows from (3.10) that there is a map $\varphi : \mathbb{Z}_{q_2/q_3} \to A_1$ such that

$$\pi_{q_2} P_{\{1,\dots,w\}} \varphi(x) = q_3 x \xi \quad \text{for } x \in \mathbb{Z}_{q_2/q_3}. \tag{3.11}$$

We distinguish several cases.

Case 1: $|\pi_{q_2^2}(P_{w+1}(\varphi(\mathbb{Z}_{q_2/q_3})))| < (q_2/q_3)^{1/2}$. Clearly there are elements $x_1, x_2 \in \mathbb{Z}_{q_2/q_3}$ with $x_1 \neq x_2 \pmod{q'}$ where $q' \mid q$, $(q')^2 < q_2/q_3$ and $P_{w+1}(\varphi(x_1) - \varphi(x_2)) \equiv 0 \pmod{q_2^2}$. Write $x_1 - x_2 = q_4 y$ with $q_4 \mid q'$ and $\pi_p(y) \neq 0$. Hence for $x \in \mathbb{Z}_{q_2/q_3}$, we have

$$\varphi(x)(\varphi(x_1) - \varphi(x_2)) \in A_1 \cdot A_1 - A_1 \cdot A_1,$$

and by construction

$$\begin{aligned}\varphi(x)(\varphi(x_1) - \varphi(x_2)) &= (P_{\{1,\dots,w\}}\varphi(x)(P_{\{1,\dots,w\}}\varphi(x_1) - P_{\{1,\dots,w\}}\varphi(x_2)), 0) \pmod{q_2^2}\\ &= (q_3^2 q_4 x y \xi^2, 0) \pmod{q_2 q_3},\end{aligned}$$

where $\pi_p(y\xi^2) \neq 0$ and

$$\frac{q_2 q_3}{q_3^2 q_4} \geq \frac{q_2}{q_3 q'} > \left(\frac{q_2}{q_3}\right)^{1/2} > q_1^{\kappa/2}.$$

Thus the claim in the proposition holds in this case.

Case 2: $|\pi_{q_2^2}(P_{w+1}(\varphi(\mathbb{Z}_{q_2/q_3})))| \geq (q_2/q_3)^{1/2}$. It follows that the set $S = P_{w+1}(A_1)$ satisfies

$$|\pi_{q_2^2}(S)| > q_1^{\kappa/2} > (q_2^2)^{\kappa/4C(\delta)}$$

(the last inequality by (3.7)). Apply Proposition 3.2 with δ replaced by $\kappa/4C(\delta)$, and q_1 by q_2^2. We assume here

$$q_2^2 < q^{\varepsilon(\kappa/4C(\delta))}, \tag{3.12}$$

where $\varepsilon(\cdot)$ is the function from Proposition 3.2. Clearly (3.12) will hold if we assume

$$\varepsilon < \frac{1}{2C(\delta)}\varepsilon\left(\frac{\kappa}{4C(\delta)}\right)$$

in the assumption $q_1 < q^{\varepsilon}$.

From Proposition 3.2 we obtain $q_5 \mid q$, $q_6 \mid q_5$ with

$$\log q_5 < 2C\left(\frac{\kappa}{4C(\delta)}\right)\log q_2, \tag{3.13}$$

$$q_5 > q_6 q_2^{\kappa/8C(\delta)}, \tag{3.14}$$

$$q_6\mathbb{Z}_{q_5} = \pi_{q_5}(r_1 S^{(s_1)} - r_1 S^{(s_1)}) = \pi_{q_5} P_{w+1}(r_1 A_1^{(s_1)} - r_1 A_1^{(s_1)}), \tag{3.15}$$

where $r_1, s_1 < C(\kappa/4C(\delta))$.

Take again $q' \mid q$ with $(q')^2 \sim q_2/q_3$. We distinguish two further cases.

Case 2.1: The map $\varphi : \mathbb{Z}_{q_2/q_3} \to A_1$ is additive $\bmod q_3 q'$. This means that

$$\varphi(x + y) = \varphi(x) + \varphi(y) \pmod{q_3 q'} \quad \text{for } x, y \in \mathbb{Z}_{q_2/q_3}.$$

It follows that for $x \in \mathbb{Z}_{q_2/q_3}$,

$$\varphi(x) = x\varphi(1) \ (\mathrm{mod}\, q_3 q'), \tag{3.16}$$

where

$$0 = \varphi(0) = \frac{q_2}{q_3}\varphi(1) \ (\mathrm{mod}\, q_3 q'). \tag{3.17}$$

Also, by (3.11) we have

$$P_{1,\dots,w}\varphi(1) \equiv q_3\xi \ (\mathrm{mod}\, q_3 q') \quad \text{ with } \pi_p(\xi) \neq 0. \tag{3.18}$$

It follows from (3.17), (3.18) that $\varphi(1) = q_3'\xi'$, where $q_3' \mid q_3$, $q_3 q' \mid \frac{q_2}{q_3} q_3'$ and $\pi_p(\xi') \neq 0$. Hence, by (3.16),

$$q_3' \mathbb{Z}_{q_3 q'/q_3'} \xi' \subset \pi_{q_3 q'}(A_1),$$

where $q_3 q'/q_3' \geq q' > q_1^{\kappa/2}$ and the claim of Proposition 3.1 is again verified.

Case 2.2: The map $\varphi : \mathbb{Z}_{q_2/q_3} \to A_1$ is not additive $\mathrm{mod}\, q_3 q'$. Hence there are $x_1, x_2 \in \mathbb{Z}_{q_2/q_3}$ such that

$$\varphi(x_1 + x_2) \neq \varphi(x_1) + \varphi(x_2). \tag{3.19}$$

Recalling (3.11), we see that

$$\zeta = \varphi(x_1 + x_2) - \varphi(x_1) - \varphi(x_2) = (q_2\eta, a), \tag{3.20}$$

where $\eta \in \mathbb{Z}_q^w$ and by (3.19) necessarily

$$a = P_{w+1}(\varphi(x_1 + x_2) - \varphi(x_1) - \varphi(x_2)) \neq 0 \ (\mathrm{mod}\, q_3 q').$$

Let

$$a = \bar{q} a_1 \quad \text{with} \quad \bar{q} \mid q_3 q' \quad \text{and} \quad \pi_p(a_1) \neq 0. \tag{3.21}$$

Clearly $\zeta \in A_1 - A_1 - A_1 \subset 3rA^{(s)} - 3rA^{(s)}$.

Let $s_2 \in \mathbb{Z}_+$ be a sufficiently large integer (to be specified). Write, by (3.20) and (3.21),

$$\zeta^{s_2} = (q_2^{s_2}\eta^{s_2}, (\bar{q})^{s_2} a_1^{s_2}). \tag{3.22}$$

At this point recall (3.15). Let $z \in \mathbb{Z}_{q_5}$. There is an element $x \in r_1 A_1^{(s_2)} - r_1 A_1^{(s_2)}$ such that

$$\pi_{q_5} P_{w+1}(x) = q_6 z. \tag{3.23}$$

Multiplying (3.22), (3.23) we obtain

$$\pi_{(\bar{q})^{s_2} q_5}(x\zeta^{s_2}) = (\pi_{(\bar{q})^{s_2} q_5}(q_2^{s_2}\eta^{s_2} P_{\{1,\dots,w\}}(x)), (\bar{q})^{s_2} q_6 a_1^{s_2} z), \tag{3.24}$$

where

$$x\zeta^{s_2} \in (r_1 A_1^{(s_2)} - r_1 A_1^{(s_2)})(3rA^{(s)} - 3rA^{(s)})^{(s_2)}. \tag{3.25}$$

Take s_2 large enough to ensure that

$$(\bar{q})^{s_2} q_5 < q_2^{s_2}. \tag{3.26}$$

From (3.24) we obtain

$$\pi_{(\bar{q})^{s_2} q_5}(x\zeta^{s_2}) = (o, a_1^{s_2})(\bar{q})^{s_2} q_6 z. \tag{3.27}$$

Recalling the definition of q' and $\bar{q}$, condition (3.26) will hold if

$$q_2/q_3 > q_5^{2/s_2},$$

hence, recalling (3.13) and (3.8), if

$$s_2 > \frac{4}{\kappa} C(\delta) C\left(\frac{\kappa}{4C(\delta)}\right),$$

where the right-hand side of (3.27) is controlled as a function of δ.

Putting $q_7 = (\bar{q})^{s_2} q_5$ and $q_8 = (\bar{q})^{s_2} q_6$, (3.25) and (3.27) give

$$q_8(o, a_1^{s_2})\mathbb{Z}_{q_7} \subset \pi_{q_7}(r' A^{(s')} - r' A^{(s')})$$

with $\pi_p(a_1) \neq 0$,

$$\frac{q_7}{q_8} = \frac{q_5}{q_6} > q_1^{\kappa^2/8C(\delta)}$$

and

$$\frac{\log q_7}{\log q_1}, r', s' < C(\kappa, \delta) < C(\delta)$$

by construction. This completes the proof of Proposition 3.1. □

We also need a generalization of Proposition 3.1 replacing $\mathbb{Z}_{p^n}$ by $\mathcal{O}/\mathcal{P}^n$ with $\mathcal{O}$ the maximal order of an algebraic extension K of $\mathbb{Q}$ (we assume $[K : \mathbb{Q}]$ bounded) and $\mathcal{P}$ a prime divisor of p. Let e be the ramification index of $\mathcal{P}$. Denote by $\pi_m : \mathcal{O} \to \mathcal{O}/\mathcal{P}^m$ ($m \in \mathbb{Z}_+$) the residue map.

Proposition 3.3. *Let $w \in \mathbb{Z}_+$ be given and consider the product ring $\mathcal{O}^w$. Given $\delta > 0$ there are $\kappa > 0$ and $r, s \in \mathbb{Z}_+$, $r, s < C(\delta)$, such that the following holds. Let $A \subset \mathcal{O}^w$ satisfy*

$$|\pi_{n_1}(A)| > p^{\delta n_1} \tag{3.28}$$

for some sufficiently large $n_1 \in \mathbb{Z}_+$. Then there are $n_2, n_3 \in \mathbb{Z}_+$ and $\xi \in \mathcal{O}^w$ such that

$$n_3 + \kappa n_1 < n_2 < C(\delta) n_1, \tag{3.29}$$

$$\pi_e(\xi) \neq 0, \tag{3.30}$$

$$\pi_{n_2}(\{x\xi \mid x \in \mathbb{Z} \text{ and } \pi_{n_3}(x) = 0\}) \subset \pi_{n_2}(rA^{(s)} - rA^{(s)}). \tag{3.31}$$

Once the case $w = 1$ is established, the same inductive argument as in the proof of Proposition 3.1 applies. In the Appendix, we will recall the proof of Proposition 3.2 and also give its generalization to $\mathcal{O}/\mathcal{P}^n$.

4. Preliminaries on random walks

Results in this section rely essentially on the theory of random products in $\mathrm{SL}_d(\mathbb{C})$ (see [2]). The next result is a generalization of Proposition 3.32 from [6] to SL_d.

Proposition 4.1. *Let ν be a symmetric, finitely supported probability measure on $\mathrm{SL}_d(\mathbb{Z})$ such that $\langle\nu\rangle$ is Zariski dense. There is a constant $c = c(\nu) > 0$ such that the following holds. Let $Q \in \mathbb{Z}_+$ be a prime power and $\xi, \eta \in \mathrm{Mat}_d(\mathbb{Z})$ satisfy*

$$\operatorname{Tr}\xi = 0, \quad \operatorname{Tr}\eta = 0, \tag{4.1}$$

$$\pi_Q(\xi) \neq 0, \tag{4.2}$$

$$\pi_Q(\eta) \neq 0. \tag{4.3}$$

Then for $l \in \mathbb{Z}_+$ with $l < c\log Q$ (and large enough),

$$\nu^{(l)}(\{g \in \mathrm{SL}_d(\mathbb{Z}) \mid \operatorname{Tr} g\xi g^{-1}\eta \equiv 0 \ (\mathrm{mod}\ \bar{Q})\}) < e^{-cl}, \tag{4.4}$$

where $\bar{Q} = Q^C$ and $C = C(d) \in \mathbb{Z}_+$ is an appropriate constant.

Proof. The two key ingredients are a quantitative Bézout theorem (we will refer to the result in [1]) and the theory of random matrix products.

By (4.2) and (4.3) there are indices $1 \le i, j, r, s \le d$ such that

$$\xi_{ij} \not\equiv 0 \ (\mathrm{mod}\ Q) \quad \text{and} \quad \eta_{rs} \not\equiv 0 \ (\mathrm{mod}\ Q). \tag{4.5}$$

We assume $i \neq j$ and $r \neq s$. The modifications of the argument below to deal with the other cases are straightforward.

Let $\|g\| < C_1$ for $g \in \operatorname{supp}\nu$ and define

$$\mathcal{G} = \{g \in \mathrm{SL}_d(\mathbb{Z}) \mid \|g\| < C_1^l \text{ and } \operatorname{Tr} g\xi g^{-1}\eta \equiv 0 \ (\mathrm{mod}\ \bar{Q})\},$$

so that (4.4) is equivalent to

$$\nu^{(l)}(\mathcal{G}) < e^{-cl}. \tag{4.6}$$

For each $g \in \mathcal{G}$ we introduce a quadratic polynomial $f_g(X, Y) \in \mathbb{Z}[X, Y]$, with

$$X = (X_{\alpha\beta})_{\substack{1\le\alpha,\beta\le d\\(\alpha,\beta)\neq(i,j)}}, \qquad Y = (Y_{\alpha\beta})_{\substack{1\le\alpha,\beta\le d\\(\alpha,\beta)\neq(r,s)}},$$

as follows:

$$f_g(X, Y) = \operatorname{Tr} g\Big(e_i \otimes e_j + \sum_{(\alpha,\beta)\neq(i,j)} X_{\alpha\beta}(e_\alpha \otimes e_\beta)\Big)g^{-1}\Big(e_r \otimes e_s + \sum_{(\alpha,\beta)\neq(r,s)} Y_{\alpha\beta}(e_\alpha \otimes e_\beta)\Big). \tag{4.7}$$

By definition of $\mathcal{G}$, the coefficients of f_g are bounded by $C_d C_1^{2l}$, hence

$$h(f_g) < 2l\log C_1 + C_d,$$

where $h(\cdot)$ denotes the height. Also

$$\xi_{ij}\eta_{rs} f_g\left(\frac{\xi_{\alpha\beta}}{\xi_{ij}}\ ((\alpha,\beta)\neq(i,j)),\ \frac{\eta_{\alpha\beta}}{\eta_{rs}}\ ((\alpha,\beta)\neq(r,s))\right)\equiv 0\ (\mathrm{mod}\ \bar{Q}). \tag{4.8}$$

In order to apply the theory of random matrix products, we "lift" our problem to $\mathbb{C}$. We claim that there is a common zero $(X, Y)\in\mathbb{C}^{d^2-1}\times\mathbb{C}^{d^2-1}$ to the system of equations

$$\sum_{\alpha=1}^{d} X_{\alpha\alpha}=0, \tag{4.9}$$

$$\sum_{\alpha=1}^{d} Y_{\alpha\alpha}=0, \tag{4.10}$$

$$f_g(X,Y)=0 \quad \text{for } g\in\mathcal{G}. \tag{4.11}$$

Note that in (4.11) we may obviously replace $\mathcal{G}$ by $N\le 2(d^2-1)$ quadratic polynomials $F_1,\dots,F_N$.

Assume the claim fails to hold. We invoke Theorem 5.1 from [1]. It follows that there is an integer $D\in\mathbb{Z}_+$ and polynomials $\varphi',\varphi'',\varphi_1,\dots,\varphi_N\in\mathbb{Z}[X,Y]$ of degree at most $b\le C(d)$ satisfying

$$D=\Big(\sum X_{\alpha\alpha}\Big)\varphi'+\Big(\sum Y_{\alpha\alpha}\Big)\varphi''+\sum_{l=1}^{N}F_l\varphi_l \tag{4.12}$$

with

$$\log D, h(\varphi'), h(\varphi''), h(\varphi_l) < C_d \max_{1\le l\le N} h(F_l) < c_\nu l. \tag{4.13}$$

In order to get a contradiction, replace in (4.12) the variables $X_{\alpha\beta}$ (respectively $Y_{\alpha\beta}$) by $\xi_{\alpha\beta}/\xi_{ij}$ (respectively $\eta_{\alpha\beta}/\eta_{rs}$) and multiply both sides by $(\xi_{ij}\eta_{rs})^{b+1}$ to get an integer. Recalling (4.1) and (4.8) it follows that

$$(\xi_{ij}\eta_{rs})^{b+1}D\equiv 0\ (\mathrm{mod}\ \bar{Q}), \tag{4.14}$$

and hence, by (4.5) and assuming $C\ge 2(b+1)+1$ in the definition of $\bar{Q}$, we obtain $D\equiv 0\ (\mathrm{mod}\ Q)$. But this contradicts (4.13) by the restriction $l<c\log Q$ for appropriate $c>0$. This proves the claim.

