COUNTEREXAMPLE TO KOUROVKA NOTEBOOK 20.4(C)

Import scope and status. This is a faithful typesetting of the archived argument, with its original claims and replay instructions retained. It concerns part (c) only. The historical runner's `PASS` is not a repository verifier verdict: the repository status remains `todo`; the full mathematical and citation audits and independent GAP corroboration remain pending. No novelty claim is made.

Problem 20.4(c)

A finite group G is said to be *cut* (or inverse semi-rational) if $\langle x\rangle = \langle y\rangle$ implies that x is conjugate to y or to y^{-1} for all $x, y \in G$. Let $O_p(G)$ denote the largest normal p-subgroup of G. Let G be a solvable cut group. Is it true that for $p \in \{5, 7\}$ the exponent of $O_p(G)$ divides p?

1. Witness and failed conclusion

Let $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, using the representatives $0, 1, 2, 3, 4$ and ordinary matrix multiplication reduced modulo 5. Let

$$G = B_6(\mathbb{F}_5) = \{\text{invertible upper triangular 6 by 6 matrices over } \mathbb{F}_5\}.$$

This finite solvable cut group has

$$O_5(G) = U_6(\mathbb{F}_5), \qquad \text{exponent } O_5(G) = 25,$$

so its normal 5-subgroup does not have exponent dividing 5. This refutes part (c), with $p = 5$. No assertion about parts (a) or (b) is needed.

The decisive cut verification is a reproducible finite computation with an elementary covering argument. It does not use a classification theorem, a database, a probabilistic test, or any unverified assertion from a prior run.

2. Finite group and solvability

The invertible upper triangular matrices form a group, as can be seen by back substitution for inverses. The diagonal homomorphism has kernel $U = U_6(\mathbb{F}_5)$ and image $(\mathbb{F}_5^*)^6$. Thus

$$|U| = 5^{15} = 30517578125,$$
$$|G| = 4^6 \cdot 5^{15} = 125000000000000,$$
$$G/U \text{ is abelian of order } 4^6.$$

Let J be the associative algebra of strictly upper triangular matrices. Then $J^6 = 0$ and $[1 + J^r, 1 + J^s]$ is contained in $1 + J^{r+s}$. Consequently $U''' = 1$, and $G'''' = 1$, so G is solvable. Since U is a normal 5-subgroup, U is contained in $O_5(G)$. The image of any 5-subgroup in G/U is trivial, so $O_5(G)$ is contained in U. Hence $O_5(G) = U$.

3. The element of order 25

Write E_{ij} for the matrix with its only nonzero entry, equal to 1, at position (i, j), where indices start at 1. Set

$$N = E_{12} + E_{23} + E_{34} + E_{45} + E_{56}, \qquad z = I_6 + N.$$

Then z belongs to U, $N^5 = E_{16}$, and $N^6 = 0$. In characteristic 5,

$$z^5 = I_6 + E_{16} \neq I_6, \qquad z^{25} = I_6.$$

Date: Draft.

Thus z has exact order 25. Every a in J satisfies $a^6 = 0$, and therefore $(I_6+a)^{25} = I_6+a^{25} = I_6$. This also proves $\operatorname{exponent} U = 25$. The producer and independent verifier both check the displayed powers.

4. The covering family for the cut computation

For $1 \le n \le 6$, let R_n be the following finite list of strictly upper triangular n by n matrices. Repetition of conjugacy classes is allowed.

R_1 consists of the zero matrix. Given A in R_m, let $W = \operatorname{im}(A)$ in $\mathbb{F}_5^m$. Compute row echelon form of the columns of A, regarded as row vectors. Let P be its pivot coordinate set and let C be the span of the standard coordinate vectors whose indices are not in P. Then $\mathbb{F}_5^m = W \oplus C$.

For this A include in R_{m+1} each matrix

$$\begin{pmatrix} A & v \\ 0 & 0 \end{pmatrix}$$

where v is zero or lies in C and has its first nonzero coordinate equal to 1. That is, include precisely one nonzero representative of every one-dimensional subspace of C, together with zero.

