

参赛学生姓名： 邓柏勋 (Baixun Deng)

中学： 东莞翰林实验学校国际部

省份： 广东

国家/地区： 中国南方

指导老师姓名： 晏雨铮

指导老师单位： Boston College

论文题目： Representation dimensions and
the order of finite kernels

Representation dimensions and the order of finite kernels

Baixun Deng

September 14, 2026

Abstract

Let K be a nontrivial normal p -subgroup of a finite group E , where p is an odd prime and K is generated by its commutators with E . Let d be the least dimension of a nontrivial simple representation of E/K over $\mathbb{F}_p$. We prove that $|K| \geq (\exp K)^d$. If equality holds, the subgroups of K normal in E form a chain. Under conjugation, its successive quotients are isomorphic nontrivial simple representations of E/K , all of dimension d . For each prime $p \geq 5$, we construct kernels attaining the bound at every exponent p^e , with $e \geq 1$, over the fixed quotient $\mathrm{PSL}_2(\mathbb{F}_p)$.

Keywords: finite p -groups; Frattini filtration; representation dimensions; group extensions.

Contents

1	Introduction	2
2	Preliminaries	3
2.1	Groups and homomorphisms	3
2.2	The Frattini filtration	3
2.3	Modules and group actions	4
3	The exponent drop and the order bound	5
4	Equality in the order bound	10
5	A family attaining the bound	12
	References	16

1 Introduction

We study the least possible order of a finite p -group kernel when its exponent and quotient are fixed. We give a lower bound using the dimensions of representations of the quotient.

Let p be an odd prime, let K be a nontrivial normal p -subgroup of a finite group E , and write $G = E/K$. Write $\exp K$ for the exponent of K , the least positive integer m such that $x^m = 1$ for every $x \in K$.

We assume $[K, E] = K$: the kernel is generated by its commutators with E . This condition rules out a nontrivial quotient of K on which the induced conjugation action of E is trivial.

These assumptions imply that G is not a p -group, as explained after Lemma 3.1. Thus G has a nontrivial simple representation over the field $\mathbb{F}_p$ of p elements by [3, Corollary 6.2.2]. Let d be the least dimension of such a representation. We prove the following bound.

Theorem 1.1. *Under these assumptions,*

$$|K| \geq (\exp K)^d. \quad (1)$$

If equality holds, Proposition 4.1 shows that the subgroups of K normal in E form a chain. Its successive quotients are nontrivial simple G -modules of dimension d . By Proposition 4.2, these quotients are isomorphic.

We construct examples that attain equality for a fixed quotient. Fix a prime $p \geq 5$ and let $G = \mathrm{PSL}_2(\mathbb{F}_p)$. Section 5 shows that $d = 3$. For each integer $e \geq 1$, Theorem 1.1 gives $|K| \geq p^{3e}$ for an extension satisfying our hypotheses with $\exp K = p^e$. Proposition 5.3 constructs such an extension with $|K| = p^{3e} = (\exp K)^d$. Thus p^{3e} is the least possible kernel order for this exponent and quotient. The group G remains fixed as e varies.

By Proposition 4.1, the chain for each of these kernels has e successive quotients. When $e = 1$, the kernel is its only layer and is abelian. For $e \geq 2$, the commutator calculation at the end of Section 5 proves it is nonabelian.

Section 2 gives the definitions and standard results used in the proofs. Section 3 uses Lemma 3.3 to prove the bound. This lemma also follows from Sambonet's exponent and lifting results (2015) [5, Theorem B(ii), Lemma C(i), §3.1]; we give a direct proof by commutators and induction.

For the equality case, the proof of Proposition 4.2 uses the power-map theorem of Glasby–Pálffy–Schneider (2011), recorded in [4, Lemma 2.3, p. 1830]. The proof checks its hypotheses for quotients formed from two consecutive steps of the chain.

2 Preliminaries

2.1 Groups and homomorphisms

Throughout, p is an odd prime, $\mathbb{Z}$ is the ring of integers, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and all groups are finite. We write $L \leq H$ for a subgroup and $L < H$ for a proper subgroup. The symbol 1 denotes the identity element, and also the subgroup consisting only of that element. The order $|H|$ of a group H is its number of elements. For $L \leq H$, the index $[H : L]$ is the number of left cosets $hL = \{h\ell : \ell \in L\}$ in H . A p -group has order p^n for some integer $n \geq 0$; a group is nontrivial if its order exceeds 1.

For a subset S of a group, $\langle S \rangle$ denotes the smallest subgroup containing S . For subgroups $A, B \leq H$, their product is the set $AB = \{ab : a \in A, b \in B\}$. The **commutator** of x and y is $[x, y] = x^{-1}y^{-1}xy$. We write $[H, J] = \langle [x, y] : x \in H, y \in J \rangle$ for subgroups H, J of the same group. A subgroup N of H is normal, written $N \triangleleft H$, if $hNh^{-1} = N$ for every $h \in H$. For normal N , the quotient group H/N consists of cosets hN , with multiplication $(hN)(kN) = hkN$ and identity N . A proper subgroup is maximal if it is contained in no larger proper subgroup. A family of subgroups is a **chain** if any two are comparable by inclusion. A group is **simple** if it is nontrivial and its only normal subgroups are 1 and the whole group.

A group homomorphism $f : H \rightarrow J$ is a map satisfying $f(xy) = f(x)f(y)$ for $x, y \in H$. A bijective homomorphism is an isomorphism; $H \cong J$ means that such a map exists. An automorphism of P is an isomorphism from P to itself. Write $\text{Aut}(P)$ for the group of these maps under composition. A subgroup $N \leq P$ is characteristic in P if $\alpha(N) = N$ for every automorphism $\alpha : P \rightarrow P$.

The order of a group element x is the least positive integer m with $x^m = 1$.

A group H is **abelian** if $xy = yx$ for all $x, y \in H$, and nonabelian otherwise. Its **derived subgroup** is $H' = [H, H]$. Write H^p for the subgroup generated by its p th powers. The center of H is $Z(H) = \{z \in H : zh = hz \text{ for every } h \in H\}$. A subgroup of H is central if it lies in $Z(H)$. For subgroups $A, B \leq H$, we say that A **centralizes** B if $ab = ba$ for every $a \in A$ and $b \in B$; equivalently, $[A, B] = 1$.

Homomorphisms preserve powers and commutators [1, 1.4.1(i), p. 18; §2.3, p. 56]. For a homomorphism $f : H \rightarrow J$, its image is $\text{im } f = f(H)$ and its kernel is $\ker f = \{h \in H : f(h) = 1\}$. For subgroups $H_1, H_2 \leq H$, we have

$$f(H_1^p) = f(H_1)^p, \quad f([H_1, H_2]) = [f(H_1), f(H_2)]. \quad (2)$$

The fixed extension. For the groups in Theorem 1.1, use the exact sequence

$$1 \longrightarrow K \longrightarrow E \longrightarrow G \longrightarrow 1 \quad (3)$$

Here $K \rightarrow E$ is the inclusion, and $E \rightarrow G$ is surjective with kernel K . Thus G is identified with E/K .

By Lagrange's theorem [1, 1.3.6, p. 11], every element order in K is a power of p . Their least common multiple is therefore the largest element order and equals $\exp K$. Write $\exp K = p^e$, with $e \geq 1$ since $K \neq 1$.

