NON-B-GROUPS OF ORDER 3^5 AND EXPONENT 9

KOREA SUPERINTELLIGENCE LABS

Abstract. A finite group H is a *B-group* if every primitive permutation group containing a regular subgroup isomorphic to H is 2-transitive; equivalently, H fails to be a B-group exactly when it occurs as a regular subgroup of a uniprimitive group. Herbig has classified the B-groups of order p^4 and names the order-p^5 classification as the next step, observing that for $p = 3$ and $p = 5$ the answer is a finite computation over the primitive-groups and small-groups libraries; the outcome of that computation is not reported there. We carry out part of the case $p = 3$ and certify the outcome inside a proof assistant. From an explicit list of 18 permutations of a 243-point set we prove that the group Γ they generate is uniprimitive — primitive by a statement quantified over *all* invariant partitions, not 2-transitive by an exhibited invariant set of 3888 ordered pairs — and that Γ contains three pairwise non-isomorphic regular subgroups of order 243: one elementary abelian, and two of exponent 9. Hence at least two groups of order 3^5 of exponent 9 are not B-groups. Externally, GAP identifies Γ as the affine primitive group $3^5{:}(2^4{:}A_5)$ of order 233280 and the two subgroups as `SmallGroup(243,51)` and `SmallGroup(243,63)`, both nonabelian with centres of order 9 and 27. Since these have order p^q with $q > p$ and exponent p^2, they show that the hypothesis $q < p$ in Herbig's Theorem B cannot be relaxed to $q > p$, and they answer an instance at $p = 3$ of his closing question on regular subgroups of $\mathrm{AGL}(5, p)$. The primitivity, the failure of 2-transitivity and the three regular subgroups with their invariants are machine-checked in Lean 4; the few steps checked outside the proof assistant are named where they are used. We do not claim the resulting list of non-B-groups of order 243 is complete, and we say precisely which part of the search did not run.

1. Introduction

Let Ω be a finite set and $G \le \mathrm{Sym}(\Omega)$. A subgroup $H \le G$ is *regular* if it is transitive on Ω and only its identity fixes a point; G is *primitive* if it is transitive and preserves no partition of Ω other than the partition into singletons and the partition $\{\Omega\}$; and G is *uniprimitive* if it is primitive but not 2-transitive. Following Wielandt [18], a finite group H is a *B-group* (Burnside group) if every primitive permutation group containing a regular subgroup isomorphic to H is 2-transitive. Unwinding the definition:

(1) H is *not* a B-group $\iff$ H is isomorphic to a regular subgroup of some uniprimitive group.

The right-hand side is what makes the negative direction finitely certifiable: a witness that H is not a B-group consists of a permutation group G on $|H|$ points together with a regular subgroup of G isomorphic to H, and of proofs that G is primitive and not 2-transitive. Every claim in this paper of the form "H is not a B-group" is an instance of that certificate; we prove no positive B-group statement anywhere.

The subject begins with Burnside, who asserted in [4, §252] that a cyclic group of order p^a with $a \ge 2$ is a B-group, while groups of prime order never are (a p-cycle generates a uniprimitive subgroup of S_p). Burnside's argument contains a well-known error; see Knapp [11] and Wildon [20] for the history. Since then: Kochendörffer [12] showed $C_{p^a} \times C_{p^b}$ with $a \ne b$ is a B-group; Wielandt [19] handled dihedral groups, as recorded in [9, Theorem 2.3]; Jones [10] settled the regular subgroups of uniprimitive groups of degree p^3; Li [13] classified the primitive groups containing an abelian regular subgroup, whence a complete criterion for abelian groups whose order has at least two prime divisors; Liebeck, Praeger and Saxl [14] classified the regular subgroups of primitive almost simple groups; Potočnik [16] classified the B-groups of order pq. Ponomarenko and Ryabov [17] review the state of the art, and their introduction is the summary we rely on: the complete classifications available are

those of the almost simple B-groups and of the B-groups of order pq, alongside Wielandt's criterion that an abelian group of composite order with a cyclic Sylow subgroup is a B-group. None of these reaches order p^5.

The order p^5 problem. Herbig [9] classifies the B-groups of order p^4 for every prime p (his Theorem A) and proves along the way that a group of order p^q for primes $q < p$ with exponent at least p^2 is a B-group (his Theorem B). His closing paragraph names the order-p^5 classification as the natural next step — the groups of that order having been classified by Bender [2] — and splits it into three regimes. For $p \geq 7$ the O'Nan–Scott theorem together with his Proposition 3.2 and Lemma 4.1 reduce the problem to the uniprimitive subgroups of $\mathrm{AGL}(5, p)$, whose Sylow p-subgroups have exponent p; for $p = 2$ there is no uniprimitive group of degree 32, so every group of order 32 is a B-group; and for $p = 3$ and $p = 5$ he writes that "the B-groups can be found using the GAP script in Listing 1", because the small-groups library contains all groups of orders 243 and 3125 and the primitive-groups library contains all primitive groups of degree below 4096. The script is printed in his appendix; *its output is not reported*.

