THE CAYLEY–HAMILTON ANALOGUE FOR FREE GROUPS FAILS IN RANKS THREE AND FOUR, AND ONLY ONE POWER WORKS IN RANK TWO

KOREA SUPERINTELLIGENCE LABS

Abstract. Problem 17.32 of the *Kourovka Notebook*, proposed by O. V. Bogopolski, asks whether the free group F_n obeys the Cayley–Hamilton pattern: if $w \in F_n$ and $\varphi \in \operatorname{Aut} F_n$ satisfy $\langle w, \varphi(w), \dots, \varphi^n(w)\rangle = F_n$, must already $\langle w, \varphi(w), \dots, \varphi^{n-1}(w)\rangle = F_n$? Two independent solutions appeared in August 2026 and are recorded in the Notebook's answer line; both refute the assertion at $n = 2$ and say nothing about any larger rank. We give explicit counterexamples at $n = 3$ and $n = 4$. Both are built from the rank-two automorphism $\varphi(x) = yx$, $\varphi(y) = x$ by adjoining generators that φ either fixes (rank three) or transposes (rank four), and each is certified on both sides: explicit words exhibiting every free generator, and an explicit homomorphism to a permutation group under which the initial segment of the orbit fixes a point that some free generator moves. We also settle, for the rank-two data of the two published solutions, every exponent at once: $\langle w, \varphi^k(w)\rangle = F_2$ holds if and only if $k = 2$, the index of the abelianised pair being the Fibonacci number $F(k)$; the two published solutions record only the cases $k = 1$ and $k = 2$. A complementary observation explains why the rank-two failure needs a non-abelian witness at all: no abelian quotient can detect it. Every theorem, proposition, corollary and lemma below is machine-checked in Lean 4 against Mathlib, by kernel evaluation only; Section 8 says exactly what is and what is not formalised. Whether Problem 17.32 fails for every $n \geq 2$ remains open.

1. Introduction

The problem. Let F_n denote the free group of rank n. For $\varphi \in \operatorname{Aut} F_n$, $w \in F_n$ and $k \geq 0$ write

$$O_k(\varphi, w) \;=\; \{\, w,\ \varphi(w),\ \varphi^2(w),\ \dots,\ \varphi^k(w) \,\}$$

for the first $k+1$ points of the orbit of w under φ. Over the free abelian group the question of how much of such an orbit is needed to generate has a classical answer. If $\alpha \in \mathrm{GL}(n, \mathbb{Z})$ and $v \in \mathbb{Z}^n$, the Cayley–Hamilton theorem writes $\alpha^n(v)$ as an integral combination of $v, \alpha(v), \dots, \alpha^{n-1}(v)$; so the last vector of the longer list is redundant, and $v, \alpha(v), \dots, \alpha^n(v)$ generate $\mathbb{Z}^n$ only if $v, \alpha(v), \dots, \alpha^{n-1}(v)$ already do. Problem 17.32 of the *Kourovka Notebook* [5], proposed by O. V. Bogopolski, asks whether the free group behaves in the same way. We quote it as it stands in the current edition, version 46 of the e-print. In the Notebook's source the problem number is preceded by a bold superscript star and the answer beneath it is opened by a second superscript star, the two separated by a short rule; the preface of issue 21 does not say what the star means, so we reproduce the typography without interpreting it.

> *__17.32.__ Is the following analogue of the Cayley–Hamilton theorem true for the free group F_n of rank n: If $w \in F_n$ and $\varphi \in \operatorname{Aut} F_n$ are such that $\langle w, \varphi(w), \dots, \varphi^n(w)\rangle = F_n$, then $\langle w, \varphi(w), \dots, \varphi^{n-1}(w)\rangle = F_n$? *O. V. Bogopolski*

---

* No, it is not true ((V. Ionin, A. Semidetnov, *Preprint*, 2026, `https://arxiv.org/pdf/2608.29219`); O. Kharlampovich, *Preprint*, 2026, `https://kourovkanotebookorg.wordpress.com/wp-content/uploads/2026/08/kourovka_14_23_17_32_note_with_problem_authors.pdf`).

Write CH(n) for the assertion inside the question: for all $\varphi \in \operatorname{Aut} F_n$ and all $w \in F_n$, if $\langle O_n(\varphi, w)\rangle = F_n$ then $\langle O_{n-1}(\varphi, w)\rangle = F_n$. So CH($n$) is a statement about $n+1$ elements of F_n failing to be reducible to n of them, and the analogous statement for $\mathbb{Z}^n$ is a theorem.

What was known. Two solutions appeared within days of each other in August 2026, and the Notebook's answer line cites exactly those two and nothing else. Ionin and Semidetnov [2] take $F_2 = \langle x, y\rangle$, $w = xy$ and $\varphi(x) = yx$, $\varphi(y) = x$, and answer: *"No. The assertion fails for $n = 2$."* The note [3] linked from the same answer line gives the same example in the mirrored basis — $F_2 = \langle a, b\rangle$, $\varphi(a) = b$, $\varphi(b) = ab$, $w = ba$, which is the above under $a \mapsto y$, $b \mapsto x$ — and states *"Problem 17.32 has a negative answer. In fact, the assertion fails for $n = 2$."* Neither source treats any rank above two, and neither considers any power of φ beyond the second. So what the literature settles is exactly $\neg\,$CH(2).

Results. The rank-two example is not an isolated accident of small rank, and the same germ of an automorphism refutes CH(3) and CH(4) once the extra generators are handled correctly. Throughout, φ denotes the automorphism determined on the first two free generators by $\varphi(x) = yx$, $\varphi(y) = x$ — the automorphism of [2] — and the counterexamples differ only in how φ is extended to the remaining generators.

