# THREE THEOREMS ON LINEAR GROUPS

BOGDAN NICA

## INTRODUCTION

A group is **linear** if it is (isomorphic to) a subgroup of $\mathrm{GL}_n(\mathbb{K})$, where $\mathbb{K}$ is a field. If we want to specify the field, we say that the group is linear over $\mathbb{K}$. The following theorems are fundamental, at least from the perspective of combinatorial group theory.

**Theorem** (Mal'cev 1940)**.** *A finitely generated linear group is residually finite.*

**Theorem** (Selberg 1960)**.** *A finitely generated linear group over a field of zero characteristic is virtually torsion-free.*

A group is **residually finite** if its elements are distinguished by the finite quotients of the group, i.e., if each non-trivial element of the group remains non-trivial in a finite quotient. A group is **virtually torsion-free** if some finite-index subgroup is torsion-free. As a matter of further terminology, Selberg's theorem is usually referred to as Selberg's lemma, and Mal'cev is alternatively transliterated as Maltsev.

Residual finiteness and virtual torsion-freeness are related to a third property - roughly speaking, a "$p$-adic" refinement of residual finiteness. A theorem due to Platonov (1968) gives such refined residual properties for finitely generated linear groups. Both Mal'cev's theorem and Selberg's lemma are consequences of this more powerful, but lesser known, theorem of Platonov.

Once we have Platonov's theorem and its proof, we are not too far from our third theorem of interest. In order to formulate it, let us first observe that every non-trivial torsion element in a group $G$ gives rise to a non-trivial idempotent in the complex group algebra $\mathbb{C}G$. Namely, if $g \in G$ has order $n > 1$, then $e = \frac{1}{n}(1 + g + \ldots + g^{n-1}) \in \mathbb{C}G$ satisfies $e^2 = e$, and $e \neq 0, 1$. The **Idempotent Conjecture** is the bold statement that the converse holds: if $G$ is a torsion-free group, then the group algebra $\mathbb{C}G$ has no non-trivial idempotents. While not yet settled in general, this conjecture is known for many classes of groups. A particularly important partial result is the following.

**Theorem** (Bass 1976)**.** *Torsion-free linear groups satisfy the Idempotent Conjecture.*

## 1. VIRTUAL AND RESIDUAL PROPERTIES OF GROUPS

Virtual torsion-freeness and residual finiteness are instances of the following terminology. Let $\mathcal{P}$ be a group-theoretic property. A group is **virtually** $\mathcal{P}$ if it has a finite-index subgroup enjoying $\mathcal{P}$. A group is **residually** $\mathcal{P}$ if each non-trivial element of the group remains non-trivial in some quotient group enjoying $\mathcal{P}$. The virtually $\mathcal{P}$ groups and the residually $\mathcal{P}$ groups contain the $\mathcal{P}$ groups. It may certainly happen that a property is virtually stable (e.g., finiteness) or residually stable (e.g., torsion-freeness).

Besides virtual torsion-freeness and residual finiteness, we are interested in the hybrid notion of **virtual residual $p$-finiteness** where $p$ is a prime. This is obtained by residualizing the property of being a finite $p$-group, followed by the virtual extension. The notion of virtual residual $p$-finiteness has, in fact, a leading role in this account for it relates both to residual finiteness and to virtual torsion-freeness.

---

*Date*: December 2013.

Observe the following.

**(Going down)** If $\mathcal{P}$ is inherited by subgroups, then both virtually $\mathcal{P}$ and residually $\mathcal{P}$ are inherited by subgroups. In particular, virtual torsion-freeness, residual finiteness, and virtual residual $p$-finiteness are inherited by subgroups.

**(Going up)** Virtually $\mathcal{P}$ passes to finite-index supergroups. In particular, both virtual torsion-freeness and virtual residual $p$-finiteness pass to finite-index supergroups. Residual finiteness passes to finite-index supergroups.

