RIGID ABELIAN GROUPS AND THE PROBABILISTIC METHOD

GÁBOR BRAUN AND SEBASTIAN POKUTTA

Dedicated to Rüdiger Göbel on the occasion of his 70th birthday.

Abstract. The construction of torsion-free abelian groups with prescribed endomorphism rings starting with Corner's seminal work (see Corner [1963]) is a well-studied subject in the theory of abelian groups. Usually these construction work by adding elements from a (topological) completion in order to get rid of (kill) unwanted homomorphisms. The critical part is to actually prove that every unwanted homomorphism can be killed by adding a suitable element. We will demonstrate that some of those constructions can be significantly simplified by choosing the elements at random. As a result, the endomorphism ring will be almost surely prescribed, i.e., with probability one.

1. Introduction

The probabilistic method, pioneered by Erdős (see Erdős [1959, 1961]) is one of the most powerful tools in combinatorics, theoretical computer science, and other branches of mathematics to show the existence of mathematical objects with prescribed properties. It is a non-constructive method which infers the existence of a mathematical object by showing that *the probability of its existence* is non-zero. Since its early days it has lead to a wide range of striking and unexpected results (cf., e.g., Erdős and Rényi [1959], Shelah and Spencer [1988, 1994]); for an extensive overview as well as a very nice introduction the interested reader is referred to Alon and Spencer [2000]. We will use the probabilistic method in order to show the existence of abelian groups with prescribed endomorphism rings. By doing so, we obtain the probabilistic counterparts of well-known constructions. While the statements of the probabilistic counterparts are more general in some sense, as they assert that almost any choice of, say, elements from the completion suffice, the proofs simplify. Another application of the probabilistic method in abelian group theory, constructing groups with prescribed Ulm sequences, was presented in Droste and Göbel [2010].

The structure of the paper is as follows. We start with a brief introduction to the probabilistic method and recall a few concepts from probability theory in Section 2. We will then apply the method to construct infinite abelian groups with prescribed endomorphism rings. For each construction, we will first recall the deterministic construction and provide a sketch of its proof, then we provide the necessary probabilistic tools and specify the distributions from which the elements or substructures are drawn, and finally we present the proof of the probabilistic variant of the construction. In the first part, in Section 3, we consider the classical Corner construction (see Corner [1963] or Corner [196X]). We first show that a uniform, random choice of countably many p-adic integers forms an algebraically independent set with probability one (Lemma 3.2) and later we generalize this construction to $2^{\aleph_0}$ elements (Lemma 3.3). We then provide a probabilistic version of Corner's construction (Theorem 3.5). In this case the actual distribution chosen for the random elements does matter and we provide an example where using a nearly uniform distribution results in a free group (Theorem 3.7). We then proceed with the Zassenhaus construction (see Zassenhaus [1967]) in Section 4 showing that every ring with a finite-rank free

Date: July 13, 2011/Draft/Revision: –revision–.

2010 *Mathematics Subject Classification.* Primary: 20K20, 20K15, 20K30, 05D40; Secondary: 60B15.

Key words and phrases. random construction, abelian groups with prescribed endomorphisms, probabilistic method.

additive group can be realized as the endomorphism ring of a torsion-free abelian group. While the proof of the deterministic version (Theorem 4.1) is rather non-trivial and slightly technical, the proof of the probabilistic version follows more naturally (Theorem 4.4) relying on an old result by Frobenius and Chebotarëv (Lemma 4.2).

In the following, let $\widehat{B}$ denote the p-adic completion of B. Let $J_p \coloneqq \widehat{\mathbb{Z}}$ denote the ring of p-adic integers. The p-adic completion is mainly of interest when B is naturally a submodule of $\widehat{B}$, which happens exactly when B is *p-reduced*, i.e., satisfying $\bigcap_{n=0}^{\infty} p^n B = 0$. Further let X_{p*} denote the *p-purification* of a submodule X of a p-torsion-free module for some prime p, i.e., X_{p*} consists of all x/p^k from the ambient module with $x \in X$ and $k \in \mathbb{N}$. We omit the ambient module from the notation as it will be clear from the context. All other notation is standard as to be found in Eklof and Mekler [2002], Jech [1978], Göbel and Trlifaj [2006], and Fuchs [1970, 1973]. Recall that an event happens *almost surely* if the probability of the event is 1. For convenience we define $[n] \coloneqq \{1, \dots, n\}$ for $n \in \mathbb{N}$.

2. The probabilistic method: a brief introduction

We will now present a brief introduction to the probabilistic method and recall the necessary notions and concepts from probability theory. For a more complete introduction we refer the interested reader to Alon and Spencer [2000]. As mentioned above, the probabilistic method establishes the existence of structures with desired properties by picking the structure randomly and showing that it has the desired properties with a positive probability. Before we continue with an example to illustrate the method, we recall a few notions and concepts from probability theory.

Recall that probability theory works with a collection of events, which form a so-called σ-algebra: it consists of some subsets of a big set closed under countable union and complements, and therefore also countable intersections. There is a *probability measure* $\mathbb{P}[.]$ assigning to each event a number in $[0,1]$, the *probability* of the event. The probability measure has to satisfy various properties, from which we mention only $\mathbb{P}\left[\bigcup_{i<\omega} A_i\right] \leq \sum_{i<\omega} \mathbb{P}[A_i]$ for any countable family of events $A_1, A_2, \dots$. A collection $\{A_i : i \in J\}$ of events is *independent*, if $\mathbb{P}\left[\bigcap_{i\in I} A_i\right] = \prod_{i\in I} \mathbb{P}[A_i]$ for any finite $I \subseteq J$. The following well-known lemma will be crucial:

Lemma 2.1 (Borel-Cantelli Lemma)**.** *Let $A_1, A_2, \dots \subseteq \mathcal{F}$ be a sequence of events. Further let $\limsup_{i\to\infty} A_i$ denote the set of outcomes that occur infinitely often. The following hold:*

(1) If $\sum_{i<\omega} \mathbb{P}[A_i] < \infty$ then $\mathbb{P}[\limsup_{i\to\infty} A_i] = 0$.
(2) If $A_1, A_2, \dots$ are independent and $\sum_{i<\omega} \mathbb{P}[A_i] = \infty$, then $\mathbb{P}[\limsup_{i\to\infty} A_i] = 1$. In other words, infinitely many events occur with probability 1.