This paper runs that computation at $p = 3$, over the part of the search space that finishes quickly, and certifies its conclusions in a proof assistant. What we obtain is a lower bound for the set of non-B-groups of order 243, together with machine-checked proofs for the entries of that bound.

Results. Fix $\Omega = \{0, 1, \ldots, 242\}$. Section 3 introduces an explicit list $t_1, \ldots, t_{18}$ of permutations of Ω and the group $\Gamma = \langle t_1, \ldots, t_{18} \rangle$.

The witness is uniprimitive (Theorems 3.1, 3.3 and 3.4). Every partition of Ω invariant under $t_1, \ldots, t_{18}$ that puts the point 0 in the same part as some other point is the partition $\{\Omega\}$; and there is a t_i-invariant set of ordered pairs containing $(0, 1)$ and missing $(0, 2)$. So Γ is primitive and not 2-transitive. The primitivity statement is quantified over all partitions, not over the partitions some algorithm happened to inspect; how a finite computation yields such a statement is the subject of Section 3.2, and is the one place in this paper where the method, rather than the answer, is the point.

Three regular subgroups (Theorems 4.1, 4.2, 4.4 and 4.5). Γ contains regular subgroups H_0, H_1, H_2 of order 243 with H_0 elementary abelian and H_1, H_2 of exponent 9; their order statistics are pairwise different, so they are pairwise non-isomorphic. By (1) none of the three is a B-group. $H_0 \cong C_3^5$ is a positive control: it is not a B-group already by Wielandt's factorization criterion, and recovering it validates the pipeline. The pair H_1, H_2 is the new part.

Consequences (Section 4). Both H_1 and H_2 have order p^q with $p = 3$, $q = 5$ and exponent $p^2 = 9$, so the hypothesis $q < p$ of Herbig's Theorem B cannot be relaxed to $q > p$; he had already observed it cannot be relaxed to $q = p$, the nonabelian group of order 27 and exponent 9 being regular in the uniprimitive action of $\mathrm{PSU}(4, 2)$ on 27 points. Externally, Γ is the affine group $3^5{:}(2^4{:}A_5)$, so H_1 and H_2 are regular subgroups of exponent 9 inside a uniprimitive subgroup of $\mathrm{AGL}(5, 3)$ — an instance at $p = 3$ of the question that closes [9], and a companion to the remark there that the Sylow 3-subgroups of $\mathrm{AGL}(4, 3)$ have exponent 9.

What is not claimed (Section 5). Completeness. Of the 30 uniprimitive groups of degree 243, the five whose Sylow 3-subgroup has order 3^9 and four more were not searched to the end, and two additional isomorphism types surfaced at the end of the run from a group that was. Section 5 lists exactly what ran and what did not.

A warning about the name. The string "B-group" carries further meanings in the current literature, none of them the one above, and a reader searching for prior art will meet them first. Two are common enough to name: Bouc's B-groups from the theory of biset functors and the Burnside ring [3], and the Kleinian b-groups of Maskit's decomposition theory for function groups [15]. A literature search for the present notion has to be done through "uniprimitive", "regular subgroup" and the names of the papers cited above, not through the phrase alone.

2. Preliminaries

Throughout, Ω is a finite set with $|\Omega| \geq 3$ and maps act on the left. A partition of Ω is recorded by a labelling: a function c defined on Ω, whose parts are the fibres $c^{-1}(v)$. For $S \subseteq \mathrm{Sym}(\Omega)$, call c *S-invariant* if

$$c(x) = c(y) \implies c(sx) = c(sy) \qquad \text{for all } s \in S,\ x, y \in \Omega. \tag{2}$$

Since each $s \in S$ is a bijection of a finite set, (2) says exactly that s permutes the parts of c; consequently a labelling is S-invariant if and only if it is invariant under $\langle S \rangle$, and the $\langle S \rangle$-invariant labellings are precisely the block systems of $\langle S \rangle$ (see [7, Ch. 1] for this and the other standard permutation-group facts used below). The formula (2) also makes sense verbatim for a family of maps $\Omega \to \Omega$ that are not known to be injective, and Section 3.2 uses it in that generality. We use the following standard reformulation without further comment.

Lemma 2.1. *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive. Then G is primitive if and only if every G-invariant labelling c for which $c(\alpha) = c(\beta)$ holds for some pair of distinct points α, β is constant on Ω.*

We also record the elementary passage from a finite table of maps to a regular subgroup; it is what turns the checks of Section 4 into group theory, and it needs no property of how the table was produced.