Letting (X,Y) be a solution of (4.9)–(4.11), consider the matrices $\tilde{X},\tilde{Y}\in V\subset \mathrm{Mat}_d(\mathbb{C})$ (where V denotes the traceless elements)

$$\tilde{X}=e_i\otimes e_j+\sum_{(\alpha,\beta)\neq(i,j)} X_{\alpha\beta}(e_\alpha\otimes e_\beta), \qquad \tilde{Y}=e_r\otimes e_s+\sum_{(\alpha,\beta)\neq(r,s)} Y_{\alpha\beta}(e_\alpha\otimes e_\beta).$$

Hence $\tilde{X},\tilde{Y}\neq 0$ and by (4.11),

$$\mathrm{Tr}\, g\tilde{X}g^{-1}\tilde{Y}=0 \quad \text{for } g\in\mathcal{G}. \tag{4.15}$$

Let $\rho : \mathrm{SL}_d(\mathbb{C}) \to \mathrm{GL}(V)$ be the representation by conjugation. Since $\langle \operatorname{supp} \nu \rangle$ is a Zariski dense subgroup, the theory of random matrix products implies

$$\nu^{(l)}\{g \mid \operatorname{Tr} g\tilde{X}g^{-1}\tilde{Y} = 0\} < e^{-cl} \tag{4.16}$$

for some $c = c(\nu) > 0$. Hence (4.6) follows from (4.15). This proves Proposition 4.1. □

The next result addresses the issue of simplicity of eigenvalues.

Proposition 4.2. *Let ν be as in Proposition* 4.1. *Let $Q \in \mathbb{Z}_+$ (Q large). For $l \geq \log Q$,*

$$\nu^{(l)}\{g \in \mathrm{SL}_d(\mathbb{Z}) \mid \operatorname{Res}(P_g, P_g') \equiv 0 \ (\mathrm{mod}\ Q)\} < Q^{-c},$$

where $c = c(\nu)$ and P_g denotes the characteristic polynomial of g.

Proof. Let $l_0 \sim \log Q$ (to be specified). It will clearly suffice to prove that

$$(\nu^{(l_0)} \otimes \nu^{(l_0)})\{(g_1, g_2) \in \mathrm{SL}_d(\mathbb{Z}) \mid \operatorname{Res}(P_g, P_g') \equiv 0 \ (\mathrm{mod}\ Q) \text{ with } g = g_1 G g_2\} < e^{-cl_0},$$

where $G \in \mathrm{SL}_d(\mathbb{Z})$ is arbitrary and the estimate is uniform in G.

We will follow the same strategy as for Proposition 4.1. Define

$$\mathcal{G} = \{(g_1, g_2) \in \mathrm{SL}_d(\mathbb{Z}) \mid \|g_i\| < C_1^{l_0} \text{ and } \operatorname{Res}(P_g, P_g') \equiv 0 \ (\mathrm{mod}\ Q);\ g = g_1 G g_2\}$$

with $c_1 = c_1(\nu)$.

The first step is to find some $\tilde{G} \in \mathrm{SL}_d(\mathbb{C})$ such that

$$\operatorname{Res}(P_{g_1\tilde{G}g_2}, P'_{g_1\tilde{G}g_2}) = 0 \quad \text{for all } (g_1, g_2) \in \mathcal{G}. \tag{4.17}$$

Assume this is not possible. The equation $\det \tilde{G} = 1$ and the equations (4.17) are of degree at most $(2d - 1)d$ in matrix elements of $\tilde{G}$ and have coefficients bounded by $C_2^{l_0}$, $C_2 = C_1^{c(d)}$. Application of Bézout's theorem leads then again to a contradiction, provided we let $\log Q > C_3 l_0$ with $C_3 \sim C_2$. Hence there is $\tilde{G} \in \mathrm{SL}_d(\mathbb{C})$ such that (4.17) holds.

Next we use the theory of random matrix products. To complete the proof it will suffice to show the following.

Lemma 4.1. *For l large enough we have an estimate*

$$\nu^{(l)} \otimes \nu^{(l)}\{(g_1, g_2) \in \mathrm{SL}_d(\mathbb{C}) \mid g_1 G g_2 \text{ has multiple eigenvalues}\} < e^{-cl}$$

whenever $G \in \mathrm{SL}_d(\mathbb{C})$, and the estimate is uniform in G with $c = c(\nu)$.

Proof. We prove simplicity of the largest eigenvalue of $g_1 G g_2$ with large probability in (g_1, g_2) (large probability means an exceptional set of measure less than e^{-cl}, $c = c(\nu)$). Reapplying the statement for the representation on the exterior powers $\bigwedge^k \mathbb{C}^d$ (which is possible since we assume $\langle \nu \rangle$ is Zariski dense in $\mathrm{SL}_d(\mathbb{C})$) then gives the required conclusion.

According to Theorem 8′ in [14], g_1 is diagonalizable and

$$g_1 = \sum_{i=1}^{d} \lambda^i v_i \otimes v_i, \tag{4.18}$$

where $|v_i| = 1$ and $(1/l) \log |\lambda^i| \sim \gamma^i$, the i-th Lyapunov exponent.

Moreover $\gamma^1 > \cdots > \gamma^d$ (only the simplicity of the top exponent γ^1 is relevant for what follows).

Next, by (4.18),

$$g_1 G g_2 = \sum \lambda^i (v_i \otimes g_2^* G^* v_i) = \lambda^1 (v_1 \otimes g_2^* G^* v_1) + S, \tag{4.19}$$

where clearly $\|S\| \lesssim |\lambda^2| \, \|g_2\| \, \|G\|$. Set $w_1 = g_2^* G^* v_1$. Then

$$\langle v_1, w_1 \rangle = \langle g_2 v_1, G^* v_1 \rangle,$$

where the distribution of g_2 is governed by $\nu^{(l)}$ independently of v_1 (which depends on g_1).

Hence, with high probability, we may ensure

$$|\langle v_1, w_1 \rangle| > e^{-\tau l} \|g_2\| \, \|G^* v_1\|$$

($\tau > 0$ is a sufficiently small constant depending on γ_2/γ_1).

Take a unit vector ξ such that $\|G\xi\| = \|G\|$. Then by (4.18) we have

$$\begin{aligned} \|G^* v_1\| \geq |\langle v_1, G\xi \rangle| &= \frac{1}{|\lambda^1|} \Big(\|g_1 G \xi\| - \sum_{i \geq 2} |\lambda^i| \, \|G\xi\| \Big) \\ &> \frac{1}{|\lambda^1|} (e^{-\tau l} \|G\| \, |\lambda^1| - d |\lambda_2| \, \|G\|) > \frac{1}{2} e^{-\tau l} \|G\| \end{aligned} \tag{4.20}$$

with high probability in g_1. It follows that

$$|\langle v_1, w_1 \rangle| > e^{-3\tau l} \|g_2\| \, \|G\|$$

with high probability in (g_1, g_2).

Multiplying (4.19) with an appropriate normalizing factor, we obtain a matrix

$$M = v \otimes v' + \tilde{M},$$

where $|v| = 1 = |v'|$ and

$$\langle v, v' \rangle > e^{-3\tau l}, \qquad \|\tilde{M}\| \lesssim e^{3\tau l} \frac{|\lambda^2|}{|\lambda^1|} < e^{-cl}.$$

Writing a matrix representation for M in a basis $v = u_1, u_2, \ldots, u_d$ with $u_2, \ldots, u_d \in (v')^\perp$, we clearly obtain

$$\begin{aligned} 1 > M_{11} &> e^{-3\tau l} - e^{3\tau l} \|\tilde{M}\| > e^{-4\tau l}, \\ |M_{ij}| &\leq e^{3\tau l} \|\tilde{M}\| < e^{-cl/2} \quad \text{for } (i, j) \neq (1, 1). \end{aligned}$$

Thus the characteristic polynomial $P_M(t)$ of M has the form

$$P_M(t) = \det(t - M) = (t - M_{11})t^{d-1} + \theta_{d-2}t^{d-2} + \cdots + \theta_0,$$

where

$$|\theta_0|, \ldots, |\theta_{d-2}| < c_d e^{-cl/2}. \tag{4.21}$$

In view of (4.21) and letting τ be small enough we conclude that the largest root ρ_1 of P_M satisfies

$$|\rho_1 - M_{11}| \lesssim c_d e^{-cl/2}/M_{11}^{d-1} < e^{-cl/3}$$

and is simple (cf. Lemma 13 in [14]).

This concludes the proof of Lemma 4.1 and of Proposition 4.2. □

By a variant of the previous argument we obtain similarly

Proposition 4.3. *Let ν be as above. Let $Q \in \mathbb{Z}_+$ (Q large) and $g_0 \in \mathrm{GL}_d(\mathbb{Z})$, $\log Q > c \log \|g_0\|$ (c an appropriate constant). For $l \geq \log Q$,*

$$\nu^{(l)}\{g \in \mathrm{SL}_d(\mathbb{Z}) \mid \mathrm{Res}(P_{gg_0}, P'_{gg_0}) \equiv 0 \ (\mathrm{mod}\ Q)\} < Q^{-c}.$$

5. Sets of commuting elements

Recall (2.8),

$$\nu^{(2l_0)}(H \cdot H) > |G|^{-2\varepsilon'} > q^{-2d^2\varepsilon'} > q^{-C_1\varepsilon}. \tag{5.1}$$

We apply Propositions 4.1 and 4.3. Hence we may take $\varepsilon n < m < C\varepsilon n$ such that the following properties hold:

$$\nu^{(m')}\{g \in \mathrm{SL}_d(\mathbb{Z}) \mid \mathrm{Res}(P_{gg_0}, P'_{gg_0}) \equiv 0 \ (\mathrm{mod}\ p^m)\} < p^{-cm} < q^{-2C_1\varepsilon} \tag{5.2}$$

for $m' > m$ whenever $g_0 \in \mathrm{GL}_d(\mathbb{Z})$, $\log \|g_0\| < cm$, and also

$$\nu^{(m)}(\{g \in \mathrm{SL}_d(\mathbb{Z}) \mid \mathrm{Tr}\, g\xi g^{-1}\eta \equiv 0 \ (\mathrm{mod}\ \bar{Q})\}) < e^{-cm} < q^{-2C_1\varepsilon} \tag{5.3}$$

if $Q \mid q$, $\log Q > cm$ and $\xi, \eta \in \mathrm{Mat}_d(\mathbb{Z})$ satisfy $\mathrm{Tr}\,\xi = 0 = \mathrm{Tr}\,\eta$, $\pi_Q(\xi) \neq 0$ and $\pi_Q(\eta) \neq 0$; here $\bar{Q} \mid q$ and $\log Q < \log \bar{Q} < C \log Q$.

Take Q so that (5.3) holds. Fix some $\xi \in \mathrm{Mat}_d(\mathbb{Z})$, $\xi \neq 0$, $\|\xi\| < Q$, such that $\mathrm{Tr}\,\xi = 0$. From (5.1) applied with $m = 2l_0$ and consecutive applications of (5.3) we obtain elements $g_3, \ldots, g_{d^2} \in H \cdot H$ such that

$$\|g_i\| < C^m \quad (3 \leq i \leq d^2), \quad \det(1, \xi, g_2\xi g_2^{-1}, \ldots, g_{d^2}\xi g_{d^2}^{-1}) \not\equiv 0 \ (\mathrm{mod}\ Q_1)$$

for some $Q_1 \mid q$ with $\log Q_1 \leq c \log Q$.

Take $\xi = dg - (\mathrm{Tr}\, g)1$ with $g \neq \pm 1$ in $H \cdot H$ such that $\|g\| < Q$. We obtain

Lemma 5.1. *There are elements $g_1, \ldots, g_{d^2} \in H^{(6)}$ and $q_0 \mid q$ with $q_0 < q^{C\varepsilon}$ such that*

$$\|g_i\| < q^{C\varepsilon}, \tag{5.4}$$

$$\det(1, g_2, \ldots, g_{d^2}) \not\equiv 0 \ (\mathrm{mod}\ q_0). \tag{5.5}$$

(Here and below, we denote by C various constants that may depend on ν and possibly also p.)

Setting $g_1 = 1$, it follows from (5.5) that the map

$$\mathrm{Mat}_d(q) \to \mathbb{Z}_q^d : g \mapsto (\mathrm{Tr}\, gg_i)_{1\le i\le d^2} \tag{5.6}$$

has multiplicity at most $q^{C\varepsilon}$.

Indeed, if $g \in \mathrm{Mat}_d(\mathbb{Z})$ and $\mathrm{Tr}\, gg_i \equiv 0 \pmod q$ for $i = 1, \dots, d^2$ then $\det(g_1, \dots g_{d^2})g \equiv 0 \pmod q$.

Fix some

$$\varepsilon \ll \varepsilon_0 \ll 1. \tag{5.7}$$

Let

$$\varepsilon_0 n < n_1 < n \quad \text{and} \quad q_1 = p^{n_1}. \tag{5.8}$$

We apply Helfgott's argument [15] to construct sets of commuting elements. First, apply (5.1) and (5.2) with $l_0 = n_1$ and $m' = 2n_1$. Hence by (5.7) and (5.8) we have

$$\nu^{(2n_1)}\{g \in \mathrm{SL}_d(\mathbb{Z}) \mid \mathrm{Res}(P_{gg_i}, P'_{gg_i}) \equiv 0 \pmod{p^m} \text{ for } 1 \le i \le d^2\} < \tfrac{1}{2} q^{-C_1\varepsilon}.$$

Invoking Kesten's bound on random walks for the free group [17], we obtain by (5.7) and (5.8) a subset $H_1 \subset H \cdot H \cap [\|g\| < C^{n_1}]$ such that

$$|H_1| > \tfrac{1}{2} q^{-C_1\varepsilon}(\mathrm{supp}\,\nu - 1)^{2n_1} > q_1^c$$
$$\mathrm{Res}(P_{gg_i}, P'_{gg_i}) \not\equiv 0 \pmod{p^m} \quad \text{for } g \in H_1 \text{ and } 1 \le i \le d^2.$$

Considering the trace map (5.6) with q replaced by q_1 we obtain a set of elements $(h_\alpha)_{1\le\alpha\le\beta} \subset H_1 \cdot H^{(6)} \subset H^{(8)}$ with $\beta > q^{-C\varepsilon} q_1^{c/d^2} > q_1^{c'}$ such that

$$\|h_\alpha\| < C^{n_1} q^{C\varepsilon} < C^{2n_1}, \tag{5.9}$$
$$\mathrm{Res}(P_{h_\alpha}, P'_{h_\alpha}) \not\equiv 0 \pmod{p^m} \tag{5.10}$$
$$\mathrm{Tr}\, h_\alpha \not\equiv \mathrm{Tr}\, h_{\alpha'} \pmod{q_1} \quad \text{if } \alpha \ne \alpha'. \tag{5.11}$$

Consider the conjugacy classes

$$C_\alpha = \{g h_\alpha g^{-1} \mid g \in H\}.$$

It follows from (5.11) that $\pi_{q_1}(C_\alpha)$, $\alpha = 1, \dots, \beta$, are disjoint subsets of $\pi_{q_1}(H)^{(10)}$. Hence, we may specify α such that

$$|\pi_{q_1}(C_\alpha)| \le \frac{1}{\beta}|\pi_{q_1}(H^{(10)})| < q_1^{-c'} q^{C\varepsilon}|\pi_{q_1}(H)| < q_1^{-c}|\pi_{q_1}(H)| \tag{5.12}$$

(we use here the earlier observation on quotients of approximate groups).

Set $h = h_\alpha$. Considering the map $g \mapsto ghg^{-1}$ from $\pi_{q_1}(H)$ to $\pi_{q_1}(C_\alpha)$, it follows from (5.12) that there is $\bar g \in H$ such that

$$|\pi_{q_1}(\{g \in H \mid ghg^{-1} \equiv \bar g h (\bar g)^{-1} \pmod{q_1}\})| > q_1^c.$$

Hence the set

$$S = \{g \in H \cdot H \mid gh = hg \pmod{q_1}\}$$

satisfies

$$|\pi_{q_1}(S)| > q_1^c. \tag{5.13}$$

Diagonalize $h \in \mathrm{SL}_d(\mathbb{Z})$ considering if necessary an extension field K of $\mathbb{Q}$. Let $\mathcal{O}$ be the integers of K and $\mathcal{P}$ a prime ideal dividing (p). We assume $\mathcal{P}$ unramified (otherwise some exponent adjustments are needed below). We replace $\mathbb{Z}_q$ by $\mathcal{O}/\mathcal{P}^n$. A suitable base change brings h into the form

$$h = \sum_{i=1}^{d} \mu_i (e_i \otimes e_i).$$

Recalling (5.10), it follows that $\prod_{i \neq j}(\mu_i - \mu_j) \notin \mathcal{P}^m$ and hence

$$\mu_i - \mu_j \notin \mathcal{P}^m \quad \text{for } i \neq j \tag{5.14}$$

(recall that $m < C\varepsilon n$). Since $g \in S$ commutes with $h \pmod{\mathcal{P}^{n_1}}$, we obtain from (5.14) a diagonal form

$$g = \sum \lambda_i (e_i \otimes e_i) \pmod{\mathcal{P}^{n_1 - m}}, \quad \text{where} \quad \prod \lambda_i = 1 \pmod{\mathcal{P}^{n_1 - m}}.$$

6. Application of the sum-product theorem

We carry on with the construction and notation from Section 5. Given elements $g, h \in \mathrm{GL}_d(\mathcal{O})$, define their commutator by

$$C(g, h) = ghg^{-1}h^{-1}.$$

The following well-known property is essential:

Lemma 6.1. *Let $g \equiv 1 \pmod{\mathcal{P}^m}$ and $h \equiv 1 \pmod{\mathcal{P}^{m'}}$. Then*

$$C(g, h) \equiv 1 + [g, h] \pmod{\mathcal{P}^{m+m'+\min(m,m')}}, \tag{6.1}$$

where we write $[g, h] = gh - hg$.