A *distribution* of a random variable is the minimal σ-algebra of events meaningful for the variable together with the probability measure on it. For a discrete random variable X, i.e., one taking only countably many values, its *expected value* is $\mathbb{E}[X] = \sum_i X_i \mathbb{P}[X = X_i]$, where the $X_i \in \mathbb{R}$ form the range of X. Occasionally, we will use expected values of more general variables, but for intuition, it is mostly sufficient to think of the expected value in its discrete form. We will later use Fubini's theorem which allows for iterated computation of expected values:

Lemma 2.2 (Fubini's Theorem)**.** *Let f be a non-negative function which is measurable (in the respective space) and let X, Y be independent random variables and*

$$\mathbb{E}_{X,Y}[f(X,Y)] < \omega.$$

Then

$$\mathbb{E}_{X,Y}[f(X,Y)] = \mathbb{E}_X\left[\mathbb{E}_Y[f(X,Y)]\right].$$

Here expected values are taken in the total distribution of the variables in the subscript, and the expected value is a function of the other random variables.

We will now illustrate the probabilistic method by computing the order of $\mathrm{GL}(n,q)$, the group of invertible $n \times n$ matrices over the field with q elements. This is merely a reformulation of a counting argument in the framework of probability theory, just as many early examples.

Proposition 2.3. *Let $n \in \mathbb{N}$ be a natural number and $\mathbb{F}_q$ be the finite field with q elements. Then the number of $n \times n$ invertible matrices over $\mathbb{F}_q$ is*

$$|\mathrm{GL}(n,q)| = \prod_{k\in[n]} (q^n - q^{k-1}).$$

Proof. Let A be a random matrix over $\mathbb{F}_q$ chosen with uniform distribution. Clearly, A is invertible if and only if its columns $a_1, \ldots, a_n$ are linearly independent. Observe that the probability of A being invertible can be rephrased by breaking it up into probabilities of linear independence of smaller subsets:

$$\begin{aligned}\mathbb{P}\left[A \text{ invertible}\right] &= \prod_{k\in[n]} \mathbb{P}\left[a_1, \ldots, a_k \text{ independent} | a_1, \ldots, a_{k-1} \text{ independent}\right] \\ &= \prod_{k\in[n]} \left(1 - \mathbb{P}\left[a_k \in \langle a_1, \ldots, a_{k-1}\rangle | a_1, \ldots, a_{k-1} \text{ independent}\right]\right)\end{aligned}$$

Provided that $a_1, \ldots, a_{k-1}$ are linearly independent, they span a $(k-1)$-dimensional subspace, so the probability that a_k is in this subspace is

$$\mathbb{P}\left[a_k \in \langle a_1, \ldots, a_{k-1}\rangle | a_1, \ldots, a_{k-1} \text{ independent}\right] = \frac{q^{k-1}}{q^n},$$

as the columns are independent random variables. We therefore obtain

$$\mathbb{P}\left[A \text{ invertible}\right] = \prod_{k\in[n]} \left(1 - \frac{q^{k-1}}{q^n}\right).$$

On the other hand we have $\mathbb{P}\left[A \text{ invertible}\right] = \frac{\ell}{q^{n^2}}$, where ℓ is the number of invertible matrices and q^{n^2} is the total number of $n \times n$ matrices over $\mathbb{F}_q$. We therefore obtain

$$\ell = q^{n^2} \cdot \prod_{k\in[n]} \left(1 - \frac{q^{k-1}}{q^n}\right) = \prod_{k\in[n]} q^n \left(1 - \frac{q^{k-1}}{q^n}\right) = \prod_{k\in[n]} (q^n - q^{k-1}).$$

□

In the following we operate under the same paradigm. However, it is not the abelian groups *per se* that are drawn from random distributions. We will use the concept in a slightly different fashion: we will pick crucial elements of the constructions, such as elements from the completion, at random. Obviously, we have to specify *how* we actually pick these elements, i.e., we have to provide the distribution. The distributions that we will use are very natural and since we are concerned about existence only, we can basically pick any (well-defined) distribution that suits our needs.

Another fact that is worthwhile to be mentioned is the structure of our results. We do not just provide mere *existence statements*, but we will show that the endomorphism properties hold *almost surely*, i.e., every random choice is satisfactory with probability 1. Actually, this is expected in view of Kolmogorov's zero-one law.

3. Groups via p-adic numbers

Our starting point is the following well-known construction of Corner (see Corner [1963] or Fuchs [1973, Theorem 110.1]). For simplicity, we restrict to p-reduced rings R.

Theorem 3.1. *For every countable p-reduced torsion-free ring R, there is a torsion-free left abelian group of countably infinite rank with endomorphism ring R.*

Sketch of proof. Let $\xi_n \in J_p$ with $n < \omega$ be quadratically independent p-adic integers and further let B be a free R-module of countably infinite rank. We define

$$G \coloneqq \langle B, Rb\xi_b : b \in B \setminus \{0\} \rangle_{p*} \subseteq \widehat{B}.$$

Then $\operatorname{End} G = R$. For details, see Corner [1963], or for a slightly different construction Fuchs [1973, Theorem 110.1], or the proof of Theorem 3.5 below. □

Note that the construction in Theorem 3.1 carries over to uncountable modules up to size $2^{\aleph_0}$. In order to establish the probabilistic version, we will choose continuum many random p-adic integers, which will be almost surely algebraically independent. First we present the easier, countable case: countably many, randomly and independently chosen p-adic integers are almost surely algebraically independent.