- *Rank three* (Theorem 4.3). In $F_3 = \langle x, y, z\rangle$ take $\varphi(z) = z$ and $w = xyz$. Then $\langle w, \varphi(w), \varphi^2(w)\rangle \neq F_3$ while $\langle w, \varphi(w), \varphi^2(w), \varphi^3(w)\rangle = F_3$. Properness is witnessed by a homomorphism onto S_3; generation by explicit words in the four elements.
- *Rank four* (Theorem 5.5). Padding by two *fixed* generators does not work (Remark 5.1). What works is to *move* them: in $F_4 = \langle x, y, z, t\rangle$ take $\varphi(z) = t$, $\varphi(t) = z$ and again $w = xyz$. Then $\langle w, \ldots, \varphi^3(w)\rangle \neq F_4$ while $\langle w, \ldots, \varphi^4(w)\rangle = F_4$, with properness witnessed by a homomorphism to S_4 whose image lies in the alternating group A_4 (and in fact equals it, Remark 5.3).
- *Exponents in rank two* (Theorem 6.3). For the data of [2] and [3], $\langle w, \varphi^k(w)\rangle = F_2$ holds if and only if $k = 2$, for every $k \geq 1$. The two published solutions record the cases $k = 1$ (their counterexample) and $k = 2$ (their generation half) and no others. The mechanism for $k \geq 3$ is abelian and quantitative: in the abelianisation φ acts by the Fibonacci matrix, w and $\varphi^k(w)$ have exponent-sum vectors $(1, 1)$ and $(F(k+2), F(k+1))$, and the subgroup of $\mathbb{Z}^2$ they span has index $F(k)$, which is 1 exactly for $k = 1, 2$.

Alongside these we record a complementary observation (Proposition 3.8) which is easy but explains the shape of every argument in the subject: for the rank-two data, *no* abelian quotient can detect the failure at $k = 1$. For every commutative group A and every homomorphism $\rho\colon F_2 \to A$ one has $\langle \rho(w), \rho(\varphi(w))\rangle = \rho(F_2)$. That is the abelian Cayley–Hamilton statement doing its work, and it is why the rank-two solution needs the non-abelian quotient S_3 while the exponents $k \geq 3$ need nothing beyond $\mathbb{Z}$.

What is not claimed. We do not claim that CH(n) fails for every $n \geq 2$; that remains open, and Section 7 explains why the padding constructions used here do not obviously continue. We do not claim minimality of any witness: not of the words w, not of the automorphisms, not of the groups S_3 and A_4 used to detect properness. Rank five is discussed in Section 7 as a computation only: counterexamples there were found by search but none has been formalised, and no statement about rank five is made in this paper. Finally, the rank-two material of Section 3 is not new mathematics; it is [2] and [3] replayed as a machine-checked development, both because the later sections build on it and because it fixes the conventions in which the new results are stated.

Related work, and where this sits. Formal verification has recently been applied to this problem collection. Van Doorn, Judin, Monticone and Morrison [9] present solutions to eight Kourovka problems, stating that all of them were autonomously discovered and formally verified in Lean by Aristotle, a formal reasoning agent developed by Harmonic; Problem 17.32 is not among the eight. The solution of 17.32 in [2] was, by the authors' own account, found with the assistance of a large

language model and checked by the authors by hand; it is not accompanied by a formal verification. Koch-Hyde and Olive [4] treat two further problems about subgroups of free groups by Stallings foldings, and do not touch 17.32. The present paper therefore does two different things at once, and we separate them: Section 3 is a formalisation of a known answer, while Sections 4–6 are new mathematics that happens also to be formalised.

Provenance of the source text. One point of bibliographic hygiene is worth recording, because it changes what counts as new. The Kourovka Notebook is a living document: [5] is issue 21, whose e-print is updated in place. The answer line quoted above entered with version 46, posted on 1 September 2026: version 45, posted on 3 July 2026, carries 17.32 with no star and no answer line at all — as an open problem — and so does the copy of the Notebook held in a full-text snapshot of arXiv sources taken before that date. Anyone grading the novelty of a rank-two counterexample against such a snapshot would conclude, wrongly, that the rank-two case was open. Everything said above about what the literature contains was therefore checked against the live e-print, retrieved together with both cited preprints on 3 September 2026 and read in full. Both refute CH(2) and neither says anything about a larger rank or a larger power.

For the record, and because a negative should say what was looked at rather than merely that nothing was found, these are the other passes we made, all on 3 September 2026. Three queries against the arXiv search interface: `all:"Kourovka Notebook"`, whose thirty most recent hits contain no treatment of 17.32 beyond [2] (its neighbours being [9] and [4]); `abs:"Cayley-Hamilton" AND abs:"free group"`, which returns nothing; and `all:"Problem 17.32"`, which returns nothing. Then a full-text snapshot of arXiv sources (369 files, 86 GB of LaTeX). The string *Kourovka* matches 1,221 lines in 192 of the files, resolving to 509 distinct papers. The phrase *analogue of the Cayley* or *analog of the Cayley* matches 86 lines in the whole snapshot, 28 of which concern a Cayley–Hamilton theorem, and exactly one of those 28 is about free groups: Problem 17.32 itself, inside the snapshot's own copy of [5]. The remaining 27 are about matrix algebras, quantum matrix algebras and Yangians, Jordan and quaternion algebras, tropical matrices, left-symmetric algebras, and non-commutative and q-analogues. Finally the literal string `17.32` matches 5,509 lines in 1,328 distinct papers; intersected with the 509 Kourovka papers, exactly three papers contain both strings, and only two of the three are real — [5], which carries the problem and its author-index entry, and [2]. The third match is the coordinate `(91.12,17.32)` inside a picture environment of an unrelated paper. The note [3] is not on arXiv and so appears in none of this; it was retrieved from the address printed in the Notebook's answer line. Section 7 records the separate, mathematical searches that produced the witnesses below.