Residual $p$-finiteness trivially implies residual finiteness. Going up, we obtain:

**Lemma 1.1.** *Virtual residual $p$-finiteness for some prime $p$ implies residual finiteness.*

On the other hand, residual $p$-finiteness imposes torsion restrictions. Namely, in a residually $p$-finite group, the order of a torsion element must be a $p$-th power. Hence, if a group is residually $p$-finite and residually $q$-finite for two different primes $p$ and $q$, then it is torsion-free. Virtualizing this statement, we obtain:

**Lemma 1.2.** *Virtual residual $p$-finiteness and virtual residual $q$-finiteness for two primes $p \neq q$ imply virtual torsion-freeness.*

## 2. Platonov's theorem

In light of Lemmas 1.1 and 1.2, we see that Mal'cev's theorem and Selberg's lemma are consequences of the following:

**Theorem** (Platonov 1968)**.** *Let $G$ be a finitely generated linear group over a field $\mathbb{K}$. If* $\operatorname{char}\mathbb{K} = 0$*, then $G$ is virtually residually $p$-finite for all but finitely many primes $p$. If* $\operatorname{char}\mathbb{K} = p$*, then $G$ is virtually residually $p$-finite.*

Actually, the zero characteristic part of Platonov's theorem had been proved slightly earlier by Kargapolov (1967) and, independently, Merzlyakov (1967).

**Example 2.1.** $\mathrm{SL}_n(\mathbb{Z})$, where $n \geq 2$, is a finitely generated linear group over $\mathbb{Q}$. Reduction modulo a positive integer $N$ defines a group homomorphism $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N)$, whose kernel

$$\Gamma(N) := \ker\big(\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N)\big) = \big\{X \in \mathrm{SL}_n(\mathbb{Z}) : X \equiv 1_n \bmod N\big\}$$

is the **principal congruence subgroup of level** $N$. The principal congruence subgroups are finite-index, normal subgroups of $\mathrm{SL}_n(\mathbb{Z})$. They are organized according to the divisibility of their levels: $\Gamma(M) \supseteq \Gamma(N)$ if and only if $M|N$, that is, "to contain is to divide". Hence the prime stratum $\{\Gamma(p) : p \text{ prime}\}$, and each descending chain $\{\Gamma(p^k) : k \geq 1\}$ corresponding to fixed prime $p$, stand out.

Elements of $\mathrm{SL}_n(\mathbb{Z})$ can be distinguished both along the prime stratum, $\cap_p \Gamma(p) = \{1_n\}$, as well as along each descending $p$-chain, $\cap_k \Gamma(p^k) = \{1_n\}$. We thus have two ways of seeing that $\mathrm{SL}_n(\mathbb{Z})$ is residually finite.

There is no prime $p$ for which $\mathrm{SL}_n(\mathbb{Z})$ is residually $p$-finite, simply because $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ has order 6. However, $\mathrm{SL}_n(\mathbb{Z})$ is virtually residually $p$-finite for each prime $p$. The reason is that $\Gamma(p)$ is residually $p$-finite, and this is easily seen by noting that each successive quotient $\Gamma(p^k)/\Gamma(p^{k+1})$ in the descending chain $\{\Gamma(p^k) : k \geq 1\}$ is a $p$-group: for $X \in \Gamma(p^k)$ we have

$$X^p = 1_n + \sum_{i=1}^{p} \binom{p}{i} (X - 1_n)^i \in \Gamma(p^{k+1}).$$

**Example 2.2.** $\mathrm{SL}_n(\mathbb{F}_p[t])$, where $n \geq 2$, is linear over $\mathbb{F}_p(t)$ and finitely generated for $n \geq 3$ (though not for $n = 2$). A similar argument to the one of the previous example, this time involving the principal congruence subgroups corresponding to the descending chain of ideals $(t^k)$ for $k \geq 1$, shows that $\mathrm{SL}_n(\mathbb{F}_p[t])$ is virtually residually $p$-finite. On the other hand, $\mathrm{SL}_n(\mathbb{F}_p[t])$ contains a copy of the infinite torsion group $(\mathbb{F}_p[t], +)$, and this prevents $\mathrm{SL}_n(\mathbb{F}_p[t])$ from being virtually torsion-free. Consequently, $\mathrm{SL}_n(\mathbb{F}_p[t])$ cannot be virtually residually $q$-finite for any prime $q \neq p$.

Platonov's theorem implies the following "$p$-adic" refinement of Mal'cev's theorem.