Lemma 3.2. *Let $\mathcal{M} = \{\xi_n \mid n < \omega\} \subseteq J_p$ be a set of countably many, randomly and independently chosen p-adic integers such that $\mathbb{P}[\xi_n = \lambda] = 0$ for every $n < \omega$ and $\lambda \in J_p$. Then $\mathcal{M}$ is almost surely algebraically independent.*

Proof. We show that every finite subset $S \subseteq \mathcal{M}$ is almost surely algebraically independent. The proof is by induction on the cardinality n of S. For $n = 0$ the statement holds trivially as $S = \emptyset$. Therefore let $n \geq 1$ and let $S = \{\xi_1, \dots, \xi_n\}$ be a finite subset of $\mathcal{M}$. Note that there are only countably many non-zero polynomials f with integer coefficients in n variables. Thus it suffices to show that $f(\xi_1, \dots, \xi_n) \neq 0$ almost surely for every such f. By assumption ξ_n is independent of $\xi_1, \dots, \xi_{n-1}$. We can therefore apply Lemma 2.2 to compute the probability $\mathbb{P}[f(\xi_1, \dots, \xi_n) \neq 0]$ by iterating expected values:

$$\mathbb{P}[f(\xi_1, \dots, \xi_n) \neq 0] = \mathbb{E}_{\xi_1,\dots,\xi_{n-1}}\left[\mathbb{P}[f(\lambda_1, \dots, \lambda_{n-1}, \xi_n) \neq 0 \mid \xi_i = \lambda_i, i \in [n-1]]\right].$$

By induction, we conclude that $f(\xi_1, \dots, \xi_{n-1}, x_n)$ is almost surely a non-zero polynomial in x_n. Therefore it has only finitely many roots and together with the assumption $\mathbb{P}[\xi_n = \lambda] = 0$ for every $n < \omega$ and $\lambda \in J_p$, we infer that ξ_n is none of these roots almost surely. It follows that

$$\mathbb{E}_{\xi_1,\dots,\xi_{n-1}}\left[\mathbb{P}[f(\lambda_1, \dots, \lambda_{n-1}, \xi_n) \neq 0 \mid \xi_i = \lambda_i, i \in [n-1]]\right] = 1$$

which completes the proof. □

Note that quadratic independence instead of algebraic independence can be easily shown without the use of Fubini's Theorem.

A slightly more involved construction allows us to choose even continuum many random p-adic numbers, which are almost surely algebraically independent. We hasten to emphasize a peculiarity of the statement: it states that almost always none of *uncountably* many events occur. Usually probability theory cannot provide an answer in such cases as it only asserts that the union of *countably* many probability-0 events has again probability 0. However here we can use that J_p is compact, hence we can *approximate* the events via the topology. To ensure this, we construct the numbers as infinite branches of a tree and we show that it suffices to confine ourselves to sufficiently long *finite* initial segments. By doing so we reduce the uncountable case to a countable one. The construction is similar to the one in Corner [196X]. Let $\operatorname{length}(s)$ denote the length of a sequence s.

Lemma 3.3. *Let p be an integer. We construct $2^{\aleph_0}$ random p-adic numbers as follows. We choose randomly and independently non-negative integers $a_s \in \{0, 1, \dots, p^{2^{n+1}-2^n} - 1\}$ with uniform distribution for every finite 0-1 sequence s where $n = \operatorname{length}(s)$. In particular, $a_{\langle\rangle} \in$*

$\{0, 1, \ldots, p-1\}$ for the empty sequence $\langle\rangle$. For every 0-1 infinite sequence f, we define the p-adic number

$$\xi_f \coloneqq \sum_{n=0}^{\infty} p^{2^n-1} a_{f\restriction n},$$

where $f \restriction n$ is the initial segment of f consisting of n elements. Then the ξ_f are almost surely algebraically independent.

Proof. To handle the ξ_f more easily we define

$$b_s \coloneqq \sum_{j=0}^{n} p^{2^j-1} a_{s\restriction j}$$

for every finite 0-1 sequence s where $n \coloneqq \text{length}(s)$. Then we have

$$\xi_f \equiv b_{f\restriction n} \pmod{p^{2^{n+1}-1}}.$$

First note that every b_s is uniformly distributed on the set of integers $\{0, 1, \ldots, p^{2^{n+1}-1}\}$, i.e., on the mod $p^{2^{n+1}-1}$ classes of J_p with $n \coloneqq \text{length}(s)$. This implies, in particular,

$$\mathbb{P}\left[b_s \equiv c \pmod{p^{2^{n+1}-1}} \middle| b_{s\restriction j} \equiv d \pmod{p^{2^{j+1}-1}}\right] = \begin{cases} \frac{1}{p^{2^{n+1}-2^{j+1}}}, & c \equiv d \pmod{p^{2^{j+1}-1}}, \\ 0, & \text{otherwise.} \end{cases}$$

For every positive integers k and n, every non-zero polynomial g with integer coefficients in k variables, and every *pairwise distinct* finite 0-1 sequences $s_1, \ldots, s_k$ of length n, we show that there is almost never an extension f_i of the s_i with $g(\xi_{f_1}, \ldots, \xi_{f_k}) = 0$. This will prove the lemma, as these are altogether countably many events, whose union is therefore the probability-0 event that the ξ_f are dependent.

We use induction on k. The statement for $k = 0$ is obvious. For $k > 0$, we prove the claim by showing that the probability of the event is at most ε for all positive $\varepsilon > 0$. Let μ denote the Haar probability measure of the compact additive group J_p^{k-1}. We say that a subset $A \subseteq J_p^{k-1}$ is *admissible* if the event that g has a solution $\xi_{f_1}, \ldots, \xi_{f_k}$ for some infinite 0-1 sequences f_i extending the s_i with $(\xi_{f_1}, \ldots, \xi_{f_{k-1}}) \in A$ has probability at most $\varepsilon\mu(A)$. We will prove the claim by partitioning J_p^{k-1} into countably many admissible subsets.