Lemma 2.2. *Let E be a finite set of maps $\Omega \to \Omega$ such that*

(a) *$\mathrm{id}_\Omega \in E$ and E is closed under composition;*
(b) *every $e \in E$ with $e \neq \mathrm{id}_\Omega$ satisfies $e(x) \neq x$ for all $x \in \Omega$;*
(c) *for every $x \in \Omega$ there is $e \in E$ with $e(0) = x$, where $0 \in \Omega$ is a fixed base point.*

Then every element of E is a permutation of Ω, E is a subgroup of $\mathrm{Sym}(\Omega)$, and E acts regularly on Ω.

Proof. Let $a \in E$. By (a) all powers $a, a^2, a^3, \ldots$ lie in E, and E is finite, so $a^i = a^j$ for some $i < j$; put $k = j - i \geq 1$, so that a^k fixes the point $a^i(0)$. By (b) this forces $a^k = \mathrm{id}_\Omega$. Hence a is invertible with $a^{-1} = a^{k-1} \in E$, so a is a bijection and E is a group. It is transitive by (c) and its point stabilizers are trivial by (b), so it is regular. (In particular $|E| = |\Omega|$ and the map $e \mapsto e(0)$ is a bijection $E \to \Omega$.) □

Finally we fix the two notions used to separate isomorphism types. For a finite group H, its *order statistic* is the list of pairs $(d, \#\{h \in H : \mathrm{ord}(h) = d\})$ over the divisors d that occur, and $\exp(H)$ is the maximal order of an element. Both are isomorphism invariants; neither, singly or together, determines an isomorphism type, and we never use them as if they did.

3. The witness data and its certificates

3.1. **The tables.** Let $\Omega = \{0, 1, \ldots, 242\}$. The formal development carries a list $t_1, t_2, \ldots, t_{18}$ of maps $\Omega \to \Omega$, stored as image tables in a single hexadecimal string, two characters per point. The first three are the generators that GAP's primitive-groups library returns for the primitive group of degree 243 and order 233280; the remaining fifteen are five generators for each of three subgroups of order 243. The data were produced by a GAP script and transcribed mechanically; nothing below depends on where they came from.

Theorem 3.1. *Each of $t_1, \ldots, t_{18}$ is a table of exactly 243 entries and satisfies $t_i(x) \in \Omega$ for every $x \in \Omega$; and there are exactly 18 of them.*

Theorem 3.1 is the non-vacuity hypothesis that every later statement consumes. Without it, "t_i-invariant partition of Ω" would be a statement about out-of-range values rather than about Ω, and the primitivity proof of Section 3.2 would be a theorem about junk. Note what it does *not* say: it does not say that the t_i are injective. Injectivity is immediate from the tables — each is a permutation, as one sees by sorting 243 numbers, and the tables were emitted by GAP from

permutations in the first place — but it is a check performed outside the formal development, and we flag it where it is used, namely in passing from the t_i to the group $\Gamma = \langle t_1, \dots, t_{18} \rangle$.

3.2. **Primitivity from an untrusted closure.** Deciding primitivity of a permutation group of degree n from generators is classical: seed the relation $\alpha \sim \beta$ for the pair one wants to separate and close it under the generators; the least invariant partition containing the seed is computed by repeated forced merges, and the group is primitive if and only if that closure is the universal partition for every choice of second point. The algorithm goes back to Atkinson [1]. Running it produces a number, and believing the number requires believing the implementation.

What is proved here instead is a soundness statement, from which the implementation drops out. A *labelling array* is a table r of 243 values in Ω; think of $r(x)$ as the name of the class currently assigned to x. Define

$$\mathrm{merge}(r, a, b) = r \quad \text{when } r(a) = r(b),$$

and otherwise $\mathrm{merge}(r, a, b)$ is the array

$$x \longmapsto \begin{cases} r(a) & \text{if } r(x) = r(b), \\ r(x) & \text{otherwise,} \end{cases}$$

so that a merge relabels one entire class. Put

$$\mathrm{step}(r, i, x) = \mathrm{merge}\big(r,\ t_i(x),\ t_i(r(x))\big).$$

A *sweep* applies $\mathrm{step}(\cdot, i, x)$ for $i = 1, \dots, 18$ and $x = 0, \dots, 242$ in a fixed order. For $b \in \Omega \setminus \{0\}$ let R_b be the result of four sweeps applied to $\mathrm{merge}(\mathrm{id}, 0, b)$, where id is the labelling $x \mapsto x$.

The point of step is that each merge it performs is *forced*: it merges the images under t_i of two points that are already in the same class. This is expressed by the following invariant. Given a labelling c on Ω, say that a labelling array r is *c-sound* if $r(x) \in \Omega$ and $c(x) = c(r(x))$ for every $x \in \Omega$.