2.2 The Frattini filtration

For a p -group P , the **Frattini subgroup** $\Phi(P)$ is the intersection of its maximal proper subgroups, with $\Phi(1) = 1$. Automorphisms permute maximal subgroups, so $\Phi(P)$ is characteristic in P .

For a finite p -group P , Burnside's basis theorem [1, Theorem 5.3.2, p. 140] gives

$$\Phi(P) = P^p[P, P]. \quad (4)$$

In particular, $P/\Phi(P)$ is elementary abelian: it is abelian and every element has p th power 1. An elementary abelian p -group is an $\mathbb{F}_p$ -vector space, with addition given by the group operation and scalar multiplication by repeated addition. For the same reason, an additive subgroup of an $\mathbb{F}_p$ -vector space is an $\mathbb{F}_p$ -subspace. For $N \triangleleft P$, apply (2) to the projection $P \rightarrow P/N$. Burnside's formula for P/N then gives

$$\Phi(P/N) = \Phi(P)N/N. \quad (5)$$

Fratini's nongenerator theorem [1, Theorem 5.2.12, p. 135] gives

$$J \leq P, \quad J\Phi(P) = P \implies J = P. \quad (6)$$

Thus elements whose images span $P/\Phi(P)$ generate P .

Set $\Phi^0(P) = P$ and $\Phi^{j+1}(P) = \Phi(\Phi^j(P))$. Repeated use of (4) gives $x^{p^j} \in \Phi^j(P)$ for $x \in P$ and $j \geq 0$. Indeed, this holds for $j = 0$, and the p th power of an element of $\Phi^j(P)$ lies in $\Phi^{j+1}(P)$. For $j \geq 0$, define $K_j = \Phi^j(P)$. The descending chain $K = K_0 \geq K_1 \geq \dots$ is the **Fratini filtration** of K . Its j -th **Fratini layer** is the quotient $V_j = K_j/K_{j+1}$; in particular, the zeroth layer is $V_0 = K/\Phi(K)$.

A subgroup characteristic in a characteristic subgroup of K is characteristic in K . A characteristic subgroup of a normal subgroup is normal [1, 1.5.6(ii)–(iii), p. 28]. Applying these facts successively shows that every K_j is characteristic in K and normal in E .

2.3 Modules and group actions

A field has *characteristic* p if p is the least positive integer for which the sum of p copies of 1 is 0. In particular, $\mathbb{F}_p$ has characteristic p .

For a group G , an $\mathbb{F}_p G$ -module is a vector space over $\mathbb{F}_p$ with a linear action of G ; this is also called a representation of G over $\mathbb{F}_p$. Here an action means that each map $v \mapsto g \cdot v$ is linear, $1 \cdot v = v$, and $(gh) \cdot v = g \cdot (h \cdot v)$. All modules here are finite-dimensional. A submodule is an invariant subspace, meaning a linear subspace preserved by every group element. A **simple module** is nonzero and has no proper nonzero submodule. An action is trivial if every group element acts as the identity, and nontrivial otherwise.

If W is a submodule of an $\mathbb{F}_p H$ -module V , the **quotient module** V/W has cosets $v + W$, the induced vector-space operations, and action $h \cdot (v + W) = h \cdot v + W$. This action is well-defined because $h \cdot W = W$. For $\mathbb{F}_p H$ -modules V and U , a module homomorphism $f : V \rightarrow U$ is an $\mathbb{F}_p$ -linear map satisfying $f(h \cdot v) = h \cdot f(v)$ for all $h \in H$ and $v \in V$. A bijective module homomorphism is a **module isomorphism**. We write $V \cong U$ when such a map exists, and $V \xrightarrow{\sim} U$ for such a map.

For an $\mathbb{F}_p H$ -module V , write $\rho_V : H \rightarrow \text{GL}_{\mathbb{F}_p}(V)$ for the action homomorphism, so $\rho_V(h)(v) = h \cdot v$. Here $\text{GL}_{\mathbb{F}_p}(V)$ is the group of invertible $\mathbb{F}_p$ -linear maps from V to itself. The **kernel of the action** is

$$\ker \rho_V = \{h \in H : h \cdot v = v \text{ for every } v \in V\}.$$

Burnside's formula (4) makes each V_j an $\mathbb{F}_p$ -vector space. Since K_j and K_{j+1} are normal in E , conjugation induces the action $h \cdot (xK_{j+1}) = h x h^{-1} K_{j+1}$ for $h \in E$ and $x \in K_j$.

A **composition series** of a module M is a chain $0 = M_0 < M_1 < \dots < M_t = M$ of submodules with simple quotients M_i/M_{i-1} ; these quotients are its **composition factors**. Every finite-dimensional module has a composition series. To obtain one, take maximal

proper submodules one after another. Each step lowers the dimension, so the process ends at 0; read this chain in reverse order. For such a series, $\dim M = \sum_{i=1}^t \dim(M_i/M_{i-1})$.

For a finite group H , write $O_p(H)$ for its largest normal p -subgroup. By [3, Corollary 6.2.2], the common kernel of the actions of H on all simple $\mathbb{F}_p H$ -modules is

$$\bigcap_{\substack{V \text{ simple} \\ \mathbb{F}_p H\text{-module}}} \ker \rho_V = O_p(H).$$

Since G is not a p -group, $O_p(G) \neq G$. If every simple $\mathbb{F}_p G$ -module were trivial, each action would have kernel G , contrary to this equality. Thus a nontrivial simple $\mathbb{F}_p G$ -module exists. We write the least dimension of such a module as

$$\delta_p(G) = \min\{\dim_{\mathbb{F}_p} V : V \text{ is a nontrivial simple } \mathbb{F}_p G\text{-module}\}. \quad (7)$$

Thus $d = \delta_p(G)$ in Theorem 1.1.

An E -module **descends to** $G = E/K$ if K acts trivially. The G -action is then $(hK) \cdot v = h \cdot v$. This is independent of the representative h , because every $k \in K$ fixes every vector: $(hk) \cdot v = h \cdot (k \cdot v) = h \cdot v$. The two actions give the same linear transformations, so they have the same invariant subspaces and are trivial at the same time. Thus descent preserves simplicity and nontriviality.

For the conjugation action on V_j , an element $k \in K$ fixes xK_{j+1} exactly when $x^{-1}kxk^{-1} = [x, k^{-1}] \in K_{j+1}$. Since $[k, x] = [x, k]^{-1}$, all elements of K act trivially exactly when $[K, K_j] \leq K_{j+1}$. Burnside's formula ensures $[K_j, K_j] \leq K_{j+1}$, which makes conjugation by K_j trivial. Thus V_0 always descends to G ; for $j > 0$, elements of K outside K_j may still act nontrivially.

Every simple composition factor of V_j descends to G . Indeed, $K \leq O_p(E)$ because K is a normal p -subgroup of E . The common-kernel theorem therefore shows that K acts trivially on every simple $\mathbb{F}_p E$ -module [3, Corollary 6.2.2].

An action of a group A on a group N by automorphisms is a homomorphism $A \rightarrow \text{Aut}(N)$. Write $a(n)$ for the image of n under the automorphism assigned to a . Define the action commutator subgroup by $[N, A] = \langle n^{-1}a(n) : n \in N, a \in A \rangle$. For conjugation, $a(n) = ana^{-1}$ and $n^{-1}a(n) = [n, a^{-1}]$. As a runs through A , so does a^{-1} ; hence this gives the same subgroup as the commutator notation above.