2. Preliminaries

Words and automorphisms. F_n is the free group on $x_1, \dots, x_n$; we write x, y, z, t for x_1, x_2, x_3, x_4 when $n \le 4$. Elements are identified with reduced words, and equality of elements is equality of reduced words. An endomorphism of F_n is determined by its values on the free generators, and is an automorphism as soon as some second endomorphism composes with it to the identity on both sides in either order; that is the only criterion used below, and in each case the inverse is exhibited.

The germ common to all three ranks is

$$\varphi(x) = yx, \qquad \varphi(y) = x,$$

with inverse $\varphi^{-1}(x) = y$, $\varphi^{-1}(y) = xy^{-1}$. Its abelianisation is the Fibonacci matrix $(\alpha, \beta) \mapsto (\alpha + \beta, \alpha)$.

Permutations. Permutations compose as functions, $(fg)(i) = f(g(i))$, and act on $\{1, \dots, m\}$. For a point p we write $\mathrm{Stab}(p)$ for its stabiliser in S_m. The convention matters only for printed cycle notation: with the opposite convention the value $\pi(w) = (1\,2)$ recorded in [2] would read $(1\,3)$, while the equality $\pi(w) = \pi(\varphi(w))$ that carries the argument holds either way. We use the function-composition convention, in which the printed values of [2] are reproduced verbatim.

The two certificates. Every generation and non-generation claim below is settled by an explicit finite certificate, of one of exactly two kinds.

Lemma 2.1 (generation)**.** *Let $S \subseteq F_n$. If every free generator x_i lies in $\langle S\rangle$, then $\langle S\rangle = F_n$.*

Proof. F_n is generated by $\{x_1, \dots, x_n\}$, so $F_n = \langle x_1, \dots, x_n\rangle \leq \langle S\rangle$. □

Lemma 2.2 (properness)**.** *Let $\rho\colon G \to H$ be a group homomorphism, $K \leq H$ a subgroup and $S \subseteq G$ a subset with $\rho(S) \subseteq K$. If $\rho(g) \notin K$ for some $g \in G$, then $\langle S\rangle \neq G$.*

Proof. $\rho^{-1}(K)$ is a subgroup containing S, hence containing $\langle S\rangle$, and it does not contain g. □

In every application below, H is a symmetric group of degree at most four and K is the stabiliser of a point, except in Section 6, where $H = \mathbb{Z}$ and K is a subgroup $m\mathbb{Z}$. Lemma 2.2 is not a restriction on what can be proved this way. M. Hall's separation theorem [1, Theorem 5.1] says that, given finitely many elements $\alpha_1, \dots, \alpha_m$ of a free group F and finitely many $\beta_1, \dots, \beta_t$ none of which lies in $\langle \alpha_1, \dots, \alpha_m\rangle$, there is a subgroup of finite index in F containing all the α_i and none of the β_j. Taking the α_i to be generators of a finitely generated proper subgroup and β_1 to be anything outside it, every such subgroup is contained in a proper subgroup of finite index, so a finite permutation witness always exists. What the sections below add is a witness small enough to write down — of degree 3, 3 and 4 in ranks two, three and four respectively.

Applying Lemma 2.1 requires writing each free generator as a word in the given set; applying Lemma 2.2 requires evaluating a handful of permutations on a handful of points. Both are finite computations of a size a reader can check by hand, and both are checked by the proof kernel in the formal development (Section 8).

3. The rank-two counterexample, replayed

Throughout this section $F_2 = \langle x, y\rangle$, $w = xy$, and φ is the germ of Section 2.

Proposition 3.1. *The endomorphism φ of F_2 with $\varphi(x) = yx$, $\varphi(y) = x$ is an automorphism, with inverse determined by $\varphi^{-1}(x) = y$ and $\varphi^{-1}(y) = xy^{-1}$; and $\varphi \neq \mathrm{id}$.*

Proof. Let ψ be the endomorphism with $\psi(x) = y$, $\psi(y) = xy^{-1}$. Both composites are checked on the two free generators: $\psi(\varphi(x)) = \psi(y)\psi(x) = xy^{-1} \cdot y = x$ and $\psi(\varphi(y)) = \psi(x) = y$; likewise $\varphi(\psi(x)) = \varphi(y) = x$ and $\varphi(\psi(y)) = \varphi(x)\varphi(y)^{-1} = yx \cdot x^{-1} = y$. Two endomorphisms agreeing on the free generators are equal, so $\psi\varphi = \varphi\psi = \mathrm{id}$. Finally $\varphi(x) = yx \neq x$. □

Proposition 3.2. *$\varphi(w) = yx^2$ and $\varphi^2(w) = xyxyx = w^2x$. Consequently $x = w^{-2}\varphi^2(w)$ and $y = x^{-1}w$, and therefore $\langle w, \varphi(w), \varphi^2(w)\rangle = F_2$.*

Proof. $\varphi(w) = \varphi(x)\varphi(y) = yx \cdot x = yx^2$, and $\varphi^2(w) = \varphi(y)\varphi(x)^2 = x \cdot yx \cdot yx = xyxyx$, which is $(xy)^2x = w^2x$. Solving gives the two displayed identities, and both x and y then lie in $\langle w, \varphi(w), \varphi^2(w)\rangle$; apply Lemma 2.1. (The generator $\varphi(w)$ is not used, which is Proposition 3.5 below.) □

Proposition 3.3. *Let $\pi\colon F_2 \to S_3$ be the homomorphism with $\pi(x) = (1\,2\,3)$ and $\pi(y) = (2\,3)$. Then $\pi(w) = \pi(\varphi(w)) = (1\,2)$, and consequently $\langle w, \varphi(w)\rangle \neq F_2$.*

Proof. $\pi(w) = (1\,2\,3)(2\,3) = (1\,2)$ and $\pi(\varphi(w)) = (2\,3)(1\,2\,3)^2 = (1\,2)$. Both fix the point 3, whereas $\pi(x) = (1\,2\,3)$ does not. Apply Lemma 2.2 with $K = \mathrm{Stab}(3)$. □

Theorem 3.4. CH(2) *is false: with φ and $w = xy$ as above, $\langle w, \varphi(w), \varphi^2(w)\rangle = F_2$ and $\langle w, \varphi(w)\rangle \neq F_2$. This is the answer to Problem 17.32 recorded in* [5] *and proved in* [2] *and* [3].