Let $S \subset H \cdot H$ be the set obtained in Section 5. Recall (5.13), i.e. $|\pi_{q_1}(S)| > q_1^c$. We may therefore produce $q_1' \mid q_1$, $q_1' = p^{n_1'}$ and an element $x_0 \in S$ and a subset $S' \subset S$ such that

$$q_1/q_1' > q_1^{c/2d^2}, \tag{6.2}$$

$$\pi_{q_1'}(S') = \pi_{q_1'}(x_0), \tag{6.3}$$

$$|\pi_{q_1''}(S')| > (q_1''/q_1')^{c/8} \quad \text{whenever} \quad q_1' \mid q_1'', q_1'' \mid q_1. \tag{6.4}$$

Considering the set $S'(S')^{-1}$, we obtain a set $\Omega \subset \mathrm{Mat}_d(\mathbb{Z})$ with the following properties:

$$1 + q_1' x \in S'(S')^{-1} \subset H^{(4)} \quad \text{for } x \in \Omega, \tag{6.5}$$

$$|\pi_Q(\Omega)| > Q^{c/8} \quad \text{if} \quad Q \mid \frac{q_1}{q_1'}. \tag{6.6}$$

It follows from (6.2) that

$$n_1 - n_1' > \frac{c}{2d^2} n_1 \gg m. \tag{6.7}$$

After the base change from Section 5, Ω will be diagonalized mod $\mathcal{P}^{n_1 - n_1' - m}$. Thus each $x \in \Omega$ has a representation

$$x = \sum \sigma_i (e_i \otimes e_i) \ (\mathrm{mod}\, \mathcal{P}^{n_1 - n_1' - m}), \tag{6.8}$$

where the $\sigma_i \in \mathcal{O}$ satisfy

$$\prod (1 + q_1' \sigma_i) = 1 \ (\mathrm{mod}\, \mathcal{P}^{n_1 - m}). \tag{6.9}$$

Take next

$$\tilde{q} = p^{\tilde{n}} \quad \text{where} \quad n_1 < \tilde{n} < n, \tag{6.10}$$

and assume $\xi \in \mathrm{Mat}_d(\mathbb{Z})$ satisfies

$$1 + \tilde{q}\xi \in H^{(4)}, \tag{6.11}$$

$$\pi_p(\xi) \neq 0, \tag{6.12}$$

$$\mathrm{Tr}\, \xi = 0. \tag{6.13}$$

According to Lemma 6.1,

$$C(1 + \tilde{q}\xi, 1 + q_1' x) = 1 + \tilde{q} q_1' [\xi, x] \ (\mathrm{mod}\, \mathcal{P}^{\tilde{n} + 2n_1'}). \tag{6.14}$$

We may assume $n_1' > n_1/2$. Substituting the representation (6.8) in (6.14) then gives

$$C(1 + \tilde{q}\xi, 1 + q_1' x) = 1 + \tilde{q} q_1' \sum_{i \neq j} (\sigma_i - \sigma_j) \xi_{ij} (e_i \otimes e_j) \ (\mathrm{mod}\, \mathcal{P}^{\tilde{n} + n_1 - m}). \tag{6.15}$$

Note that since $n_1' > n_1/2$, also by (6.9),

$$\sum_{i=1}^{d} \sigma_i \equiv 0 \ (\mathrm{mod}\, \mathcal{P}^{n_1 - n_1' - m}).$$

Therefore the map $x \mapsto (\sigma_i - \sigma_j)_{i \neq j}$ is one-to-one on Ω (mod $\mathcal{P}^l$) for $1 \leq l \leq n_1 - n_1' - m$. Define

$$A = \{(\sigma_i - \sigma_j)_{i \neq j} \mid x \in \Omega\} \subset \mathcal{O}^w, \tag{6.16}$$

where $w = d^2 - d$.

It follows from (6.6) and the preceding that for $1 \le l \le n_1 - n_1' - m$ we have

$$|\pi_l(A)| = |\pi_{\mathcal{P}^l}(A)| > p^{c'l} \tag{6.17}$$

for some $c' > 0$.

Our aim is to apply Proposition 3.3 to the set A. In view of (6.17), condition (3.28) from Proposition 3.3 holds with n_1 replaced by any sufficiently large $l_1 < n_1 - n_1' - m$ and $\delta = c'$. In view of (6.7) we may take

$$l_1 > c'' n_1 \tag{6.18}$$

(to be specified).

From Proposition 3.3 we obtain $l_2, l_3 \in \mathbb{Z}_+$ and some $\eta \in \mathcal{O}^w$ such that

$$l_3 + \kappa l_1 < l_2 < c l_1, \tag{6.19}$$

$$\pi_1(\eta) \ne 0, \tag{6.20}$$

$$p^{l_3}\mathbb{Z}\eta \in rA^{(s)} - rA^{(s)} \pmod{\mathcal{P}^{l_2}}. \tag{6.21}$$

Here $r, s \in \mathbb{Z}_+$ and $\kappa, c > 0$ are constants.

Note that by (6.16) we may let $\eta_{ii} = 0$.

Next we introduce the product sets $A^{(s)}$ by iteration of the commutator formula (6.15). Let $x^{(1)}, \dots, x^{(s)} \in \Omega$. By (6.15),

$$C(1 + \tilde{q}\xi, 1 + q_1' x^{(1)}) = 1 + \tilde{q} q_1' \sum_{i \ne j} (\sigma_i^1 - \sigma_j^1)\xi_{ij}(e_i \oplus e_j) \pmod{\mathcal{P}^{\tilde{n}+n_1-m}}.$$

Replacing $\tilde{q}$ by $\tilde{q}q_1'$ and ξ by $\sum_{i\ne j}(\sigma_i^1 - \sigma_j^1)\xi_{ij}(e_i \oplus e_j)$, it easily follows that

$$\begin{aligned} &C(C(1 + \tilde{q}\xi, 1 + q_1' x^{(1)}), 1 + q_1' x^{(2)}) \\ &\quad = 1 + \tilde{q}(q_1')^2 \Big[\sum_{i\ne j}(\sigma_i^1 - \sigma_j^1)\xi_{ij}(e_i \otimes e_j), x^{(2)}\Big] \pmod{\mathcal{P}^{\tilde{n}+n_1+n_1'-m}} \\ &\quad = 1 + \tilde{q}(q_1')^2 \sum_{i\ne j}(\sigma_i^1 - \sigma_j^1)(\sigma_i^2 - \sigma_j^2)\xi_{ij}(e_i \otimes e_j) \pmod{\mathcal{P}^{\tilde{n}+n_1+n_1'-m}}. \end{aligned}$$

By (6.5) and (6.11), clearly

$$C(1 + \tilde{q}\xi, 1 + q_1' x^{(1)}) \in H^{(16)}$$

and

$$C(C(1 + \tilde{q}\xi, 1 + q_1' x^{(1)}), 1 + q_1' x^{(2)}) \in H^{(40)}.$$

It will be convenient to introduce the notation

$$H' = \bigcup_s H^{(s)}$$

with the understanding that the exponent s remains bounded. Therefore

$$1+\tilde{q}(\tilde{q}_1)^2\sum_{i\neq j}(\sigma_i^1-\sigma_j^1)(\sigma_i^2-\sigma_j^2)\xi_{ij}(e_i\otimes e_j)\in H' \ (\mathrm{mod}\, \mathcal{P}^{\tilde{n}+n_1+n_1'-m}),$$

and carrying on, we conclude that

$$1+\tilde{q}(\tilde{q}_1)^s\sum_{i\neq j}\prod_{r=1}^{s}(\sigma_i^r-\sigma_j^r)\xi_{ij}(e_i\otimes e_j)\in H' \ (\mathrm{mod}\, \mathcal{P}^{\tilde{n}+sn_1'+(n_1-n_1'-m)}).$$

We assume here that

$$\tilde{n}+(s+1)n_1<n. \tag{6.22}$$

Introducing sum/difference sets of the sets $A^{(s)}$ is straightforward, as we certainly have

$$(1+\tilde{q}(q_1')^s\zeta_1)(1+\tilde{q}(q_1')^s\zeta_2)^{\pm 1}=1+\tilde{q}(q_1')^s(\zeta_1\pm\zeta_2) \ (\mathrm{mod}\, \mathcal{P}^{\tilde{n}+sn_1'+(n_1-n_1'-m)}).$$

In conclusion, we have proven that if $\tau=(\tau_{ij})_{i\neq j}$ is in $rA^{(s)}-rA^{(s)}$ then

$$1+\tilde{q}(q_1')^s\sum_{i\neq j}\tau_{ij}\xi_{ij}(e_i\otimes e_j)\in H' \ (\mathrm{mod}\, \mathcal{P}^{\tilde{n}+sn_1'+(n_1-n_1'-m)}). \tag{6.23}$$

Returning to (6.19)–(6.21), take $l_1\sim n_1$ such that $l_2\leq n_1-n_1'-m$. From (6.21) and (6.23) it then follows that

$$1+p^{\tilde{n}+sn_1'+l_3}\mathbb{Z}\sum_{i\neq j}\eta_{ij}\xi_{ij}(e_i\otimes e_j)\subset H' \ (\mathrm{mod}\, \mathcal{P}^{\tilde{n}+sn_1'+l_2}).$$

In the preceding we may replace ξ by any conjugate $\xi'=g\xi g^{-1}$ with $g\in H\cdot H$; by (6.11) we have

$$g(1+\tilde{q}\xi)g^{-1}\in H^{(8)}.$$

Defining $\bar{\eta}=\sum_{i\neq j}\eta_{ij}(e_i\otimes e_j)\in \mathrm{Mat}_d(\mathcal{O})$, we have $\pi_{\mathcal{P}}(\bar{\eta})\neq 0$ by (6.20) and $\mathrm{Tr}\,\bar{\eta}=0$. In order to ensure that for some $m'<C\varepsilon m$,

$$\sum_{i\neq j}\eta_{ij}\xi_{ij}'e_i\otimes e_j\neq 0 \ (\mathrm{mod}\, \mathcal{P}^{m'}), \tag{6.24}$$

we require

$$\mathrm{Tr}(g\xi g^{-1}\bar{\eta})\neq 0 \ (\mathrm{mod}\, \mathcal{P}^{m'}). \tag{6.25}$$

We apply Proposition 4.1 and more precisely statement (5.3) (taking an integral basis for $\mathcal{O}$, we first replace $\bar{\eta}$ by an element of $\mathrm{Mat}_d(\mathbb{Z})$).

Recalling also that ξ satisfies (6.12), (6.13), the existence of the required $g\in H\cdot H$ satisfying (6.25) is clear.

Hence there is an element $\beta\in\mathrm{Mat}_d(\mathbb{Z})$ such that

$$\mathrm{Tr}\,\beta=0,\qquad \pi_p(\beta)\neq 0,$$
$$1+p^{\tilde{n}+sn_1'+l_3+m'}\mathbb{Z}\beta\subset H' \ (\mathrm{mod}\, p^{\tilde{n}+sn_1'+l_2}),$$

where $m'<C\varepsilon n$.

Replacing β by further conjugated $g\beta g^{-1}$ with $g \in H \cdot H$ and reapplying (5.3) we may obtain $g_1, \dots, g_{d^2-1} \in H \cdot H$ such that

$$\det(1, g_i\beta g_i^{-1}\ (1 \le i \le d^2)) \not\equiv 0 \ (\mathrm{mod}\ p^{m''}) \tag{6.26}$$

with $m'' < C\varepsilon n$. Since also

$$1 + p^{\tilde{n}+sn'_1+l_3+m'} \sum_{i=1}^{d^2-1} \mathbb{Z}(g_i\beta g_i^{-1}) \subset H' \ (\mathrm{mod}\ p^{\tilde{n}+sn'_1+l_2})$$

and by (6.26),

$$p^{m''}V = p^{m''}\{\zeta \in \mathrm{Mat}_d(\mathbb{Z}) \mid \mathrm{Tr}\,\zeta = 0\} \subset \sum_{i=1}^{d^2-1} \mathbb{Z}(g_i\beta g_i^{-1}),$$

it follows that

$$1 + p^{\tilde{n}+sn'_1+l_3+m'+m''}V \subset H' \ (\mathrm{mod}\ p^{\tilde{n}+sn'_1+l_2}).$$

Recall that by (6.18) and (6.19),

$$l_2 - l_3 > \kappa l_1 > cn_1,$$

and $m', m'' < C\varepsilon n$.

Here $\varepsilon_0 n < n_1 < \tilde{n}$ is arbitrary (cf. (6.10) and (5.8)) (subject to the condition (6.22)). Since s is bounded by a constant we have proved

Lemma 6.2. *Assume $\varepsilon_0 n < \tilde{n} < n$ and $\xi \in V$ are such that*

$$\pi_p(\xi) \ne 0, \qquad \pi_{p^n}(1 + p^{\tilde{n}}\xi) \in H'.$$

Then for $\varepsilon_0 n < n_1 < c(n - \tilde{n})$ there is $\tilde{n} < \bar{n} < \tilde{n} + Cn_1 < n$ such that

$$1 + p^{\bar{n}}V \subset H' \ (\mathrm{mod}\ p^{\bar{n}+[cn_1]}), \tag{6.27}$$

where c, C are constants.

Note that if $\xi \in \mathrm{Mat}_d(\mathbb{Z})$, $\pi_p(\xi) \ne 0$ and $\pi_{p^n}(1 + p^{\tilde{n}}\xi) \in H'$, then $\det(1 + p^{\tilde{n}}\xi) \equiv 1 \ (\mathrm{mod}\ p^n)$ and hence, assuming $2\tilde{n} < n$,

$$\mathrm{Tr}\,\xi \equiv 0 \ (\mathrm{mod}\ p^{\tilde{n}}). \tag{6.28}$$

Assume further that $\xi \equiv 0 \pmod d$ and write $a = (1/d)\operatorname{Tr}\xi \in p^{\tilde{n}}\mathbb{Z}$ and $\xi' = \xi - (1/d)\operatorname{Tr}\xi \in V$. Hence, by (6.28), $1 + p^{\tilde{n}}\xi' \in \pi_{p^{2\tilde{n}}}(H')$. Applying now Lemma 6.2 with H replaced by $\pi_{p^{2\tilde{n}}}(H)$ and letting $n_1 < c\tilde{n}$ be small enough to ensure that $\bar{n} + n_1 < 2\tilde{n}$, the conclusion (6.27) remains valid.

Take $q_0 \mid q = p^n$ with $q_0 \sim q^{\varepsilon_0}$ and define

$$H_0 = \{x \in H^{(4)} \mid x \equiv 1 \pmod{dq_0}\}.$$

It easily follows from (5.1) that

$$\nu^{(4l_0)}(H_0) \geq \frac{(\nu^{(2l_0)}(H \cdot H))^2}{(dq_0)^{d^2}} > q^{-C\varepsilon}(dq_0)^{-d^2} > q^{-(d^2+1)\varepsilon_0}. \tag{6.29}$$

Hence for a suitable choice of $l_0 \sim \varepsilon_0 \log q$, we get from (6.29) an element $g_0 \in H^{(4)}$ satisfying

$$g_0 \equiv 1 \pmod{q_0 d}, \qquad g_0 \neq 1,$$
$$\|g_0\| < C^{l_0} < q^{C\varepsilon_0}.$$

Therefore

$$g_0 = 1 + \tilde{q}d\xi_0, \ \tilde{q} = p^{\tilde{n}} \quad \text{with } \varepsilon_0 n < \tilde{n} < C\varepsilon_0 n \text{ and } \pi_p(\xi_0) \neq 0.$$

From the preceding discussion, we conclude the following, which is the main conclusion of this section.

Lemma 6.3. *Let $\varepsilon \ll \delta_0 \ll 1$. There are $q_1 > q_2$ dividing q such that $q_1 < q^{\delta_0}$, $q_1/q_2 > q^{c\delta_0}$ and for each $z \in V$ there is some $g \in H'$ satisfying*

$$g \equiv 1 + q_2 z \pmod{q_1}.$$

7. Completion of the proof

7.1. Proof of Theorem 1.1

With Lemma 6.3 at hand we may repeat the argument at the end of Section 6 in [6] and show that there is $q_3 \mid q$ with $q_3 < q^{C\delta_0}$ such that if $z \in \operatorname{Mat}_d(\mathbb{Z})$ satisfies

$$\det(1 + q_3 z) = 1 \pmod q$$

then

$$1 + q_3 z \in H' \pmod q.$$

Therefore, since H is an approximate subgroup,

$$|\mathrm{SL}_d(q)|^{1-\gamma+C\varepsilon} > p^{C\varepsilon}|H| > |H'| > |\{x \in \mathrm{SL}_d(q) \mid x \equiv 1 \pmod{q_3}\}|$$
$$= \frac{|\mathrm{SL}_d(q)|}{|\mathrm{SL}_d(q_3)|} > |\mathrm{SL}_d(q)|q^{-Cd^2\delta_0}.$$

Here $\gamma > 0$ is given and letting ε, δ_0 be small enough, a contradiction follows.