Lemma 3.2. *Let c be a $\{t_1, \dots, t_{18}\}$-invariant labelling on Ω, in the sense of (2), and suppose every t_i maps Ω into Ω. Then:*

(i) id *is c-sound;*
(ii) *if r is c-sound and $a, b \in \Omega$ satisfy $c(a) = c(b)$, then* $\mathrm{merge}(r, a, b)$ *is c-sound;*
(iii) *if r is c-sound then* $\mathrm{step}(r, i, x)$ *is c-sound for all $i \le 18$ and $x \in \Omega$; hence so is any number of sweeps applied to r.*

Proof. (i) is immediate. For (ii), write $r' = \mathrm{merge}(r, a, b)$ and let $x \in \Omega$. If $r(a) = r(b)$ then $r' = r$. Otherwise $r'(x)$ is either $r(x)$, and there is nothing to prove, or $r(a)$, which happens only when $r(x) = r(b)$; in that case soundness of r gives $c(x) = c(r(x)) = c(r(b)) = c(b) = c(a) = c(r(a)) = c(r'(x))$, using $c(a) = c(b)$ in the middle. Ranges are preserved because r' takes values among those of r. For (iii), soundness of r gives $c(x) = c(r(x))$, and $x, r(x) \in \Omega$, so invariance (2) yields $c(t_i(x)) = c(t_i(r(x)))$; now apply (ii) with $a = t_i(x)$ and $b = t_i(r(x))$, both in Ω. The last clause follows by induction along the fixed order of a sweep. □

Theorem 3.3. *Let c be a labelling on Ω that is invariant under $t_1, \dots, t_{18}$ in the sense of (2), and suppose $c(0) = c(b)$ for some $b \in \Omega$ with $b \neq 0$. Then c is constant on Ω.*

Proof. By Lemma 3.2(i)–(ii), $\mathrm{merge}(\mathrm{id}, 0, b)$ is c-sound, using the hypothesis $c(0) = c(b)$; by (iii) so is R_b. A finite computation, described below, shows that R_b is constant, i.e. $R_b(x) = R_b(0)$ for every $x \in \Omega$. Soundness then gives $c(x) = c(R_b(x)) = c(R_b(0)) = c(0)$ for every $x \in \Omega$. □

What rests on computation. Exactly one thing: that R_b is a constant array, for each of the 242 values $b \in \Omega \setminus \{0\}$. This is a closed Boolean expression, evaluated by compiled execution; the search it performs is 242 closures, each of four sweeps of 18×243 merge steps, each step rewriting a table of 243 labels — about 10^9 elementary operations in total. Three sweeps already reach the fixed point for every b; the fourth is run for margin. No property of the algorithm is used: were the closure

buggy, or the sweep count too small, the Boolean would come out false and Theorem 3.3 would not be proved. It could not come out true and yield a false theorem, because Lemma 3.2 — which is where all the mathematics sits — is proved for an arbitrary invariant c and an arbitrary sequence of merges of the given shape.

3.3. **Failure of 2-transitivity.**

Theorem 3.4. *There is a set S of ordered pairs of points of Ω such that $(0,1) \in S$; such that $(x,y) \in S$ implies $(t_i(x), t_i(y)) \in S$ for all $i \le 18$ and $x, y \in \Omega$; and such that $(0,2) \notin S$.*

The set exhibited is the closure of $\{(0,1)\}$ under $t_1, \dots, t_{18}$, computed as a bit array indexed by $243x + y$; the certified content is the three displayed properties, checked directly, and not any claim that the closure algorithm computed an orbit. For orientation: $|S| = 3888$ out of the $243 \cdot 242 = 58806$ ordered pairs of distinct points, a value obtained by an ordinary computation outside the formal development, so the check is nowhere near a boundary case. The invariance check alone is $18 \cdot 243^2 = 1\,062\,882$ implications.

3.4. **The witness group.**

Corollary 3.5. *Suppose, as is the case, that each t_i is a bijection of Ω. Then $\Gamma = \langle t_1, \dots, t_{18} \rangle \le \mathrm{Sym}(\Omega)$ is uniprimitive of degree 243.*

Proof. Γ is transitive: the subgroup H_0 of Theorem 4.1 below is contained in Γ and is already transitive. A Γ-invariant labelling is t_i-invariant, so by Theorem 3.3 any such labelling with two distinct points in one part is constant; by Lemma 2.1, Γ is primitive. For the second half, the set S of Theorem 3.4 is closed under each t_i, hence under the monoid they generate, which is the finite group Γ; since $(0,1) \in S$ and $(0,2) \notin S$, the pairs $(0,1)$ and $(0,2)$ lie in different Γ-orbits, so Γ is not 2-transitive. □

Remark 3.6. The following facts about Γ are *not* part of the formal development; they were computed in GAP and are recorded because they locate the witness in the literature. The group generated by t_1, t_2, t_3 is `PrimitiveGroup(243,19)`, of order $233280 = 2^6 \cdot 3^6 \cdot 5$ and named $3^5{:}(2^4{:}A_5)$ by the library; all eighteen tables lie in it, so Γ is that group. It is of affine type: its socle is an elementary abelian regular normal subgroup of order 3^5, and the point stabilizer, of order 960, is $2^4{:}A_5$ acting irreducibly on $\mathbb{F}_3^5$. Its rank is 7, with subdegrees $1, 10, 16, 16, 40, 80, 80$; the subdegree 16 matches $|S|/243 = 16$ in Theorem 3.4. Moreover the point stabilizer has an orbit of length 5 on the 121 hyperplanes of the socle whose members intersect trivially, so Γ preserves a Cartesian decomposition $\Omega \cong \{0,1,2\}^5$ and is a subgroup of index 4 in $S_3 \wr S_5$ acting with the product action.