Proof. Combine Propositions 3.1, 3.2 and 3.3. □

The two halves of Theorem 3.4 isolate two different phenomena, and the following facts — all elementary, and recorded here because they bound what the argument shows — keep them apart.

Proposition 3.5. $\langle w, \varphi^2(w)\rangle = F_2$.

Proof. Immediate from the identities $x = w^{-2}\varphi^2(w)$ and $y = x^{-1}w$ of Proposition 3.2, which never mention $\varphi(w)$; apply Lemma 2.1. In the basis of [3] this is the displayed conclusion of its Proposition 1, with the identities $b = w^{-2}\varphi^2(w)$ and $a = \varphi^2(w)^{-1}w^3$ of its Remark 1. □

Proposition 3.6. $\pi\colon F_2 \to S_3$ *is surjective.*

Proof. A preimage of each of the six permutations is exhibited: $1, y, x, x^2, xy, x^2y$ map respectively to $\mathrm{id}, (2\,3), (1\,2\,3), (1\,3\,2), (1\,2), (1\,3)$. □

Proposition 3.7. *The following hold, and none is used in the proof of Theorem 3.4.*

1. $\langle x, \varphi(x)\rangle = F_2$*: properness in Proposition 3.3 is a property of the pair* $\{w, \varphi(w)\}$*, not of* φ*.*
2. $\pi(\varphi^2(w)) \notin \mathrm{Stab}(3)$*: the* S_3 *test of Proposition 3.3 genuinely fails on the third element, so it does not accidentally prove more than it should.*

Proof. For (1), $\varphi(x)x^{-1} = yx \cdot x^{-1} = y$, so x and y both lie in $\langle x, \varphi(x)\rangle$; apply Lemma 2.1. For (2), $\pi(\varphi^2(w)) = \pi(xyxyx) = (1\,2\,3)(2\,3)(1\,2\,3)(2\,3)(1\,2\,3) = (1\,2\,3)$, which moves 3. □

The last of these is the one that explains the shape of the whole subject.

Proposition 3.8. *For every commutative group* A *and every homomorphism* $\rho\colon F_2 \to A$*,*

$$\langle \rho(w),\ \rho(\varphi(w))\rangle \ =\ \rho(F_2).$$

No abelian quotient of F_2 *detects the properness of* $\langle w, \varphi(w)\rangle$*.*

Proof. Write $H = \langle \rho(w), \rho(\varphi(w))\rangle$. Since A is commutative, $\rho(\varphi(w))\rho(w)^{-1} = \rho(y)\rho(x)^2 \cdot \rho(y)^{-1}\rho(x)^{-1} = \rho(x)$, so $\rho(x) \in H$, and then $\rho(y) = \rho(x)^{-1}\rho(w) \in H$. As $\rho(F_2)$ is generated by $\rho(x)$ and $\rho(y)$, we get $\rho(F_2) \le H$; the reverse inclusion is clear. □

Proposition 3.8 is the abelian Cayley–Hamilton statement specialised to this pair, and it says that the non-abelian witness of Proposition 3.3 is not an artefact of the authors' choice: some non-abelian quotient is unavoidable.

4. Rank three

Let $F_3 = \langle x, y, z\rangle$, extend the germ by fixing the third generator, and take a word that uses it:

$$\varphi(x) = yx, \qquad \varphi(y) = x, \qquad \varphi(z) = z, \qquad w = xyz.$$

The inverse is $\varphi^{-1}(x) = y$, $\varphi^{-1}(y) = xy^{-1}$, $\varphi^{-1}(z) = z$, so $\varphi \in \mathrm{Aut}\, F_3$, and $\varphi \neq \mathrm{id}$. The first four points of the orbit are

$$w = xyz, \qquad \varphi(w) = yx^2z, \qquad \varphi^2(w) = xyxyxz, \qquad \varphi^3(w) = yx^2yx^2yxz.$$

Proposition 4.1. *Let* $\rho\colon F_3 \to S_3$ *be the homomorphism with* $\rho(x) = (2\,3)$ *and* $\rho(y) = \rho(z) = (1\,2)$*. Then* ρ *is surjective,*

$$\rho(w) = (2\,3), \qquad \rho(\varphi(w)) = \rho(\varphi^2(w)) = \mathrm{id},$$

all of which fix the point 1*, while* $\rho(y) = (1\,2)$ *does not. Consequently* $\langle w, \varphi(w), \varphi^2(w)\rangle \neq F_3$*.*

Proof. $\rho(w) = (2\,3)(1\,2)(1\,2) = (2\,3)$; $\rho(\varphi(w)) = (1\,2)(2\,3)(2\,3)(1\,2) = \mathrm{id}$; and $\varphi^2(w) = xyxyxz$ has ρ-image $\big((2\,3)(1\,2)\big)^3 = \mathrm{id}$, since $(2\,3)(1\,2)$ is a 3-cycle. Surjectivity is witnessed by $1, x, y, xy, yx, xyx$. Apply Lemma 2.2 with $K = \mathrm{Stab}(1)$. □

For the generating half, note that $w, \varphi(w), \varphi^2(w), \varphi^3(w)$ all end in the letter z, so the three elements

$$e_1 = w\,\varphi(w)^{-1}, \qquad e_2 = w\,\varphi^2(w)^{-1}, \qquad e_3 = w\,\varphi^3(w)^{-1}$$

lie in $\langle x, y\rangle$; explicitly $e_1 = xyx^{-2}y^{-1}$, and e_2, e_3 are the analogous cancellations.