If N and M have A -actions, a homomorphism $f : N \rightarrow M$ is **A -equivariant** when $f(a(n)) = a(f(n))$. For each action commutator, $f(n^{-1}a(n)) = f(n)^{-1}a(f(n))$. Taking the subgroups generated by these elements gives $f([N, A]) = [f(N), A]$. Equivariance also makes the kernel and image A -invariant: $f(a(n)) = a(f(n))$ is 1 when $f(n) = 1$, and lies in $f(N)$ for every n . If a normal subgroup $L \triangleleft N$ is A -invariant, the induced action on N/L is $a(nL) = a(n)L$ [1, §1.5, "Operator Groups," p. 29]. For an E -invariant quotient K/L , triviality of the induced action means $k^{-1}hkh^{-1} \in L$ for every $k \in K$ and $h \in E$. Thus $[K, E] \leq L$. Under our assumption $[K, E] = K$, this forces $L = K$, which explains the condition in the introduction.

3 The exponent drop and the order bound

To prove Theorem 1.1, it is enough to show $\dim_{\mathbb{F}_p} V_j \geq d$ for every $0 \leq j < e$. The product of the orders of these layers is $|K/K_e|$, so these inequalities give $|K| \geq |K/K_e| \geq p^{ed}$. Every simple factor of V_j descends to G by Section 2, so one nontrivial simple factor in each layer suffices.

If all factors of V_j were trivial, each map $v \mapsto h \cdot v - v$ would send every term of a composition series into the preceding term. Proposition 3.5 uses this fact to show that the image of E on V_j is a p -group. Lemma 3.4 would then give $\exp K \mid p^j$, contradicting $\exp K = p^e$.

Lemma 3.1. *If a finite p -group A acts on a finite p -group N , then*

$$[N, A] = N \implies N = 1. \quad (8)$$

Proof. Suppose $N \neq 1$. Since $\Phi(N)$ is characteristic in N , the A -action induces an action on the vector space $N/\Phi(N)$ from (4). If $N = \Phi(N)$, then (6), with $J = 1$, would give $N = 1$. Thus this module is nonzero. Choose a maximal proper submodule M of $N/\Phi(N)$, which exists by finite dimension. Then $W = (N/\Phi(N))/M$ is a nonzero simple module by the submodule correspondence [1, 1.4.6, p. 20; §1.5, p. 29].

Since A is a p -group, its largest normal p -subgroup is $O_p(A) = A$. By [3, Corollary 6.2.2], every element of $O_p(A)$ acts as the identity on every simple $\mathbb{F}_p A$ -module. Applying this to W gives $aw = w$ for all $a \in A$ and $w \in W$.

Let $q : N \rightarrow W$ be the composite of the two quotient maps, with W written additively. Since q respects the A -action, for $n \in N$ and $a \in A$ we have

$$q(n^{-1}a(n)) = -q(n) + aq(n) = -q(n) + q(n) = 0.$$

Thus $[N, A] \leq \ker q$. The map q is onto and $W \neq 0$, so $\ker q$ is a proper subgroup of N . Hence $[N, A] \neq N$. $\square$

This lemma shows that $G = E/K$ in our fixed extension cannot be a p -group. Otherwise, the index formula [1, 1.3.5, p. 11] would give $|E| = |K||G|$, making E a p -group. Apply the lemma to the conjugation action of E on K . Since $[K, E] = K$, it would give $K = 1$, contrary to our assumption.

A central Frattini subgroup makes the p th-power map a homomorphism.

Lemma 3.2. *Let P be a finite p -group with p odd and $\Phi(P) \leq Z(P)$. Then $x \mapsto x^p$ is a homomorphism from P into $\Phi(P)$:*

$$(xy)^p = x^p y^p \quad (x, y \in P). \quad (9)$$

Proof. Burnside's formula (4) shows that both P' and P^p lie in $Z(P)$. For central commutators, the identity $[y, x]^p = [y^p, x]$ holds [1, Exercise 5.1.4, p. 128]. Since y^p is central, $[y, x]^p = 1$. Since $P' \leq Z(P)$, [1, 5.3.5, pp. 141–142] gives

$$(xy)^p = x^p y^p [y, x]^{\binom{p}{2}}.$$

Since p is odd, $\binom{p}{2} = p(p-1)/2$ is divisible by p . Since $[y, x]^p = 1$, the commutator factor is therefore 1, and the image lies in $P^p \leq \Phi(P)$. $\square$

The assumption that p is odd removes the commutator factor. Lemmas 3.3 and 3.4 use this identity to prove Theorem 1.1.

More generally, a central term $\Phi^j(P)$ makes the higher power map $x \mapsto x^{p^j}$ a homomorphism. The next lemma also follows from Sambonet's exponent and lifting results [5, Theorem B(ii), Lemma C(i), §3.1; author version, pp. 4–5, 8]. We give a direct proof by induction.

Lemma 3.3. *Let P be a finite p -group, with p odd. If $\Phi^j(P) \leq Z(P)$ for an integer $j \geq 0$, then*

$$P \longrightarrow Z(P), \quad x \longmapsto x^{p^j}, \quad (10)$$

is a homomorphism commuting with every automorphism of P .

Proof. When $j = 0$, the hypothesis is $P = Z(P)$ and the map is the inclusion. The case $j = 1$ is Lemma 3.2.

Suppose $j \geq 2$ and the assertion holds for $j - 1$. Let $N = \Phi(P)$. Since $\Phi^{j-1}(N) = \Phi^j(P) \leq Z(P)$, this subgroup also lies in $Z(N)$. The induction hypothesis applied to N gives a homomorphism $n \mapsto n^{p^{j-1}}$. Its image lies in $\Phi^{j-1}(N) \leq Z(P)$ by (4). This gives

$$f : N \longrightarrow Z(P), \quad f(n) = n^{p^{j-1}}.$$

Conjugation by P preserves N and powers, so $f(x^{-1}nx) = x^{-1}f(n)x$ for $n \in N$ and $x \in P$. Since $f(N) \leq Z(P)$, we obtain

$$f([n, x]) = f(n)^{-1}x^{-1}f(n)x = 1.$$

Thus $[N, P] \leq \ker f$.

Since $N = \Phi(P)$ is normal in P , each commutator $[n, x]$ with $n \in N$ and $x \in P$ lies in N , so $[N, P] \leq N$. Conjugation by P preserves N and P , and hence preserves $[N, P]$ by (2). Thus $[N, P]$ is normal in P . The quotient $P/[N, P]$ has Frattini subgroup $N/[N, P]$ by (5), applied to the normal subgroup $[N, P] \leq N$. The subgroup $N/[N, P]$ is central in $P/[N, P]$, because $[n, x] \in [N, P]$ for every $n \in N$ and $x \in P$. Lemma 3.2 therefore gives

$$(xy)^p \equiv x^p y^p \pmod{[N, P]} \quad (x, y \in P).$$

Both $(xy)^p$ and $x^p y^p$ lie in $N = \Phi(P)$. The congruence means that $(x^p y^p)^{-1}(xy)^p \in [N, P] \leq \ker f$. Applying f gives $f((xy)^p) = f(x^p y^p)$, so

$$(xy)^{p^j} = f((xy)^p) = f(x^p y^p) = f(x^p)f(y^p) = x^{p^j}y^{p^j}.$$

For every $x \in P$, we have $x^p \in N$, so $x^{p^j} = f(x^p) \in Z(P)$. For an automorphism α of P , the identity $\alpha(x^{p^j}) = \alpha(x)^{p^j}$ shows that this homomorphism commutes with α . $\square$

For a finite p -group P , Hall's theorem [1, Theorem 5.3.3, p. 140] states that

$$\ker(\text{Aut}(P) \longrightarrow \text{Aut}(P/\Phi(P))) \quad \text{is a } p\text{-group.} \quad (11)$$

For $P = K_j$, the quotient $P/\Phi(P)$ is V_j . The map from the image of E on K_j to its image on V_j has kernel contained in the p -group in (11). The next proof uses this map to compare the two action images.