For this, write g in the form:

$$g(x_1, \ldots, x_k) = g_m(x_1, \ldots, x_{k-1})x_k^m + \cdots + g_0(x_1, \ldots, x_{k-1}),$$

where $g_m \neq 0$. We choose one of the partitions to be the solution set of g_m, which is admissible (actually has probability 0) by the induction hypothesis on k. The other partitions will be basic open sets, i.e., mod p^N-classes. As there are only countably many mod p^N-classes and every family of such classes contains a pairwise disjoint subfamily with the same union, it is enough to prove that every $(\eta_1, \ldots, \eta_{k-1}) \in J_p^{k-1}$ with $g_m(\eta_1, \ldots, \eta_{k-1}) \neq 0$ is contained in an admissible mod p^N-class for some N. Actually, we show that the mod p^N-class A of $(\eta_1, \ldots, \eta_{k-1}) \in J_p^{k-1}$ is admissible for N large enough, because even the event that there are extensions f_i of the s_i with $\xi_{f_i} \equiv \eta_i \pmod{p^N}$ and $\xi_{f_1}, \ldots, \xi_{f_k}$ is a solution of g mod p^N, i.e., $g(\eta_1, \ldots, \eta_{k-1}, \xi_{f_k}) \equiv 0 \pmod{p^N}$ has probability at most $\varepsilon\mu(A)$.

Let $f \succ s$ denote that the sequence f is an extension of s. We consider the probability modulo the values of the b_{s_i}, as this makes the conditions on the ξ_{f_i} independent:

$$\begin{aligned}(3.1)\quad \mathbb{P}\Big[\exists f_i \succ s_i : \xi_{f_i} \equiv \eta_i \pmod{p^N}, g(\eta_1,\dots,\eta_{k-1},\xi_{f_k}) \equiv 0 \pmod{p^N}\Big| b_{s_1},\dots,b_{s_k}\Big] \\ = \prod_{i\in[k-1]} \mathbb{P}\Big[\exists f_i \succ s_i : \xi_{f_i} \equiv \eta_i \pmod{p^N}\Big| b_{s_1},\dots,b_{s_k}\Big] \\ \cdot \mathbb{P}\Big[\exists f_k \succ s_k : g(\eta_1,\dots,\eta_{k-1},\xi_{f_k}) \equiv 0 \pmod{p^N}\Big| b_{s_1},\dots,b_{s_k}\Big].\end{aligned}$$

Let us fix a positive integer $r := \lceil \log_2(N+1) - 1\rceil = O(\log N)$ so that $\xi_f \equiv b_{f\restriction r} \pmod{p^N}$ for every infinite 0-1 sequence f. For every $i \in [k]$, there are 2^{r-n} extensions of s_i into a 0-1 sequence of length r where n is the length of the s_i. Therefore the probability that there exists an extension which is equivalent to η_i mod p^N is at most

$$(3.2)\qquad \mathbb{P}\Big[\exists f_i \succ s_i : \xi_{f_i} \equiv \eta_i \pmod{p^N}\Big| b_{s_1},\dots,b_{s_k}\Big] \le \frac{2^{r-n}}{p^{N-2^{n+1}}}.$$

For $i = k$, by a similar argument,

$$(3.3)\qquad \mathbb{P}\Big[\exists f_k \succ s_k : g(\eta_1,\dots,\eta_{k-1},\xi_{f_k}) \equiv 0 \pmod{p^N}\Big| b_{s_1},\dots,b_{s_k}\Big] \le \frac{2^{r-n}R(N)}{p^{N-2^{n+1}}},$$

where $R(N)$ is the number of roots of $g(\eta_1,\dots,\eta_{k-1},x)$ in x mod p^N.

To estimate $R(N)$, let us consider the factorization over J_p

$$(3.4)\qquad g(\eta_1,\dots,\eta_{k-1},x) = h(x)\prod_{i\in[l]}(x-\lambda_i)$$

for some p-adic integers λ_i. The polynomial h has no roots among the p-adic integers. So there is a highest p-power p^M which can divide $h(x)$ for any p-adic number x.

Let us estimate the number of roots of (3.4) modulo p^N. For every root x, the product is divisible by p^N. As $h(x)$ is divisible by at most p^M, there must be an i for which $x-\lambda_i$ is divisible by $p^{\lceil (N-M)/l\rceil}$. So every root is contained in the mod $p^{\lceil (N-M)/l\rceil}$-class of some λ_i, and hence

$$(3.5)\qquad R(N) \le l p^{N-\lceil (N-M)/l\rceil}.$$

By combining (3.1), (3.2), (3.3) and (3.5), we finally obtain

$$\begin{aligned}&\mathbb{P}\Big[\exists f_i \succ s_i : \xi_{f_i} \equiv \eta_i \pmod{p^N}, g(\eta_1,\dots,\eta_{k-1},\xi_{f_k}) \equiv 0 \pmod{p^N}\Big| b_{s_1},\dots,b_{s_k}\Big] \\ &\qquad \le \left(\frac{2^{r-n}}{p^{N-2^{n+1}}}\right)^{k-1} \cdot \frac{2^{r-n} l p^{N-\lceil (N-M)/l\rceil}}{p^{N-2^{n+1}}} \\ &\qquad = \frac{l\left(2^{r-n}p^{2^{n+1}}\right)^k}{p^{\lceil (N-M)/l\rceil}} \cdot \underbrace{\frac{1}{p^{N(k-1)}}}_{\mu(A)} = O\left(\frac{N^k}{p^{N/l}}\right)\cdot\mu(A).\end{aligned}$$

Hence A is indeed admissible for large N. □

For a countable module B, we will randomly and independently choose elements $a_n = \sum_{b\in I_n} b\xi_{n,b} \in J_pB$ for all $n < \omega$. To this end, we select the support I_n and the coefficients $\xi_{n,b}$ according to the following distribution.