Recapitulating all of the preceding, this provides us with the following analogue of Proposition 6.1 in [6] for $d \geq 2$.

Proposition 7.1. *Let ν be as in Section 2 and p be a given sufficiently large prime. For all $\gamma > 0$, there is $C(\gamma) > 0$ such that if $q \in \mathbb{Z}_+$ is of the form $q = p^n$ (n large enough), then*

$$\|\pi_q(\nu^{(l)})\|_\infty < q^\gamma |\mathrm{SL}_d(q)|^{-1}$$

for $l > C(\gamma)\log q$.

The proof of Theorem 1.1 is then completed by the argument of Section 8 in [6] (using the multiplicity bound established in Section 7 of [6], which is clearly sufficient also in the higher rank case).

7.2. Proof of Corollary 1.2

Let G be a subgroup of $\mathrm{SL}_d(\mathbb{F}_p)$. Following Nori [22] let G^+ denote the normal subgroup of G generated by $G \cap U_d(\mathbb{F}_p)$, where $U_d(\mathbb{F}_p)$ are the elements of $\mathrm{SL}_d(\mathbb{F}_p)$ of order p. Denote by $\tilde{G}$ the algebraic subgroup generated by the one-parameter groups $t \mapsto x^t = \exp(t \log x)$ for all $x \in G$ such that $x^p = 1$. Theorem B in [22] states that there is a constant $c_1(d) \geq 2d - 2$ such that for all primes $p > c_1(d)$, if G is a subgroup of $\mathrm{SL}_d(\mathbb{F}_p)$ then $G^+ = \tilde{G}(\mathbb{F}_p)^+$. So for all sufficiently large primes (depending only on d), G^+ is an algebraic subgroup of SL_d defined over $\mathbb{F}_p$.

Now a classical result of Jordan (see Theorem 8.29 in [23]) asserts that every finite subgroup X of $\mathrm{SL}_d(\mathbb{C})$ has a commutative normal subgroup Y such that $[X : Y] \leq c_2(d)$, where $c_2(d)$ is a constant depending only on d. If we let f_G denote the equations describing $\tilde{G}(\mathbb{F}_p)$, since we can regard G/G^+ as a subgroup of $\mathrm{SL}_d(\mathbb{C})$, we conclude that for all $p > c_1(d)$ the elements of G satisfy

$$f_G(C(x^{c_2(d)}, y^{c_2(d)})) = 0.$$

Corollary 1.2 now follows from Corollary 1.1.

Appendix. Sum-product theorem for extension fields

by Jean Bourgain

A.1. Theorem A.1

Let p be a large and fixed rational prime. Let $\mathcal{O}$ denote the integers in our extension K of $\mathbb{Q}$ and let $\mathcal{P}$ be a prime divisor of (p) in $\mathcal{O}$. Denote by d the degree of $\mathcal{P}$ and by e its ramification. Our purpose is to establish a sum-product theorem in $\mathcal{O}/\mathcal{P}^n$, generalizing the result from [3] for $\mathbb{Z}/p^n\mathbb{Z}$.

In what follows, p is given and we let $n \to \infty$. We do not seek uniformity in p although the statements (Theorem A.1, Corollary A.1) can be proven uniformly in p (cf. [3]).

For large p, the sum-product and exponential sums results from [10, 9, 4] are required however, while in the present situation (p fixed), only elementary estimates (such as Lemma A.1 below) will be used.

Since our problem is obviously local, we replace $\mathbb{Q}$ and K by their respective completions $\mathbb{Q}_p$ and $K_{\mathcal{P}}$. Thus $K_{\mathcal{P}}$ is an extension of $\mathbb{Q}_p$ of degree de; $K_{\mathcal{P}}$ is the totally ramified extension of its inertial field $\mathbb{Q}_p \subset K^I \subset K_{\mathcal{P}}$, $[K_{\mathcal{P}} : K^I] = e$ and K^I is a totally unramified extension of $\mathbb{Q}_p$ with $[K^I : \mathbb{Q}_p] = d$. The Galois group $\mathrm{Gal}(K^I/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ is the cyclic group on d elements. Note that since p is large compared with d, $K_{\mathcal{P}}$ is a tamely ramified extension of K^I.

Let $u_1, \dots, u_d$ be an integral basis for K^I. We then get

$$\mathcal{O} = \mathcal{O}_{\mathcal{P}} = \mathbb{Z}_p[u_i \mathcal{P}^j \mid 1 \le i \le d,\ 0 \le j < e]$$

where $\mathbb{Z}_p$ stands for the p-adic integers, and

$$\mathcal{O}^I = \mathcal{O}_{\mathcal{P}} \cap K^I = \mathbb{Z}_p[u_i \mid 1 \le i \le d].$$

Further, $(p) = \mathcal{P}^e$ and

$$\mathcal{O}/(p) \simeq \mathbb{F}_{p^d} + \mathbb{F}_{p^d}\mathcal{P} + \cdots + \mathbb{F}_{p^d}\mathcal{P}^{e-1}.$$

Theorem A.1. *Given $\delta_1, \delta_2 > 0$, there are $\varepsilon, \delta_3 > 0$ such that the following holds. Let $A \subset \mathcal{O}/p^n\mathcal{O}$ satisfy*

$$\pi_1(A) = \mathcal{O}/p\mathcal{O}, \tag{A.1}$$

$$|\pi_{n_1}(A)| > p^{\delta_2 n_1} \quad \textit{for all } \varepsilon n < n_1 < n, \tag{A.2}$$

where $\pi_n : \mathcal{O} \to \mathcal{O}/p^n\mathcal{O}$ denotes the quotient map and

$$|A| < p^{(1-\delta_1)nde}.$$

Then

$$|A \cdot A \cdot A + A \cdot A \cdot A| > p^{n\delta_3}|A|. \tag{A.3}$$

Corollary A.1. *Given $\delta > 0$ and $\tau > 0$ there are $\varepsilon > 0$ and $r_1, r_2 \in \mathbb{Z}_+$ such that the following holds. Let $A \subset \mathcal{O}/p^n\mathcal{O}$ satisfy*

$$\pi_1(A) = \mathcal{O}/p\mathcal{O},$$

$$|\pi_{n_1}(A)| > p^{\delta n_1} \quad \textit{for all } \varepsilon n < n_1 < n.$$

Then letting $m = [\tau n]$ we have

$$r_2 A^{r_1} - r_2 A^{r_1} \supset \{x \in \mathcal{O}/p^n\mathcal{O} \mid \pi_m(x) = 0\}.$$

We assume $\mathcal{P}$ is unramified, i.e. $(p) = \mathcal{P}$. The modifications for the ramified case are minor. The arguments below are in fact straightforward adaptations of [3]. Note however that if $\mathcal{P}$ is ramified, assumption (A.1) may not be replaced by $\pi_p(A) = \mathcal{O}/\mathcal{P}$. Compared with the case of subsets $A \subset \mathbb{Z}/p^n\mathbb{Z}$, there is a problem when applying previous results due to the possible failure of condition (A.1) (as $\mathcal{O}/p\mathcal{O}$ has nontrivial subrings), and this issue will have to be addressed.

Proof of Corollary A.1. Write $q = p^{nd}$. In view of Theorem A.1 (which needs to be iterated) and taking $\varepsilon = \varepsilon(\delta, \delta_1)$ small enough, we may ensure that $|r_2 A^{r_1}| > q^{1-\delta_1}$ for some r_1, r_2 depending on δ and δ_1.

Thus we may start from a set $A_1 \subset \mathcal{O}/p^n\mathcal{O}$, $|A_1| > q^{1-\delta_1}$ with $\delta_1 > 0$ arbitrary. Define next

$$n_0 = \max\{n' \mid n' \text{ such that } \max_{\xi} |A_1 \cap \pi_{n'}^{-1}(\xi)| > p^{-\frac{3}{4}dn'}|A_1|\}.$$

Clearly

$$p^{d(n-n')} > p^{-\frac{3}{4}dn'} q^{1-\delta_1},$$

hence

$$n' < 4\delta_1 n \quad \text{and} \quad n_0 < 4\delta_1 n.$$

Take $\xi \in \mathcal{O}/p^{n_0}\mathcal{O}$ with

$$|A_2| > p^{-\frac{3}{4}dn_0}|A_1| \quad \text{where} \quad A_2 = A_1 \cap \pi_{n_0}^{-1}(\xi). \tag{A.4}$$

Taking some element $\bar{x} \in A_2$, we have

$$A_2 = \bar{x} + p^{n_0}B \quad \text{where} \quad B \subset \mathcal{O}/p^{n-n_0}\mathcal{O}, |A_2| = |B|.$$

Let $1 \le m \le n - n_0$. From the definition of n_0 we have, by (A.4),

$$\max_{\xi} |B \cap \pi_m^{-1}(\xi)| \le \max_{\xi} |A_1 \cap \pi_{m+n_0}^{-1}(\xi)| \le p^{-\frac{3}{4}d(m+n_0)}|A_1| < p^{-\frac{3}{4}dm}|B|.$$

Apply then Lemma A.1 below with $\gamma_1 = \gamma_2 = 3/4$ to the set $B \subset \mathcal{O}/p^{n-n_0}\mathcal{O}$. It follows that

$$100B \cdot B = \mathcal{O}/p^{n-n_0}\mathcal{O},$$

implying (since $0 \in B$)

$$100(A_1 - A_1)(A_1 - A_1) \supset 100(A_2 - A_2)(A_2 - A_2) \supset \{x \in \mathcal{O}/p^n\mathcal{O} \mid \pi_{2n_0}(x) = 0\}.$$

The claim follows with $\tau = 8\delta_1$. □

A.2. Lemma A.1

Lemma A.1. *Let $\gamma_1, \gamma_2 > 0$ with $\gamma_1 + \gamma_2 > 1$ and $k \in \mathbb{Z}_+$ be such that $k > 4/\gamma_1 + \gamma_2 - 1$. Let $A_i, B_i \subset \mathcal{O}/p^m\mathcal{O}$ $(1 \le i \le k)$ satisfy, for all $1 \le m' \le m$,*

$$\max_{\xi} |\{x \in A_i \mid \pi_{m'}(x) = \xi\}| < p^{-dm'\gamma_1}|A_i|, \tag{A.5}$$

$$\max_{\xi} |\{x \in B_i \mid \pi_{m'}(x) = \xi\}| < p^{-dm'\gamma_2}|B_i|. \tag{A.6}$$

Let ν be the image measure on $\mathcal{O}/p^m\mathcal{O}$ of the normalized counting measure on $\prod_{i=1}^{k}(A_i \times B_i)$ under the map

$$(x_1, y_1, \dots, x_k, y_k) \mapsto x_1 y_1 + \cdots + x_k y_k.$$

Then

$$\max_{\xi \in \mathbb{Z}_q} \left| \nu(\xi) - \frac{1}{q} \right| < \frac{1}{qp}, \quad \text{where} \quad q = p^{md}. \tag{A.7}$$

Proof. Denote by $\mathrm{Tr} : \mathcal{O} \to \mathbb{Z}_p$ the usual trace map and let $e_a(x) = e^{\frac{2\pi i}{a}\mathrm{Tr}\, x}$ for $a = p^m$ and $x \in \mathcal{O}/a\mathcal{O}$. Hence $\{e_{p^m}(z\,\cdot\,) \mid z \in \mathcal{O}/p^m\mathcal{O}\}$ is a complete set of additive characters for $\mathcal{O}/p^m\mathcal{O}$.

We establish (A.7) with a standard exponential sum approach. Thus for $\xi \in \mathcal{O}/p^m\mathcal{O}$,

$$\begin{aligned}
&\nu(\xi)\\
&= \frac{1}{\prod |A_i|\,|B_i|} |\{(x_1, y_1, \dots, x_k, y_k) \in A_1 \times B_1 \times \cdots \times A_k \times B_k \mid x_1 y_1 + \cdots + x_k y_k = \xi\}|\\
&= \frac{1}{q \prod |A_i||B_i|} \sum_{\substack{x_i \in A_i,\, y_i \in B_i\\ z \in \mathcal{O}/p^m\mathcal{O}}} e_{p^m}(z(\xi - x_1 y_1 - \cdots - x_k y_k)) = \frac{1}{q} + F,
\end{aligned}$$

where

$$F \le \frac{1}{q} \sum_{\substack{z \in \mathcal{O}/p^m\mathcal{O}\\ z \neq 0}} \frac{1}{\prod |A_i|\,|B_i|} \prod_{i=1}^{k} \Big| \sum_{x \in A_i,\, y \in B_i} e_{p^m}(zxy) \Big|. \tag{A.8}$$

Write $z \in \mathcal{O}/p^m\mathcal{O}$, $z \neq 0$, in the form $z = p^{m'} w$ with $0 \le m' < m$ and $w \in (\mathcal{O}/p^{m-m'}\mathcal{O})^*$. Fix $0 \le m' < m$ and estimate ($A = A_i$, $B = B_i$)

$$\max_{(w,p)=1} \Big| \sum_{x \in A, y \in B} e_{p^{m-m'}}(wxy) \Big|. \tag{A.9}$$

Define

$$\eta_1(\xi) = |\{x \in A \mid \pi_{m-m'}(x) = \xi\}| \overset{(A.5)}{<} p^{-d(m-m')\gamma_1} |A|, \tag{A.10}$$

$$\eta_2(\xi) = |\{x \in B \mid \pi_{m-m'}(x) = \xi\}| \overset{(A.6)}{<} p^{-d(m-m')\gamma_2} |B|. \tag{A.11}$$

Hence, by Cauchy–Schwarz and Parseval, we can bound (A.9) as follows:

$$\begin{aligned}
\text{(A.9)} &= \Big| \sum_{\xi_1, \xi_2} \eta_1(\xi_1)\eta_2(\xi_2) e_{p^{m-m'}}(w\xi_1\xi_2) \Big|\\
&\times \Big(\sum_{\xi_1} \eta_1(\xi_1)^2 \Big)^{1/2} \Big(\sum_{\xi_1} \Big| \sum_{\xi_2} \eta_2(\xi_2) e_{p^{m-m'}}(w\xi_1\xi_2) \Big|^2 \Big)^{1/2}\\
&\overset{(A.10)}{<} p^{-d\frac{m-m'}{2}\gamma_1} |A| p^{\frac{m-m'}{2}d} \Big(\sum_{\xi_2} \eta_2(\xi_2)^2 \Big)^{1/2}\\
&\overset{(A.11)}{<} p^{-d(\gamma_1+\gamma_2)\frac{m-m'}{2} + d\frac{m-m'}{2}} |A|\,|B|.
\end{aligned} \tag{A.12}$$

Substitution of (A.12) in (A.8) clearly gives the estimate

$$\frac{1}{q}\sum_{0\le m'<m} p^{d(m-m'-1)}(p^d-1)p^{-\frac{k}{2}(m-m')(\gamma_1+\gamma_2-1)d} < \frac{1}{q}\sum_{s\ge 1} p^{ds(1-\frac{k}{2}(\gamma_1+\gamma_2-1))} < \frac{1}{pq}. \tag{A.13}$$

This proves (A.7). □

A.3. Regularization of the set

Returning to Theorem A.1 and $A \subset \mathcal{O}/p^n\mathcal{O}$, we will perform several preliminary constructions before proceeding with the amplification process. The first step is a regularization with respect to the natural tree structure $\mathcal{O}/p^n\mathcal{O} \to \mathcal{O}/p^{n-1}\mathcal{O} \to \cdots \to \mathcal{O}/p\mathcal{O}$ by passing to a large subset of A.

Fix a large integer $T = T(\delta_1, \delta_2)$. We may assume n to be a multiple of T (since p is fixed and $n \to \infty$), writing

$$n = Tn_1 \quad \text{and} \quad q = p^{dTn_1}.$$

The regularization process will lead to a subset $B \subset A$ and sequences

$$m_s \in [Ts, T(s+1)[\quad \text{and} \quad 1 \le K_s \le p^{dT}$$

for $0 \le s < n_1$, satisfying the following conditions:

$$\text{If} \quad x \in \pi_{m_s}(B), \quad \text{then} \quad |\pi_{m_{s+1}}(B(x))| = K_s, \tag{A.14}$$

where we write $B(x) = B \cap \pi_{m_s}^{-1}(\{x\})$.

$$\text{If} \quad K_s > 1 \quad \text{and} \quad x \in \pi_{m_s}(B), \quad \text{then} \quad |\pi_{m_{s+1}}(B(x))| \ge 2. \tag{A.15}$$

$$|B| > \left(\frac{1}{10T^2 \log p^d}\right)^{n_1} |A| > q^{-o(1)}|A| \quad \text{(for } T \text{ large enough).} \tag{A.16}$$

The construction is straightforward, starting at the bottom of the tree $\mathcal{O}/p^n\mathcal{O}$. We detail the first step and leave the continuation to the reader.