Lemma 3.4 (Exponent drop). *If the image of E on V_j is a p -group for some $j \geq 0$, then $\exp K$ divides p^j .*

Proof. Let $\rho : E \rightarrow \text{Aut}(K_j)$ be the conjugation map and write $A = \rho(E)$. Here $V_j = K_j/\Phi(K_j)$ is the zeroth Frattini layer of K_j . Write $U = \ker(\text{Aut}(K_j) \rightarrow \text{Aut}(V_j))$ for the subgroup of automorphisms acting trivially on this layer. Hall's theorem (11) makes U a p -group. The kernel of the restricted action $A \rightarrow \text{Aut}(V_j)$ is $A \cap U$, a p -group by Lagrange's theorem [1, 1.3.6, p. 11].

The first isomorphism theorem [1, 1.4.3, p. 19] gives

$$|A| = |A \cap U| |\text{im}(A \rightarrow \text{Aut}(V_j))|.$$

This action image equals the image of E on V_j , since $\rho : E \rightarrow A$ is onto. Both factors are therefore powers of p , so A is a p -group.

To prove that K centralizes K_j , let $B = \rho(K)$. Since $K \triangleleft E$ and $\rho : E \rightarrow A$ is onto, $B \triangleleft A$ by the normal-subgroup correspondence [1, 1.4.6, p. 20]. Equation (2) gives $[B, A] = \rho([K, E]) = \rho(K) = B$. Lemma 3.1, applied to the conjugation action of A on its normal subgroup B , gives $B = 1$. Thus K acts trivially on K_j , which means $K_j \leq Z(K)$.

Since $K_j = \Phi^j(K) \leq Z(K)$, Lemma 3.3 gives a homomorphism $f : K \rightarrow Z(K)$, $f(x) = x^{p^j}$. Since K is normal in E , conjugation by each element of E is an automorphism of K . Thus f is E -equivariant. Write $Z = f(K) \leq Z(K)$ for its image. This image lies in K_j , since successive p th powers enter successive Frattini subgroups by (4). The image Z is E -invariant because f is E -equivariant.

The equivariant commutator identity gives

$$[Z, E] = [f(K), E] = f([K, E]) = f(K) = Z.$$

Each $a \in A$ equals $\rho(h)$ for some $h \in E$. Since $Z \leq K_j$ is E -invariant, a preserves Z and acts on it by restriction: $a(z) = hzh^{-1}$. Thus A and E induce the same automorphisms of Z , so $[Z, A] = [Z, E] = Z$. Lemma 3.1, applied to A acting on Z , gives $Z = 1$. Thus $x^{p^j} = 1$ for every $x \in K$, as required. $\square$

If all simple factors of V_j are trivial, the image of E on V_j is a p -group.

Proposition 3.5. *For every $0 \leq j < e$, the layer V_j has a nontrivial simple E -composition factor. This factor descends to G and has dimension at least d .*

Proof. Fix $0 \leq j < e$. If $V_j = 0$, the image of E on V_j is trivial. Lemma 3.4 would then give $\exp K \mid p^j$, contrary to $\exp K = p^e$. Thus $V_j \neq 0$. Suppose that all composition factors of V_j were trivial. Choose a composition series with r factors:

$$0 = W_0 < W_1 < \cdots < W_r = V_j.$$

Since $V_j \neq 0$, we have $r \geq 1$. Each W_i is an E -submodule, and E acts trivially on W_i/W_{i-1} .

For $h \in E$, define the linear map

$$N_h : V_j \longrightarrow V_j, \quad N_h(v) = h \cdot v - v.$$

Since h acts trivially on W_i/W_{i-1} , we have $N_h(W_i) \subseteq W_{i-1}$. Applying N_h successively gives $N_h^r(V_j) \subseteq W_0 = 0$, so $N_h^r = 0$. Here powers of a linear map mean repeated composition.

Choose an integer $m \geq 0$ with $p^m \geq r$, and write id for the identity map on V_j . This map commutes with N_h . The binomial formula in characteristic p therefore gives $(\text{id} + N_h)^p = \text{id} + N_h^p$: for $0 < t < p$, the coefficient $\binom{p}{t}$ is divisible by p , since p divides $p!$ but not $t!(p-t)!$. Repeating the identity m times gives

$$\rho_{V_j}(h)^{p^m} = (\text{id} + N_h)^{p^m} = \text{id} + N_h^{p^m} = \text{id}.$$

Thus every element of the image of E on V_j has p -power order. Cauchy's theorem states that a prime dividing the order of a finite group is the order of some element of that group [1, Theorem 1.6.17, p. 40]. A prime other than p dividing the order of this image would therefore contradict the preceding conclusion. Hence the image is a p -group.

Lemma 3.4 would give $\exp K \mid p^j$, contrary to $\exp K = p^e$ and $j < e$. Thus a nontrivial simple factor exists. The normal p -subgroup K acts trivially on it by [3, Corollary 6.2.2], so the factor descends to a nontrivial simple G -module, as explained in Section 2. Its dimension is therefore at least d by (7). $\square$

Proof of Theorem 1.1. Proposition 3.5 gives the required nontrivial simple composition factor in each V_j with $j < e$. The index formula $[H : L] = [H : J][J : L]$ for $L \leq J \leq H$ [1, 1.3.5, p. 11], applied along the Frattini chain, gives

$$|K| = \left(\prod_{j=0}^{e-1} |V_j| \right) |K_e|. \quad (12)$$

Dimension is the sum of the dimensions of the composition factors. Proposition 3.5 therefore gives $\dim V_j \geq d$, and hence $|V_j| = p^{\dim V_j} \geq p^d$. Since $|K_e| \geq 1$, equation (12) gives the bound (1). $\square$

Comparison with the zeroth layer. Proposition 3.5, applied at $j = 0$, gives $|K/\Phi(K)| \geq p^d$. Choose $x \in K$ of order p^e , which exists by the exponent calculation in Section 2, and write $\langle x \rangle$ for the cyclic subgroup it generates.