Proposition 4.2. *With e_1, e_2, e_3 as above,*

$$x = e_2^{-1}e_2^{-1}e_3e_1^{-1}e_2^{-1}e_2^{-1}e_3, \qquad y = e_3^{-1}e_2e_2e_1e_3^{-1}e_2e_1e_3^{-1}e_2e_2, \qquad z = y^{-1}x^{-1}w,$$

and therefore $\langle w, \varphi(w), \varphi^2(w), \varphi^3(w)\rangle = F_3$.

Proof. Each of the three displayed identities is an identity between reduced words in F_3 and is verified by reducing both sides; the longest right-hand side, that for y, expands to seventy-five letters before reduction. Each e_i lies in the subgroup generated by the four orbit points, so all three free generators do, and Lemma 2.1 applies. □

Theorem 4.3. CH(3) *is false. With $F_3 = \langle x, y, z\rangle$, $\varphi(x) = yx$, $\varphi(y) = x$, $\varphi(z) = z$ and $w = xyz$,*

$$\langle w, \varphi(w), \varphi^2(w), \varphi^3(w)\rangle = F_3 \qquad \textit{while} \qquad \langle w, \varphi(w), \varphi^2(w)\rangle \neq F_3.$$

Proof. Propositions 4.1 and 4.2. □

Proposition 4.4. *$\rho(\varphi^3(w)) = (1\,3)$, which moves the point 1. So the witness of Proposition 4.1 does not also show the four-element set proper — as, by Theorem 4.3, it must not.*

Proof. $\varphi^3(w) = yx^2yx^2yxz$, whose ρ-image is $(1\,2)(2\,3)^2(1\,2)(2\,3)^2(1\,2)(2\,3)(1\,2) = (1\,3)$. □

5. Rank four

The rank-three construction pads the germ by a *fixed* generator. That trick does not iterate.

Remark 5.1. Extend the germ to $F_4 = \langle x, y, z, t\rangle$ by $\varphi(z) = z$ and $\varphi(t) = t$. With $w = xyz$ the letter t occurs in no $\varphi^i(w)$, so the five orbit points generate only $\langle x, y, z\rangle$ and the hypothesis of CH(4) is not met; with $w = xyzt$ the five points still do not generate F_4 — this second verdict by folding, outside the formal development. Nothing is refuted either way.

What works at rank four is to *move* the two extra generators. Let $F_4 = \langle x, y, z, t\rangle$ and

$$\varphi(x) = yx, \quad \varphi(y) = x, \quad \varphi(z) = t, \quad \varphi(t) = z, \qquad w = xyz.$$

The inverse is $\varphi^{-1}(x) = y$, $\varphi^{-1}(y) = xy^{-1}$, $\varphi^{-1}(z) = t$, $\varphi^{-1}(t) = z$, so $\varphi \in \operatorname{Aut} F_4$, and $\varphi \neq \mathrm{id}$. The first five points of the orbit are

$$w = xyz, \qquad \varphi(w) = yx^2t, \qquad \varphi^2(w) = xyxyxz,$$
$$\varphi^3(w) = yx^2yx^2yxt, \qquad \varphi^4(w) = xyxyx^2yxyx^2yxz.$$

Proposition 5.2. *Let $\rho\colon F_4 \to S_4$ be the homomorphism with $\rho(x) = \rho(t) = (1\,2)(3\,4)$ and $\rho(y) = \rho(z) = (1\,3\,2)$. Then $\rho(\varphi^2(w)) = \rho(\varphi^3(w)) = \mathrm{id}$, and all four of $\rho(w)$, $\rho(\varphi(w))$, $\rho(\varphi^2(w))$, $\rho(\varphi^3(w))$ fix the point 1, while $\rho(x) = (1\,2)(3\,4)$ does not. Consequently $\langle w, \varphi(w), \varphi^2(w), \varphi^3(w)\rangle \neq F_4$.*

Proof. Each value is the product of the listed images of the letters, evaluated on the four points: $\rho(w) = (2\,4\,3)$ and $\rho(\varphi(w)) = (2\,3\,4)$, both fixing 1, while $\rho(\varphi^2(w)) = \big(\rho(x)\rho(y)\big)^3 = \mathrm{id}$ because $\rho(x)\rho(y) = (1\,4\,3)$ has order three, and $\rho(\varphi^3(w)) = \mathrm{id}$ because $\varphi^3(w) = yx^2yx^2yxt$ while $\rho(x)^2 = \rho(x)\rho(t) = \mathrm{id}$, which leaves $\rho(y)^3 = \mathrm{id}$. Then apply Lemma 2.2 with $K = \mathrm{Stab}(1)$. □

Remark 5.3. Both generating values of ρ are even permutations, so $\rho(F_4) \leq A_4$; a direct orbit computation, carried out outside the formal development, gives $|\rho(F_4)| = 12$, so the image is exactly A_4. Only the containment is used above, and only through Lemma 2.2; the equality is recorded to say that the witness is a genuinely non-abelian quotient and not a small degenerate image.

For the generating half, w, $\varphi^2(w)$ and $\varphi^4(w)$ all end in the letter z, so

$$u_1 = w\,\varphi^2(w)^{-1}, \qquad u_2 = w\,\varphi^4(w)^{-1}$$

lie in $\langle x, y\rangle$.