4. Regular subgroups

Each of the three subgroups below is presented by a *spanning structure*: a table of pairs (i_k, p_k), $1 \le k \le 242$, from which the list $e_0, e_1, \dots, e_{242}$ of maps $\Omega \to \Omega$ is rebuilt by

$$e_0 = \mathrm{id}_\Omega, \qquad e_k = t_{i_k} \circ e_{p_k} \quad (1 \le k \le 242), \qquad p_k < k. \tag{3}$$

Every listed element is therefore visibly a word in $t_1, \dots, t_{18}$, so the set they form lies in Γ by construction, with no membership test to trust. Write $\mathcal{R}(E)$ for the conjunction of four finite checks on the resulting list $E = \{e_0, \dots, e_{242}\}$:

- (R1) the 243 entries are pairwise distinct;
- (R2) E is closed under composition: $e \circ f \in E$ for all $e, f \in E$;
- (R3) every $e \in E$ other than id_Ω satisfies $e(x) \ne x$ for all $x \in \Omega$;
- (R4) $\{e(0) : e \in E\} = \Omega$.

By Lemma 2.2, $\mathcal{R}(E)$ implies that E is a regular subgroup of Γ of order 243. Checking $\mathcal{R}(E)$ costs $243^2 = 59\,049$ compositions for (R2), the same number of comparisons for (R1), and 243^2 evaluations for each of (R3), (R4).

4.1. **The elementary abelian control.**

Theorem 4.1. *The list E_0 built by* (3) *from the first spanning structure satisfies $\mathcal{R}(E_0)$. Hence $H_0 := E_0$ is a regular subgroup of Γ of order* 243.

Theorem 4.2. *H_0 has order statistic $(1,1),(3,242)$; its exponent is* 3*; and all* 243 *of its elements commute with each of the five listed generators $t_4,\dots,t_8$.*

Corollary 4.3. *H_0 is elementary abelian of order 3^5, hence C_3^5 is not a B-group.*

Proof. Every non-identity element of H_0 has order 3 by Theorem 4.2, and $t_4,\dots,t_8$ lie in H_0 and generate it (an elementary finite check, performed outside the formal development), so the second clause of Theorem 4.2 says H_0 is abelian. An abelian group of order 3^5 and exponent 3 is C_3^5. Now apply Corollary 3.5 and (1). □

Corollary 4.3 is not new: C_3^5 is 3-factorizable, and Wielandt's argument ([18, Theorem 25.7], restated as [9, Proposition 2.2] and cited to the same place in [17]) embeds any m-factorizable group with $m \geq 3$ as a regular subgroup of $S_m \wr S_k$ in the product action, which is primitive and not 2-transitive. We include it because it is the positive control for everything else here: a pipeline that could not recover the non-B-group of order 243 that Wielandt's criterion already supplies would not be worth reporting, and Remark 3.6 places the very same witness Γ inside $S_3 \wr S_5$, which is where Wielandt's argument puts C_3^5.

4.2. **Two non-B-groups of exponent** 9**.**

Theorem 4.4. *The lists E_1 and E_2 built by* (3) *from the second and third spanning structures satisfy $\mathcal{R}(E_1)$ and $\mathcal{R}(E_2)$. Hence $H_1 := E_1$ and $H_2 := E_2$ are regular subgroups of Γ of order* 243*.*

Theorem 4.5. *H_1 has order statistic $(1,1),(3,134),(9,108)$, exponent* 9*, and exactly* 9 *of its elements commute with each of $t_9,\dots,t_{13}$. H_2 has order statistic $(1,1),(3,80),(9,162)$, exponent* 9*, and exactly* 27 *of its elements commute with each of $t_{14},\dots,t_{18}$.*

Corollary 4.6. *H_0, H_1 and H_2 are pairwise non-isomorphic groups of order* 243*, none of which is a B-group. H_1 and H_2 have exponent* 9*, and H_1 is nonabelian.*

Proof. The three order statistics in Theorems 4.2 and 4.5 are pairwise different, so the groups are pairwise non-isomorphic. Each is regular in Γ, which is uniprimitive by Corollary 3.5, so (1) applies to each. For the last clause, an abelian group of order 3^5 and exponent 9 is $C_9 \times C_9 \times C_3$ or $C_9 \times C_3^3$, with 26 respectively 80 elements of order 3; H_1 has 134, so it is not abelian. □