Burnside's formula (4) gives $K^p \leq \Phi(K)$, so $x^p \in \Phi(K)$. Therefore

$$(x\Phi(K))^p = x^p\Phi(K) = \Phi(K).$$

Thus the image of x in $K/\Phi(K)$ has order dividing p . The restriction of the quotient map to $\langle x \rangle$ has kernel $\langle x \rangle \cap \Phi(K)$, so the first isomorphism theorem [1, 1.4.3, p. 19] gives

$$|\langle x \rangle \cap \Phi(K)| = \frac{|\langle x \rangle|}{|K/\Phi(K)|} \geq p^{e-1}.$$

Since this intersection is contained in $\Phi(K)$, index multiplication [1, 1.3.5, p. 11] gives

$$|K| = |K/\Phi(K)| |\Phi(K)| \geq p^d p^{e-1} = p^{e+d-1}.$$

The preceding calculation uses the dimension bound only for V_0 . Proposition 3.5 gives $\dim V_j \geq d$ for every $0 \leq j < e$, and Theorem 1.1 therefore yields $|K| \geq p^{ed}$. The ratio of the two lower bounds is

$$\frac{p^{ed}}{p^{e+d-1}} = p^{(e-1)(d-1)}.$$

Thus Theorem 1.1 gives a strictly stronger lower bound when $e > 1$ and $d > 1$. The two bounds coincide when $e = 1$ or $d = 1$.

4 Equality in the order bound

Assume throughout this section that $|K| = p^{ed}$.

Proposition 4.1. *Each V_j , for $0 \leq j < e$, is a nontrivial simple G -module of dimension d . The subgroups of K normal in E are exactly*

$$K = K_0 > K_1 > \cdots > K_e = 1. \quad (13)$$

Proof. By Proposition 3.5, each $|V_j| \geq p^d$ for $0 \leq j < e$. Since $|K| = p^{ed}$, the product formula (12) forces $K_e = 1$ and $\dim V_j = d$ for every such j . The nontrivial simple factor supplied by Proposition 3.5 has dimension at least d . Since the factor dimensions are positive and sum to d , there is only one factor, namely V_j itself. Proposition 3.5 therefore also shows that K acts trivially on V_j , so V_j is a nontrivial simple G -module.

Let $1 \neq N \leq K$ be normal in E . Since $K_0 = K$ and $K_e = 1$, there is a largest $j < e$ such that $N \leq K_j$. Maximality gives $N \not\leq K_{j+1}$, so its image NK_{j+1}/K_{j+1} in V_j is nonzero. This image is an $\mathbb{F}_p$ -subspace by Section 2. It is E -invariant because N is normal in E , and hence is a G -submodule because the action descends to G . Simplicity gives $NK_{j+1}/K_{j+1} = V_j$, so $NK_{j+1} = K_j$. Since $K_{j+1} = \Phi(K_j)$, apply (6) with $P = K_j$ and $J = N$ to get $N = K_j$. Conversely every K_j is characteristic in K and normal in E . This proves (13). $\square$

To compare adjacent layers, we use the power-map theorem of Glasby–Pálffy–Schneider (2011), recorded in [4, Lemma 2.3, p. 1830]. It applies to groups of exponent p^2 with exactly one proper nontrivial characteristic subgroup. We check these hypotheses for K_j/K_{j+2} and obtain the isomorphism below.

Proposition 4.2. *The maps*

$$V_j \xrightarrow{\sim} V_{j+1}, \quad xK_{j+1} \mapsto x^p K_{j+2} \quad (0 \leq j < e-1) \quad (14)$$

are G -module isomorphisms. Thus all $V_0, \dots, V_{e-1}$ are isomorphic.

Proof. Fix $0 \leq j < e-1$, and let $Q = K_j/K_{j+2}$. Apply (5) to K_j and its normal subgroup K_{j+2} . Since $\Phi(K_j) = K_{j+1}$, it gives $\Phi(Q) = K_{j+1}/K_{j+2}$, an elementary abelian group. The subgroup correspondence identifies subgroups of Q with subgroups of K_j containing K_{j+2} , and it preserves E -invariance [1, 1.4.6, p. 20; §1.5, p. 29]. Every characteristic subgroup of Q is preserved by all automorphisms induced from E . Its preimage in K_j is therefore E -invariant, which means that it is normal in E . By Proposition 4.1, this preimage must be K_{j+2} , K_{j+1} , or K_j .

The characteristic subgroups of Q are therefore exactly 1, $\Phi(Q) = K_{j+1}/K_{j+2}$, and Q . The middle one is proper and nontrivial.

Every p th power in Q lies in $\Phi(Q)$, which has exponent p , so $\exp Q \mid p^2$. If $\exp Q = p$, then $K_j^p \leq K_{j+2}$. For every $x \in K$, repeated use of (4) gives $x^{p^j} \in K_j$. The assumption $K_j^p \leq K_{j+2}$ then gives

$$x^{p^j} \in K_j \implies x^{p^{j+1}} \in K_{j+2} \implies x^{p^{e-1}} \in K_e = 1.$$

The last implication uses $e-j-2$ further p th powers, each entering the next Frattini subgroup by (4). When $j = e-2$, no further power is needed because $K_{j+2} = K_e$. Thus every element of K has order dividing p^{e-1} , contrary to $\exp K = p^e$. Hence $\exp Q = p^2$.

For a finite p -group with p odd, exponent p^2 , and a unique proper nontrivial characteristic subgroup, the power-map theorem [4, Lemma 2.3, p. 1830] gives an $\mathbb{F}_p \text{Aut}(Q)$ -module isomorphism

$$Q/\Phi(Q) \longrightarrow \Phi(Q), \quad x\Phi(Q) \mapsto x^p.$$

Our group Q satisfies these hypotheses. For $x \in K_j$, the third isomorphism theorem [1, 1.4.5, pp. 19–20] identifies the class $(xK_{j+2})\Phi(Q)$ in $Q/\Phi(Q)$ with xK_{j+1} in V_j . Also $(xK_{j+2})^p = x^pK_{j+2}$ in $\Phi(Q) = V_{j+1}$. Thus the cited power map gives exactly (14). Conjugation by E induces automorphisms of Q , so the resulting isomorphism is E -equivariant. By Proposition 4.1, K acts trivially on both layers. Their actions therefore factor through $G = E/K$, and the same map is the G -module isomorphism (14). When $e = 1$, there is only one layer and no map to construct. $\square$

A nonzero class remains nonzero under successive power isomorphisms.

Corollary 4.3. *For $0 \leq j < e$, one has $K_j^p = K_{j+1}$. Every element of $K_j \setminus K_{j+1}$ has order p^{e-j} .*

Proof. For $0 \leq j < e - 1$ and $y \in K_{j+1}$, surjectivity in Proposition 4.2 gives $x \in K_j$ with $yK_{j+2} = x^pK_{j+2}$. Thus $y \in K_j^pK_{j+2}$. Both factors lie in K_{j+1} , since $K_j^p \leq K_{j+1}$ by (4) and $K_{j+2} \leq K_{j+1}$ by definition. Therefore $K_j^pK_{j+2} = K_{j+1}$. Apply (6) with $P = K_{j+1}$ and $J = K_j^p$. As $\Phi(P) = K_{j+2}$, it gives $K_j^p = K_{j+1}$. For $j = e - 1$, Burnside's formula (4) gives $K_{e-1}^p \leq \Phi(K_{e-1}) = K_e = 1$, so $K_{e-1}^p = K_e$. When $e = 1$ only this case occurs. In particular $\Phi(K) = K^p$.

If $x \in K_j \setminus K_{j+1}$, its class in V_j is nonzero. Successive isomorphisms in (14) show that $x^{p^{e-j-1}}$ has nonzero class in K_{e-1}/K_e . Since $K_e = 1$, this element is not the identity. Its p th power lies in $K_e = 1$ by (4). Thus $x^{p^{e-j-1}} \neq 1$ and $x^{p^{e-j}} = 1$, so x has order p^{e-j} . $\square$

For $1 \leq j \leq e$, repeated use of (5) gives $\Phi^i(K/K_j) = K_i/K_j$ for $0 \leq i \leq j$. The quotients between consecutive Frattini subgroups are therefore isomorphic to $V_0, \dots, V_{j-1}$, and $\Phi^j(K/K_j) = 1$.