Define

$$\Omega = \{\xi \in \mathcal{O}/p^{T(n_1-1)}\mathcal{O} \mid |\pi_{T(n_1-1)}^{-1}(\xi) \cap A| = 1\}.$$

We distinguish two possibilities:

If $|\pi_{T(n_1-1)}^{-1}(\Omega) \cap A| \ge \frac{1}{2}|A|$ define

$$K_{n_1-1} = 1 \quad \text{and} \quad m_{n_1-1} = T(n_1-1)$$

and let

$$A_1 = A \cap \pi_{T(n_1-1)}^{-1}(\Omega).$$

Hence

$$|A_1(\xi)| = 1 \quad \text{for } \xi \in \pi_{T(n_1-1)}(A_1), \qquad |A_1| \geq \tfrac{1}{2}|A|.$$

Assume next $|\pi^{-1}_{T(n_1-1)}(\Omega) \cap A| < \frac{1}{2}|A|$. From the definition of Ω, we may then find some $m = m_{n_1-1} \in [T(n_1-1), Tn_1[$ such that

$$|\{x \in A \mid \{\pi_{m+1}(x') \mid x' \in A \text{ and } \pi_m(x) = \pi_m(x')\} \text{ has at least 2 elements}\}| > \frac{|A|}{4T} \tag{A.17}$$

and we take $m \in [T(n_1-1), Tn_1[$ as small as possible such that (A.17) holds. We may then introduce $A_1 \subset A$ and a dyadic integer $1 \leq K_{n_1-1} < p^{dT}$ such that

$$|\pi_m(A_1(\xi))| = 1 \quad \text{for } \xi \in \pi_{T(n_1-1)}(A_1), \tag{A.18}$$

$$|\pi_{m+1}(A_1(\xi))| \geq 2 \quad \text{for } \xi \in \pi_m(A_1), \tag{A.19}$$

$$|A_1 \cap \pi_m^{-1}(\xi)| = K_{n_1-1} \quad \text{for } \xi \in \pi_m(A_1), \tag{A.20}$$

$$|A_1| > \frac{|A|}{4T \log p^{dT}}. \tag{A.21}$$

In the next step, replace A by A_1, consider $\pi^{-1}_{T(n_1-2}(\xi) \cap A_1$ for $\xi \in \pi_{T(n_1-2)}(A_1)$ and introduce $T(n_1-2) \leq m_{n_1-2} < T(n_1-1)$, $1 \leq K_{n_1-2} < p^{dT}$ and $A_2 \subset A_1$ similarly. Note that for $\xi \in \pi_{T(n_1-1)}(A_2)$ we have $A_1(\xi) = A_2(\xi)$, and if $\xi \in \pi_{m_{n_1-2}}(A_2)$, then by construction

$$|\pi_{m_{n_1-1}}(A_2(\xi))| = |\pi_{T(n_1-1)}(A_2(\xi))| = K_{n_1-2}, \tag{A.22}$$

which is condition (A.14) with $s = n_1 - 2$.

Assume we have obtained the set $B \subset A$ satisfying (A.14)–(A.16). Next, define

$$\bar{s} = \max\Big\{0 \leq s < n_1 \;\Big|\; \prod_{s'<s} K_{s'} < p^{\frac{1}{2}\delta_2 m_s}\Big\}. \tag{A.23}$$

Thus there are $\xi \in \mathcal{O}/p^{m_{\bar{s}}}\mathcal{O}$ and $B' \subset B$ such that

$$\pi_{m_{\bar{s}}}(B') = \{\xi\}, \tag{A.24}$$

$$|B'| > p^{-\frac{1}{2}\delta_2 m_{\bar{s}}}|B|. \tag{A.25}$$

Suppose $m_{\bar{s}} > \varepsilon n$. Then, by (A.2), $|\pi_{m_{\bar{s}}}(A)| > p^{\delta_2 m_{\bar{s}}}$ and therefore by (A.16), (A.25), we get

$$|A + A| \geq |A + B'| \geq |\pi_{m_{\bar{s}}}(A)|\,|B'| > p^{\frac{1}{2}\delta_2 m_{\bar{s}}} q^{-o(1)}|A|. \tag{A.26}$$

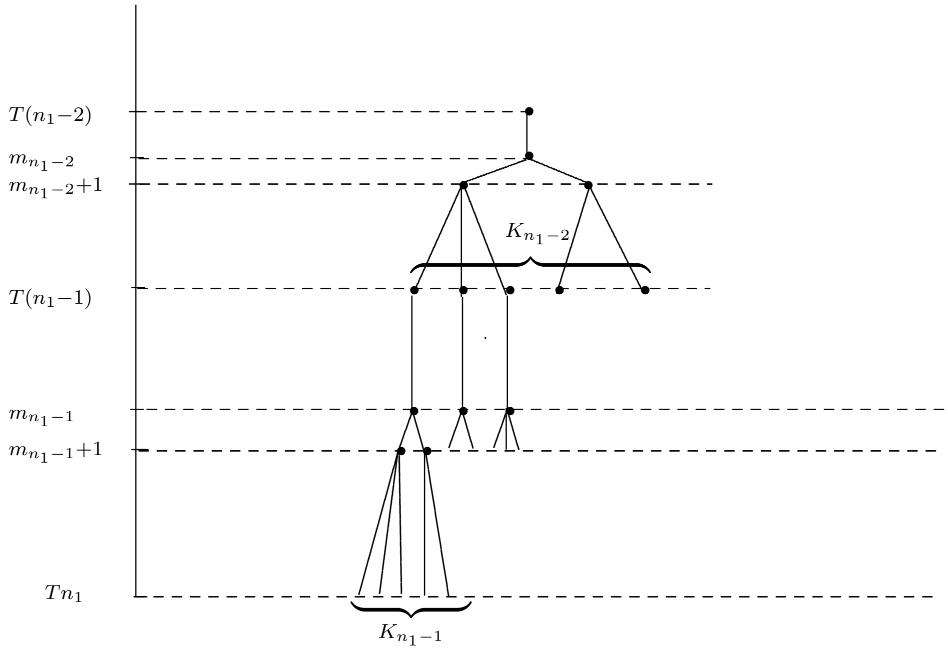
Assume (A.3) fails to hold, i.e.

$$|A \cdot A \cdot A + A \cdot A \cdot A| < q^{0+}|A|.$$

Note that by the Plünnecke–Ruzsa sumset inequalities we also have

$$|rA \cdot A \cdot A - rA \cdot A \cdot A| \ll_{(r)} q^{0+}|A| \tag{A.27}$$

for the r-fold sumset, assuming r is bounded.



In particular, (A.26) implies

$$p^{\frac{1}{2}\delta_2 m_{\bar{s}}} q^{-o(1)} < q^{o(1)}$$

or

$$m_{\bar{s}} = o(1)n.$$

Therefore, certainly

$$m_{\bar{s}} \le \varepsilon n. \tag{A.28}$$

Since (A.24) holds and taking some $b' \in B'$ we have, for some $A' \subset \mathcal{O}/p^{n-m_{\bar{s}}}\mathcal{O}$,

$$B' - b' = p^{m_{\bar{s}}} A',$$

where by (A.16), (A.25), (A.28),

$$|A'| = |B'| > q^{-\varepsilon}|A|.$$

Define for $1 \le s < n_1 - \bar{s}$,

$$m'_s = m_{\bar{s}+s} - m_{\bar{s}}. \tag{A.29}$$

Hence from (A.14) and (A.15),

$$|\pi_{m'_{s+1}}(A'(x))| = K_{s+\bar{s}} \quad \text{for } x \in \pi_{m'_s}(A'),$$
$$|\pi_{m'_{s+1}}(A'(x))| \ge 2 \quad \text{if } K_{s+\bar{s}} \ge 2 \text{ and } x \in \pi_{m'_s}(A').$$

From the definition (A.23) of $\bar{s}$ it also follows that

$$|\pi_{m'_s}(A')| = |\pi_{m_{\bar{s}+s}}(B')| = \prod_{\bar{s}\le s'<\bar{s}+s} K_{s'} = \frac{\prod_{s'<\bar{s}+s} K_{s'}}{\prod_{s'<\bar{s}} K_{s'}} > p^{\frac{1}{2}\delta_2(m_{\bar{s}+s}-m_{\bar{s}})} = p^{\frac{1}{2}\delta_2 m'_s}.$$

Also, since $p^{m_{\bar{s}}}A' \subset A - A$, it follows from (A.27) and (A.28) that

$$|rA' \cdot A' \cdot A| < p^{2dm_{\bar{s}}}|r(A-A)^{(2)} \cdot A| < q^{2\varepsilon+o(1)}|A|.$$

We simplify notation at this point replacing K_s by $K_{\bar{s}+s}$ and m_s by m'_s ($1 \le s < n_1 - \bar{s}$). Summarizing the relevant properties we have

$$|\pi_{m_s}(A')| > p^{\frac{1}{2}\delta_2 m_s}, \tag{A.30}$$

$$|\pi_{m_{s+1}}(A'(x))| = K_s \quad \text{for } x \in \pi_{m_s}(A'), \tag{A.31}$$

$$\text{if} \quad K_s > 1, \quad \text{then} \quad |\pi_{m_{s+1}}(A'(x))| \ge 2 \text{ for } x \in \pi_{m_s}(A'), \tag{A.32}$$

$$|rA' \cdot A' \cdot A| \ll_{(r)} q^{o(1)}|A| \quad \text{for any given } r \in \mathbb{Z}_+, \tag{A.33}$$

$$|A'| > q^{-o(1)}|A| \tag{A.34}$$

(letting ε be small enough).

The core of our argument is of course to obtain a lower bound on $rA' \cdot A' \cdot A$ that will contradict (A.33). Before proceeding, we need one more manipulation.

We construct further sequences $k_i = m_{s_i}$, $k'_i = m_{s'_i}$ where $s_i \le s'_i < s_{i+1}$, hence $k_i \le k'_i < k_{i+1}$ ($i < j$).

Take a sufficiently small $\delta = \delta(\delta_1, \delta_2) > 0$ (to be specified) and let

$$R = [100/\delta]. \tag{A.35}$$

Assume s_i is obtained. Define

$$s'_i = \min\{s \ge s_i \mid K_s \ge 2\} \tag{A.36}$$

if possible. Otherwise we terminate at $j = i$ defining $s'_i = n_1 - \bar{s} - 1$. Assuming s'_i can be defined by (A.36), if $s'_i + R \ge n_1 - \bar{s} - 1$, we terminate again at $j = i$. Assume now $s'_i + R < n_1 - \bar{s} - 1$. There are two cases.

Case I: We have

$$\prod_{s'_i \le s < s'_i + R} K_s < p^{(1-\delta)d(m_{s'_i+R} - m_{s'_i})}.$$

Then take $s_{i+1} = s'_i + R$.

Case II: We have

$$\prod_{s'_i \le s < s'_i + R} K_s \ge p^{(1-\delta)d(m_{s'_i+R} - m_{s'_i})}.$$

Then take s_{i+1} to be the smallest $s \geq s'_i + R$ such that

$$\prod_{s'_i \leq s' < s} K_{s'} < p^{(1-\delta)d(m_s - m_{s'_i})}. \tag{A.37}$$

This is possible unless

$$\prod_{s'_i \leq s' < n_1 - \bar{s}} K_{s'} > p^{(1-\delta)d(m_{n_1-\bar{s}-1} - m_{s'_i})}, \tag{A.38}$$

in which case we can again terminate at $i = j$.

In Case II, it follows from the construction of s_{i+1} that if $m_{s'-1} \leq k < m_{s'}$ with $s'_i + R \leq s' < s_{i+1}$ then for all $\xi \in \pi_{m_{s'_i}}(A')$ we have

$$\begin{aligned} |\pi_k(A'(\xi))| &\geq p^{-d(m_{s'}-k)} |\pi_{m_{s'}}(A'(\xi))| = p^{-d(m_{s'}-k)} \prod_{s'_i \leq t < s'} K_t \\ &\geq p^{-d(m_{s'}-k) + d(m_{s'} - m_{s'_i})(1-\delta)} > p^{(1-2\delta)d(k - m_{s'_i})}. \end{aligned} \tag{A.39}$$

Also, for $m_{s_{i+1}-1} \leq k < m_{s_{i+1}}$, from $k - m_{s'_i} \geq (R-1)T$ and (A.35) we have

$$\begin{aligned} |\pi_k(A'(\xi))| \geq |\pi_{m_{s_{i+1}-1}}(A'(\xi))| &\overset{(A.39)}{>} p^{(1-2\delta)d(m_{s_{i+1}-1} - m_{s'_i})} \\ &> p^{(1-2\delta)d(k - m_{s'_i}) - dT} > p^{(1-3\delta)d(k - m_{s'_i})}, \end{aligned} \tag{A.40}$$

so that (A.40) holds whenever $m_{s'_i} \leq k \leq m_{s_{i+1}}$.

From the preceding and (A.38), the construction terminates at $i = j$ when either

$$\prod_{t \geq s_j} K_t < p^{dTR}, \tag{A.41}$$

or

$$\prod_{s'_j \leq t < n_1 - \bar{s}} K_t > p^{(1-\delta)d(m_{n_1-\bar{s}-1} - m_{s'_j})}. \tag{A.42}$$

Since the amplification performed in the next section will only relate to the levels $m \in \bigcup_{i<j} [m_{s'_i}, m_{s_{i+1}}]$, we need a lower bound on

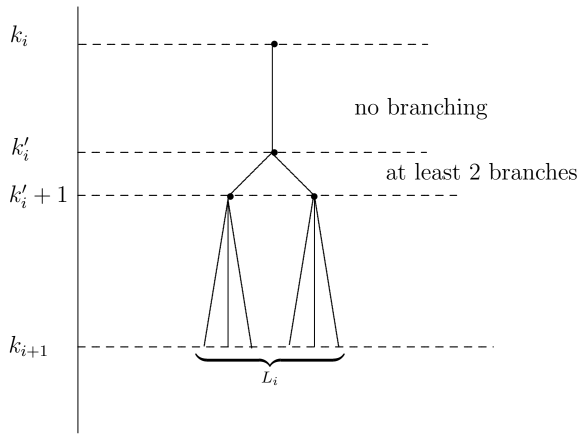
$$\prod_{i<j} \prod_{s'_i \leq t < s_{i+1}} K_t = |\pi_{m_{s_j}}(A')| = |\pi_{m_{s'_j}}(A')|. \tag{A.43}$$

If (A.41) holds, then obviously

$$(A.43) > p^{-dTR} |A'| > q^{-o(1)} |A|. \tag{A.44}$$

If (A.42) holds we argue as follows:

$$q^{1-\delta_1} > q^{-\delta} p^{d(m_{n_1-\bar{s}-1} - m_{s'_j})} \overset{(A.29)}{>} q^{1-\delta} p^{-dm_{\bar{s}} - dm_{s'_j}} \overset{(A.28)}{>} q^{1-\delta-\varepsilon} p^{-dm_{s'_j}},$$



and hence

$$m_{s_j'} \geq (\delta_1 - \delta - \varepsilon)n > \frac{\delta_1}{2} n \tag{A.45}$$

if we let ε, δ be small enough.

Recalling (A.30), it also follows that

$$\text{(A.43)} \geq p^{\frac{1}{2}\delta_2 m_{s_j'}} > p^{\frac{1}{4}\delta_1\delta_2 n}. \tag{A.46}$$

Consequently, we introduce sequences $k_1 \leq k_i' < k_{i+1}$ $(i < j)$ such that

$$\text{if} \quad x \in \pi_{k_i'}(A'), \quad \text{then} \quad |\pi_{k_i'+1}(A'(x))| \geq 2; \tag{A.47}$$

$$\text{if} \quad k_{i+1} - k_i' > 2RT \text{ and } x \in \pi_{k_i'}(A'), \quad \text{then}$$
$$|\pi_{k_{i+1}}(A'(x))| = L_i < p^{(1-\delta)d(k_{i+1}-k_i')}, \tag{A.48}$$

and for $k_i' + RT < k \leq k_{i+1}$,

$$|\pi_k(A'(x))| > p^{(1-3\delta)d(k-k_i')}, \tag{A.49}$$

$$|\pi_{k_j}(A')| = \prod_{i \leq j} L_i > p^{\frac{1}{4}\delta_1\delta_2 n}, \tag{A.50}$$

$$|\pi_k(A')| > p^{\frac{1}{4}\delta_2 k} \quad \text{for } T < k < n_1 \quad \text{(by (A.30))}. \tag{A.51}$$

We may of course also assume

$$\pi_1(x) \neq 0 \quad \text{for } x \in A'. \tag{A.52}$$

Indeed, since $|\pi_{m_1}(A')| \geq 2$ and thus $\pi_{m_1}(A') \neq \{0\}$ we may replace A' by the set $p^{-k_0}\{x \in A' \mid \pi_{k_0}(x) = 0; \pi_{k_0+1}(x) \neq 0\}$ for some $0 \leq k_0 < m_1$.

A.4. The amplification

Recalling (A.1), there is a subset C of a suitable sumset of A, with $|C| = p^{2RTd}$, such that

$$\pi_{2RT}|_C : C \to \mathcal{O}/p^{2RT}\mathcal{O} \quad \text{is one-to-one,} \tag{A.53}$$

and moreover

$$\pi_{2RT+1}(x) \neq 0 \quad \text{for } x \in C. \tag{A.54}$$

Let A' and $k_i \leq k'_i < k_{i+1}$ $(i \leq j)$ be as in Section A.3, satisfying (A.47)–(A.50). Let $r \in \mathbb{Z}_+$, $r = r(\delta_1, \delta_2)$, be large enough (to be specified). Define

$$\Omega = (A' \times A' \times C)^r \subset (\mathcal{O}/p^n\mathcal{O})^{3r},$$

the product set equipped with the normalized counting measure $\mathbb{P}$.