Distribution 3.4. For a countable set B and for $n < \omega$, let I_n be independent, identical distributed random variables taking values in the non-empty finite subsets of B. Every non-empty finite subset should be contained in I_n (for a fixed n) with positive probability.

Furthermore, for all n and $b \in I_n$ and $\alpha < 2^{\aleph_0}$ let the $\xi_{n,b}^\alpha$ be random p-adic numbers chosen as in Lemma 3.3. Note that the $\xi_{n,b}^\alpha$ are almost surely algebraically independent for all $n < \omega, b \in I_n, \alpha < 2^{\aleph_0}$.

We can prove the following probabilistic variant of Theorem 3.1.

Theorem 3.5. *Let R be a countable p-reduced, torsion-free ring. Let B be an at most countably generated, non-zero, free R-module. Furthermore, let I_n be random finite subsets of B and $\xi_{n,b}^\alpha$ for $b \in I_n$ and $\alpha < 2^{\aleph_0}$ be random p-adic numbers with Distribution 3.4, and define*

$$a_n^\alpha := \sum_{b \in I_n} b\xi_{n,b}^\alpha \in J_pB. \tag{3.6}$$

Then the groups

$$G^A := \langle B, Ra_n^\alpha : n < \omega, \alpha \in A \rangle_{p*} \subseteq \widehat{B}.$$

for $\emptyset \neq A \subseteq 2^{\aleph_0}$ have endomorphism ring $\operatorname{End} G^A = R$ and form a fully rigid system, i.e.,

$$\operatorname{Hom}(G^A, G^D) = \begin{cases} R, & A \subseteq D \\ 0, & A \nsubseteq D \end{cases}$$

almost surely.

Proof. By Lemma 3.3 the family $\{\xi_{n,b}^\alpha \mid n < \omega, b \in I_n, \alpha < 2^{\aleph_0}\}$ is almost surely algebraically independent. Moreover, every finite $F \subseteq B$ is almost surely contained in some (actually infinitely many) I_n with $n < \omega$. We will show that these two properties guarantee that $\operatorname{Hom}(G^A, G^D)$ is R or 0 almost surely, as claimed, i.e., all homomorphisms are multiplications by ring elements.

Let φ be a homomorphism from G^A to G^D and let $\alpha \in A \subseteq 2^{\aleph_0}$ be arbitrary but fixed for the moment. Obviously, $b\varphi, a_n^\alpha\varphi \in G^D$ for $b \in B$ so there are $d_b, c_n, \in \mathbb{Z}[1/p]B$ and $t_{m,b}, r_{m,n} \in R[1/p]$ together with $\beta_{m,b}, \delta_{m,n} \in D$ such that

$$\begin{aligned} b\varphi = d_b + \sum_m t_{m,b} a_m^{\beta_{m,b}} &= d_b + \sum_{m,f\colon f \in I_m} t_{m,b} f \xi_{m,f}^{\beta_{m,b}}, \\ a_n^\alpha \varphi &= c_n + \sum_{m,f\colon f \in I_m} r_{m,n} f \xi_{m,f}^{\delta_{m,n}}. \end{aligned} \tag{3.7}$$

On the other hand, by continuity, we also obtain from (3.6) and (3.7)

$$a_n^\alpha\varphi = \sum_{b \in I_n} d_b \xi_{n,b}^\alpha + \sum_{\substack{m,f\colon f \in I_m, \\ b \in I_n}} t_{m,b} f \xi_{m,f}^{\beta_{m,b}} \xi_{n,b}^\alpha.$$

By combining the two expressions for $a_n^\alpha\varphi$ we therefore obtain

$$\sum_{b \in I_n} d_b \xi_{n,b}^\alpha + \sum_{\substack{m,f\colon f \in I_m, \\ b \in I_n}} t_{m,b} f \xi_{m,f}^{\beta_{m,b}} \xi_{n,b}^\alpha = c_n + \sum_{m,f\colon f \in I_m} r_{m,n} f \xi_{m,f}^{\delta_{m,n}}.$$

Using the algebraic independence of the $\xi_{n,b}^\gamma$, we compare coefficients and obtain among others

$$\begin{aligned} t_{m,b} f &= 0, && (f \in I_m) \\ d_b &= r_{n,n} b && (b \in I_n) \\ d_b &= 0 && (\alpha \notin D). \end{aligned} \tag{3.8}$$

We have used that for every $b \in B$ there is an n with $b \in I_n$. For example, to obtain the first equation, we choose $n \neq m$ with $b \in I_n$ and compare the coefficients of $\xi_{m,f}^{\beta_{m,b}} \xi_{n,b}^\alpha$. We conclude that if $\alpha \notin D$ then $b\varphi = 0$ for all $b \in B$ and hence $\varphi = 0$. This is enough for the case $A \nsubseteq D$. If $\alpha \in D$ then $b\varphi = d_b = r_{n,n} b$ for all n and $b \in I_n$. We now show that essentially all the $r_{n,n}$

are equal, i.e., $b\varphi = rb$ for some $r \in R[1/p]$. As B is free, there is an element b' with zero annihilator, e.g., a basis element. As a consequence, all the $r_{n,n}$ are equal for which $b' \in I_n$. Let r be the common value of these $r_{n,n}$, choose $b \in B$ arbitrary and pick n with $b', b \in I_n$, which exists by hypothesis. So $r = r_{n,n}$, and using (3.8) we obtain $b\varphi = r_{n,n}b = rb$ as claimed. We therefore conclude that the homomorphism φ is multiplication by an $r \in R[1/p]$.

