A non-powerful subgroup of p-th powers for every odd prime

Kyrylo Muliarchyk

Abstract

For each odd prime p, let $V = \mathbb{F}_p[r]/(r^{2p})$, regarded as a vector space. We first construct two explicit linear automorphisms Y, T and determine the subgroup $B_p = \langle Y, T\rangle \le \mathrm{GL}(V)$: it is $(C_{p^2} \times C_p^{p-2}) \rtimes C_p$, of order p^{p+1}, with the action specified below. The affine semidirect product of the additive group of V by B_p has order p^{3p+1} and exponent p^2. Its literal set of p-th powers is a subgroup isomorphic to $\mathrm{UT}_3(\mathbb{F}_p) \times C_p^{p-1}$, and hence is nonabelian of exponent p. This gives a uniform negative answer to the odd-prime part of Kourovka Notebook Problem 21.137. The proof is self-contained.

1 The problem and the earlier examples

Question. Problem 21.137, posed by L. Wilson, is the following [1, p. 187].

> **21.137.** If the p-th powers in a finite p-group form a subgroup, must that subgroup be powerful? That is, for $p \neq 2$, if the p-th powers in a p-group of exponent p^2 form a subgroup, must that subgroup be abelian? For a 2-group of exponent 8, if the squares form a subgroup, must that subgroup be abelian?
>
> *L. Wilson*

For a finite group X, distinguish

$$\mathcal{P}_p(X) = \{x^p : x \in X\} \qquad \text{from} \qquad X^p = \langle x^p : x \in X\rangle.$$

For odd p, a finite p-group K is powerful if $[K, K] \le K^p$. Thus an exponent-p subgroup is powerful exactly when it is abelian. It is essential to determine the literal power set, not merely the subgroup it generates.

For $p = 3$, the solution comment in [1, p. 187] cites the author's earlier counterexample [2], which has order 3^{15}, exponent 9, and cube subgroup $\mathrm{UT}_3(\mathbb{F}_3) \times C_3^3$. The present construction gives a smaller example of order 3^{10} and extends uniformly to every odd prime. Its affine structure emerged from the order-3^{10} example; the proof below does not depend on the discovery computation or on the earlier Lie-theoretic construction.

2 The vector space and its linear automorphism group

Fix an odd prime p. Put

$$V = \mathbb{F}_p[r]/(r^{2p}) = \mathrm{span}_{\mathbb{F}_p}\{1, r, \dots, r^{2p-1}\}.$$

We use multiplication in this truncated polynomial ring to describe linear maps, but V will enter the final group as its *additive* group. In particular,

$$\mathrm{Aut}(V, +) = \mathrm{GL}_{\mathbb{F}_p}(V) = \mathrm{GL}(V).$$

All fractions below are interpreted in the truncated ring. For example, $(1-r)^{-1} = 1 + r + \cdots + r^{2p-1}$.

Write each vector $f \in V$ as its unique polynomial representative $f = f(r)$ of degree less than $2p$. Define $Y, T : V \to V$ by

$$Y(f)(r) = (1 + r)f(r), \qquad T(f)(r) = \frac{1}{1-r} f\Big(\frac{r}{1-r}\Big). \tag{2.1}$$

Both expressions are reduced modulo r^{2p}. In the second formula, first substitute $r/(1-r)$ for the variable in $f(r)$, then multiply by $(1-r)^{-1}$. On basis monomials,

$$Y(r^i) = r^i + r^{i+1}, \qquad T(r^i) = \sum_{j=i}^{2p-1} \binom{j}{i} r^j, \quad 0 \le i < 2p, \tag{2.2}$$

where $r^{2p} = 0$ and the binomial coefficients are reduced modulo p. Thus both maps have triangular matrices with diagonal entries one, and are invertible $\mathbb{F}_p$-linear maps. They are not ring automorphisms. We now define the linear group

$$\boxed{B_p = \langle Y, T \rangle \le \mathrm{Aut}(V, +) = \mathrm{GL}(V).} \tag{2.3}$$

We determine its structure and size before forming the affine group.