Corollary 4.4. *For $1 \leq j \leq e$, the kernel K/K_j has exponent p^j and order p^{jd} . The induced extension*

$$1 \longrightarrow K/K_j \longrightarrow E/K_j \longrightarrow G \longrightarrow 1$$

has minimum kernel order among extensions of G satisfying the same commutator condition and having p -group kernel exponent at least p^j .

Proof. Since $K_j \leq K$ and K_j is normal in E , the map

$$E/K_j \longrightarrow G = E/K, \quad hK_j \longmapsto hK,$$

is well-defined and onto: replacing h by hk with $k \in K_j$ does not change hK , and every coset hK has a preimage hK_j . Its value is the identity exactly when $h \in K$, so its kernel is the subgroup K/K_j . This proves exactness of the sequence in the statement.

For $1 \leq j \leq e$, Proposition 4.1 gives

$$|K/K_j| = \prod_{i=0}^{j-1} |V_i| = p^{jd}.$$

For every $x \in K$, repeated use of (4) gives $x^{p^j} \in K_j$, so every element of K/K_j has order dividing p^j . Choose $x \in K \setminus K_1$. The successive maps in (14) give $x^{p^{j-1}} \in K_{j-1} \setminus K_j$; for $j = 1$, this is simply the choice of x . Hence xK_j has order p^j , proving that $\exp(K/K_j) = p^j$. Apply (2) to $E \rightarrow E/K_j$ to obtain

$$[K/K_j, E/K_j] = [K, E]K_j/K_j = K/K_j.$$

Any other kernel satisfying the hypotheses, of exponent p^a with $a \geq j$, has order at least $p^{ad} \geq p^{jd}$ by Theorem 1.1. Thus p^{jd} is the minimum kernel order. $\square$

5 A family attaining the bound

For a commutative ring R with identity, write $M_2(R)$ for its 2×2 matrix ring and $\det A$ for the determinant of a matrix A . Write $\mathrm{SL}_2(R)$ for the group of matrices in $M_2(R)$ with determinant one. Write I for the identity matrix and E_{ij} for the matrix with entry 1 in position (i, j) and zero elsewhere. Write $\mathrm{diag}(a, b)$ for the diagonal matrix with entries a, b , and set $D = \mathrm{diag}(1, -1)$. The trace $\mathrm{tr}(A)$ of $A \in M_2(R)$ is the sum of its diagonal entries. Write $\mathrm{GL}_n(\mathbb{F}_p)$ for the group of invertible $n \times n$ matrices over $\mathbb{F}_p$.

Homomorphisms to abelian groups. Every homomorphism $f : H \rightarrow A$ to an abelian group annihilates H' :

$$H' \leq \ker f. \quad (15)$$

This is the abelian-quotient property [2, Theorem 2.23, p. 33; Theorem 2.24, p. 35]. Write $\mathbb{F}_p^\times$ for the group of nonzero field elements under multiplication. In particular, when $H' = H$, every one-dimensional representation is trivial, since $\mathrm{GL}_1(\mathbb{F}_p) = \mathbb{F}_p^\times$ is abelian.

For any representation $\rho : H \rightarrow \mathrm{GL}_n(\mathbb{F}_p)$, determinant multiplicativity makes $\det \circ \rho : H \rightarrow \mathbb{F}_p^\times$ a homomorphism [1, §1.4, “Examples of Homomorphisms,” p. 18]. Applying (15) to this map gives

$$H' = H \implies \det \rho(h) = 1 \quad \text{for every } h \in H.$$

Fix $p \geq 5$ and set $G = \mathrm{PSL}_2(\mathbb{F}_p) = \mathrm{SL}_2(\mathbb{F}_p)/\{I, -I\}$. Let V be the space of matrices in $M_2(\mathbb{F}_p)$ with trace zero; these are called traceless matrices. Each has a unique expression $aD + bE_{12} + cE_{21}$ with $a, b, c \in \mathbb{F}_p$, so D, E_{12}, E_{21} form a basis and $\dim_{\mathbb{F}_p} V = 3$. Conjugation acts by $A \mapsto gAg^{-1}$ for $g \in \mathrm{SL}_2(\mathbb{F}_p)$. The identity $\mathrm{tr}(BC) = \mathrm{tr}(CB)$ gives $\mathrm{tr}(gAg^{-1}) = \mathrm{tr}(Ag^{-1}g) = \mathrm{tr}(A)$, so this action preserves V . A scalar matrix is a multiple of I . The matrices I and $-I$ commute with every matrix, so they act trivially. The two representatives g and $-g$ of an element of G give the same action, since $(-g)A(-g)^{-1} = gAg^{-1}$. Thus conjugation defines an action of G on V .

Lemma 5.1. *For $p \geq 5$, the conjugation module V is nontrivial and simple, and $\delta_p(G) = 3$.*

Proof. Since $p \geq 5$, the Jordan–Moore theorem shows that G is simple [2, Theorem 8.13, p. 225]. Let $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and let t be its image in G . Since $w^2 = -I$ and $w \notin \{I, -I\}$, the element t has order 2. The identity

$$w(I + E_{12})w^{-1} = I - E_{21}$$

shows that t does not commute with the image of $I + E_{12}$: the matrix $I - E_{21}$ is neither $I + E_{12}$ nor $-(I + E_{12})$. Thus t is noncentral and G is nonabelian. The derived subgroup G' is normal and nontrivial [2, Theorem 2.23, p. 33]; simplicity therefore gives $G' = G$.

Equation (15) makes every one-dimensional representation trivial. Suppose that $\rho : G \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$ were nontrivial. The kernel of a homomorphism is normal, and a homomorphism is injective exactly when its kernel is trivial [1, 1.4.1(ii), 1.4.2(i), p. 18]. Since ρ is nontrivial, its kernel is not G . Simplicity therefore gives $\ker \rho = 1$, so ρ is faithful (injective). Applying (15) to the determinant gives $\rho(G) \leq \mathrm{SL}_2(\mathbb{F}_p)$.

A field is algebraically closed if every nonconstant polynomial over it has a root in the field. Over such a field of characteristic p , an invertible matrix of finite order relatively prime to p is diagonalizable, meaning diagonal in a suitable basis [3, Corollary 2.1.7].

Let $T \in \mathrm{SL}_2(\mathbb{F}_p)$ be an involution, meaning an element of order 2. Since p is odd, this order is coprime to p . The cited criterion makes T diagonalizable over an algebraically closed field containing $\mathbb{F}_p$. Since $T^2 = I$, its eigenvalues lie in $\{1, -1\}$. Their product is $\det T = 1$, so they are both 1 or both -1 . By diagonalizability, $T = I$ or $T = -I$. As T has order 2, it follows that $T = -I$. Thus $-I$ is the only involution in $\mathrm{SL}_2(\mathbb{F}_p)$.