Consider the map

$$\phi : \Omega \to \mathcal{O}/p^n\mathcal{O} : (x_1, y_1, z_1, \ldots, x_r, y_r, z_r) \to x_1y_1z_1 + \cdots + x_ry_rz_r. \tag{A.55}$$

Hence $\phi(\Omega) \subset rA' \cdot A' \cdot C \subset rA' \cdot A' \cdot A$ and our aim is to contradict (A.33) by establishing a lower bound on $|\phi(\Omega)|$. Note that for $k \leq n$, $(\pi_k\phi)(\xi)$ only depends on $\pi_k(\xi)$. Let μ_k be the normalized counting measure on $\mathcal{O}/p^k\mathcal{O}$ for $k \leq n$ and $\mathbb{E}_k$ the corresponding expectation operator.

Define the density

$$F = F_n = \frac{d\phi(\mathbb{P})}{d\mu_n} \tag{A.56}$$

and for $k \leq n$,

$$F_k = \mathbb{E}_k(F) = \frac{d\pi_k\phi(\mathbb{P})}{d\mu_k}. \tag{A.57}$$

Fix i. The key estimate is a bound on

$$\int \max_{\pi_{k_{i+1}}(x)=x'} F_{k_{i+1}}(x)\, \mu_{k'_i}(dx'). \tag{A.58}$$

We will show that

$$\text{(A.58)} < 2, \tag{A.59}$$

which means that, conditional on $\pi_{k'_i}$, $\pi_{k_{i+1}}\phi$ is almost uniformly distributed.

Let $k = k_{i+1}$ and $k' = k'_i$. By (A.57),

$$F_k(x) = p^{kd}|\Omega|^{-1}|\{\xi \in \Omega \mid \pi_k\phi(\xi) = x\}|. \tag{A.60}$$

Hence

$$\int \max_{\pi_{k'}(x)=x'} F_k(x)\,\mu_{k'}(dx') = p^{(k-k')d}|\Omega|^{-1} \sum_{x'\in\mathcal{O}/p^{k'}\mathcal{O}} \max_{\pi_{k'}(x)=x'} |\{\xi \in \Omega \mid \pi_k\phi(\xi) = x\}|$$

$$\le p^{(k-k')d}|\Omega|^{-1} \sum_{\zeta\in\pi_{k'}(\Omega)} \max_x |\{\xi \in \Omega \mid \pi_{k'}(\xi) = \zeta \text{ and } \pi_k\phi(\xi) = x\}|$$

$$= p^{(k-k')d}|A'|^{-2r}|C|^{-r} \times \sum_{\substack{x'_1,\dots,x'_r\in\pi_{k'}(A')\\ y'_1,\dots y'_r\in\pi_{k'}(A')\\ z_1,\dots,z_r\in C}} \max_x |\{x_s \in A'(x'_s),\ y_s \in A'(y'_s)\ (1\le s\le r) \mid \pi_k(x_1y_1z_1+\cdots+x_ry_rz_r) = x\}|$$

$$= p^{(k-k')d}|\pi_k(A')|^{-2r}|C|^{-r} \times \sum_{\substack{x'_1,\dots,x'_r\in\pi_{k'}(A')\\ y'_1,\dots y'_r\in\pi_{k'}(A')\\ z_1,\dots,z_r\in C}} \max_x |\{x_s \in \pi_k(A'(x'_s)),\ y_s \in \pi_k(A'(y'_s))(1\le s\le r) \mid x_1y_1\pi_k(z_1)+\cdots+x_ry_r\pi_k(z_r) = x\}| \tag{A.61}$$

(for the last equality, we use the regular tree structure of A').

We evaluate the inner $\max_x$ in (A.61) by an exponential sum estimate. Thus

$$\max_x |\dots| \le \frac{1}{|\mathcal{O}/p^k\mathcal{O}|} \sum_{\eta\in\mathcal{O}/p^k\mathcal{O}} \Big| \sum_{\substack{x_s\in\pi_k(A'(x'_s))\\ y_s\in\pi_k(A'(y'_s))}} e_{p^k}\Big(\eta \sum_{s=1}^r x_sy_sz_s\Big)\Big| \tag{A.62}$$

with the notation from Lemma A.1. Note that (A.62) has become independent of x. Substitution in (A.61) gives

$$\le p^{-k'd}|\pi_k(A')|^{-2r}|C|^{-r} \sum_{\eta\in\mathcal{O}/p^k\mathcal{O}} \Big(\sum_{\substack{x'\in\pi_{k'}(A')\\ y\in\pi_k(A')\\ z\in C}} \Big| \sum_{x\in\pi_k(A'(x'))} e_{p^k}(\eta xyz)\Big|\Big)^r. \tag{A.63}$$

Using Cauchy–Schwarz for the second summation we obtain

$$\text{(A.63)} \le p^{-k'd}|\pi_k(A')|^{-3r/2}|\pi_{k'}(A')|^{r/2}|C|^{-r/2} \times \sum_{\eta\in\mathcal{O}/p^k\mathcal{O}} \Big(\sum_{\substack{x'\in\pi_{k'}(A')\\ y\in\pi_k(A')\\ z\in C}} \Big| \sum_{x\in\pi_k(A'(x'))} e_{p^k}(\eta xyz)\Big|^2\Big)^{r/2}$$

$$\le p^{-k'd}|\pi_k(A')|^{-r}|A'|^{-r/2}|\pi_{k'}(A')|^{r/2}|C|^{-r/2} \times \sum_{\eta\in\mathcal{O}/p^k\mathcal{O}} \Big(\sum_{x'\in\pi_{k'}(A')} \Big| \sum_{\substack{x_1,x_2\in\pi_k(A'(x'))\\ y\in A'\\ z\in C}} e_{p^k}(\eta(x_1-x_2)yz)\Big|\Big)^{r/2}. \tag{A.64}$$

Since $\pi_{k'}(x_1 - x_2) = 0$,

$$\begin{aligned}(\mathrm{A}.64) &= |\pi_k(A')|^{-r}|A'|^{-r/2}|\pi_{k'}(A')|^{r/2}|C|^{-r/2}\\ &\times \sum_{\eta\in\mathcal{O}/p^{k-k'}\mathcal{O}} \Big(\sum_{x'\in\pi_{k'}(A')}\Big|\sum_{\substack{x_1,x_2\in\pi_k(A'(x'))\\ y\in A',\, z\in C}} e_{p^k}(\eta(x_1-x_2)yz)\Big|\Big)^{r/2}. \end{aligned} \tag{A.65}$$

We now proceed to estimate, for $x' \in \pi_{k'}(A')$,

$$\sum_{\substack{x_1,x_2\in\pi_k(A'(x'))\\ y\in A', z\in C}} e_{p^k}(\eta(x_1-x_2)yz) \tag{A.66}$$

using the properties (A.37)–(A.51) of A'.

Recall that $k' = k_i'$, $k = k_{i+1}$ and $|\pi_k(A'(x'))| = L_i$. There are two cases.

Case I: $k - k' \le 2RT$. Since C satisfies (A.53) and $0 \notin \pi_1(A')$ by (A.52),

$$\sum_{z\in C} e_{p^{k-k'}}\left(\eta \frac{x_1-x_2}{p^{k'}} yz\right) = 0$$

unless $x_1 \equiv x_2 \pmod{p^{k'+1}}$ or $\pi_{k-k'}(\eta) = 0$ (since we assumed (p) prime). Recall that $|\pi_{k'+1}(A'(x'))| \ge 2$ according to (A.47). Hence, if $\pi_{k-k'}(\eta) \ne 0$,

$$\begin{aligned}(\mathrm{A}.66) &\le |A'|\,|C| \sum_{t\in\pi_{k'+1}(A'(x'))} |\pi_k(A'(t))|^2\\ &\le |A'|\,|C|(|\pi_k(A'(x'))|^2 - |\pi_k(A'(x'))|) \le |A'|\,|C| L_i^2(1-p^{-2dRT}).\end{aligned}$$

Substituting (A.66) in (A.65) gives the contribution

$$(\mathrm{A}.65) \le 1 + (p^{(k-k')d} - 1)(1-p^{-2dRT})^{r/2} < 2,$$

provided we take

$$r = r(p, \delta_1, \delta_2) > p^{4dRT} \tag{A.67}$$

(this choice of r will also ensure that $C \subset rA$ with C satisfying (A.53), (A.54)).

Case II: $k - k' > 2RT$. Let $\pi_{k-k'}(\eta) \ne 0$ and write $\eta = p^m\eta_1$ with $0 \le m < k - k'$ and $\eta_1 \in (\mathcal{O}/p^{k-k'-m}\mathcal{O})^*$. We need to evaluate

$$\sum_{\substack{x_1,x_2\in\pi_k(A'(x'))\\ y\in A',\, z\in C}} e_{p^{k-k'-m}}\left(\eta_1 \frac{x_1-x_2}{p^{k'}} yz\right). \tag{A.68}$$

Set

$$0 < l = k - k' - m \le k - k'.$$

If $l \le 2RT$, we again invoke (A.53) to claim that $\sum_{z\in C} e_{p^l}(\eta_1 \frac{x_1-x_2}{p^{k'}} yz) = 0$ unless $\pi_{k-m}(x_1-x_2) = 0$, hence $\pi_{k'+1}(x_1-x_2) = 0$. The same calculation from Case I implies that

$$|(\text{A.68})| < |A'|\,|C|\,|\pi_k(A'(x'))|^2(1 - p^{-2dRT}). \tag{A.69}$$

Assume next $l > 2RT$. Fix $x_0 \in A'(x')$. For $\xi \in \mathcal{O}/p^l\mathcal{O}$ define

$$\lambda_1(\xi) = \left|\left\{x \in \pi_k(A'(x')) \;\middle|\; \pi_l\left(\frac{x - x_0}{p^{k'}}\right) = \xi\right\}\right|,$$
$$\lambda_2(\xi) = |\{y \in A' \mid \pi_l(y) = \xi\}|,$$
$$\lambda_3(\xi) = |\{(y,z) \in A' \times C \mid \pi_l(yz) = \xi\}|.$$

Hence

$$|(\text{A.68})| \le |\pi_k(A'(x'))| \left|\sum_{\xi,\xi'} e_{p^l}(\eta_1\xi\xi')\lambda_1(\xi)\lambda_3(\xi')\right|. \tag{A.70}$$

Since A' is regular and $l > 2RT$,

$$\lambda_1(\xi) \underset{p^{dT}}{\sim} \frac{|\pi_k(A'(x'))|}{|\pi_{k'+l}(A'(x'))|} < p^{-(1-3\delta)dl+dT}|\pi_k(A'(x'))| < \frac{|\pi_k(A'(x'))|}{p^{(1-4\delta)dl}} \tag{A.71}$$

by applying (A.49) with $k_i' = k'$, $k_{i+1} = k$ and replacing k by $k' + l$.

Also, by (A.51),

$$\lambda_2(\xi) \underset{p^{dT}}{\sim} \frac{|A'|}{|\pi_l(A')|} < p^{-\frac{1}{4}l\delta_2}|A'|. \tag{A.72}$$

Recalling (A.54) we have $C = \bigcup_{0\le a\le 2RT} C_{(a)}$, where

$$C_{(a)} = \{z \in C \mid \pi_a(z) = 0 \text{ and } \pi_{a+1}(z) \neq 0\}$$

and

$$|C_{(a)}| = p^{-ad}|C|.$$

Since the map $\mathcal{O}/p^l\mathcal{O} \to \mathcal{O}/p^l\mathcal{O} : x \mapsto zx$ has multiplicity p^{ad} for $z \in C_{(a)}$, it follows that

$$\lambda_3(\xi) \le \sum_{a\le 2RT}\sum_{z\in C_{(a)}} |\{y \in A' \mid \pi_l(yz) = \xi\}| \le \sum_{a\le 2RT} |C_{(a)}|(\max_{\xi'} \lambda_2(\xi'))p^{ad}$$
$$\overset{(\text{A.72})}{<} (1 + 2RT)p^{-\frac{1}{4}l\delta_2}|A'|\,|C| \le p^{-\frac{1}{8}\delta_2 l}|A'|\,|C| \tag{A.73}$$

(since $l > RT$ and (A.35) with $\delta < \delta_2^2$).

Returning to (A.70), in view of (A.71) and (A.73), take $\delta > 0$ so as to ensure that

$$1 - 4\delta + \frac{1}{8}\frac{\delta_2}{d} > 1 + \frac{\delta_2}{10d}. \tag{A.74}$$

Proceeding as in the proof of Lemma A.1, this gives

$$(\text{A.70}) \le |\pi_k(A'(x'))|^2|A'|\,|C|p^{-d\frac{l}{2}\frac{\delta_2}{10d}}. \tag{A.75}$$

Hence using the estimates (A.69) and (A.75) we see that in Case 2,

$$\begin{aligned}(\text{A.65}) \le 1 &+ \sum_{k-k'-2RT\le m<k-k'} p^{d(k-k'-m)}(1-p^{-2dRT})^r \\ &+ \sum_{0\le m<k-k'-2RT} p^{d(k-k'-m)-\frac{1}{40}\delta_2 rd(k-k'-m)} < 2\end{aligned}$$

if we take r as in (A.67). This establishes (A.59).

Next we proceed with an entropy calculation. With $k=k_{i+1}$ and $k'=k_i'$, write

$$\int F_k \log^+ F_k \, d\mu_k \le \int F_{k'} \log^+ F_{k'} \, d\mu_{k'} + \int F_k \log^+ \frac{F_k}{F_{k'}} \, d\mu_k$$

and

$$\begin{aligned}\int F_k \log^+ \frac{F_k}{F_{k'}} \, d\mu_k &\le \int \left(\log^+ \left(\max_{\pi_{k'}(x)=x'} \frac{F_k(x)}{F_{k'}(x')}\right)\right) F_{k'}(x') \, d\mu_{k'} \\ &\le \int \left(\max_{\pi_{k'}(x)=x'} F_k(x)\right) d\mu_{k'} \overset{(\text{A.59})}{<} 2. \end{aligned} \tag{A.76}$$

Hence, letting j be as in Section A.3 we have

$$\begin{aligned}\int F_{k_j} \log^+ F_{k_j} \, d\mu &\le \sum_{i<j} \int F_{k_{i+1}} \log^+ \frac{F_{k_{i+1}}}{F_{k_i'}} d\mu + \sum_{i<j} \int F_{k_i'} \log^+ \frac{F_{k_i'}}{F_{k_i}} d\mu \\ &\overset{(\text{A.76})}{<} 2j + \log \prod_{i<j} p^{d(k_i'-k_i)}. \end{aligned} \tag{A.77}$$

Next, set $S = \operatorname{supp} F_{k_j} = \pi_{k_j}(\phi(\Omega)) \subset \pi_{k_j}(rA' \cdot A' \cdot A)$. Let $0<\gamma<1$ be a parameter. Since $\int_S F_{k_j} \, d\mu_{k_j} = 1$, we have

$$\begin{aligned}1-\gamma < \int_{[F_{k_j} > \gamma/\mu_{k_j}(S)]} F_{k_j} \, d\mu_{k_j} &< \frac{1}{\log^+(\gamma/\mu_{k_j}(S))} \int F_{k_j} \log^+ F_{k_j} \, d\mu \\ &\overset{(\text{A.77})}{\le} \frac{1}{\log^+(\gamma/\mu_{k_j}(S))} \log e^{2j} \prod_{i<j} p^{d(k_i'-k_i)}\end{aligned}$$

and therefore

$$\left(\frac{\gamma}{\mu_{k_j}(S)}\right)^{1-\gamma} < e^{2j} \prod_{i<j} p^{d(k_i'-k_i)}.$$

Hence

$$
\begin{aligned}
|S| = p^{dk_j}\mu_{k_j}(S) &> \gamma p^{dk_j}\Big(e^{2j}\prod_{i<j} p^{d(k_i'-k_i)}\Big)^{-1/(1-\gamma)}\\
&> p^{dk_j}\frac{e^{-2j}}{\log q}\prod_{i<j} p^{d(k_i-k_i')} \quad \text{(for appropriate } \gamma)\\
&= \frac{e^{-2j}}{\log q}\prod_{i<j} p^{d(k_{i+1}-k_i')}\\
&\overset{(A.48)}{>} q^{-1/T}\Big(\prod_{i<j} L_i\Big)^{1/(1-\delta)}\\
&\overset{(A.50)}{>} q^{-1/T}|\pi_{k_j}(A')|^{1/(1-\delta)}.
\end{aligned}
\tag{A.78}
$$

Take $\xi \in \mathcal{O}/p^{k_j}\mathcal{O}$ such that

$$
|\pi_{k_j}^{-1}(\xi)\cap A'| \geq \frac{|A'|}{|\pi_{k_j}(A')|}.
$$

Clearly

$$
\begin{aligned}
|(r+1)A'\cdot A'\cdot A| &\geq |\pi_{k_j}(rA'\cdot A'\cdot A)|\frac{|A'|}{|\pi_{k_j}(A')|}\\
&\overset{(A.78)}{>} q^{-1/T}\,|\,|A'|\,|\pi_{k_j}(A')|^{\delta/(1-\delta)}\\
&\overset{(A.34),(A.50)}{>} q^{-1/T-o(1)+\frac{1}{4d}\delta_1\delta_2\delta}|A|.
\end{aligned}
$$

In order to satisfy (A.45) and (A.74), which are the only conditions on δ, let

$$
\delta = \frac{1}{100d}\min(\delta_1,\delta_2).
$$

We obtain a contradiction to (A.33) for T large enough. This proves Theorem A.1.