Proposition 5.4. *With u_1, u_2 as above,*

$$x = u_1^{-1}u_1^{-1}u_2u_1^{-1}u_1^{-1}u_1^{-1}u_2u_1^{-1}u_2^{-1}u_1u_1, \qquad y = x^{-1}u_1u_2^{-1}u_1u_1,$$
$$z = y^{-1}x^{-1}w, \qquad t = x^{-1}x^{-1}y^{-1}\varphi(w),$$

and therefore $\langle w, \varphi(w), \varphi^2(w), \varphi^4(w)\rangle = F_4$; a fortiori $\langle w, \varphi(w), \varphi^2(w), \varphi^3(w), \varphi^4(w)\rangle = F_4$.

Proof. Each identity is verified by reducing both sides to normal form; the right-hand side of the first expands to 101 letters before reduction. The elements u_1 and u_2 lie in the subgroup generated by $\{w, \varphi(w), \varphi^2(w), \varphi^4(w)\}$, hence so do all four free generators, and Lemma 2.1 applies. Note that $\varphi^3(w)$ appears nowhere. □

Theorem 5.5. CH(4) *is false. With $F_4 = \langle x, y, z, t\rangle$, $\varphi(x) = yx$, $\varphi(y) = x$, $\varphi(z) = t$, $\varphi(t) = z$ and $w = xyz$,*

$$\langle w, \varphi(w), \varphi^2(w), \varphi^3(w), \varphi^4(w)\rangle = F_4 \qquad \textit{while} \qquad \langle w, \varphi(w), \varphi^2(w), \varphi^3(w)\rangle \neq F_4.$$

Proof. Propositions 5.2 and 5.4. □

Proposition 5.4 says slightly more than Theorem 5.5 needs, and the extra is the sharpest thing we can say about what fails at rank four.

Corollary 5.6. *$\langle w, \varphi(w), \varphi^2(w), \varphi^4(w)\rangle = F_4$. So the four-element subset of the orbit that fails to generate is the* initial segment*, not any four of the five points: the failure is about which points are taken, not about how many.*

Proposition 5.7. *$\rho(\varphi^4(w)) \notin \mathrm{Stab}(1)$; the witness of Proposition 5.2 does not also show the five-element set proper.*

Proof. Evaluate ρ on the fourteen letters of $\varphi^4(w)$: the value is $(1\,2)(3\,4)$, which moves the point 1. □

6. Which powers of φ pair with w

Return to the rank-two data of [2] and [3]: $F_2 = \langle x, y\rangle$, $w = xy$, $\varphi(x) = yx$, $\varphi(y) = x$. Between them the two sources record exactly two facts about pairs $\{w, \varphi^k(w)\}$: that the pair fails to generate at $k = 1$ (Proposition 3.3) and that it generates at $k = 2$ (Proposition 3.5). No exponent $k \geq 3$ is considered in either. All of them behave the same way, and for a reason with nothing to do with S_3.

Let F denote the Fibonacci sequence, $F(0) = 0$, $F(1) = F(2) = 1$, $F(k+2) = F(k+1) + F(k)$. Write $\varepsilon\colon F_2 \to \mathbb{Z}^2$ for the abelianisation, $\varepsilon(u) = (\varepsilon_x(u), \varepsilon_y(u))$ the pair of exponent sums.

Lemma 6.1. *$\varepsilon(\varphi(u)) = M\varepsilon(u)$ for every $u \in F_2$, where $M(\alpha, \beta) = (\alpha + \beta, \alpha)$. Consequently, for every $k \geq 0$,*

$$\varepsilon(\varphi^k(w)) = \big(F(k+2),\ F(k+1)\big).$$

Proof. Both $\varepsilon \circ \varphi$ and $M \circ \varepsilon$ are homomorphisms $F_2 \to \mathbb{Z}^2$, and they agree on x (both give $(1, 1)$) and on y (both give $(1, 0)$), hence agree. The second claim is an induction on k: at $k = 0$, $\varepsilon(w) = (1, 1) = (F(2), F(1))$; and $M(F(k+2), F(k+1)) = (F(k+3), F(k+2))$ by the Fibonacci recurrence. □

For $k \geq 1$ the index of the subgroup of $\mathbb{Z}^2$ spanned by $\varepsilon(w) = (1, 1)$ and $\varepsilon(\varphi^k(w))$ is therefore

$$\left|\det \begin{pmatrix} 1 & 1 \\ F(k+2) & F(k+1) \end{pmatrix}\right| \;=\; \big|F(k+1) - F(k+2)\big| \;=\; F(k),$$

which equals 1 exactly for $k \in \{1, 2\}$ and is at least 2 for $k \geq 3$. That is the whole mechanism, and it turns into a certificate of the shape of Lemma 2.2 with $H = \mathbb{Z}$.

Proposition 6.2. *Let $k \geq 3$ and let $\chi_k\colon F_2 \to \mathbb{Z}$ be the homomorphism with $\chi_k(x) = F(k+1)$ and $\chi_k(y) = -F(k+2)$. Then*

$$\chi_k(w) = -F(k), \qquad \chi_k(\varphi^k(w)) = 0,$$

both divisible by $F(k)$, whereas $\chi_k(x) = F(k+1)$ is not. Consequently $\langle w, \varphi^k(w)\rangle \neq F_2$.