Remark 4.7. The same argument does not settle H_2: its order statistic $(1,1),(3,80),(9,162)$ is exactly that of $C_9 \times C_3^3$. What separates them is the centralizer count: only 27 of the 243 elements of H_2 commute with all of $t_{14},\dots,t_{18}$, and those five permutations lie in H_2 and generate it, so $\mathrm{Z}(H_2)$ has order 27 and H_2 is nonabelian with $H_2 \ncong C_9 \times C_3^3$. The membership and generation statements are immediate finite checks — one composes 243 tables and compares — and they have been re-run from the same tables in an implementation independent of the one that produced them; but they were run outside the formal development, so we state the machine-checked part (the count) and the external part (the membership) separately. The same caveat applies to the word "commute" being read as "central" in Theorems 4.2 and 4.5. Adding that check to the formal development is a one-line addition with the machinery already present; we have not made it. Nothing in Corollaries 4.6 and 4.9 depends on it — those use only order statistics and exponents — but the word "elementary abelian" in Corollary 4.3, and H_2 being nonabelian here, do.

Remark 4.8. Externally, GAP identifies the three subgroups, with the structure descriptions

$$H_0 = \texttt{SmallGroup(243,67)} \cong C_3^5, \qquad H_1 = \texttt{SmallGroup(243,51)} \cong C_3 \times \left(C_3^3{:}C_3\right),$$
$$H_2 = \texttt{SmallGroup(243,63)} \cong C_3 \times C_3 \times (C_9{:}C_3),$$

with centres of order 243, 9 and 27 and derived subgroups of order 1, 9 and 3 respectively. These identifications use GAP's `IdGroup`, which is not machine-checked here; the formal development pins the types only up to the invariants of Theorems 4.2 and 4.5, which happen to separate the three groups that occur but do not, in general, determine an isomorphism type. Every statement in Corollary 4.6 is independent of these labels.

Corollary 4.9. *The hypothesis $q < p$ in* [9, Theorem B] *cannot be relaxed to $q > p$: at $p = 3$, $q = 5$ the group H_1 has order p^q and exponent p^2 and is not a B-group.*

Herbig's Theorem B states that a group of order p^q, for primes $q < p$, with exponent at least p^2 is a B-group; the proof reduces, via the O'Nan–Scott theorem, to two cases in which $q < p$ forces exponent p — the regular subgroups of $S_p \wr S_q$ in the product action [9, Lemma 4.1] and the regular subgroups of $\mathrm{AGL}(q, p)$ [9, Proposition 5.1] — the almost simple case having been excluded outright by [9, Proposition 3.2]. Both reductions fail at $p = 3$, $q = 5$, and Corollary 4.9 shows the conclusion fails with them. [9] already records that $q = p$ is not allowed, citing the nonabelian group of order 27 and exponent 9 inside $\mathrm{PSU}(4, 2)$ on 27 points; what is new is a witness with $q > p$, and one that is nonabelian of exponent p^2 inside an affine group, by Remark 3.6. In the same vein, [9] closes with the question *"Which regular subgroups of* $\mathrm{AGL}(5, p)$ *lie in a uniprimitive subgroup of* $\mathrm{AGL}(5, p)$*?"*; since $\Gamma \leq \mathrm{AGL}(5, 3)$ is uniprimitive, H_0, H_1 and H_2 are three answers at $p = 3$, two of them of exponent 9.

5. The scope of the computation

This section states what was searched, because the value of a lower bound is exactly the description of what it is a lower bound over.

The census. GAP's primitive-groups library returns 36 primitive groups of degree 243. Six are 2-transitive: the two of orders $58806 = 243 \cdot 242$ and 294030, the two the library names $\mathrm{AGL}(5, 3)$ and $\mathrm{ASL}(5, 3)$ (its numbers 17 and 18), and A_{243}, S_{243}. That leaves 30 uniprimitive groups, every one of them of affine type, with an elementary abelian regular socle of order 3^5. Their Sylow 3-subgroups have order 3^5 for fourteen of them, 3^6 for seven, 3^7 for four and $3^9 = 19683$ for five. Every regular subgroup of order 243 of such a group is a 3-group, hence conjugate into a Sylow 3-subgroup, and conjugates of regular subgroups are regular; so it suffices to enumerate the subgroups of order 243 of one Sylow 3-subgroup per group and test each for regularity. This is the strategy of the script in [9]; we replaced its call to `ConjugacyClassesSubgroups` of the Sylow subgroup by `LatticeByCyclicExtension` with the subgroup-closed filter $|H| \leq 243$, which is complete at the order needed and strictly cheaper.

What ran. All fourteen uniprimitive groups with Sylow 3-subgroup of order 3^5, five of the seven with Sylow order 3^6, and two of the four with Sylow order 3^7. Every candidate was tested twice, by the restricted-permutation-character test of [9] and by an independent orbit test, and the two tests agreed on every candidate. Five isomorphism types of regular subgroup were found in that range. Three of them — C_3^5 and the groups H_1 and H_2 of Corollary 4.6, all three inside `PrimitiveGroup(243,19)`, which is the witness Γ used throughout this paper — are the ones carried into the formal development. The other two came from the last group of the range, after the formal development had been built; they are Remark 5.1 below and enter no theorem here.