A faithful ρ would send the involution t to $-I$: it preserves the order of t , and $-I$ is the only involution in $\mathrm{SL}_2(\mathbb{F}_p)$. Then $\rho([t, g]) = I$ for every $g \in G$ because $-I$ is central. Injectivity gives $[t, g] = 1$ for every g , contrary to the noncentrality of t proved above. Hence every representation of G of dimension one or two is trivial. The involution t also shows that G is not a p -group, by Lagrange's theorem [1, 1.3.6, p. 11].

The action on V is nontrivial because it moves $D \in V$. Since $E_{12}^2 = 0$, the inverse of $I + E_{12}$ is $I - E_{12}$, and

$$(I + E_{12})D(I - E_{12}) = D - 2E_{12} \neq D.$$

The inequality holds because p is odd, so $2 \neq 0$ in $\mathbb{F}_p$.

Suppose $0 < W < V$ is invariant. Both W and V/W have dimension one or two, so the preceding argument shows that G acts trivially on them. Every element of G fixes W pointwise. Triviality on V/W means that $gv - v \in W$ for every $g \in G$ and $v \in V$. Thus, for $g, h \in G$, the vectors $hv - v$ and $gv - v$ are fixed by every element of G . By linearity,

$$g(hv) = gv + (hv - v) = hv + (gv - v) = h(gv).$$

Hence the action maps commute, so their image is an abelian group. Since $G' = G$, equation (15) would make every element of G act as the identity on V , contrary to the calculation with D . Thus V is simple. Together with the exclusion of dimensions one and two, this gives $\delta_p(G) = 3$. $\square$

Fix $e \geq 1$ and write $R_{e+1} = \mathbb{Z}/p^{e+1}\mathbb{Z}$ for the ring of integers modulo p^{e+1} . The multiples of successive powers of p form the chain

$$R_{e+1} \supsetneq pR_{e+1} \supsetneq \cdots \supsetneq p^e R_{e+1} \supsetneq p^{e+1} R_{e+1} = 0.$$

For matrices over R_{e+1} , the notation $A \equiv B \pmod{p^a}$ means that every entry of $A - B$ lies in $p^a R_{e+1}$.

For $1 \leq a \leq e + 1$, let P_a be the **congruence subgroup** of $\mathrm{SL}_2(R_{e+1})$ consisting of matrices entrywise congruent to I modulo p^a . It is the kernel of entrywise reduction to $\mathrm{SL}_2(\mathbb{Z}/p^a\mathbb{Z})$, so it is normal. Let $K = P_1$. Since $p^{e+1}R_{e+1} = 0$, we have $P_{e+1} = 1$. The next lemma determines the e quotients P_a/P_{a+1} , indexed by $1 \leq a \leq e$.

Lemma 5.2. *The group K has order p^{3e} and exponent p^e . Its Frattini filtration is given by $\Phi^j(K) = P_{j+1}$ for $0 \leq j \leq e$. Under conjugation by $\mathrm{SL}_2(R_{e+1})$, each quotient P_a/P_{a+1} , for $1 \leq a \leq e$, is the module V , with the action through entrywise reduction modulo p , followed by the quotient map $\mathrm{SL}_2(\mathbb{F}_p) \rightarrow G$.*

Proof. For $1 \leq a \leq e$, write an element of P_a as $I + p^a A$, with $A \in M_2(R_{e+1})$. Two choices of A differ entrywise by multiples of p^{e+1-a} . Since $a \leq e$, they have the same reduction modulo p . Multiplication and determinant give a map

$$P_a/P_{a+1} \longrightarrow V, \quad (I + p^a A)P_{a+1} \longmapsto A \pmod{p}. \quad (16)$$

In $(I + p^a A)(I + p^a B)$, the term $p^{2a}AB$ vanishes modulo p^{a+1} because $2a \geq a + 1$. Thus multiplication adds the coefficients of p^a . Also $\det(I + p^a A) = 1 + p^a \mathrm{tr}(A) + p^{2a} \det(A)$, which reduces to $1 + p^a \mathrm{tr}(A)$ modulo p^{a+1} . Since the determinant equals 1, we have $p^a \mathrm{tr}(A) \equiv 0 \pmod{p^{a+1}}$, so $\mathrm{tr}(A) \equiv 0 \pmod{p}$.

The resulting homomorphism $P_a \rightarrow V$ has kernel P_{a+1} : its value is zero exactly when $A \equiv 0 \pmod{p}$, or equivalently $I + p^a A \equiv I \pmod{p^{a+1}}$. Multiplying a representative by an element of P_{a+1} therefore does not change its image, so (16) is well-defined.

To see surjectivity, use $I + p^a E_{12}$, $I + p^a E_{21}$, and $\text{diag}(1 + p^a, (1 + p^a)^{-1})$. Since $1 + p^a$ is coprime to p^{e+1} , it is invertible in R_{e+1} , so the diagonal matrix is defined. The identity $(1 + p^a)(1 - p^a) = 1 - p^{2a}$ gives $(1 + p^a)^{-1} \equiv 1 - p^a \pmod{p^{a+1}}$. Thus the three images are the basis vectors E_{12} , E_{21} , and D , respectively. The image is an additive subgroup of V and hence an $\mathbb{F}_p$ -subspace, so the map is onto. The first isomorphism theorem [1, 1.4.3, p. 19] now identifies P_a/P_{a+1} with V . For $g \in \text{SL}_2(R_{e+1})$, we have

$$g(I + p^a A)g^{-1} = I + p^a(gAg^{-1}).$$

Thus the induced action on $A \bmod p$ is conjugation by $g \bmod p$. Since I and $-I$ act trivially on V , this is precisely the action through G stated in the lemma. Each of the e quotients has order p^3 , and $P_{e+1} = 1$; index multiplication [1, 1.3.5, p. 11] gives $|K| = p^{3e}$.

For any $A \in M_2(\mathbb{Z})$ and $a \geq 1$, the binomial formula gives

$$(I + p^a A)^p \equiv I + p^{a+1} A \pmod{p^{a+2}}. \quad (17)$$

For $2 \leq t < p$, the prime p divides $\binom{p}{t}$, since it divides $p!$ but not $t!(p-t)!$. Thus the term $\binom{p}{t} p^{at} A^t$ is divisible by p^{at+1} , and $at + 1 \geq a + 2$ because $a \geq 1$. The term with $t = p$ is divisible by p^{ap} . Since p is odd, $p \geq 3$ and hence $ap \geq a + 2$. This last inequality fails for $p = 2$ at $a = 1$. For $I + p^a A \in P_a$, apply this congruence to an integer representative of A and reduce to R_{e+1} . This gives $P_a^p \leq P_{a+1}$ for $1 \leq a \leq e$.

For the reverse inclusion, fix $1 \leq a < e$ and write $y = I + p^{a+1} B \in P_{a+1}$. Since $B \bmod p \in V$ and (16) is onto, there is $x = I + p^a A \in P_a$ with $A \equiv B \pmod{p}$. Equation (17) then gives $x^p \equiv y \pmod{p^{a+2}}$, so $x^{-p} y \in P_{a+2}$. Thus $P_{a+1} = P_a^p P_{a+2}$ for $1 \leq a < e$. The power formula gives $P_e^p = P_{e+1} = 1$. For the descending induction on a , suppose $P_{a+1}^p = P_{a+2}$. Then $P_{a+2} \leq P_a^p$ because $P_{a+1} \leq P_a$. Substituting this containment into $P_{a+1} = P_a^p P_{a+2}$ gives $P_a^p = P_{a+1}$.