Proof. By Lemma 6.1, $\chi_k(w) = F(k+1) - F(k+2) = -F(k)$ and $\chi_k(\varphi^k(w)) = F(k+1)F(k+2) - F(k+2)F(k+1) = 0$. Consecutive Fibonacci numbers are coprime, so $F(k) \mid F(k+1)$ would force $F(k) = 1$; but $F(k) \geq F(3) = 2$ for $k \geq 3$ since F is monotone from index 1 on. Now apply Lemma 2.2 with $K = F(k)\mathbb{Z} \leq \mathbb{Z}$ and $g = x$. □

Theorem 6.3. *For the data $F_2 = \langle x, y\rangle$, $w = xy$, $\varphi(x) = yx$, $\varphi(y) = x$ and every $k \geq 1$,*

$$\langle w,\ \varphi^k(w)\rangle = F_2 \qquad \Longleftrightarrow \qquad k = 2.$$

Proof. If $k = 2$ the pair generates by Proposition 3.5. Conversely, suppose $k \neq 2$. If $k = 1$ the pair is proper by Proposition 3.3; if $k \geq 3$ it is proper by Proposition 6.2. □

Remark 6.4. The two ends of Theorem 6.3 are proved by genuinely different means, and Proposition 3.8 says the difference is necessary rather than a matter of taste. At $k \geq 3$ the abelianised index $F(k)$ is at least 2 and the obstruction is visible in $\mathbb{Z}$. At $k = 1$ the index is $F(1) = 1$ and, by Proposition 3.8, no abelian quotient whatsoever sees the failure, so a non-abelian witness such as S_3 is unavoidable. At $k = 2$ the index is $F(2) = 1$ as well, and there the pair really does generate.

7. How the witnesses were found, and what is not proved

None of the proofs above rests on a search: each is a two-sided certificate — explicit words on one side, an explicit finite quotient on the other — that a reader or a proof checker can verify without reference to how it was obtained. What the searches below did is find those certificates, and this section records them for reproducibility and to delimit exactly which statements in this paper are search-dependent. The answer to the last question is: no numbered result, and only those remarks that say so of themselves — Remarks 5.1 and 5.3 above, and Remarks 7.1, 7.2 and 7.3 below.

The search runs over pairs (φ, w) and uses one necessary condition to cut the space cheaply. If $\langle O_n(\varphi, w)\rangle = F_n$ then the abelianisation of that subgroup is all of $\mathbb{Z}^n$; by Cayley–Hamilton applied to the abelianised automorphism M, the vector $M^n\varepsilon(w)$ is an integral combination of the earlier ones, so already $\varepsilon(w), M\varepsilon(w), \ldots, M^{n-1}\varepsilon(w)$ must span $\mathbb{Z}^n$, i.e.

$$\left|\det\left[\varepsilon(w),\ M\varepsilon(w),\ \ldots,\ M^{n-1}\varepsilon(w)\right]\right| = 1.$$

Pairs failing this are discarded before any group-theoretic work. Survivors are decided by Stallings folding [8]: fold the wedge of loops labelled by the given words and check whether the core graph is the one-vertex rose with all n labels, which decides $\langle S\rangle = F_n$. Automorphisms are enumerated by breadth-first search in $\mathrm{Aut}\, F_n$ over eight Nielsen-type generators (two cyclic shifts of the basis, one transposition, one inversion, and four transvections $x_1 \mapsto x_1 x_2^{\pm 1}, x_2^{\pm 1} x_1$), keeping only those all of whose generator images have length at most two, and truncating the enumeration at a fixed count; so the automorphism list is a truncated breadth-first prefix, not all automorphisms with short generator images. Words are enumerated exhaustively up to a length bound. Each run is exhaustive over the pairs (enumerated automorphism, word within the length bound).

rank	automorphisms	words		folding tests	pairs found	wall clock
3	4,000	186	$(1 \leq \lvert w\rvert \leq 3)$	174,880	2,412	29 s
4	6,000	3,200	$(1 \leq \lvert w\rvert \leq 4)$	2,360,014	7,160	595 s
5	4,000	910	$(1 \leq \lvert w\rvert \leq 3)$	542,212	498	145 s

The witnesses of Theorems 4.3 and 5.5 were selected from the first two rows; the generating words of Propositions 4.2 and 5.4 came from a meet-in-the-middle search for a short expression of each free generator, cross-checked against Nielsen reduction with expression tracking. Every generation verdict used in the search was computed twice, by folding and by Nielsen reduction, and the two agreed on every instance.

Three things this section reports are not theorems of this paper, and we flag them as such.

Remark 7.1. The third row of the table says that counterexamples exist at rank five — 498 pairs were found — but none of them has been formalised, and no rank-five statement is claimed here.

The obstruction is bookkeeping, not mathematics: a rank-five counterexample needs a permutation witness and a fresh set of generating words, both cheap to produce with the machinery above.

Remark 7.2. A uniform construction for all n does not come from the shape used here. The obvious candidate — the germ φ on $\langle x, y\rangle$ extended by an arbitrary permutation of the remaining $n-2$ generators, with $|w| \le 3$ — was scanned over all $(n-2)!$ permutations and all such words, and yields 8 counterexamples at $n = 3$, 40 at $n = 4$, and none at all at $n = 5$, 6 or 7. So rank four is the end of that family, and the general question needs a different idea.

Remark 7.3. In the rank-three example, folding reports that no three of the four elements $w, \varphi(w), \varphi^2(w), \varphi^3(w)$ generate F_3 — not merely the initial segment. Formalising that would need three further finite-quotient witnesses and has not been done, so Theorem 4.3 is stated for the initial segment only. Contrast Corollary 5.6, where the corresponding rank-four statement is proved and comes out the other way.

We close with the question the two published solutions and this paper leave open.

Question 7.4. Does CH(n) fail for every $n \ge 2$?

What such a construction has to produce is precisely described by the filter above: for every n, an automorphism φ and a word w such that $\langle O_{n-1}(\varphi, w)\rangle$ is proper in F_n and yet abelianises onto all of $\mathbb{Z}^n$. The proper subgroup is generated by n elements and surjects onto $\mathbb{Z}^n$; it is the tension between those two facts that makes the search cheap and a general construction hard.