What did not run. The five uniprimitive groups whose Sylow 3-subgroup has order 3^9, and the remaining two with Sylow order 3^7 together with the two of Sylow order 3^6 that followed them in the enumeration order. On a Sylow subgroup of order 3^9 the cyclic-extension lattice had not returned after 26 minutes on one core, against roughly 30 seconds for the 3^6 cases; the search was stopped rather than completed.

Hence: no completeness claim. Nothing here says that the non-B-groups of order 243 are exactly the ones listed. Two pieces of evidence say the list is still growing. First, the unsearched groups include the largest Sylow subgroups, where the subgroup lattice is richest. Second:

Remark 5.1. Two further isomorphism types of order 243, which GAP names `SmallGroup(243,38)` $= (C_3 \times C_3)$:$(C_9$:$C_3)$ and `SmallGroup(243,6)` $= ((C_9 \times C_3)$:$C_3)$:C_3, were found as regular subgroups of `PrimitiveGroup(243,29)`, the affine group 3^5:$(2 \times M_{11})$ of order 3849120, at the very end of the run — one of the two Sylow-3^7 groups that did finish. That computation has been repeated: the Sylow 3-subgroup, of order $3^7 = 2187$, has 61 classes of subgroups of order 243, both regularity tests agree on all 61, and the regular ones realise exactly four isomorphism types — the two above, together with the types of H_0 and H_1. This is GAP output only: no witness for the two new types has been transcribed into the formal development, no statement about them is machine-checked, and they are excluded from every theorem and corollary above. We record them because they are direct evidence that the search was still producing new types when it stopped.

The control that did not run. The natural positive control for the whole pipeline is degree 81, where [9, Lemma 6.2] determines the B-groups of order 81 — exactly C_{81}, $C_{27} \times C_3$ and `SmallGroup(81,`k`)` for $k = 6, 10, 14$ — so what a run of the script should return is the other ten of the fifteen groups of that order. It was launched and *did not finish* inside a ten-minute budget, because the primitive groups of degree 81 include AGL$(4, 3)$, whose Sylow 3-subgroup has order 3^{10}. We do not claim to have reproduced Herbig's order-81 list. The controls that did run are the ones described above: two independent regularity tests inside GAP, an independent reimplementation of the composition and closure arithmetic in Python before any formal statement was written, Theorem 3.1 as the non-vacuity check, and Theorem 3.4 as the check that the witness is not accidentally 2-transitive — in which case its regular subgroups would say nothing at all about B-groups.

6. Verification

Lemma 3.2 and Theorems 3.1, 3.3, 3.4, 4.1, 4.2, 4.4 and 4.5 have been formally verified in Lean 4, in a development free of `sorry` and of user-declared axioms; repository reference to be added at submission. The core module imports nothing at all — no *Mathlib*, no *Batteries* — so that the finite computations run in a small memory footprint. Lemma 3.2 and the derivation of Theorem 3.3 from it are kernel-clean: they depend on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`. What is delegated to compiled evaluation, through Lean's `native_decide`, is exactly the finite searches, and only those: the range and size check of Theorem 3.1; the 242 closure runs behind Theorem 3.3; the three properties of the pair set in Theorem 3.4; the four checks (R1)–(R4) for each of the three spanning structures in Theorems 4.1 and 4.4; and the order statistics, exponents and commutation counts of Theorems 4.2 and 4.5. Everything else — Lemmas 2.1 and 2.2, the corollaries, and the arithmetic of Corollary 4.6 — is ordinary mathematics, and the passages that were checked outside the formal development are named where they occur (injectivity of the tables before Corollary 3.5; the membership statements in Corollary 4.3 and Remark 4.7; everything in Remarks 3.6, 4.8 and 5.1). The two files compile in about 8 seconds and 2 minutes 40 seconds respectively. All permutation data were produced in GAP [8] and re-derived independently in Python before being transcribed; the regularity of each of H_0, H_1, H_2 was established three times over — by GAP's restricted-character test, by a GAP orbit test, and by the Python implementation — before any of it was stated formally.

7. Open questions

Question 7.1. Complete the case $p = 3$. What is missing is the five uniprimitive groups of degree 243 with Sylow 3-subgroup of order 3^9, plus four smaller ones. Enumerating every subgroup of order 243 inside a group of order 3^9 is the wrong instrument: what is wanted is only the semiregular subgroups of order equal to the degree, and those can be built up directly — point by point along an orbit — instead of being filtered out of a full subgroup lattice. All thirty uniprimitive groups of degree 243 are of affine type, and it would be worth knowing whether the standard description of the regular subgroups of an affine group as extra algebraic structure on the underlying vector space makes the remaining cases a computation of a different and cheaper kind: the regular subgroups of

the affine group of a vector space over a field F correspond to F-braces [6], and the abelian ones to radical F-algebras [5].