**Corollary 2.3.** *A finitely generated linear group is virtually residually $p$-finite for some prime $p$.*

This corollary, combined with Example 2.2, leads us to a simple example of a finitely generated group which is non-linear but residually finite: $\mathrm{SL}_n(\mathbb{F}_p[t]) \times \mathrm{SL}_n(\mathbb{F}_q[t])$, where $p$ and $q$ are different primes, and $n \geq 3$.

## 3. Proof of Platonov's theorem

Let $G$ be a finitely generated linear group over a field $\mathbb{K}$, say $G \leq \mathrm{GL}_n(\mathbb{K})$. In $\mathbb{K}$, consider the subring $A$ generated by the multiplicative identity 1 and the matrix entries of a finite, symmetric set of generators for $G$. Thus $A$ is a finitely generated domain, and $G$ is a subgroup of $\mathrm{GL}_n(A)$. Platonov's theorem is then a consequence of the following:

**Theorem 3.1.** *Let $A$ be a finitely generated domain. If* $\mathrm{char}\, A = 0$, *then* $\mathrm{GL}_n(A)$ *is virtually residually $p$-finite for all but finitely many primes $p$. If* $\mathrm{char}\, A = p$, *then* $\mathrm{GL}_n(A)$ *is virtually residually $p$-finite.*

Here, and for the remainder of the section, rings are commutative and unital. The proof of Theorem 3.1 is a straightforward variation on the example of $\mathrm{SL}_n(\mathbb{Z})$, as soon as we know the following facts:

**Lemma 3.2.** *Let $A$ be a finitely generated domain. Then the following hold:*

i. *$A$ is noetherian.*
ii. $\cap_k I^k = 0$ *for any ideal $I \neq A$.*
iii. *If $A$ is a field, then $A$ is finite.*
iv. *The intersection of all maximal ideals of $A$ is* $0$.
v. *If* $\mathrm{char}\, A = 0$, *then only finitely many primes $p = p \cdot 1$ are invertible in $A$.*

Let us postpone the proof of Lemma 3.2 for the moment, and focus instead on deriving Theorem 3.1. The principal congruence subgroup of $\mathrm{GL}_n(A)$ corresponding to an ideal $I$ of $A$ is defined by

$$\Gamma(I) = \ker\big(\mathrm{GL}_n(A) \to \mathrm{GL}_n(A/I)\big).$$

If $\pi$ is a maximal ideal then $A/\pi$ is a finite field, by part (iii) of Lemma 3.2, so $\Gamma(\pi)$ has finite index in $\mathrm{GL}_n(A)$. Also $\cap_\pi \Gamma(\pi) = \{1_n\}$ as $\pi$ runs over the maximal ideals of $A$, by part (iv) of Lemma 3.2. This shows that $\mathrm{GL}_n(A)$ is residually finite, thereby proving Mal'cev's theorem.

For each $k \geq 1$, the quotient $\pi^k/\pi^{k+1}$ is naturally an $A/\pi$-module. It inherits finite generation from the finite generation of the $A$-module $\pi^k$, the latter due to $A$ being noetherian. As $A/\pi$ is finite, $\pi^k/\pi^{k+1}$ is finite as well. It follows that the ring $A/\pi^k$ is finite, and so $\Gamma(\pi^k)$ has finite index in $\mathrm{GL}_n(A)$. Furthermore, $\cap_k \Gamma(\pi^k) = \{1_n\}$ by part (ii) of Lemma 3.2, which shows once again that $\mathrm{GL}_n(A)$ is residually finite. Now let $p$ denote the characteristic of $A/\pi$, so $p = p \cdot 1 \in \pi$. Then $\Gamma(\pi^k)/\Gamma(\pi^{k+1})$ is a $p$-group: for $X \in \Gamma(\pi^k)$ we have

$$X^p = 1_n + \sum_{i=1}^{p} \binom{p}{i} (X - 1_n)^i \in \Gamma(\pi^{k+1}).$$

To conclude, $\mathrm{GL}_n(A)$ is virtually residually $p$-finite for each prime $p$ not invertible in $A$. By part (v) of Lemma 3.2, this happens for all but finitely many primes $p$ in the zero characteristic case. In characteristic $p$, there is only such prime, namely $p$ itself. Theorem 3.1 is proved.