8. Formal verification

Every lemma, proposition, theorem and corollary stated above, with the explicit exceptions of Remarks 5.1, 5.3, 7.1, 7.2 and 7.3, is formalised and machine-checked in Lean 4 [6] against Mathlib [7]. The development is five files and 1,268 lines, and declares 121 theorems — every declaration introduced by the keyword `theorem`, including the 15 private ones and the 9 tagged `simp` — together with 55 definitions. The check is by kernel evaluation only: the development uses no compiled-evaluation escape hatch and contains no incomplete proof; the axiom set of the three negative answers, of the exponent classification, and of the generation, properness and control statements they rest on was printed, and each is contained in the standard triple — propositional extensionality, quotient soundness and choice — so the same holds for every declaration they depend on. The exponent-sum formula $\varepsilon(\varphi^k(w)) = (F(k+2), F(k+1))$ of Lemma 6.1 needs only the first two. Three things are worth naming precisely. First, what the finite computations inside the kernel are: an identity between words is decided by reducing both sides to normal form through the decidable equality of the free group, and a permutation identity by evaluating the permutation on each of the at most four points; the largest single such reduction is the first identity of Proposition 5.4, whose right-hand side expands to 101 letters. These are the only computations the theorems depend on, and they are small enough to check by hand. Second, a handful of intermediate values that are displayed here but are recorded formally only through the consequence the argument uses: the reduced form of e_1 in Section 4, the cycle values $\pi(\varphi^2(w)) = (1\,2\,3)$, $\rho(w) = (2\,4\,3)$, $\rho(\varphi(w)) = (2\,3\,4)$ and $\rho(\varphi^4(w)) = (1\,2)(3\,4)$, and the index $F(k)$ of the abelianised pair in Section 6. What the development proves in their place is the membership or non-membership in the relevant point stabiliser, and the divisibility by $F(k)$, that the proofs actually invoke; each displayed value is one evaluation of a permutation on at most four points, or one 2×2 determinant. Third, what lies outside altogether: the *discovery* of the certificates, described in Section 7, together with the five remarks named above; none of the search programs' correctness is used anywhere, since every certificate is re-verified from scratch inside the kernel. Before any formalisation, every printed value of [2] and [3] was independently recomputed, which is how the composition convention of Section 2 was pinned down. The five files elaborate in about one hundred seconds in total, each of them dominated by loading the library, which is also what sets the peak memory. The repository is private; repository reference to be added at submission.

References

[1] M. Hall, Jr., *Coset representations in free groups*, Trans. Amer. Math. Soc. **67** (1949), no. 2, 421–432; DOI 10.1090/S0002-9947-1949-0032642-4. Its §5 is headed "A separation theorem" and its Theorem 5.1 is the statement quoted in Section 2, read there against the published text. Cited only to say that the method of Lemma 2.2 is not a restriction; no proof here depends on it.

[2] V. Ionin and A. Semidetnov, *On Some More Problems from the Kourovka Notebook*, arXiv:2608.29219v1 (29 August 2026), 20 pages; primary classification math.GR. Its section "The Cayley–Hamilton analogue for free groups" contains the solution of Problem 17.32 quoted and replayed in Section 3; its Answer reads "No. The assertion fails for $n = 2$." Read in full on 3 September 2026, when the arXiv record showed v1 as the only version, with no journal reference and no DOI.

[3] O. Kharlampovich, *Two Observations on Problems 14.23 and 17.32 of the Kourovka Notebook*, August 2026, 4 pages, available at https://kourovkanotebookorg.wordpress.com/wp-content/uploads/2026/08/kourovka_14_23_17_32_note_with_problem_authors.pdf. Its Proposition 1 and Remark 1 are the rank-two counterexample in the basis $\varphi(a) = b$, $\varphi(b) = ab$, $w = ba$; its abstract states that no claim of priority is made. Retrieved and read in full on 3 September 2026. The note itself carries no author line and no author field in its metadata; the attribution is the Notebook's, which cites this same file from the answer lines of both 17.32 and 14.23 under the name O. Kharlampovich and lists 17.32 under that name in its index of names.

[4] L. Koch-Hyde and É. Olive, *Two problems about subgroups of free groups concerning the lengths of their generators*, arXiv:2609.00382v1 (31 August 2026), 9 pages. Cited in Section 1 only as a contemporaneous treatment of other problems about subgroups of free groups; it does not concern Problem 17.32.

[5] E. I. Khukhro and V. D. Mazurov (editors), *Unsolved Problems in Group Theory. The Kourovka Notebook*, No. 21, Sobolev Institute of Mathematics, Novosibirsk, 2026; e-print arXiv:1401.0300. Problem 17.32 is due to O. V. Bogopolski. The e-print is updated in place; all quotations in this paper are from the source of version 46, posted 1 September 2026 and retrieved on 3 September 2026, which was the current version on that date. That version's arXiv comment field begins "Quite a few new solutions added in this update, including some solutions obtained using AI". Version 45, posted 3 July 2026, carries Problem 17.32 without an answer line, as discussed in Section 1.

[6] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science, Springer, 2021, pp. 625–635; DOI 10.1007/978-3-030-79876-5_37.

[7] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381; DOI 10.1145/3372885.3373824.

[8] J. R. Stallings, *Topology of finite graphs*, Invent. Math. **71** (1983), no. 3, 551–565; DOI 10.1007/BF02095993. Cited only for the folding algorithm used by the search of Section 7, which no theorem depends on.

[9] W. van Doorn, E. Judin, P. Monticone and D. Morrison, *On Some Problems from the Kourovka Notebook*, arXiv: 2607.17477v2 (26 July 2026), 21 pages. Its abstract states that solutions to eight Kourovka problems are presented and that all of them were autonomously discovered and formally verified in Lean by Aristotle, a formal reasoning agent developed by Harmonic; the eight are listed there and Problem 17.32 is not among them. Metadata and abstract read on 3 September 2026.