As B is free, $R[1/p] \cap \operatorname{End} B = R$, and it follows that $r \in R$ and thus φ is a multiplication with the ring element r. This finishes the case $A \subseteq D$ and hence the proof. □

We also obtain a probabilistic version of Corner's construction of finite-rank groups as a corollary (see Corner [1963, Theorem B] or Göbel and Trlifaj [2006, Corollary 12.1.3]).

Corollary 3.6. *Let A be a p-reduced, p-torsion-free ring of finite rank n. Then*

$$G \coloneqq \langle A, wA \rangle_{p*}$$

is of rank $2n$ and $\operatorname{End}(G) \cong A$ almost surely.

In the usual way Theorem 3.5 and Corollary 3.6 can be generalized to $\mathbb{S}$-reduced, $\mathbb{S}$-torsion free algebras A of finite rank over some $\mathbb{S}$-ring R whose completion $\widehat{R}$ has sufficiently high transcendence degree; we confined ourselves to the simplified case purely for expository reasons and the generalization is left to the interested reader.

Note that the elements $a_n^\alpha \in \widehat{B}$ that we chose at random in Theorem 3.5 were contained in the submodule J_pB. It would be natural to expect that a nearly uniform choice of random elements from the completion $\widehat{B}$ should already suffice. However, it fails: the constructed group is actually almost surely free. This shows in a nice way that the actual distribution does matter which is somewhat counterintuitive. It seems that especially the implicit assumption of finite support in Distribution 3.4 is advantageous.

Theorem 3.7. *Let B be a free abelian group of countably infinite rank and let*

$$G \coloneqq \langle B, a_n \rangle_{p*} \subseteq \widehat{B}$$

where the a_n with $n < \omega$ are independent, random elements chosen with a nearly uniform distribution from the completion $\widehat{B}$*, i.e., for some $\alpha > 1$, all $n < \omega$, and $x \in B/p^nB$ we have $\mathbb{P}[a_m + p^nB = x] \leq p^{-n^\alpha}$. Then G is almost surely free.*

Proof. First we claim that the random elements a_m are almost never contained in the J_p-module generated by any fixed $b_1, \dots, b_k \in \widehat{B}$, i.e.,

$$\mathbb{P}\left[a_m \in \langle b_1, \dots, b_k \rangle_{J_p}\right] = 0. \tag{3.9}$$

The event is the intersection of the descending sequence of events that a_m is contained in the subgroup generated by the b_i in the factor group $\widehat{B}/p^n\widehat{B}$. We estimate the probability of the latter events:

$$\mathbb{P}[a_m \in \langle b_1, \dots, b_k \rangle + p^nB] \leq |\langle b_1, \dots, b_k \rangle \bmod p^n| \cdot \frac{1}{p^{n^\alpha}} \leq \frac{p^{nk}}{p^{n^\alpha}}.$$

This tends to zero as n goes to infinity, proving the claim.

Next we show that the family of all the e_n and a_m is almost surely linearly independent over J_p. If the family is linearly dependent then

$$\sum_{i=0}^{k} \eta_i e_i + \sum_{j=0}^{l} \mu_j a_j = 0$$

for some p-adic integers η_i and μ_j, where not all of those are zero. The e_i form a basis of B, so they remain linearly independent over J_p, hence there must be a non-zero μ_j. Since J_p is a

discrete valuation domain, there is a μ_m dividing all the μ_j. It follows that μ_m divides $\sum_{i=0}^{k} \eta_i e_i$. Because $J_pB = \bigoplus_{n=0}^{\infty} J_p e_i$ is pure in $\widehat{B}$, the number μ_m must divide all of the η_i. All in all, we obtain

$$a_m = -\sum_{i=0}^{k} \mu_m^{-1} \eta_i e_i - \sum_{j=0}^{l} \mu_m^{-1} \mu_j a_j$$

and therefore

$$a_m \in \langle e_0, \dots, e_k, a_0, \dots, a_{m-1}, a_{m+1}, \dots, a_l \rangle_{J_p}. \tag{3.10}$$

Since the a_j are independent random variables, the event (3.10) has probability zero by (3.9) for fixed m, k, and l. Varying m, k, and l, there are only countably many such events, so almost surely none of them occurs, and hence the family of all the e_n and a_m are almost surely linearly independent over J_p.

Finally, we show that the linear independence ensures that G is free. Recall that G is countable, and hence we can apply Pontryagin's criterion (see Fuchs [1970, Theorem 19.1] or Eklof and Mekler [2002, Theorem 2.3]): a countable torsion-free abelian group is free if and only if every finite-rank subgroup is free. Therefore it suffices to show that the purifications $\langle e_0, \dots, e_k, a_0, \dots, a_m \rangle_*$ are actually free groups. Recall that $\widehat{B}$ as a J_p-module has the property that every pure finite-rank submodule is a free module. Therefore $\langle e_0, \dots, e_k, a_0, \dots, a_m \rangle_{J_p,*}$ is free, and in particular for some $k > 0$, we have $p^k \langle e_0, \dots, e_k, a_0, \dots, a_m \rangle_{J_p,*} \subseteq \langle e_0, \dots, e_k, a_0, \dots, a_m \rangle_{J_p}$. It follows that every element of $p^k \langle e_0, \dots, e_k, a_0, \dots, a_m \rangle_*$ is a linear combination of the $e_0, \dots, e_k, a_0, \dots, a_m$ with coefficients in J_p. On the other hand, the coefficients are also in $\mathbb{Z}[1/p]$, since $p^k \langle e_0, \dots, e_k, a_0, \dots, a_m \rangle_*$ is a subgroup of G. All in all, using linear independence, the coefficients are in $J_p \cap \mathbb{Z}[1/p] = \mathbb{Z}$, so $p^k \langle e_0, \dots, e_k, a_0, \dots, a_m \rangle_*$ is contained in $\langle e_0, \dots, e_k, a_0, \dots, a_m \rangle$. Therefore $\langle e_0, \dots, e_k, a_0, \dots, a_m \rangle_*$ must be free. □

4. Small-rank groups

In this section we provide a probabilistic counterpart for Zassenhaus's construction (see Zassenhaus [1967] or Göbel and Trlifaj [2006, Theorem 12.1.6]).