Question 7.2. Settle $p = 5$. The small-groups library contains all 77 groups of order 3125 and the primitive-groups library all 122 primitive groups of degree 3125, of which seven are 2-transitive, leaving 115 uniprimitive. Their Sylow 5-subgroups have order 5^5 for eight of them and 5^6 for ninety-nine — but 5^9 for the remaining eight, the library's numbers 84 to 91. So the obstruction that stopped the case $p = 3$ recurs at $p = 5$, on the same scale and in the same shape, and the group-theoretic half is *not* cheaper than at $p = 3$. The certification half is dearer again: the block closure of Section 3.2 costs $\Theta(n^2)$ per seed and is run at $n - 1$ seeds, so a full sweep grows like n^3; from $n = 243$ to $n = 3125$ that is a factor of about 170 per seed and about 2100 over the sweep, which puts a straight port of the degree-243 file far outside the cost that file took. Closing one seed per orbit of a point stabilizer, rather than one per point, would divide the work by the average suborbit length, and is the natural next step for the instrument.

Question 7.3. For which ranks a is the elementary abelian group C_2^a a B-group? It is known to fail to be one whenever $2^a - 1$ is composite [20], and [9] records that no complete criterion is known; the ranks with $2^a - 1$ prime are the ones left over. Rank 5 is settled by the absence of any uniprimitive group of degree 32, so C_2^5 *is* a B-group [9]. Rank 7, degree 128, is the first case the primitive-groups library can decide, and the three certificates of Section 3 apply verbatim and cost materially less at degree 128 than at degree 243.

References

[1] M. D. Atkinson, *An algorithm for finding the blocks of a permutation group*, Math. Comp. **29** (1975), no. 131, 911–913.

[2] H. A. Bender, *A determination of the groups of order p^5*, Ann. of Math. (2) **29** (1927), 61–72.

[3] S. Bouc, *Relative B-groups*, Doc. Math. **24** (2019), 2431–2462.

[4] W. Burnside, *Theory of Groups of Finite Order*, 2nd ed., Cambridge University Press, 1911; reprinted by Dover, New York, 1955, §§251–252.

[5] A. Caranti, F. Dalla Volta and M. Sala, *Abelian regular subgroups of the affine group and radical rings*, Publ. Math. Debrecen **69** (2006), no. 3, 297–308.

[6] F. Catino and R. Rizzo, *Regular subgroups of the affine group and radical circle algebras*, Bull. Aust. Math. Soc. **79** (2009), no. 1, 103–107.

[7] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics **163**, Springer, New York, 1996.

[8] The GAP Group, *GAP – Groups, Algorithms, and Programming*. The computations reported here used version 4.11.1 with the `primgrp` and `smallgrp` packages; library index numbers such as `PrimitiveGroup(243,19)` are that version's.

[9] C. Herbig, *A Determination of B-groups of Order p^4*, arXiv:2608.26463v1 (2026). Numbered results are cited from v1.

[10] G. A. Jones, *Regular subgroups of uniprimitive permutation groups of degree p^3, where p is prime*, Quart. J. Math. Oxford Ser. (2) **23** (1972), no. 3, 325–336.

[11] W. Knapp, *On Burnside's method*, J. Algebra **175** (1995), no. 2, 644–660.

[12] R. Kochendörffer, *Untersuchungen über eine Vermutung von W. Burnside*, Schr. Math. Semin. Inst. Angew. Math. Univ. Berlin **3** (1937), 155–180.

[13] C. H. Li, *The finite primitive permutation groups containing an abelian regular subgroup*, Proc. London Math. Soc. (3) **87** (2003), no. 3, 725–747.

[14] M. W. Liebeck, C. E. Praeger and J. Saxl, *Regular subgroups of primitive permutation groups*, Mem. Amer. Math. Soc. **203** (2010), no. 952, vi+74 pp.

[15] B. Maskit, *On boundaries of Teichmüller spaces and on Kleinian groups. II*, Ann. of Math. (2) **91** (1970), 607–639.

[16] P. Potočnik, *B-groups of order a product of two distinct primes*, Math. Slovaca **51** (2001), no. 1, 63–67.

[17] I. Ponomarenko and G. Ryabov, *Notes on B-groups*, arXiv:2410.22998v2 (2024).

[18] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York–London, 1964 (translated from the German by R. Bercov).

[19] H. Wielandt, *Zur Theorie der einfach transitiven Permutationsgruppen. II*, Math. Z. **52** (1949/50), 384–393.

[20] M. Wildon, *Permutation groups containing a regular abelian subgroup: the tangled history of two mistakes of Burnside*, Math. Proc. Cambridge Philos. Soc. **168** (2020), no. 3, 613–633.