Every strictly upper triangular n by n matrix is $B_n(\mathbb{F}_5)$-conjugate to at least one element of R_n. Here is a direct induction verifying this coverage assertion. Put its upper left m by m block into R_m using $\operatorname{diag}(S, 1)$, with S upper triangular and invertible. The resulting matrix has the form displayed above for some v. Conjugating by

$$\begin{pmatrix} I_m & w \\ 0 & 1 \end{pmatrix}$$

changes v to $v - Aw$ and leaves A unchanged. Thus v can be reduced to the unique vector in C representing $v + W$. If this vector is nonzero, conjugation by $\operatorname{diag}(I_m, c)$, with c its first nonzero coordinate, scales v by c^{-1}. The result is a listed member of R_{m+1}. All matrices used for these conjugations are in $B_{m+1}(\mathbb{F}_5)$. The base case $n = 1$ is immediate.

For a parent of nullity k there are $1 + (5^k - 1)/4$ children. The zero child has nullity $k+1$; all nonzero children have nullity k. This recurrence gives the following list lengths, also obtained by both programs:

n	1	2	3	4	5	6
$\lvert R_n \rvert$	1	2	9	83	1676	72127

Their sum is 73898. Neither uniqueness of these conjugacy representatives nor the enumeration of all elements of G is claimed or needed.

5. What the exact certificate checks

For each A in these six lists, the certificate supplies an upper triangular matrix T over $\mathbb{F}_5$ whose diagonal entries are all nonzero and which satisfies

$$T(I_n + A) = (I_n + A)^2 T. \tag{1}$$

In particular, T is invertible and conjugates $I_n + A$ to its square. For discovery, `certify_b6.py` solves $TA = (2A + A^2)T$ by Gaussian elimination over $\mathbb{F}_5$ and exhausts possible nonzero values of its free diagonal variables. All chosen intertwiners are checked by direct matrix multiplication before being saved. No success assertion depends on the linear solver alone.

The certificate `data/b6_certificate.jsonl` has 73898 JSON lines. Each line has `n`, `a`, `t`. The array `a` lists the strictly upper triangular entries of A in row-major order ($i = 1, \dots, n$ and $j = i+1, \dots, n$); `t` lists the upper triangular entries of T in row-major order ($j = i, \dots, n$). All unspecified entries are zero. Every scalar is an integer in $\{0, 1, 2, 3, 4\}$. The SHA-256 of the file is

`d6cc4393146b5614824ae92d8ac558d0f47489a8046ff7d59db898cd9fca7759`.

The independent program `verify_b6.py` does not import the producer and does not solve conjugacy equations. It regenerates R_n using a different column space elimination implementation and base-5 enumeration of quotient lines. It checks that the certificate supplies exactly the regenerated list in every dimension, checks all scalar ranges and all diagonal entries, and

checks (1) by full matrix multiplication. It also checks list counts using the independent nullity recurrence, checks the powers of z, and checks that 2 has multiplicative order 20 modulo 25. The output is saved in `data/b6_verification_report.json`. All 73898 checks passed.

6. Why these checks prove that the particular group G is cut

First, every u in $U_n(\mathbb{F}_5)$, for $n \le 6$, is conjugate to u^2 by an element of $B_n(\mathbb{F}_5)$. Indeed, apply the covering argument to $u - I_n$ and transfer (1) along its upper triangular conjugation. Every such u has order dividing 25. The residues 2^j, $0 \le j < 20$, are all the units modulo 25. Repeated conjugation by the matrix taking u to u^2 therefore takes u to u^r for every integer r coprime to 5. This establishes the needed rational power property for these unipotent matrices, including each of the smaller dimensions.

Next take an arbitrary g in G. Its diagonal entries have fourth power 1, so g^4 lies in U and $g^{100} = 1$. Set $s = g^{25}$ and $u = g^{-24}$. Then

$$g = su = us, \qquad s^4 = 1, \qquad u^{25} = 1.$$

The polynomial $X^4 - 1$ has four distinct roots in $\mathbb{F}_5$. Consequently s can be diagonalized by an invertible upper triangular matrix over $\mathbb{F}_5$, as can also be verified constructively: for each i let $\lambda_i = s_{ii}$ and let $P_\lambda(X)$ be the interpolation polynomial equal to 1 at λ and 0 at the other three nonzero field elements. The vector $P_{\lambda_i}(s)e_i$ is a λ_i-eigenvector in $\operatorname{span}(e_1, \dots, e_i)$ whose i-th coordinate is 1. These six vectors form an upper unitriangular eigenbasis. In that basis write $g = dv$, where d is diagonal, $d^4 = 1$, v is unitriangular, $v^{25} = 1$, and $dv = vd$.