2.1 The normal subgroup of multiplication operators

For a unit $q = q(r)$ of the truncated ring, write $M_q(f)(r) = q(r)f(r)$. Put

$$h_a = 1 - ar \quad (a \in \mathbb{F}_p), \qquad U = \langle M_{h_a} : a \in \mathbb{F}_p^\times \rangle, \qquad c = Y^p = M_{1+r^p}.$$

The representation $q \mapsto M_q$ is faithful, since $M_q(1) = q$. Where convenient, we identify a unit with its multiplication operator. For $a \in \mathbb{F}_p$, set

$$\phi_a(r) = \frac{r}{1-ar}, \qquad T_a(f)(r) = \frac{1}{1-ar} f(\phi_a(r)).$$

These substitutions are well defined modulo r^{2p}, since $\phi_a(r)$ is divisible by r. Direct substitution gives

$$T_a T_b = T_{a+b}, \qquad T_a M_q T_{-a} = M_{q \circ \phi_a}, \qquad h_b \circ \phi_a = \frac{h_{a+b}}{h_a}. \tag{2.4}$$

In particular, $T = T_1$ has order p and normalizes U.

Lemma 2.1. *The linear group has the internal semidirect-product decomposition*

$$B_p = U \rtimes \langle T \rangle.$$

Every element of B_p has a unique form $M_q T_a$, with $M_q \in U$ and $a \in \mathbb{F}_p$. The action of $\langle T \rangle$ on U is

$$T M_{h_b} T^{-1} = M_{h_{b+1}/h_1}.$$

Proof. Since $Y = M_{h_{-1}}$, its conjugates by T_a are multiplication by h_{a-1}/h_a. These ratios generate every h_a: start with $h_0 = 1$ and recover successive h_a around the additive cycle $\mathbb{F}_p$. Hence $B_p = U\langle T \rangle$.

If $a \neq 0$, then T_a is not multiplication by a unit. Its value on 1 is $(1-ar)^{-1}$, but

$$T_a(r) = \frac{r}{(1-ar)^2} \neq \frac{r}{1-ar};$$

the coefficient of r^2 in the difference is $a \neq 0$. Thus $U \cap \langle T \rangle = 1$. Normalization follows from (2.4), proving all assertions. □

Lemma 2.2. *Reduction modulo r^{p+1} induces an isomorphism*

$$U \longrightarrow 1 + r\mathbb{F}_p[r]/(r^{p+1}).$$

Consequently,

$$U \cong C_{p^2} \times C_p^{p-2}, \qquad |U| = p^p.$$

Proof. The group U is abelian. Each generator satisfies

$$h_a^p = 1 - ar^p = (1 + r^p)^{-a}.$$

The operator $c = M_{1+r^p}$ has order p, and $Y^p = c$, so $U^p = \langle c \rangle$. The quotient U/U^p is elementary abelian and is generated by at most $p-1$ elements. Thus $|U| \le p^p$.

To prove surjectivity of reduction, define

$$q_1 = 1 + r, \qquad q_{j+1} = \frac{q_j(\phi_1(r))}{q_j(r)}.$$

By (2.4), all the M_{q_j} lie in U. If $q = 1 + \lambda r^j + O(r^{j+1})$, then

$$\frac{q(\phi_1(r))}{q(r)} = 1 + j\lambda r^{j+1} + O(r^{j+2}). \tag{2.5}$$

Here $O(r^m)$ denotes an element of the ideal $r^m V$. Inductively,

$$q_j = 1 + (j-1)! r^j + O(r^{j+1}) \qquad (1 \le j \le p-1).$$

The leading coefficients are nonzero. These units, together with $1 + r^p$, prescribe the coefficients of any principal unit modulo r^{p+1} successively, from degree one through degree p. Indeed, multiplying by a suitable integer power of a unit beginning in degree j changes that coefficient arbitrarily and leaves all lower coefficients unchanged. Reduction is therefore surjective.