We now return to the proof of the lemma.

*Proof of Lemma 3.2.* The first two points are standard: i) follows from the Hilbert Basis Theorem, and ii) is the Krull Intersection Theorem for domains.

iii) We claim the following: if $F \subseteq F(u)$ is a field extension with $F(u)$ finitely generated as a ring, then $F \subseteq F(u)$ is a finite extension and $F$ is finitely generated as a ring.

We use the claim as follows. Let $F$ be the prime field of $A$ and let $a_1, \ldots, a_k$ be generators of $A$ as a ring. Thus $A = F(a_1, \ldots, a_k)$. Going down the chain

$$A = F(a_1, \ldots, a_k) \supseteq F(a_1, \ldots, a_{k-1}) \supseteq \ldots \supseteq F$$

we obtain that $F \subseteq A$ is a finite extension, and that $F$ is finitely generated as a ring. Then $F$ is a finite field, as $\mathbb{Q}$ is not finitely generated as a ring, and so $A$ is finite.

Now let us prove the claim. Assume that $u$ is transcendental over $F$, i.e., $F(u)$ is the field of rational functions in $u$. Let $P_1/Q_1, \ldots, P_k/Q_k$ generate $F(u)$ as a ring, where $P_i, Q_i \in F[u]$. The multiplicative inverse of $1 + u \cdot \prod Q_i$ is a polynomial expression in the $P_i/Q_i$'s, which can be written as $R/\prod Q_i^{s_i}$. Therefore $\prod Q_i^{s_i} = (1 + u \cdot \prod Q_i)R$ in $F[u]$. But this is impossible, since $\prod Q_i^{s_i}$ is relatively prime to $1 + u \cdot \prod Q_i$.

Thus $u$ is algebraic over $F$. Let $X^d + \alpha_1 X^{d-1} + \cdots + \alpha_d$ be the minimal polynomial of $u$ over $F$. Let also $a_1, \ldots, a_k$ be ring generators of $F(u) = F[u]$. We may write each $a_i$ as $\sum_{0 \le m \le d-1} \beta_{i,m}\, u^m$, with $\beta_{i,m} \in F$. We claim that the $\alpha_j$'s and the $\beta_{i,m}$'s are ring generators of $F$. Let $c \in F$. Then $c$ is a polynomial in $a_1, \ldots, a_k$ over $F$, hence a polynomial in $u$ over the subring of $F$ generated by the $\beta_{i,m}$'s, hence a polynomial in $u$ of degree less than $d$ over the subring of $F$ generated by the $\alpha_j$'s and the $\beta_{i,m}$'s. By the linear independence of $\{1, u, \ldots, u^{d-1}\}$, the latter polynomial is actually of degree 0. Hence $c$ ends up in the subring of $F$ generated by the $\alpha_j$'s and the $\beta_{i,m}$'s.

iv) Let $a \neq 0$ in $A$. To find a maximal ideal of $A$ not containing $a$, we rely on the basic avoidance: maximal ideals do not contain invertible elements. Consider the localization $A' = A[1/a]$. Let $\pi'$ be a maximal ideal in $A'$, so $a \notin \pi'$. The restriction $\pi = \pi' \cap A$ is an ideal in $A$, and $a \notin \pi$. We show that $\pi$ is maximal. The embedding $A \hookrightarrow A'$ induces an embedding $A/\pi \hookrightarrow A'/\pi'$. As $A'/\pi'$ is a field which is finitely generated as a ring, it follows from iii) that $A'/\pi'$ is finite field. Therefore the subring $A/\pi$ is a finite domain, hence a field as well.

v) We shall use Noether's Normalization Theorem: if $R$ is a finitely generated algebra over a field $F \subseteq R$, then there are elements $x_1, \ldots, x_k \in R$ algebraically independent over $F$ such that $R$ is integral over $F[x_1, \ldots, x_k]$.