Theorem 4.1. *Let A be a ring with a finite-rank free additive group. Then there is a torsion-free abelian group M of the same rank with endomorphism ring A.*

Sketch of proof. For every pair of non-zero elements a_i, e_i of A, choose an integer c_i and a prime p_i such that $c_i - a_i$ is invertible in $\mathbb{Q}A$, and p_i divides the order of $(c_i - a_i)^{-1} e_i$ in $\mathbb{Q}A/A$. Make the choices such that the primes p_i are pairwise distinct. We choose positive integers r_i, d_i such that $p_i^{r_i} d_i (c_i - a_i)^{-1} \in A$ and d_i is relative prime to p_i. Now the abelian group

$$M \coloneqq \left\langle A, p_i^{-r_i}(c_i - a_i)A : i < \omega \right\rangle \subseteq \mathbb{Q}A$$

has endomorphism ring A acting on it by multiplication on the right.

To see this, first we note that for every $m \in \mathbb{Q}A$ with $p_i^{-r_i}(c_i - a_i)m \in M$, the order of m in $\mathbb{Q}A/A$ is not divisible by p_i. Indeed, there are $a, b_j \in A$ such that

$$p_i^{-r_i}(c_i - a_i)m = a + \sum_j p_j^{-r_j}(c_j - a_j)b_j.$$

Multiplying by $\tilde{a} \coloneqq p_i^{r_i} d_i (c_i - a_i)^{-1} \in A$ on the left

$$d_i m = d_i b_i + \tilde{a}a + \sum_{j \neq i} p_j^{-r_j} \tilde{a}(c_j - a_j)b_j.$$

The order of the right-hand side is clearly not divisible by p_i. As d_i is not divisible by p_i, it also follows that p_i does not divide the order of m.

We will now prove that the only $\phi \in \operatorname{End} M$ mapping 1 to 0 is the zero map. Suppose for contradiction that there is a non-zero ϕ with $1\phi = 0$. Thus there exists $a \in A$ with $a\phi \neq 0$. By multiplying a with a large positive integer if necessary, we can assume $a\phi \in A$. In fact there is an i with $a_i = a$ and $-e_i = a\phi$.

Since

$$p_i^{-r_i} e_i = p_i^{-r_i}(c_i - a_i)\phi \in M,$$

the order of $(c_i - a_i)^{-1} e_i$ in $\mathbb{Q}A/A$ is not divisible by p_i contradicting one of our assumptions.

Next we establish that $\mathbb{Q}A \cap \operatorname{End} M = A$, where every $a \in \mathbb{Q}A$ is identified with multiplication by a on the right. So let $m \in \mathbb{Q}A \cap \operatorname{End} M$. Then $m = 1m \in M$, so the order of m in $\mathbb{Q}A/A$ can have only the p_i as prime divisors. On the other hand, since $p_i^{-r_i}(c_i - a_i)m \in M$, the order of m in $\mathbb{Q}A/A$ is not divisible by p_i. Hence the order of m must be 1, i.e., $m \in A$.

It remains to show that $\operatorname{End} M = A$. Let $\phi \in \operatorname{End} M$. There is a positive integer n with $1 \cdot n\phi \in A$. Now $n\phi - 1 \cdot n\phi$ is an endomorphism of M mapping 1 to 0, hence it is zero. Thus $\phi = 1\phi \in \mathbb{Q}A \cap \operatorname{End} M = A$. □

For the probabilistic version of this construction, we shall use a consequence of a theorem of Frobenius (see Frobenius [1896]) or Chebotarëv's density theorem (see Chebotarëv [1923], Tschebotareff [1926]) which is a generalization of Frobenius's theorem.

Lemma 4.2. *For every non-constant (univariate) polynomial $f \in \mathbb{Z}[x]$ the sum of the reciprocals of primes p for which f has a root modulo p diverges, i.e.,*

$$\sum_{\substack{p \text{ prime} \\ f \text{ has root mod } p}} \frac{1}{p} = \infty.$$

We first specify the distribution according to which we choose the random elements:

Distribution 4.3. Let A be a ring with a finite-rank, free additive group. For every prime p we choose uniformly and independently a non-zero element $a_p \in A$ and an integer $c_p \in [p, 2p-1]$. Whenever $c_p - a_p$ is invertible in $\mathbb{Q}A$, we choose positive integers r_p and d_p arbitrarily with $p^{r_p} d_p (c_p - a_p)^{-1}$ in A and d_p relative prime to p.

We are ready to prove the probabilistic variant of Theorem 4.1.

Theorem 4.4. *Let A be a ring with a finite-rank free additive group and let M be the torsion-free abelian group*

$$M \coloneqq \left\langle A, p^{-r_p}(c_p - a_p)A : p \text{ prime and } \exists (c_p - a_p)^{-1} \right\rangle$$

with c_p, a_p, r_p chosen via Distribution 4.3. Then $\operatorname{End} M = A$ almost surely, where A acts on M by multiplication on the right.

Proof. With the argumentation in the sketch of proof of Theorem 4.1, it suffices to prove that for every pair of non-zero elements e and a of A there is a prime p such that $a_p = a$, the difference $c_p - a_p$ is invertible in $\mathbb{Q}A$, and p divides the order of $(c_p - a_p)^{-1} e$ in $\mathbb{Q}A/A$.

