AN EXPLICIT FINITE 2-GROUP FOR KOUROVKA NOTEBOOK PROBLEM 20.76

Abstract. This draft typesets an imported counterexample claim. The submitted argument gives a finite 2-group of order 2^{144e+1}, where $e = 2^{56363762}$, with every abelian normal subgroup of order at most 2^{42e} and an elementary abelian subgroup of order 2^{85e}. Its certificate is mathematical. The historical validator's PASS is an external record; this import has not completed the repository's verification, citation, novelty, or GAP checks.

Problem and import status

Problem 20.76 of the Kourovka Notebook asks:

> Let G be a finite p-group and assume that all abelian normal subgroups of G have order at most p^k. Is it true that every abelian subgroup of G has order at most p^{2k}? L. Pyber

The statement comes from the repository's problem record, which uses Kourovka Notebook version `arXiv:1401.0300v45`. The following five sections preserve the submitted mathematical certificate. This is an imported claim, not a repository candidate or solved result. No novelty claim or new bibliographic citation is added. The final section distinguishes the historical checks from the verification still required.

All fields, vector spaces, and bilinear forms in this construction have characteristic two. All integer parameters below are exact. The construction is extremely large; its certificate is mathematical and does not require enumerating its elements or its subgroups.

1. Parameters and a fully specified finite field

Put

$$r = 59, \qquad s = 13, \qquad d = 9, \qquad n = s\binom{r}{2} = 22243,$$

$$\ell = n + d(r-d) - s\binom{d}{2} = 22225,$$

$$t = 56363762 = 2534n, \qquad e = 2^t, \qquad b = 2^{2534}.$$

Thus $b^n = e$. Let F be the following explicitly specified field of order 2^e, with specified element α of degree e over $\mathbb{F}_2$.

Start with $K_0 = \mathbb{F}_2$ and $\beta_0 = 1$. For $j = 1, \dots, t$, define

$$K_j = K_{j-1}[Y_j]/(Y_j^2 + Y_j + \beta_{j-1}), \qquad \theta_j = \overline{Y_j}, \qquad \beta_j = \beta_{j-1}\theta_j.$$

Use the natural embeddings of the earlier fields into the later fields. Set $F = K_t$ and $\alpha = \theta_t$. This recursive quotient description fixes the field and all subsequent coefficients; it involves no search for a group or for forms with a desired property.

Here is a verification that the recursion defines fields and that α has the required degree. In a finite field K of characteristic two, the image of $\xi \mapsto \xi^2 + \xi$ is exactly the kernel of the absolute trace to $\mathbb{F}_2$: the image is contained in that kernel, and both have $|K|/2$ elements. Consequently $Y^2 + Y + \gamma$ is irreducible over K if $\mathrm{Tr}_{K/\mathbb{F}_2}(\gamma) = 1$. Initially $\mathrm{Tr}_{K_0/\mathbb{F}_2}(\beta_0) = 1$. At each step the relative trace of θ_j to K_{j-1} is 1, so trace transitivity gives

$$\mathrm{Tr}_{K_j/\mathbb{F}_2}(\beta_j) = \mathrm{Tr}_{K_{j-1}/\mathbb{F}_2}(\beta_{j-1}) = 1.$$

Inductively all the quadratic polynomials used above are irreducible and $[K_j : \mathbb{F}_2] = 2^j$. Moreover $\theta_j \notin K_{j-1}$. Every proper subfield of K_j lies in its unique maximal proper subfield K_{j-1},

Date: Draft.

since 2^j is a power of two. Thus $[\mathbb{F}_2(\theta_j) : \mathbb{F}_2] = 2^j$. In particular the minimal polynomial of α over $\mathbb{F}_2$ has degree e. The elementary finite-field facts used here also follow from the Frobenius map and its fixed fields.

2. Explicit alternating forms with no common 9-dimensional isotropic space

List the triples

$$(h, i, j), \qquad 1 \le h \le 13, \qquad 1 \le i < j \le 59,$$

in lexicographic order, indexed by $a = 0, \dots, n-1$. To the ath triple assign $c_{h,i,j} = \alpha^{b^a}$. On $U = F^{59}$ define thirteen alternating bilinear forms

$$S_h(u, v) = \sum_{i<j} c_{h,i,j}(u_i v_j + u_j v_i).$$

We prove that no 9-dimensional F-subspace of U is simultaneously isotropic for these forms. This proof specifies a certificate without needing to compute the coefficients of any eliminant.

First treat the n coefficients $C_{h,i,j}$ as independent indeterminates over $\mathbb{F}_2$. Fix a set I of nine coordinate positions. Every 9-dimensional subspace whose projection to those positions is an isomorphism has a unique basis matrix whose nine columns in I are the identity matrix. Its remaining entries are $d(r-d) = 450$ free parameters.