In our case, $\mathbb{Z}$ is a subring of $A$, and $A$ is an integral domain which is finitely generated as a $\mathbb{Z}$-algebra. Extending to rational scalars, we have that $A_{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} A$ is a finitely generated $\mathbb{Q}$-algebra. By the Normalization Theorem, there exist elements $x_1, \ldots, x_k$ in $A_{\mathbb{Q}}$ which are algebraically independent over $\mathbb{Q}$, and such that $A_{\mathbb{Q}}$ is integral over $\mathbb{Q}[x_1, \ldots, x_k]$. Up to replacing each $x_i$ by an integral multiple of itself, we may assume that $x_1, \ldots, x_k$ are in $A$. There is some positive $m \in \mathbb{Z}$ such that each ring generator of $A$ is integral over $\mathbb{Z}[1/m][x_1, \ldots, x_k]$. Thus $A[1/m]$ is integral over the subring $\mathbb{Z}[1/m][x_1, \ldots, x_k]$. If a prime $p$ is invertible in $A$, then it is also invertible in $A[1/m]$ while at the same time $p \in \mathbb{Z}[1/m][x_1, \ldots, x_k]$.

Now we use the following general fact. Let $R$ be a ring which is integral over a subring $S$. If $s \in S$ is invertible in $R$, then $s$ is already invertible in $S$. The proof is easy. Let $r \in R$ with $rs = 1$. We have $r^d + s_1 r^{d-1} + \cdots + s_{d-1} r + s_d = 0$ for some $s_i \in S$, since $r$ is integral over $S$. Multiplying through by $s^{d-1}$ yields $r \in S$.

Returning to our proof, we infer that $p$ is invertible in $\mathbb{Z}[1/m][x_1, \ldots, x_k]$. By the algebraic independence of $x_1, \ldots, x_k$, it follows that $p$ is actually invertible in $\mathbb{Z}[1/m]$. But only finitely many primes have this property, namely the prime factors of $m$. □

## 4. The Idempotent Conjecture for linear groups

Our approach to Bass's theorem relies on the following criterion of Formanek [2], whose proof is postponed for the next section.

**Theorem 4.1** (Formanek 1973)**.** *Let $G$ be a torsion-free group with the property that, for infinitely many primes $p$, $G$ has no $p$-self-similar elements. Then the Idempotent Conjecture holds for $G$.*

Given a group $G$, we say that a non-trivial element $g \in G$ is **self-similar** if $g$ is conjugate in $G$ to a proper power $g^N$, where $N \geq 2$. Clearly, torsion elements are self-similar. It turns out that the converse holds for linear groups in positive characteristic.

**Lemma 4.2.** *In a linear group over a field of positive characteristic, every self-similar element is torsion.*

*Proof.* Let char $\mathbb{K} = p$, and consider the relation $g^N = x^{-1}gx$ in $\mathrm{GL}_n(\mathbb{K})$, where $N \geq 2$. Without loss of generality, $\mathbb{K}$ is algebraically closed and $g$ is in Jordan normal form. Each Jordan block is of the form $\lambda \cdot 1_k + \Delta_k$, where $\Delta_k$ is the $k \times k$-matrix with 1's on the super-diagonal and 0's everywhere else. Since $(\lambda \cdot 1_k + \Delta_k)^{p^s} = \lambda^{p^s} \cdot 1_k + \Delta_k^{p^s}$, and $\Delta_k^{p^s} = 0$ for large enough $s$, it follows that $g^{p^s}$ is diagonal for large enough $s$. Thus, up to replacing $g$ by $g^{p^s}$, we may assume that $g$ is diagonal. So let $g$ have $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ along the diagonal, and write out the relation $gx = xg^N$ in matrix form: $(x_{ij}\, \lambda_i) = (x_{ij}\, \lambda_j^N)$. Compare the $i$-th row on the two sides. At least one of $x_{i1}, x_{i2}, \ldots, x_{in}$ is non-zero, hence $\lambda_i = \lambda_{\sigma(i)}^N$ for some $\sigma(i) \in \{1, \ldots, n\}$. Since $\sigma^s = \sigma^{s+t}$ for some positive integers $s$ and $t$, it follows that

$$\lambda_i = \lambda_{\sigma^{s+t}(i)}^{N^{s+t}} = \big(\lambda_{\sigma^s(i)}^{N^s}\big)^{N^t} = \lambda_i^{N^t}$$

for each $i$. We conclude that $g^{N^t - 1} = 1$ in $\mathrm{GL}_n(\mathbb{K})$. $\square$

In characteristic zero, a linear group may contain self-similar elements of infinite order. A simple example in, say, $\mathrm{GL}_2(\mathbb{R})$ is provided by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, which is conjugated into its $N$-th power by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right)$. Furthermore, it can be checked that the entire subgroup generated by these two matrices is torsion-free.