Commutation with d implies $v_{ij} = 0$ whenever d_{ii} differs from d_{jj}. Thus v splits into unitriangular matrices on the four coordinate sets having each possible diagonal value. Each coordinate set is given its inherited increasing order and has size at most 6. The preceding checked unipotent power property applies on each such set. Its conjugating matrices can be embedded and combined to form an invertible upper triangular matrix t commuting with d. Therefore, for any r coprime to 5, we can choose t so that

$$tvt^{-1} = v^r, \qquad tdt^{-1} = d. \tag{2}$$

Finally, let k be coprime to $|g|$. If v is nontrivial, then 5 divides $|g|$, so k is coprime to 5. Choose ϵ in $\{1, -1\}$ so that $d^{\epsilon k} = d$. Such a choice exists: when $|d| = 4$, k is odd and ϵ can be chosen with ϵk congruent to 1 modulo 4; when $|d| = 2$, k is odd and $\epsilon = 1$ works; when $|d| = 1$, $\epsilon = 1$ works. Apply (2) with $r = \epsilon k$ to obtain

$$t(dv)t^{-1} = dv^{\epsilon k} = (dv)^{\epsilon k}.$$

If $v = 1$, the same conclusion holds directly with $t = 1$. Returning to the original basis, g is conjugate to g^k or to g^{-k}. For any x, y generating the same cyclic subgroup, write $y = x^k$ with k coprime to $|x|$. The result just established is exactly the definition of a cut group in the question. This verifies the cut hypothesis for the explicit group G above.

7. Replay instructions and software conventions

Both scripts use only Python's standard library and exact integer arithmetic; the recorded run used Python 3.12.14. No GAP, SageMath, NumPy, external data, network access, or classification theorem is required for replay. From the workspace root, the independent certificate can be checked with

```
python verify_b6.py
```

The supplied runner can be used to obtain bounded command output:

```
python tools/krun.py --name b6-verify -- python verify_b6.py
```

To regenerate the certificate from its mathematical description, run

```
python certify_b6.py
python verify_b6.py
```

The scripts use only literal paths inside `data/` and print compact summaries. The certificate contains the mathematical computation data, not runner logs. The source files, certificate, and reports listed here suffice for standalone verification. The elementary arguments above verify the coverage, reduction to arbitrary group elements, solvability, and the precise failed conclusion.

Provenance and current package instructions

The preceding argument is imported from

`experiments/imported-counterexample/source/data/counterexample.txt`

under `problems/20.4/`. Its original bytes, source manifest, and selected solver and validator records remain in the archive.

The source runner recorded `SOLVED_VALIDATED`; its validator recorded `PASS`. These labels are historical. This typesetting makes no new mathematical argument, citation judgment, independent verifier verdict, or novelty claim.

The imported report records completion of 73898/73898 certificate checks with dimension counts $1, 2, 9, 83, 1676, 72127$. This is the historical computation record, not a new repository verification. The complete mathematical gate, citation audit, and independent GAP corroboration remain pending; the repository status remains `todo`. The problem statement is taken from the repository's Notebook transcription. The background bibliographic label in the inherited result metadata is unverified in this packaging pass; no `refs.bib` or new bibliographic entry is supplied.

The preceding replay commands are preserved as historical text. In this repository use `uv run python`, from a working copy of the archived `source/` directory. The verifier overwrites `data/b6_verification_report.json`; the producer overwrites `data/b6_certificate.jsonl` and `data/b6_producer_report.json`. The optional original `tools/krun.py` logging wrapper is not included and is not required. The staged `tools/kdata.py` helper is preserved but neither program imports it. See the problem README and packaging record for current file links and replay evidence.