Its target has p^p elements. The upper bound on $|U|$ shows that reduction is an isomorphism. Finally, U has exponent p^2 and $|U^p| = p$. Its decomposition into cyclic factors therefore contains one factor of order p^2, with all other nontrivial factors of order p. The order gives the stated $p-2$ additional factors. □

Proposition 2.3. *With the action specified in Lemma 2.1,*

$$\boxed{B_p \cong (C_{p^2} \times C_p^{p-2}) \rtimes C_p, \qquad |B_p| = p^{p+1}.} \tag{2.6}$$

Moreover, for $M_q \in U$ and $a \in \mathbb{F}_p$,

$$(M_q T_a)^p = \begin{cases} M_{q^p} \in \langle c \rangle, & a = 0, \\ I, & a \neq 0. \end{cases} \tag{2.7}$$

Proof. The structure and order follow from the two lemmas. For $a \neq 0$, (2.4) shows that the multiplier in $(M_q T_a)^p$ is

$$\prod_{j=0}^{p-1} q(\phi_{ja}(r)).$$

This is multiplicative in q. On a generator h_b, its value is

$$\prod_{j=0}^{p-1} \frac{h_{b+ja}}{h_{ja}} = 1,$$

since ja and $b + ja$ both run through $\mathbb{F}_p$. Hence the product is one on every $M_q \in U$. When $a = 0$, use $U^p = \langle c \rangle$. □

3 The affine semidirect product and the theorem

Having defined and determined $B_p \le \mathrm{GL}(V)$, we form

$$\boxed{G_p = (V, +) \rtimes B_p = (V, +) \rtimes \langle Y, T \rangle.} \tag{3.1}$$

The action in this semidirect product is exactly the linear action already defined; no further action is chosen. Explicitly,

$$(v, b)(w, d) = (v + b(w), bd) \qquad (v, w \in V,\ b, d \in B_p). \tag{3.2}$$

Thus (v, b) is the affine transformation $f \mapsto b(f) + v$. The normal subgroup V consists of all translations, the subgroup B_p consists of linear transformations, and

$$(0, b)(v, I)(0, b)^{-1} = (b(v), I).$$

In particular,

$$|G_p| = |V|\,|B_p| = p^{2p}p^{p+1} = p^{3p+1}. \tag{3.3}$$

Put

$$W = r^{p-1}V = \operatorname{span}_{\mathbb{F}_p}\{r^{p-1}, r^p, \dots, r^{2p-1}\}, \qquad R_p = W \rtimes \langle c\rangle.$$

The space W is c-invariant, so R_p is a subgroup of G_p.

Theorem 3.1. *For every odd prime p, the group G_p has order p^{3p+1}, exponent p^2, and*

$$\mathcal{P}_p(G_p) = R_p \cong \mathrm{UT}_3(\mathbb{F}_p) \times C_p^{p-1}. \tag{3.4}$$

Thus its literal set of p-th powers is a nonabelian subgroup of order p^{p+2} and exponent p, and is not powerful.

3.1 The power formula and containment

From (3.2),

$$(v, b)^p = (N_b v, b^p), \qquad N_b = I + b + \cdots + b^{p-1} = (b - I)^{p-1}. \tag{3.5}$$

The last equality follows by expanding $(X - 1)^{p-1}$ in characteristic p. Every $b \in B_p$ preserves the ideals r^iV and acts trivially on each successive quotient. Hence

$$(b - I)(r^iV) \subseteq r^{i+1}V, \qquad N_bV \subseteq r^{p-1}V = W.$$

Proposition 2.3 gives $b^p \in \langle c\rangle$. Therefore

$$\mathcal{P}_p(G_p) \subseteq R_p. \tag{3.6}$$

3.2 The structure of the candidate power subgroup

On W, multiplication by $c = 1 + r^p$ satisfies

$$c(r^{p-1}) = r^{p-1} + r^{2p-1}, \qquad c(r^j) = r^j \quad (p \le j \le 2p - 1). \tag{3.7}$$

Thus c acts by one nontrivial shear. The subgroup generated by c and the translations by r^{p-1}, r^{2p-1} is the Heisenberg group $\mathrm{UT}_3(\mathbb{F}_p)$. The remaining translations $r^p, \dots, r^{2p-2}$ form a central direct factor C_p^{p-1}. This proves the asserted structure of R_p, and its order is $p^{p+1}p = p^{p+2}$.