There are only finitely many c for which $c - a$ is non-invertible, namely, the roots of the characteristic polynomial of (left) multiplication by a. Furthermore $(c-a)^{-1} e$ is a rational function of c of degree at most -1, i.e., the coordinates are rational functions in (any) basis of $\mathbb{Q}A$. Now p divides the order of $(c_p - a_p)^{-1} e$ in $\mathbb{Q}A/A$ if and only if there is a coordinate where p occurs with negative exponent, e.g., p divides the denominator but not the numerator. We simplify the coordinates to make the numerator and denominator relative prime polynomials, so there are only finitely many primes such that at any place c, at most these among all primes divide both the numerator and denominator of a coordinate. Note that for non-zero coordinates, the denominator is still non-constant, as the coordinate has negative degree.

All in all, there is a non-constant polynomial f (the denominator of a coordinate) with integer coefficients for which all but finitely many primes p and any root c of f modulo p, the order of $(c-a)^{-1}e$ in $\mathbb{Q}A/A$ is divisible by p. For every p where f has a root modulo p, we choose c_p a root with probability at least $1/p$. Since these events are independent and the sum of their probabilities is infinite by Lemma 4.2, infinitely many of these events occur almost surely. Again by independence, $a_p = a$ almost surely for infinitely many of these p, finishing the proof. □

5. Concluding remarks and open questions

So far the proposed method only works for constructions up to continuum in size. This is due to the lack of a strong probability theory beyond $2^{\aleph_0}$. However we believe that this method is likely to be generalized to such cases as well; a step in this direction is Lemma 3.3. A potential route to carry over the probabilistic tools might be to work with a countable model of set theory; however this is speculation. In particular, the following questions remain open, where the last one is probably the most intricate one:

(1) Generalize to Butler (locally free): There is a well-known generalization of Zassenhaus's Theorem 4.1 to the locally free case by Butler (see Butler [1968]). It turns out that our randomized construction does not easily generalize to this case.

Can the construction be generalized to the locally free case?

(2) Use randomness in a more involved way: So far randomness has been used either to construct algebraically independent elements or to ensure that all elements of a countable set have been chosen. However randomness has not been directly employed in the construction itself.

Can we use randomization in the constructions itself in order to obtain simplified or even stronger constructions?

(3) Generalize beyond $2^{\aleph_0}$: Probability theory is defined on σ-algebras and countability plays a central role in the arguments.

Are there probabilistic constructions of objects larger than $2^{\aleph_0}$?

(4) It is independent of ZFC whether for $\aleph_0 < \lambda < 2^{\aleph_0}$, the union of λ events of probability 0 from the continuous uniform distribution (e.g., of a random real number from $[0,1]$) has again probability zero.

*Is there a randomized construction for a (natural) statement in abelian group theory, so that the actual probability for the theorem to hold is **independent** of ZFC?*

For example, is there a realization theorem for some (family of) ring A so that $\mathrm{End}(G) = A$ with probability 1 in one universe and probability 0 in another?

6. Acknowledgments

We are indebted to Brendan Goldsmith for the valuable feedback and comments as well as pointing us to related work. We would also like to thank Winfried Bruns for the helpful discussions on Lemma 4.2.

References

N. Alon and J.H. Spencer. *The probabilistic method*. Wiley-Interscience, 2000.

M.C.R. Butler. On locally free torsion-free rings of finite rank. *Journal of the London Mathematical Society*, 1(1):297, 1968.

N.G. Chebotarëv. Opredelenie plotnosti sovokupnosti prostykh chisel, prinadlezhashchikh zadannomu klassu podstanovok. *Izv. Ross. Akad. Nauk*, 17:205–250, 1923.

A.L.S. Corner. Every countable reduced torsion-free ring is an endomorphism ring. *Proc. London Math. Soc. (3)*, 13:687–710, 1963. ISSN 0024-6115.

A.L.S Corner. Every countable reduced torsion-free algebra is an endomorphism algebra (alternative version). unpublished manuscript, 196X.

M. Droste and R. Göbel. Countable random p-groups with prescribed Ulm-invariants. *Proc. Amer. Math. Soc. (to appear)*, 2010.

P.C. Eklof and A.H. Mekler. *Almost free modules: set-theoretic methods*. North-Holland, 2002.

P. Erdős. Graph theory and probability. *Canadian Journal of Mathematics*, 11:34–38, 1959.

P. Erdős. Graph theory and probability, II. *Canadian Journal of Mathematics*, 13:346–352, 1961.

P. Erdős and A. Rényi. On Random Graphs I. *Publicationes Mathematicae*, 6:290–297, 1959.

G. Frobenius. Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. *S'ber. Akad. Wiss. Berlin*, pages 689–703, 1896.

L. Fuchs. *Infinite abelian groups, Volume 1*. Academic Press, 1970.

L. Fuchs. *Infinite abelian groups, Volume 2*. Academic Press, 1973.

R. Göbel and J. Trlifaj. *Approximations and endomorphism algebras of modules*. de Gruyter, 2006.

T.J. Jech. *Set theory*. Academic Press, 1978.

S. Shelah and J. Spencer. Zero-one laws for sparse random graphs. *Journal of the American Mathematical Society*, 1(1):97–115, 1988.

S. Shelah and J. Spencer. Random sparse unary predicates. *Random Structures and Algorithms*, 5(3):375–394, 1994.

N. Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Mathematische Annalen*, 95(1):191–228, 1926.

H. Zassenhaus. Orders as endomorphism rings of modules of the same rank. *Journal of the London Mathematical Society*, 1(1):180, 1967.

Universität Duisburg–Essen, Campus Essen, Fachbereich Mathematik, AG Göbel–Strüngmann Universitätsstrasse 2, 45117 Essen

E-mail address: gabor.braun@uni-duisburg-essen.de

Friedrich-Alexander-University of Erlangen-Nürnberg, Am Weichselgarten 9, 91058 Erlangen, Germany

E-mail address: sebastian.pokutta@math.uni-erlangen.de