The analogue of Lemma 4.2 in characteristic zero involves the following refined notion of self-similarity. Given a group $G$ and a prime $p$, let us say that a non-trivial element $g \in G$ is ***p*-self-similar** if $g$ is conjugate in $G$ to a proper $p$-th power $g^{p^k}$, where $k \geq 1$.

**Lemma 4.3.** *In a finitely generated linear group over a field of characteristic zero, the following holds for all but finitely many primes $p$: every $p$-self-similar element is torsion.*

*Proof.* The characteristic zero case of Platonov's theorem reduces the claim to showing that, in a virtually residually $p$-finite group, every $p$-self-similar element is torsion. This easily follows from the observation that a residually $p$-finite group has no $p$-self-similar elements. $\square$

The upshot of Lemmas 4.2 and 4.3 is that a finitely generated, torsion-free linear group comfortably meets the requirement of Formanek's criterion, and so it satisfies the Idempotent Conjecture. The theorem of Bass follows.

## 5. Proof of Formanek's criterion

The proof of Theorem 4.1 uses tracial methods. Let us first recall that a **trace** on a $\mathbb{K}$-algebra $\mathcal{A}$ is a $\mathbb{K}$-linear map $\tau : \mathcal{A} \to \mathbb{K}$ with the property that $\tau(ab) = \tau(ba)$ for all $a, b \in \mathcal{A}$. In short, traces are linear functionals which vanish on commutators. The ersatz commutativity afforded by a trace is extremely valuable in a noncommutative world.

On a group algebra $\mathbb{K}G$, the **standard trace** $\mathrm{tr} : \mathbb{K}G \to \mathbb{K}$ is the linear functional which records the coefficient of the identity element:

$$\mathrm{tr}\big(\textstyle\sum a_g\, g\big) = a_1$$

In general, traces on $\mathbb{K}G$ are in bijective correspondence with maps $G \to \mathbb{K}$ which are constant on conjugacy classes. The characteristic map $1_C : G \to \mathbb{K}$ of a conjugacy class $C \subseteq G$ defines the trace

$$\tau_C\big(\sum a_g\, g\big) = \sum_{g \in C} a_g$$

so $\mathrm{tr} = \tau_{\{1\}}$ with this notation. The traces $\tau_C$, where $C$ runs over the conjugacy classes of $G$, provide a natural basis for the $\mathbb{K}$-linear space formed by the traces of $\mathbb{K}G$. Another distinguished trace is the **augmentation map** $\epsilon : \mathbb{K}G \to \mathbb{K}$ given by

$$\epsilon\big(\sum a_g\, g\big) = \sum a_g.$$

This is the trace on $\mathbb{K}G$ defined by the constant map $1 : G \to \mathbb{K}$. The augmentation map is in fact a unital $\mathbb{K}$-algebra homomorphism, hence $\epsilon$ is a trace which is $\{0,1\}$-valued on idempotents.

Understanding the range of the standard trace on idempotents is much more difficult. The following theorem addresses this problem in the case of complex group algebras.

**Theorem 5.1** (Kaplansky 1969)**.** *Let $e$ be an idempotent in $\mathbb{C}G$. Then $\mathrm{tr}(e) \in [0,1]$. Furthermore, $\mathrm{tr}(e) = 0$ if and only if $e = 0$, and $\mathrm{tr}(e) = 1$ if and only if $e = 1$.*

Now let us return to the proof of Formanek's criterion. It consists of two steps.

**(Positive characteristic claim)** Fix a prime $p$. If $G$ has no $p$-self-similar elements and $\mathbb{K}$ is a field of characteristic $p$, then the standard trace is $\{0,1\}$-valued on the idempotents of $\mathbb{K}G$.