For each form, its vanishing on the 36 pairs of distinct basis vectors determines the 36 coefficients indexed by pairs within I. Indeed the coefficient on the corresponding pivot pair occurs with coefficient 1, and all the other pivot-pair coefficients occur with coefficient 0. The determined coefficient is a polynomial of total degree at most three in the 450 basis parameters and the other coefficients of the forms. Therefore all arrays admitting an isotropic subspace in this chart are in the image of a polynomial map

$$f_I : \mathbb{A}^\ell \longrightarrow \mathbb{A}^n, \qquad \ell = 22225,$$

defined over $\mathbb{F}_2$ and with coordinate polynomials of degree at most three. This parametrization is valid over every field extension of $\mathbb{F}_2$.

Let $D = 2^{2500}$. The number of monomials of total degree at most D in n variables is $\binom{n+D}{n}$. After substitution by f_I these monomials lie in the space of polynomials of total degree at most $3D$ in ℓ variables, of dimension $\binom{\ell+3D}{\ell}$. The former dimension is strictly larger. For completeness, $D \ge \ell$, $n - \ell = 18$, and $n < 2^{15}$, so

$$\frac{\binom{n+D}{n}}{\binom{\ell+3D}{\ell}} \ge \frac{D^{18}}{4^\ell n^{18}} > 2^{18\cdot 2500 - 2\cdot 22225 - 18\cdot 15} = 2^{280} > 1.$$

The first inequality follows by writing each binomial coefficient as a product and using $n!/\ell! \le n^{18}$.

Linear dependence over $\mathbb{F}_2$ thus provides a nonzero polynomial P_I in the n coefficient variables, of total degree at most D, for which $P_I(f_I) = 0$ identically. This is a polynomial identity, not merely a statement about points rational over $\mathbb{F}_2$.

There are $M = \binom{59}{9} = 12565671261 < 2^{34}$ charts. The product $P = \prod_I P_I$ is a nonzero polynomial over $\mathbb{F}_2$, of total degree at most $MD < 2^{2534} = b$. Every coefficient array that admits a common 9-dimensional isotropic space, over any extension field, makes P vanish: such a space belongs to at least one of the charts.

Now substitute $C_a = \tau^{b^a}$ in P, using the coefficient ordering specified above. Distinct monomials of P remain distinct powers of τ, since every individual variable exponent is less than b and base-b expansions are unique. The resulting polynomial $Q(\tau) \in \mathbb{F}_2[\tau]$ is nonzero and has degree at most

$$(b-1)(1 + b + \cdots + b^{n-1}) = b^n - 1 = e - 1.$$

Since α has degree e over $\mathbb{F}_2$, $Q(\alpha)$ is nonzero. Hence the specified coefficient array makes P nonzero, and it cannot admit a common 9-dimensional isotropic subspace. In fact the same assertion holds over the algebraic closure of F, although only the assertion over F is needed.

3. The group

Define the bilinear map $A : U \times U \longrightarrow F^{13}$ by

$$A_h(u, v) = \sum_{i<j} c_{h,i,j} u_i v_j.$$

Then $S(u, v) = A(u, v) + A(v, u)$.

Let T have underlying set $U \times U \times F^{13} \times F^{13}$. Define multiplication by

$$\begin{aligned}(u, v, z, w)&(u', v', z', w') \\ &= (u + u',\ v + v',\ z + z' + A(u, v'),\ w + w' + A(v', u)).\end{aligned}$$

The identity is $(0, 0, 0, 0)$. The inverse of (u, v, z, w) is

$$(u, v, z + A(u, v), w + A(v, u)).$$

Associativity follows directly by expanding the bilinear terms on both sides. In particular T is a group of order $|F|^{2r+2s} = |F|^{144}$. The subgroup

$$W = \{(0, 0, z, w) : z, w \in F^{13}\}$$

is central in T, and T/W identifies with $U \oplus U$ under addition.

Define

$$\sigma(u, v, z, w) = (v, u, w + A(v, u), z + A(u, v)).$$

This is an involutory automorphism of T. To check it, write

$$\Phi(u, v) = (A(u, v), A(v, u))$$

and let J exchange the two F^{13} summands, so that $J\Phi(u, v) = \Phi(v, u)$. The multiplication's central cocycle is $\Phi(u, v')$. The central correction in σ is $\Phi(v, u)$. Bilinearity and the displayed identity show $\sigma(xy) = \sigma(x)\sigma(y)$, and applying σ twice adds $J\Phi(v, u) + \Phi(u, v) = 0$. On T/W the automorphism exchanges the two U summands, so it is not the identity. It preserves W.