For completeness, on W write $c = I + D$, where $D^2 = 0$. For $s \in \mathbb{F}_p$,

$$\sum_{j=0}^{p-1} c^{sj} = pI + s\binom{p}{2}D = 0,$$

because p is odd. Formula (3.5) then shows that R_p has exponent p. Consequently (3.6) implies that every element of G_p has order dividing p^2. Since Y has order p^2, the exponent is exactly p^2.

4 Every element of the candidate subgroup is a power

We prove the reverse of (3.6). This is the step that establishes closure of the literal power set.

4.1 The cosets with nonidentity linear part

Let $1 \le s \le p - 1$. The norm N_{Y^s} is multiplication by

$$\big((1 + r)^s - 1\big)^{p-1}.$$

Since $(1 + r)^s - 1 = sr + O(r^2)$, this multiplier is r^{p-1} times a unit, so its image is exactly W. Also $(Y^s)^p = c^s$. It follows from (3.5) that every element of $W \times \{c^s\}$ is a single p-th power.

4.2 The pure translations

For a nonzero polynomial w, write $\nu(w)$ for its smallest nonzero degree.

Lemma 4.1. *Two nonzero vectors of W are in the same U-orbit if and only if they have the same smallest degree and the same coefficient in that degree.*

Proof. Multiplication by a unit with constant coefficient one preserves these data. Conversely, write the two vectors as $w = \lambda r^d u$ and $w' = \lambda r^d u'$, where $d \geq p-1$, $\lambda \neq 0$, and u, u' are principal units modulo r^{2p-d}. Since $2p - d \leq p+1$, Lemma 2.2 supplies a multiplier $q \in U$ whose reduction is u'/u to that precision. Then $qw = w'$. □

For $k = 0, 1, \ldots, p$, define a mixed linear transformation

$$b_k = Y^{-k}T \in B_p.$$

Proposition 2.3 shows that $b_k^p = I$. Expanding its action on a monomial gives

$$\begin{aligned} b_k(r^i) &= (1+r)^{-k}\frac{r^i}{(1-r)^{i+1}}, \\ (b_k - I)(r^i) &= (i+1-k)r^{i+1} + O(r^{i+2}). \end{aligned} \tag{4.1}$$

Starting with r^k and applying $b_k - I$ successively $p-1$ times, the leading coefficients encountered are $1, 2, \ldots, p-1$. None vanishes, and their product is -1 by Wilson's theorem. Higher-degree terms cannot change this leading coefficient, since each application raises degree by at least one. Therefore

$$N_{b_k}(r^k) = -r^{p+k-1} + O(r^{p+k}), \qquad 0 \leq k \leq p. \tag{4.2}$$

The exponents $p+k-1$ run through every possible smallest degree $p-1, \ldots, 2p-1$ in W. Since $b_k^p = I$, (3.5) realizes each vector in (4.2) as a pure translation that is a p-th power. Scaling the input r^k realizes every nonzero leading coefficient.

Finally, being a p-th power is invariant under conjugation, and

$$(0, M_q)(w, I)(0, M_q)^{-1} = (qw, I) \qquad (M_q \in U).$$

Lemma 4.1 therefore turns these witnesses into every nonzero translation in W. The zero translation is a power as well. Together with the nonidentity linear-part cosets, this proves $R_p \subseteq \mathcal{P}_p(G_p)$, and hence equality. The group R_p is nonabelian by (3.7), while $R_p^p = 1$, so it is not powerful. This completes the proof of Theorem 3.1.

Remark ($p = 2$). The final question for $p = 2$ also has a negative answer. The solution comment to Problem 21.137 in [1, p. 187] records this answer and attributes it to a letter of A. Chang. The construction in the present paper treats all odd primes.

Acknowledgement

This work was carried out with assistance from ChatGPT.

References

[1] E. I. Khukhro and V. D. Mazurov (eds.), *Unsolved Problems in Group Theory. The Kourovka Notebook*, 21st ed., Novosibirsk, 2026, version 46, Problem 21.137, p. 187. arXiv:1401.0300v46.

[2] K. Muliarchyk, *A counterexample to Kourovka Problem 21.137 for $p = 3$*, preprint, 2026. Kourovka Notebook repository.