It is a familiar fact that the identity $(a+b)^p = a^p + b^p$ holds in any *commutative* $\mathbb{K}$-algebra. Its noncommutative generalization, somewhat lesser known, says that, in a $\mathbb{K}$-algebra, $(a+b)^p - a^p - b^p$ is a sum of commutators. Indeed, we may assume that we are in the free $\mathbb{K}$-algebra on $a$ and $b$. We expand $(a+b)^p$ into monomials of degree $p$ in $a$ and $b$, and we let the cyclic group of order $p$ act on these monomials by cyclic permutations. We see orbits of size $p$, except for $a^p$ and $b^p$, which are fixed by the action. Now we observe that the sum of monomials corresponding to each orbit of size $p$ is a sum of commutators. This follows from the identity

$$\begin{aligned} &x_1x_2\dots x_{p-1}x_p + x_2x_3\dots x_px_1 + \dots + x_px_1\dots x_{p-2}x_{p-1} \\ &\quad = p\cdot x_1x_2\dots x_{p-1}x_p - [x_1, x_2\dots x_p] - [x_1x_2, x_3\dots x_p] - \dots - [x_1\dots x_{p-1}, x_p]. \end{aligned}$$

Next, let us iterate: we show by induction that $(a+b)^{p^k} - a^{p^k} - b^{p^k}$ is a sum of commutators for every positive integer $k$. For the induction step we write

$$(a+b)^{p^{k+1}} = \Big(a^{p^k} + b^{p^k} + \sum [u_i, v_i]\Big)^p = a^{p^{k+1}} + b^{p^{k+1}} + \sum [u_i, v_i]^p + \sum [u'_j, v'_j]$$

and

$$[u,v]^p = (uv)^p - (vu)^p + \sum [y_l, z_l] = \big[(uv)^{p-1}u, v\big] + \sum [y_l, z_l].$$

In particular, a trace $\tau$ on a $\mathbb{K}$-algebra has the property that $\tau\big((a+b)^{p^k}\big) = \tau\big(a^{p^k}\big) + \tau\big(b^{p^k}\big)$ for every positive integer $k$. For a basic trace $\tau_C$, where $C \neq \{1\}$, and an idempotent $e \in \mathbb{K}G$, we obtain

$$\tau_C(e) = \tau_C(e^{p^k}) = \tau_C\Big(\big(\sum e_g\, g\big)^{p^k}\Big) = \sum \tau_C\big((e_g\, g)^{p^k}\big) = \sum e_g^{p^k} 1_C\big(g^{p^k}\big)$$

for each positive integer $k$. The hypothesis that $G$ has no $p$-self-similar elements implies that, for each $g$ in the support of $e$, there is at most one $k$ so that $g^{p^k} \in C$. Thus, taking $k$ large enough, we see that $\tau_C(e) = 0$. Using the relation $\epsilon = \mathrm{tr} + \sum_{C \neq \{1\}} \tau_C$, we conclude that tr is $\{0,1\}$-valued on the idempotents of $\mathbb{K}G$.

**(Zero characteristic claim)** Assume that, for infinitely many primes $p$, the following holds: the standard trace is $\{0,1\}$-valued on the idempotents of $\mathbb{K}G$, whenever $\mathbb{K}$ is a field of characteristic $p$. Then the standard trace is $\{0,1\}$-valued on the idempotents of $\mathbb{C}G$.

Arguing by contradiction, we assume that $e$ is an idempotent in $\mathbb{C}G$ with $e_1 = \mathrm{tr}(e) \notin \{0,1\}$. Let $A \subseteq \mathbb{C}$ be the subring generated by the support of $e$ together with $1/e_1$ and $1/(1-e_1)$, and view $e$ as an idempotent in the group ring $AG$. By part (v) of Lemma 3.2, for all but finitely many primes $p$ there is a quotient map $A \twoheadrightarrow \mathbb{K}$, $a \mapsto \overline{a}$, onto a field of characteristic $p$. Note that $\overline{e}_1 \neq 0, 1$ in $\mathbb{K}$, since $e_1$ and $1 - e_1$ are invertible in $A$. The induced ring homomorphism $AG \to \mathbb{K}G$ sends $e$ to an idempotent $\overline{e}$ in $\mathbb{K}G$ with $\mathrm{tr}(\overline{e}) \neq 0, 1$, thereby contradicting our hypothesis.