Define $G = T \rtimes \langle\sigma\rangle$, where σ has order two. Equivalently, on $T \times \{0, 1\}$ use

$$(x, \epsilon)(y, \eta) = (x\sigma^{\epsilon}(y), \epsilon + \eta \pmod 2).$$

Then

$$|G| = 2|F|^{144} = 2^{144e+1},$$

so G is a finite 2-group.

For elements of T with images $(u, v), (u', v')$ in T/W, their commutator is central and has coordinates

$$(A(u, v') + A(u', v),\ A(v', u) + A(v, u')).$$

In particular the commutator on the diagonal subspace

$$\Delta = \{(u, u) : u \in U\}$$

is $(S(u, u'), S(u, u'))$.

4. Bound on every abelian normal subgroup

Let B be any abelian normal subgroup of G. First B is contained in T. If not, choose $x \in B$ outside T. Its conjugation action on T/W exchanges the two U summands: the T part of x acts trivially on T/W. Since B is normal, $[T, x]$ is contained in $B \cap T$. The images of these commutators in T/W range over all of Δ, because the image of swap $- 1$ on $U \oplus U$ is exactly Δ. Since B is abelian, the commutator form must vanish on Δ. The preceding formula would then make all S_h identically zero. This contradicts Section 2, since $r = 59 \geq 9$. Therefore $B \leq T$.

As W is central in T and normal in G, BW is also abelian and normal in G. Let $L = BW/W \leq T/W$. This is an $\mathbb{F}_2$-linear subspace, stable under the swap, on which the displayed commutator map vanishes. Let L_F be its F-linear span. Because the commutator map is F-bilinear and the swap is F-linear, L_F is still isotropic and swap-invariant.

Put $X = L_F \cap \Delta$. Under Δ's identification with U, X is simultaneously isotropic for the thirteen S_h. Thus $\dim_F X \le 8$. The endomorphism swap $- 1$ of L_F has kernel X and image contained in X. Rank–nullity therefore gives

$$\dim_F L_F \le 2 \dim_F X \le 16.$$

It follows that

$$|B| \le |BW| = |W|\,|L| \le |F|^{26+16} = 2^{42e}.$$

This applies to every abelian normal subgroup, without assumptions on its exponent or on whether it is initially F-linear.

5. Failure of the proposed conclusion

The subgroup

$$H = \{(u, 0, z, w) : u \in U,\ z, w \in F^{13}\} \le T \le G$$

is elementary abelian: its multiplication is coordinatewise addition. Its order is

$$|H| = |F|^{59+26} = 2^{85e}.$$

Take $p = 2$ and $k = 42e$. Section 4 proves that every abelian normal subgroup of G has order at most p^k. But

$$|H| = 2^{85e} > 2^{84e} = p^{2k}.$$

Thus G, $p = 2$, and $k = 42e$ give a counterexample to the exact statement of Kourovka Notebook Problem 20.76.

Verification scope and provenance

The decisive certificate is the mathematical argument above. It does not rely on a heuristic, on computing an eliminant, on a random choice, or on a claim that the enormous group has been enumerated. The supplied Python verifier checks the integer inequalities, polynomial chart identities, and group identities on small exact instances. Those finite sanity checks supplement, and do not replace, the proof above.

The source is `counterexample.txt` from the external run

`counterexample-only-astra-all-20260906-01-20.76-2c21c1f31c-e0-r0`.

That run records solver status `COMPLETE_COUNTEREXAMPLE` and a historical validator `PASS`. These labels are preserved as external claims. They do not establish the two independent repository CLEAN passes, citation audit, novelty search, or independent GAP corroboration required for repository candidate status; those checks remain pending.

The imported proof invokes elementary finite-field facts, polynomial dimension counting, and bilinearity and rank–nullity. The source supplies the displayed derivations and no bibliographic citations for these inputs. This transcription adds no citation and makes no claim of originality. Codex, using `gpt-6-astra`, prepared this draft on 14 September 2026. The prose and mathematical argument are retained; typography and notation are normalized. The source's polynomial indeterminate T is τ here, its tower indeterminates X_j are Y_j, its generic field variable x is ξ, its generic scalar c is γ, and its central-pair map F_0 is Φ. The group T, subspace X, and coefficient array $c_{h,i,j}$ retain their source meanings.

Byte-preserved originals, SHA256 hashes, and the check record are under `problems/20.76/experiments/imported-counterexample/`; packaging and notation checks are recorded in `problems/20.76/verification/import-packaging.md`.