Since $P_a/P_{a+1} \cong V$ is abelian, (15) applied to the projection gives $[P_a, P_a] \leq P_{a+1}$. The product of the layer orders gives $|P_a| = p^{3(e+1-a)}$, so each P_a is a finite p -group. Burnside's formula (4) therefore gives $\Phi(P_a) = P_a^p [P_a, P_a] = P_{a+1}$ for $1 \leq a \leq e$. Starting from $K = P_1$ and iterating gives $\Phi^j(K) = P_{j+1}$ for $0 \leq j \leq e$. For $x \in K = P_1$, induction gives $x^{p^j} \in P_{j+1}$ for $0 \leq j \leq e$. Since $P_{e+1} = 1$, we obtain $\exp K \mid p^e$. The matrix $I + pE_{12}$ has order p^e : its m th power is $I + mpE_{12}$, which equals I in $M_2(R_{e+1})$ exactly when $p^e \mid m$. $\square$

Proposition 5.3. *For $p \geq 5$ and $e \geq 1$, let $E = \text{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z})/\{I, -I\}$. Entrywise reduction modulo p induces an exact sequence*

$$1 \longrightarrow K \longrightarrow E \longrightarrow G \longrightarrow 1 \quad (18)$$

with $[K, E] = K$, $\exp K = p^e$, and $|K| = p^{3e} = (\exp K)^{\delta_p(G)}$.

Proof. The entrywise reduction map

$$\text{SL}_2(R_{e+1}) \longrightarrow \text{SL}_2(\mathbb{F}_p), \quad (a_{ij}) \longmapsto (a_{ij} \bmod p),$$

is onto. Let $A \in \text{SL}_2(\mathbb{F}_p)$. Choose an integer representative of each entry of A , and view the resulting matrix $\tilde{A}$ over R_{e+1} . Then $\tilde{A} \bmod p = A$.

Let $u = \det \tilde{A} \in R_{e+1}$. Since $\det A = 1$, we have $u \equiv 1 \pmod{p}$. An integer representative of u is therefore coprime to p^{e+1} , so u has an inverse in R_{e+1} . Define

$$B = \tilde{A} \begin{pmatrix} u^{-1} & 0 \\ 0 & 1 \end{pmatrix}.$$

This multiplies the first column of $\tilde{A}$ by u^{-1} , so $\det B = u u^{-1} = 1$. Also $u^{-1} \equiv 1 \pmod{p}$, so the diagonal matrix reduces to I and $B \bmod p = A$. Thus $B \in \mathrm{SL}_2(R_{e+1})$ is a preimage of A .

Let $q : \mathrm{SL}_2(R_{e+1}) \rightarrow E$ be the quotient map. For $A \in \mathrm{SL}_2(R_{e+1})$, its class is $q(A) = \{A, -A\}$; in particular, $q(A) = q(-A)$. Reduction sends $\{I, -I\}$ to $\{I, -I\}$, so it induces a surjection $\pi : E \rightarrow G$ given by

$$\pi(q(A)) = (A \bmod p)\{I, -I\}.$$

Since p is odd, $-I$ is not congruent to I modulo p , so $K \cap \{I, -I\} = \{I\}$. Thus q is injective on K . Its restriction to K is the map $K \rightarrow E$ in (18).

The identity of G is the coset $\{I, -I\}$. Hence $q(A) \in \ker \pi$ exactly when $A \bmod p$ is I or $-I$. If $A \bmod p = I$, then $A \in K$. If $A \bmod p = -I$, then $-A \bmod p = I$, so $-A \in K$; since $q(-A) = q(A)$, the same class again lies in $q(K)$. Conversely, every matrix in K reduces to I , so its class lies in $\ker \pi$. Therefore $\ker \pi = q(K)$, proving exactness of (18). We identify K with this normal subgroup of E through the injection $q|_K$.

By Lemma 5.2, the action on $K/\Phi(K)$ is the conjugation action of G on V . This module is simple and nontrivial by Lemma 5.1. The span of $\{gv - v : g \in G, v \in V\}$ is nonzero because the action is nontrivial. It is invariant: $h(gv - v) = (hgh^{-1})(hv) - hv$ for $g, h \in G$. Simplicity therefore makes this span all of V .

To identify the image of $[K, E]$, let v be the image of $k \in K$ under $K \rightarrow K/\Phi(K) \cong V$, and let $g \in G$ be the image of $h \in E$. Then the image of $[k, h^{-1}] = k^{-1}hkh^{-1}$ in V is $-v + gv$. Since $K \rightarrow V$ and $E \rightarrow G$ are onto, these are exactly the vectors $gv - v$. Their additive subgroup is their $\mathbb{F}_p$ -span, so the image of $[K, E]$ is all of V . Hence $[K, E]\Phi(K) = K$.

Apply (6) with $P = K$ and $J = [K, E]$ to obtain $[K, E] = K$. The order and exponent follow from Lemma 5.2, and the least dimension is 3 by Lemma 5.1. $\square$

For $e \geq 2$, the identities $E_{12}^2 = E_{21}^2 = 0$ give $(I + pE_{12})^{-1} = I - pE_{12}$ and $(I + pE_{21})^{-1} = I - pE_{21}$. Multiplication gives

$$[I + pE_{12}, I + pE_{21}] = \begin{pmatrix} 1 + p^2 + p^4 & p^3 \\ -p^3 & 1 - p^2 \end{pmatrix} \equiv I + p^2 D \pmod{p^3},$$

so the $(1, 1)$ -entry of this commutator minus I is congruent to p^2 modulo p^3 and is nonzero. Hence the commutator is nonidentity in $\mathrm{SL}_2(R_{e+1})$ for $e \geq 2$, and K is nonabelian.

References

- [1] D. J. S. Robinson. *A Course in the Theory of Groups*, second edition. Graduate Texts in Mathematics, vol. 80. Springer, 1996. [doi:10.1007/978-1-4419-8594-1](https://doi.org/10.1007/978-1-4419-8594-1). [Public copy of the second edition](#).
- [2] J. J. Rotman. *An Introduction to the Theory of Groups*, fourth edition. Graduate Texts in Mathematics, vol. 148. Springer, 1995. [doi:10.1007/978-1-4612-4176-8](https://doi.org/10.1007/978-1-4612-4176-8). [Public copy of the fourth edition](#).
- [3] P. Webb. *A Course in Finite Group Representation Theory*. Cambridge University Press, 2016. [doi:10.1017/CBO9781316677216](https://doi.org/10.1017/CBO9781316677216). [Public author text](#). The source links use this version, whose pagination differs from the published book; the [author confirms](#) that its mathematical content is the same.
- [4] S. P. Glasby, F. A. M. Ribeiro, and C. Schneider. Duality between p -groups with three characteristic subgroups and semisimple anti-commutative algebras. *Proceedings of the Royal Society of Edinburgh A* **150** (2020), no. 4, 1827–1852. [doi:10.1017/prm.2018.159](https://doi.org/10.1017/prm.2018.159). [Published text](#).
- [5] N. Sambonet. The unitary cover of a finite group and the exponent of the Schur multiplier. *Journal of Algebra* **426** (2015), 344–364. [doi:10.1016/j.jalgebra.2014.12.013](https://doi.org/10.1016/j.jalgebra.2014.12.013). [Public author version](#): [arXiv:1312.5196](https://arxiv.org/abs/1312.5196). The source links use the 2013 author version and its page numbering.