The proof of Theorem 4.1 is concluded by invoking Kaplansky's theorem.

## NOTES

**Platonov's theorem.** Besides the Russian original [4], the only other source in the literature for Platonov's theorem appears to be the presentation by Wehrfritz in *Infinite linear groups. An account of the group-theoretic properties of infinite groups of matrices* (Springer 1973). The proof presented herein seems considerably simpler. It is mainly influenced by the discussion of Mal'cev's theorem in lecture notes by Stallings (*Commutative rings and groups*, UC Berkeley 2000), and it has a certain degree of similarity with Platonov's own arguments in [4].

**Selberg's lemma.** It is important to note that Selberg's lemma is just a minor step in Selberg's paper [5], whose true importance is that it started the rich stream of rigidity results for lattices in higher rank. An alternative road to Selberg's lemma is to use valuations. This is the approach taken by Cassels in *Local fields* (Cambridge University Press 1986), and by Ratcliffe in *Foundations of hyperbolic manifolds* (2nd edition, Springer 2006).

**The Idempotent Conjecture.** The Idempotent Conjecture is usually attributed to Kaplansky, but a reference seems elusive. What Kaplansky did state on more than one occasion (Problem 1, p.122 in *Fields and rings*, The University of Chicago Press 1969; Problem 6, p.448 in Amer. Math. Monthly 1970) is a problem nowadays referred to as the **Zero-Divisor Conjecture**: if $G$ is a torsion-free group and $\mathbb{K}$ is a field, then the group algebra $\mathbb{K}G$ has no zero-divisors, i.e., $ab \neq 0$ whenever $a, b \neq 0$ in $\mathbb{K}G$. The Zero-Divisor Conjecture over the complex field, which clearly implies the Idempotent Conjecture, is still not settled for the class of (torsion-free) linear groups.

**Kaplansky's theorem.** We refer to Burger and Valette (J. Lie Theory 1998) for a proof, as well as for a nice complementary reading. The main insight of Kaplansky's analytic proof is to pass from the group algebra $\mathbb{C}G$ to a completion afforded by the regular representation on $\ell^2 G$. One can use the weak completion, that is the von Neumann algebra $\mathrm{L}G$, or the norm completion, the so-called reduced $\mathrm{C}^*$-algebra $\mathrm{C}^*_r G$. Kaplansky's proof, while remarkable in itself, is perhaps more important for suggesting what came to be known as the **Kadison Conjecture**: for every torsion-free group $G$, the reduced $\mathrm{C}^*$-algebra $\mathrm{C}^*_r G$ has no non-trivial idempotents. At the time of writing, the Kadison Conjecture for the class of (torsion-free) linear groups is still open.

**Bass's theorem.** As we have seen, the step from Formanek's criterion to the theorem of Bass is rather short, and it uses results on linear groups which were known - certainly on the eastern side of the Iron Curtain, but probably also on its western side - at the time of [2]. Ascribing the theorem to Bass *and* Formanek is therefore not entirely unwarranted. The hard facts, however, are that Bass actually proves much more in [1] whereas Formanek states less in [2].

## REFERENCES

[1] H. Bass: *Euler characteristics and characters of discrete groups*, Invent. Math. 35 (1976), 155–196
[2] E. Formanek: *Idempotents in Noetherian group rings*, Canad. J. Math. 25 (1973), 366–369
[3] A.I. Mal'cev: *On isomorphic matrix representations of infinite groups of matrices* (Russian), Mat. Sb. 8 (1940), 405–422 & Amer. Math. Soc. Transl. (2) 45 (1965), 1–18
[4] V.P. Platonov: *A certain problem for finitely generated groups* (Russian), Dokl. Akad. Nauk BSSR 12 (1968), 492–494
[5] A. Selberg: *On discontinuous groups in higher-dimensional symmetric spaces*, in "Contributions to Function Theory", Tata Institute of Fundamental Research, Bombay (1960), 147–164

MATHEMATISCHES INSTITUT, GEORG-AUGUST UNIVERSITÄT GÖTTINGEN
*E-mail address*: bogdan.nica@gmail.com