A.5. Proof of Proposition 3.3

Let $\pi_n : \mathcal{O} \to \mathcal{O}/p^n\mathcal{O}$ be the projection. Let $A \subset \mathcal{O}$ with

$$
|\pi_{n_1}(A)| > p^{\delta n_1}.
$$

We may construct $1 \leq n_0 < n_1$ and $B \subset A$ such that

$$
n_1 - n_0 > \delta n_1/4, \quad p^{n_0}B \subset A - A, \quad |\pi_m(B)| > p^{\delta m/4} \quad \text{for } m < n_1 - n_0.
$$

Replacing A by B we can therefore assume

$$
|\pi_m(A)| > p^{\delta m} \quad \text{for all } m \leq n_1. \tag{A.79}
$$

Replacing further A by a multiplicative translate, we ensure moreover that $1 \in A$.

Let R be the subring of $\mathcal{O}$ generated by A (hence $1 \in R$). Replacing A by a sum-product set, we may assume

$$\pi_1(A) = \pi_1(R). \tag{A.80}$$

Defining, for $m \in \mathbb{Z}_+$,

$$\Lambda_m = \{\pi_1(x) \mid p^m x \in R\} \subset \mathcal{O}/p\mathcal{O}$$

we obtain an increasing sequence of subsets of $\mathcal{O}/p\mathcal{O}$ with $\Lambda_0 = \pi_1(R)$.

Set

$$\bar{n} = \min\{n \in \mathbb{Z}_+ \mid \Lambda_n \neq \pi_1(R)\}. \tag{A.81}$$

It follows that if $n \leq \bar{n}$ and $z \in \mathcal{O}$ with $p^n z \in R$ then there is an element $x \in R$ with $\pi_{\bar{n}-n}(x - z) = 0$.

Assume $\bar{n} < n_1$. Using sum-product estimates developed above we will prove in Section A.6 that

$$\pi_{\bar{n}}(\tilde{A}) \supset \pi_{\bar{n}}(p^k R) \quad \text{for } k = [\bar{n}/10], \tag{A.82}$$

where $\tilde{A}$ is a further sum-product set of A.

Also, by (A.81), there is $z_0 \in \mathcal{O}$ such that

$$p^{\bar{n}} z_0 \in R \quad \text{and} \quad \pi_1(z_0) \notin \pi_1(R). \tag{A.83}$$

We make a few preliminary observations. Assume $\pi_{\bar{n}+1}(\tilde{A}) \supset \pi_{\bar{n}+1}(R)$. Hence there is $\tilde{a} \in \tilde{A}$ such that $\tilde{a} - p^{\bar{n}} z_0 \in p^{\bar{n}+1}\mathcal{O}$ and thus

$$\pi_1\left(\frac{\tilde{A} \cap p^{\bar{n}}\mathcal{O}}{p^{\bar{n}}}\right) \not\subseteq \pi_1(R). \tag{A.84}$$

Note that by (A.82), also

$$\pi_1\left(\frac{\tilde{A} \cap p^{\bar{n}}\mathcal{O}}{p^{\bar{n}}}\right) \supset \pi_1(R) \tag{A.85}$$

and therefore

$$\pi_1\left(\frac{\tilde{A} \cap p^{\bar{n}}\mathcal{O}}{p^{\bar{n}}}\right) \supsetneq \pi_1(R). \tag{A.86}$$

Assume next that instead of (A.82) we have the stronger property

$$\pi_{\bar{n}}(\tilde{A}) \supset \pi_{\bar{n}}(R). \tag{A.87}$$

Hence $\pi_{\bar{n}+1}(\tilde{A})$ is a subset of $\pi_{\bar{n}+1}(R)$ that certainly satisfies

$$\frac{|\pi_{\bar{n}+1}(\tilde{A})|}{|\pi_{\bar{n}+1}(R)|} > \frac{1}{p^d}$$

as a consequence of (A.87).

Passing to a further sum-product set $\tilde{\tilde{A}}$ we may clearly ensure that $\pi_{\bar{n}+1}(\tilde{\tilde{A}})$ is a ring. Since obviously $\pi_{\bar{n}+1}(R)$ is generated by $\pi_{\bar{n}+1}(A)$ it follows that $\pi_{\bar{n}+1}(R) = \pi_{\bar{n}+1}(\tilde{\tilde{A}})$, which enables us to deduce (A.84)–(A.86) (replacing $\tilde{A}$ by $\tilde{\tilde{A}}$).

Returning to (A.82), define

$$B = \frac{\tilde{A} \cap p^k \mathcal{O}}{p^k} \subset \mathcal{O} \tag{A.88}$$

satisfying

$$\pi_{\bar{n}-k}(B) = \pi_{\bar{n}-k}(R) \tag{A.89}$$

by (A.82). In particular, there is an element $\xi \in B$ such that

$$\pi_{\bar{n}-k}(1 - \xi) = 0. \tag{A.90}$$

Take $\eta \in \mathcal{O}$ such that $1 = \xi\eta$ (recall that $\mathcal{O}$ are the integers of the completion) and let $B_1 = \eta B$. Hence B_1 has a unit and by (A.89), also

$$\pi_{\bar{n}-k}(B_1) = \pi_{\bar{n}-k}(R). \tag{A.91}$$

Next, let R_1 be the ring generated by B_1. By (A.91), also

$$\pi_{\bar{n}-k}(R) = \pi_{\bar{n}-k}(R_1). \tag{A.92}$$

Defining

$$m_1 = \min\{m \in \mathbb{Z}_+ \mid \pi_1(R_1) \neq \{\pi_1(x) \mid x \in \mathcal{O},\, p^m x \in R_1\}\}$$

it follows from (A.92) and the definition of $\bar{n}$ that

$$m_1 \geq \bar{n} - k.$$

Again, if $m \leq m_1$ and $z \in \mathcal{O}$, $p^m z \in R_1$ then there is an element $x \in R_1$ with $\pi_{m_1-m}(x - z) = 0$. We distinguish two cases.

Case 1: $m_1 \leq \bar{n}+1$. Since $\pi_{\bar{n}-k}(B_1) = \pi_{\bar{n}-k}(R_1)$ with $k = [\bar{n}/10]$, it easily follows that

$$\pi_{m_1}(R_1) = \pi_{m_1}(B_1 + B_1^{(3)}) = \pi_{m_1}(\tilde{B}_1).$$

This is condition (A.87) with A replaced by B_1. Therefore

$$\pi_1\left(\frac{\tilde{B}_1 \cap p^{m_1}\mathcal{O}}{p^{m_1}}\right) \supsetneq \pi_1(R). \tag{A.93}$$

By (A.87) and (A.88) we easily deduce from (A.93) that

$$\pi_1\left(\frac{\tilde{A} \cap p^{m_2}\mathcal{O}}{p^{m_2}}\right) \supsetneq \pi_1(R)$$

for some $k + m_1 \leq m_2 < m_1 + ck < c\bar{n}$.

Case 2: $m_1 > \bar{n}+1$. Again we get

$$\pi_{\bar{n}+1}(\tilde{B}_1) = \pi_{\bar{n}+1}(R_1). \tag{A.94}$$

Returning to (A.83), we claim that

$$\pi_{\bar{n}+1}(p^{\bar{n}} z_0) \notin \pi_{\bar{n}+1}(R_1).$$

Indeed, otherwise $p^{\bar{n}} z_0 = x_1 + p^{\bar{n}+1} z_1 = p^{\bar{n}} x_1' + p^{\bar{n}+1} z_1'$ for some $x_1, x_1' \in R_1$ and $z_1, z_1' \in \mathcal{O}$, implying that $\pi_1(z_0) = \pi_1(x_1') \in \pi_1(R)$ (a contradiction). Hence $\pi_{\bar{n}+1}(R) \not\subseteq \pi_{\bar{n}+1}(R_1)$ and thus

$$\pi_{\bar{n}+1}(A) \not\subseteq \pi_{\bar{n}+1}(R_1).$$

This gives an element $a \in A$ such that

$$a = y + p^{m_3} z_1 \tag{A.95}$$

with $y \in R_1$, $m_3 \le \bar{n}$ and $z_1 \in \mathcal{O} \setminus (R_1 + p\mathcal{O})$. By (A.94),

$$y = \tilde{b}_1 + p^{\bar{n}+1} z' \quad \text{with } \tilde{b}_1 \in \tilde{B}_1,\ z' \in \mathcal{O}$$

and substituting in (A.95) gives

$$a = \tilde{b}_1 + p^{m_3} z_2 \quad \text{with } z_2 \in \mathcal{O} \setminus (R_1 + p\mathcal{O}). \tag{A.96}$$

Multiplying (A.96) with an appropriate bounded power ξ^r of ξ introduced in (A.90) we obtain

$$a\xi^r = \tilde{b} + p^{m_3} z_3 \tag{A.97}$$

for some $\tilde{b}$ in a sumset of $B^{(r)}$ and $z_3 \in \mathcal{O} \setminus (R_1 + p\mathcal{O})$. Next multiply (A.97) with p^{rk} to get

$$p^{m_3+rk} z_3 \in A(\tilde{A})^r - s(\tilde{A})^r \subset \tilde{\tilde{A}}.$$

Hence again

$$\pi_1\left(\frac{\tilde{A} \cap p^{m_4}\mathcal{O}}{p^{m_4}}\right) \supsetneq \pi_1(R)$$

for some $k \le m_4 < m_3 + ck < c\bar{n}$. In conclusion, we see that there is some $m_5 < c\bar{n}$ such that

$$\pi_1\left(\frac{\tilde{A} \cap p^{m_5}\mathcal{O}}{p^{m_5}}\right) \supsetneq \pi_1(R).$$

In particular, there is an element $\zeta \in 1 + p\mathcal{O}$ such that $p^{m_5}\zeta \in \tilde{A}$. Hence $A\tilde{A} \cap p^{m_5}\mathcal{O} \supset p^{m_5}\zeta A$ and

$$A' = \frac{\tilde{A}A \cap p^{m_5}\mathcal{O}}{p^{m_5}} \supset \zeta A.$$

Property (A.79) therefore remains valid for the set A' generating a ring R' with

$$\pi_1(R') \supsetneq \pi_1(R).$$

Since $|\pi_1(R)| \leq |\mathcal{O}/p\mathcal{O}| < p^d$, the procedure has to terminate after at most d steps, meaning that we obtain $\bar{n} \geq n_1$ for which in particular (A.82) holds. Therefore there is $m < cn_1$ such that

$$\pi_{n_1}\left(\frac{\tilde{A} \cap p^m\mathcal{O}}{p^m}\right) \supset \pi_{n_1}(p^k\mathbb{Z}) \quad \text{with } k = [n_1/10]. \tag{A.98}$$

Note that in (A.98) the set A is a multiplicative translate of the original set so that (A.98) corresponds to condition (3.31) in Section 3.

This proves Proposition 3.3 up to verification of the assertion (A.82).

A.6. Subfield reduction

Our aim is to establish (A.82) for rings satisfying condition (A.101) below and subsets $A \subset R$ satisfying (A.79) and (A.80), i.e.

$$\pi_p(A) = \pi_p(R), \tag{A.99}$$

$$|\pi_m(A)| > p^{\delta m} \quad \text{for all } m \leq N, \tag{A.100}$$

where our assumption on R is the following property:

$$\begin{aligned} &\text{If } n < N \text{ and } x \in \mathcal{O},\ p^n x \in R, \text{ then there is} \\ &y \in R \text{ such that } \pi_{p^{N-n}}(x - y) = 0 \end{aligned} \tag{A.101}$$

(N plays the role of $\bar{n}$ in Section A.5).

Returning to the discussion at the beginning of Section A.1, recall that

$$\mathcal{O} = \mathcal{O}_{\mathcal{P}} = \mathbb{Z}_p[u_i\mathcal{P}^j \mid 1 \leq i \leq d,\ 0 \leq j < e],$$
$$\mathcal{O}^I = \mathcal{O}_{\mathcal{P}} \cap K^I = \mathbb{Z}_p[u_i \mid 1 \leq i \leq d],$$
$$\mathcal{O}/p\mathcal{O} \simeq \mathbb{F}_{p^d} + \mathbb{F}_{p^d}\mathcal{P} + \cdots + \mathbb{F}_{p^d}\mathcal{P}^{e-1}.$$

We assume in what follows that

$$N > C(p, d), \tag{A.102}$$

where $C(p, d)$ is a suitable constant depending on p and d, as will be clear from the considerations below.

For $x \in R$ write

$$\pi_p(x) = x_0 + x_1\mathcal{P} + \cdots + x_{e-1}\mathcal{P}^{e-1} \quad \text{with } x_0, \ldots, x_{e-1} \in \mathbb{F}_{p^d}. \tag{A.103}$$

Hence $\pi_p(x^{p^d}) = x_0 \in \pi_p(R)$ and it follows that $\pi_p(R)$ contains the subfield F_0 of $\mathbb{F}_{p^d}$ generated by $\{x_0 \mid x \in R\}$. Thus

$$\pi_{\mathcal{P}}(R) = F_0 \subset \pi_p(R). \tag{A.104}$$

Next, consider the set

$$S_1 = \{t \in \mathbb{F}_{p^d} \mid t\mathcal{P} \in \pi_{\mathcal{P}^2}(R)\}.$$

It follows from (A.104) that $x_1 \in S_1$ for all $x \in R$ in the representation (A.103). Assume

$$S_1 \neq \{0\}.$$

Let $t_1 \in S_1 \setminus \{0\}$ and consider the set $S_1' = t_1^{-1} S_1 \subset \mathbb{F}_{p^d}$ (which contains 1). Let F_1 be the subfield of $\mathbb{F}_{p^d}$ generated by S_1'. Since $1 \in S_1'$, F_1 will be obtained as a sumset of the product set $(S_1')^{(r)}$ of S_1' for any sufficiently large $r \in \mathbb{Z}_+$.

Note that if $s_1, \dots, s_r \in S_1'$, then

$$s_i t_1 \mathcal{P} \in \pi_{\mathcal{P}^2}(R) \quad (1 \le i \le r)$$

and hence

$$s_1 \dots s_r t_1^r \mathcal{P}^r \in \pi_{\mathcal{P}^{r+1}}(R).$$

Therefore

$$t t_1^r \mathcal{P}^r \in \pi_{\mathcal{P}^{r+1}}(R) \qquad \text{for } t \in F_1.$$

Taking r of the form $r \equiv 1 \pmod{e(p^d - 1)}$ we get some integer $r_1 \in \mathbb{Z}_+$ such that

$$t t_1^r \mathcal{P} p^{r_1} \in \pi_{\mathcal{P}^{e r_1 + 2}}(R).$$

Therefore, if $t \in F_1$, there is $z \in \mathcal{O}$ such that

$$p^{r_1}(t t_1^r \mathcal{P} + z\mathcal{P}^2) \in R.$$

Since $r_1 < C(p,d)$ it follows from (A.101) and (A.102) that

$$\pi_p(t t_1^r \mathcal{P} + z\mathcal{P}^2) = \pi_p(t t_1 \mathcal{P} + z\mathcal{P}^2) \in \pi_p(R).$$

Hence $F_1 t_1 \mathcal{P} \subset \pi_{\mathcal{P}^2}(R)$ and from the definition of S_1 and F_1 we therefore obtain

$$\pi_{\mathcal{P}^2}(R) = F_0 + F_1 t_1 \mathcal{P}.$$

If $S_1 = \{0\}$, put $t_1 = 0$ and $F_1 = \mathbb{F}_p$. Continuing the process, we obtain elements $t_1, \dots, t_{e-1} \in \mathbb{F}_{p^d}$ and subfields $F_0, F_1, \dots, F_{e-1}$ of $\mathbb{F}_{p^d}$ such that

$$\pi_p(R) = F_0 + F_1 t_1 \mathcal{P} + \dots + F_{e-1} t_{e-1} \mathcal{P}^{e-1}. \tag{A.105}$$

Let F_i be the largest subfield among $F_0, \dots, F_{e-1}$; $t_i \neq 0$. Since $t_i F_i \mathcal{P}^i \subset \pi_p(R)$, we have

$$t_i^e F_i p^i \subset \pi_{\mathcal{P}^{(e-1)i+e}}(R),$$

and again from (A.101) and (A.102), (A.6) implies

$$t_i^e F_i \subset \pi_{\mathcal{P}}(R) = F_0.$$

Hence $F_i = F_0$, $t_i^e \in F_0$. Also, if $t_j \neq 0$ it follows from (A.105) that $F_0 F_j t_j \mathcal{P}^j \subset \pi_p(R)$, implying $F_j = F_0$. Hence we may specify (A.105) as

$$\pi_p(R) = F_0 + F_0 t_1 \mathcal{P} + \cdots + F_0 t_{e-1} \mathcal{P}^{e-1}, \tag{A.106}$$

where $t_j = 0$ or $t_j^e \in F_0$.

Set

$$I = \{0 \leq i < e \mid t_i \neq 0\} \subset \mathbb{Z}/e\mathbb{Z}.$$

If $i, j \in I$, then clearly

$$t_i t_j \mathcal{P}^{i+j} \in \pi_{\mathcal{P}^{e+\min(i,j)}}(R). \tag{A.107}$$

Define $0 \leq k < e$ by $i + j \equiv k \pmod{e}$. If $i + j = k$, (A.107) implies $t_i t_j \mathcal{P}^k \in \pi_p(R)$ and hence $t_i t_j \in t_k F_0$. If $i + j = e + k$, then $k < \min(i, j)$ and (A.107), (A.101) imply $t_i t_j \mathcal{P}^k \in \pi_{pmc^{k+1}}(R)$. In either case

$$t_i t_j \in t_k F_0.$$

In particular, $t_k \neq 0$ and it follows that I is an additive subgroup of $\mathbb{Z}/e\mathbb{Z}$. Therefore (A.106) may be rewritten as

$$\pi_p(R) = F_0 + \tau\beta F_0 + \cdots + \tau^{e_1-1}\beta^{e_1-1} F_0 \tag{A.108}$$

for some $e_1 \mid e$, $\beta = \mathcal{P}^{e/e_1}$ and some $\tau \in \mathbb{F}_{p^d}$ with $\tau^{e_1} \in F_0$. Let $\mathbb{Q}_p \subset K' \subset K^I$ be the subfield of K^I of degree $[K' : \mathbb{Q}_p] = [F_0 : \mathbb{F}_p]$ and let $K_1 = K'(\tau\beta) \subset K_{\mathcal{P}}$, hence $[K_1 : K'] = e_1$. Define

$$\mathcal{O}_1 = K_1 \cap \mathcal{O}, \quad \mathcal{O}' = K' \cap \mathcal{O}.$$

Hence by (A.108),

$$\pi_p(R) = \pi_p(\mathcal{O}_1). \tag{A.109}$$

Remark. A subring $\mathcal{R}$ of $\pi_p(\mathcal{O})$ is nor necessarily of the form $\pi_p(\mathcal{O}_1)$ for the integers in a subfield. Taking $K = \mathbb{Q}(p^{1/4})$ and $\mathcal{R} = \mathbb{F}_p + p^{1/2}\mathbb{F}_p + p^{3/4}\mathbb{F}_p \subset \pi_p(\mathcal{O})$ gives an example. Thus to conclude (A.109) we used (A.101) where N is sufficiently large.

Returning to the analysis of R, define

$$M = \max\{m \in \mathbb{Z}_+ \mid \pi_{p^m}(R) \subset \pi_{p^m}(\mathcal{O}_1)\}.$$

We claim that

$$M \geq N - 1. \tag{A.110}$$

Note that if $\Gamma \subset R$ is a set of representatives of $\pi_p(R)$ then all elements in the set $\Gamma + p\Gamma + \cdots + p^{m-1}\Gamma \subset R$ are distinct mod p^m. Therefore

$$|\pi_{p^m}(R)| \geq |\pi_p(R)|^m.$$

Conversely, from assumption (A.101) we get

$$|\pi_{p^m}(R)| = |\pi_p(R)|^m \quad \text{for } m \leq N. \tag{A.111}$$

Since $|\pi_{p^m}(\mathcal{O}_1)| = |\pi_p(\mathcal{O}_1)|^m = |\pi_p(R)|^m$, it follows from (A.6) and (A.111) that

$$\pi_{p^M}(R) = \pi_{p^M}(\mathcal{O}_1). \tag{A.112}$$

Assume (A.110) fails, thus

$$N \geq M + 2. \tag{A.113}$$

If (A.113) holds, (A.111) implies

$$|\pi_{p^{M+1}}(R)| = |\pi_p(R)|^{M+1} = |\pi_{p^{n+1}}(\mathcal{O}_1)|,$$

and since we assume $\pi_{p^{M+1}}(R) \nsubseteq \pi_{p^{M+1}}(\mathcal{O}_1)$, also

$$\pi_{p^{M+1}}(\mathcal{O}_1) \nsubseteq \pi_{p^{n+1}}(R). \tag{A.114}$$

Next, let $y \in \mathcal{O}_1$ be such that

$$\pi_p(y) \in \pi_p(\mathcal{O}')^* = F_0^*. \tag{A.115}$$

Hence $\pi_p(y^r) = 1$, $r = |F_0| - 1$ and so

$$y^r = 1 + pz' \quad \text{for some } z' \in \mathcal{O}_1. \tag{A.116}$$

Since $1 \in R$ and $\pi_{p^M}(z') \in \pi_{p^M}(R)$, it follows that

$$\pi_{p^{M+1}}(y^r) \in \pi_{p^{M+1}}(R). \tag{A.117}$$

Also, from (A.112), $\pi_{p^M}(y) \in \pi_{p^M}(R)$, hence there is some $z \in \mathcal{O}$ such that

$$y + p^M z = x \in R. \tag{A.118}$$

Taking the r-th power of (A.118) we get clearly

$$\pi_{p^{2M}}(y^r + ry^{r-1}zp^M) \in \pi_{p^{2M}}(R),$$

and recalling (A.117),

$$\pi_{p^{M+1}}(ry^{r-1}zp^M) \in \pi_{p^{M+1}}(R). \tag{A.119}$$

From (A.101) and assumption (A.113), (A.119) implies

$$\pi_p(ry^{r-1}z) \in \pi_p(R).$$

Since $\pi_p(y) \in \pi_p(R)$, also

$$\pi_p(rz) \overset{\text{(A.116)}}{=} \pi_p(ry^r z) \in \pi_p(R).$$

Finally, since $(r, p) = 1$, we conclude that

$$\pi_p(z) \in \pi_p(R).$$

Recalling (A.118), we have proved that

$$\pi_{p^{M+1}}(y) \in \pi_{p^{M+1}}(R) \quad \text{if } y \in \mathcal{O}_1 \text{ satisfies (A.115).} \tag{A.120}$$

Given $y \in \mathcal{O}_1$, we may write

$$y = y_0 + \beta y_1 \quad \text{with } y_0 \in \mathcal{O}', \pi_p(y_0) \neq 0 \text{ if } y_0 \neq 0, \text{ and } y_1 \in \mathcal{O}_1. \tag{A.121}$$

In particular, y_0 satisfies (A.115) if $y_0 \neq 0$, and $\pi_{p^{M+1}}(y_0) \in \pi_{p^{M+1}}(R)$ by (A.120). Since $\pi_{p^M}(y_1) \in \pi_{p^M}(R)$, there is an element $x_1 \in R$ such that $\pi_{p^M}(x_1 - y_1) = 0$ and hence

$$\pi_{p^M\beta}(y - \beta x_1) \in \pi_{p^M\beta}(R). \tag{A.122}$$

Since $\pi_{p^M}(\beta) \in \pi_{p^M}(R)$ there is $z \in \mathcal{O}$ such that

$$\beta + p^M z \in R, \tag{A.123}$$

and therefore, taking the e_1-th power, $\pi_{p^{2M}}(p + e_1\beta^{e_1-1}p^M z) \in \pi_{p^{2M}}(R)$ or

$$\pi_{p^{2M}}(\beta^{e_1-1}p^M z) \in \pi_{p^{2M}}(R). \tag{A.124}$$

From (A.101) and since $N > M$, (A.124) implies

$$\pi_p(\beta^{e_1-1}z) \in \pi_p(R) = \pi_p(\mathcal{O}_1).$$

Therefore there is $w \in \mathcal{O}$ such that $\beta^{e_1-1}z + pw \in \mathcal{O}_1$, implying that also $z + \beta w \in K_1 \cap \mathcal{O} = \mathcal{O}_1$ and $\pi_\beta(z) \in \pi_\beta(R)$. Substitution in (A.123) shows that

$$\beta + p^M \beta z' \in R \quad \text{for some } z' \in \mathcal{O}. \tag{A.125}$$

Taking the e_1-th power of (A.125) it follows that $p(1 + p^M z')^{e_1} \in R$ and

$$\pi_{p^{2M}}(e_1 p^{M+1} z') \in \pi_{p^{2M}}(R). \tag{A.126}$$

Since (A.101) also holds for $n = M + 1$, (A.126) implies

$$\pi_p(z') \in \pi_p(R).$$

Let $x' \in R$ and $z'' \in \mathcal{O}$ be such that

$$z' = x' + pz''$$

and substitute in (A.125) to get

$$\beta(1 + p^M x' + p^{M+1}z'') \in R. \tag{A.127}$$

Finally, multiplying both sides of (A.127) by $1 - p^M x' \in R$ gives $\beta(1 + p^{M+1}z''') \in R$ for some $z''' \in \mathcal{O}$ and

$$\pi_{p^{M+1}}(\beta) \in \pi_{p^{M+1}}(R). \tag{A.128}$$

From (A.122) and (A.128) we obtain

$$\pi_{p^M\beta}(y) \in \pi_{p^M\beta}(R),$$

proving that

$$\pi_{p^M\beta}(\mathcal{O}_1) \subset \pi_{p^M\beta}(R). \tag{A.129}$$

Returning to (A.121), it follows from (A.129) that there is an element $x_2 \in R$ such that $\pi_{p^M\beta}(y_1 - x_2) = 0$ and hence, assuming $e_1 \geq 2$, $\pi_{p^M\beta^2}(y - \beta x_2) \in \pi_{p^M\beta^2}(R)$. By (A.128), it follows that $\pi_{p^M\beta^2}(y) \in \pi_{p^M\beta^2}(R)$ and therefore $\pi_{p^M\beta^2}(\mathcal{O}_1) \subset \pi_{p^M\beta^2}(R)$. Iteration gives $\pi_{p^{M+1}}(\mathcal{O}_1) \subset \pi_{p^{M+1}}(R)$, contradicting (A.114).

Therefore we have proved that

$$M \geq N - 1$$

and thus

$$\pi_{p^{N-1}}(R) = \pi_{p^{N-1}}(\mathcal{O}_1). \tag{A.130}$$

We now return to the set $A \subset R$ satisfying (A.99) and (A.100). Since $\pi_p(A) = \pi_p(R)$, by (A.101) we have

$$\pi_{p^N}(R) = \pi_{p^N}(A + pA + \cdots + p^{N-1}A).$$

In case $N < C(p, d)$ this gives

$$\pi_{p^N}(R) = \pi_{p^N}(\tilde{A})$$

and hence certainly (A.82).

If $N > C(p, d)$, (A.130) holds, reducing the problem to the integers $\mathcal{O}_1$ in a number field K_1. From Corollary A.1 in Section A.1 (see also the remarks at the end of Section A.1) it follows that

$$\pi_{p^{N-1}}(\tilde{A}) \supset \pi_{p^{N-1}}(p^k\mathcal{O}_1) \tag{A.131}$$

with $k = [N/10]$ say and $\tilde{A}$ a suitable sum-product set of A. Thus given $y \in p^k\mathcal{O}_1$ there exist $\tilde{a} \in \tilde{A}$ and $z \in \mathcal{O}$ such that

$$y = \tilde{a} + p^{N-1}z.$$

We have

$$\pi_{p^N}(p^{N-1}z) \in \pi_{p^N}(R) + \pi_{p^N}(p^k\mathcal{O}_1) \overset{\text{(A.130)}}{=} \pi_{p^N}(R),$$

hence by (A.101),

$$\pi_p(z) \in \pi_p(R) = \pi_p(A).$$

Thus there is $a \in A$ such that $\pi_{p^N}(p^{N-1}z - p^{N-1}a) = 0$, while by (A.131) there is some $a_1 \in \tilde{A}$ such that $\pi_{p^N}(p^{N-1} - a_1) = 0$. Thus

$$\pi_{p^N}(y) \in \pi_{p^N}(\tilde{A} - a_1 a) \in \pi_{p^N}(\tilde{A}).$$

Therefore $\pi_{p^N}(p^kR) = \pi_{p^N}(p^k\mathcal{O}_1) \subset \pi_{p^N}(\tilde{A})$, which is (A.82).

Acknowledgments. It is a pleasure to thank Bob Guralnick for very helpful discussions.

The first author was supported in part by the NSF grant DMS-0808042. The second author was supported in part by DARPA, NSF, and the Sloan Foundation.

References

[1] Berenstein, C., Yger, A.: Effective Bezout identities in $\mathbb{Q}[z_1, \ldots, z_n]$. Acta Math. **166**, 69–120 (1991) Zbl 0724.32002 MR 1088983

[2] Bougerol, P., Lacroix, J.: Products of Random Matrices with Applications to Schrödinger Operators. Progr. Probab. Statist. 8, Birkhäuser (1985) Zbl 0572.60001 MR 0886674

[3] Bourgain, J.: The sum-product theorem $\mathbb{Z}_q$ with q arbitrary. J. Anal. Math. **106**, 1–93 (2008) Zbl pre05508687 MR 2448982

[4] Bourgain, J., Chang, M.-C.: Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_q^*$, where q is composite with few prime factors. Geom. Funct. Anal. **16**, 327–366 (2006) Zbl pre05045669 MR 2231466

[5] Bourgain, J., Gamburd, A.: Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. Ann. of Math. **167**, 625–642 (2008) MR 2415383

[6] Bourgain, J., Gamburd, A.: Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$: I. J. Eur. Math. Soc. **10**, 987–1011 (2008) Zbl pre05365142 MR 2443926

[7] Bourgain, J., Gamburd, A., Sarnak, P.: Sieving and expanders. C. R. Math. Acad. Sci. Paris **343**, 155–159 (2005) Zbl pre05058405 MR 2246331

[8] Bourgain, J., Gamburd, A., Sarnak, P.: Affine linear sieve, expanders, and sum-product. Preprint.

[9] Bourgain, J., Glibichuk, A., Konyagin, S.: Estimates for the number of sums and products and for exponential sums in fields of prime order. J. London Math. Soc. **73**, 380–398 (2006) Zbl 1093.11057 MR 2225493

[10] Bourgain, J., Katz, N., Tao, T.: A sum-product estimate in finite fields and applications. Geom. Funct. Anal. **14**, 27–57 (2004) Zbl 1145.11306 MR 2053599

[11] Dawson, C. M., Nielsen, M. A.: The Solovay–Kitaev algorithm. Quantum Information Comput. **6**, 81–95 (2006) Zbl 1152.81706 MR 2212257

[12] Dinai, O.: Poly-log diameter bounds for some families of finite groups. Proc. Amer. Math. Soc. **134**, 3137–3142 (2006) Zbl 1121.05058 MR 2231895

[13] Gamburd, A., Shahshahani, M.: Uniform diameter bounds for some families of Cayley graphs. Int. Math. Res. Notices **2004**, no. 71, 3813–3824 Zbl 1066.05072 MR 2104475

[14] Guivarc'h, Y.: Produits de matrices aléatoires et applications aux propriétés géométriques des sous-groupes du groupe linéaire. Ergodic Theory Dynam. Systems **10**, 483–512 (1990) MR 1074315

[15] Helfgott, H.: Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Ann. of Math. **167**, 601–623 (2008) MR 2415382

[16] Helfgott, H.: Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$. Preprint

[17] Kesten, H.: Symmetric random walks on groups. Trans. Amer. Math. Soc. **92**, 336–354 (1959) Zbl 0092.33503 MR 0109367

[18] Long, D. D., Lubotzky, A., Reid, A. W.: Heegaard genus and property τ for hyperbolic 3-manifolds. J. Topology **1**, 152–158 (2008) Zbl 1158.57018 MR 2365655

[19] Lubotzky, A.: Cayley graphs: eigenvalues, expanders and random walks. In: Surveys in Combinatorics, P. Rowlinson (ed.), London Math. Soc. Lecture Note Ser. 218, Cambridge Univ. Press, 155–189 (1995) Zbl 0835.05033 MR 1358635

[20] Lubotzky, A., Weiss, B.: Groups and expanders. In: DIMACS Ser. Discrete Math. Theor. Comput. Sci. 10, J. Friedman (ed.), 95–109 (1993) Zbl 0787.05049 MR 1235570

[21] Matthews, C., Vaserstein, L., Weisfeiler, B.: Congruence properties of Zariski-dense subgroups. Proc. London Math. Soc. **48**, 514–532 (1984) Zbl 0551.20029 MR 0735226

[22] Nori, M. V.: On subgroups of $\mathrm{GL}_n(F_p)$. Invent. Math. **88**, 257–275 (1987) Zbl 0632.20030 MR 0880952

[23] Ragunathan, M. S.: Discrete Subgroups of Lie Groups. Ergeb. Math. Grenzgeb. 68, Springer (1972)

[24] Sarnak, P.: What is an expander? Notices Amer. Math. Soc. **51**, 762–763 (2004) Zbl 1161.05341 MR 2072849

[25] Sarnak, P., Xue, X.: Bounds for multiplicities of automorphic representations. Duke Math. J. **64**, 207–227 (1991) Zbl 0741.22010 MR 1131400

[26] Tao, T., Product set estimates for non-commutative groups. Combinatorica **28**, 547–594 (2008) Zbl pre05494691 MR 2501249

[27] Tao, T., Vu, V.: Additive Combinatorics. Cambridge Univ. Press (2006) Zbl 1127.11002 MR 2289012