

Levchuk’s Problem on Diagonal Matrices in $\mathrm{SL}_n(q)$ (Kourovka Notebook 7.27): An Affirmative Answer as a Corollary of Theorems of Fulman and Guralnick

Alper Ferudun*

October 18, 2026

Abstract

V. M. Levchuk asked in 1980 (Kourovka Notebook, Problem 7.27) whether, for all sufficiently large q , the group $\mathrm{SL}_n(q)$ contains a diagonal matrix lying in no proper irreducible subgroup except block-monomial ones. We show that the answer is yes for every n , as a short corollary of density theorems of Fulman and Guralnick; it is not presented as a new theorem. For fixed n and $q \rightarrow \infty$, almost all regular diagonal matrices d of $\mathrm{SL}_n(q)$ have the property that every proper subgroup containing d that is irreducible over $\mathbb{F}_q$ permutes the summands of a decomposition of $\mathbb{F}_q^n$ into coordinate subspaces. The deduction combines the density theorems with an elementary count of the classes of regular diagonal matrices, a description of the maximal subgroups of maximal rank, and an eigenvalue argument excluding extension field subgroups; the bound for q is not explicit. For $n = 2$, Dickson’s list of subgroups gives the complete answer: a diagonal matrix with this property exists if and only if $q \in \{4, 8\}$ or $q \geq 13$ (if irreducibility is meant absolutely, also for $q = 2$), and $\mathrm{diag}(w, w^{-1})$ works for every generator w of $\mathbb{F}_q^*$ when $q \geq 13$. No printed statement of the general answer was found, and no priority is claimed. This is an unrefereed note.

1 Introduction

1.1 The problem

Problem 7.27 of the Kourovka Notebook [KM26], posed by V. M. Levchuk in the 7th issue (1980), asks whether the group $\mathrm{SL}_n(q)$ contains, for sufficiently large q , a diagonal matrix which lies in no proper irreducible subgroup of $\mathrm{SL}_n(q)$ “with the exception of block-monomial ones”. The Notebook adds that the answer is affirmative for $n = 2$ and $n = 3$, by work of Levchuk in a Krasnoyarsk volume of 1973 [Lev73], and that similar problems are of interest for other Chevalley groups. In the current edition (No. 21, version 48 of the arXiv preprint, October 2026) the problem stands in the list of open problems, without a comment, and no other problem refers to it. It is record KOU-7.27 of the UnsolvedMath collection [ula26], where it is listed as open.

Conventions. Throughout, $n \geq 2$, q is a prime power, $V_0 = \mathbb{F}_q^n$ has the standard basis $e_1, \dots, e_n$, and V_I is the span of the e_i with $i \in I \subseteq \{1, \dots, n\}$. The diagonal matrices $d = \mathrm{diag}(l_1, \dots, l_n)$ of $\mathrm{SL}_n(q)$ form a group T of order $(q - 1)^{n-1}$; d is *regular* if $l_1, \dots, l_n$ are pairwise distinct, and T^{reg} is the set of regular elements of T (it is empty if $q \leq n$). A subgroup H of $\mathrm{GL}_n(q)$ is *irreducible* if 0 and V_0 are the only H -invariant subspaces, and *block-monomial* if it permutes the summands of a decomposition $V_0 = U_1 \oplus \dots \oplus U_t$ with $t \geq 2$ and all $U_j \neq 0$; in an adapted basis its matrices have

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: <https://github.com/AlperTheKing>. Unrefereed preprint. CC BY 4.0.

one non-zero block in each block row and block column. An irreducible block-monomial H permutes the U_j transitively, so they have equal dimension; such H lie in members of Aschbacher's class $\mathcal{C}_2$ [Asc84, KL90]. We read the problem with n fixed, asking for a bound $q_1(n)$; a bound independent of n is not asked and is not treated. For $d \in T$ we consider

$P(d)$: every proper irreducible subgroup H of $\mathrm{SL}_n(q)$ with $d \in H$ permutes the summands of a decomposition $V_0 = V_{I_1} \oplus \cdots \oplus V_{I_t}$ into coordinate subspaces, $t \geq 2$.

A matrix with $P(d)$ answers the question in each reading: irreducibility is taken over $\mathbb{F}_q$, so absolutely irreducible subgroups are covered, and the blocks are coordinate subspaces.

1.2 Results

Theorem 1.1. *Let $n \geq 2$, and for a prime power q let $\mathcal{G}_q$ be the set of regular diagonal matrices d of $\mathrm{SL}_n(q)$ with property $P(d)$. Then*

$$\frac{|\mathcal{G}_q|}{|T^{\mathrm{reg}}|} \rightarrow 1 \quad \text{and} \quad \frac{|\mathcal{G}_q|}{|T|} \rightarrow 1 \quad (q \rightarrow \infty).$$

In particular there is $q_1(n)$ such that $\mathrm{SL}_n(q)$ contains a regular diagonal matrix d with $P(d)$ for every prime power $q \geq q_1(n)$, and the answer to Problem 7.27 is affirmative.

The bound $q_1(n)$ is not explicit, because the rate in the density theorem that we use is not explicit (Remark 5.1). For $n = 2$ the answer is complete:

Theorem 1.2. *Let q be a prime power. There is a diagonal matrix $d \in \mathrm{SL}_2(q)$ with $P(d)$ if and only if $q \in \{4, 8\}$ or $q \geq 13$; for $q \geq 13$, $\mathrm{diag}(w, w^{-1})$ has $P(d)$ for every generator w of $\mathbb{F}_q^*$. For $q \in \{3, 5, 7, 9, 11\}$ every diagonal matrix lies in a proper absolutely irreducible subgroup of $\mathrm{SL}_2(q)$ that is not block-monomial (Table 1). For $q = 2$ the identity lies in a proper subgroup that is irreducible over $\mathbb{F}_2$ and not block-monomial, but in no proper absolutely irreducible subgroup.*

Proposition 6.3 describes, for every $q \geq 4$, all diagonal $d \in \mathrm{SL}_2(q)$ with $P(d)$; Table 2 lists them for $q \leq 64$.

1.3 What is known and what is new

Theorem 1.1 is a short corollary of density theorems of Fulman and Guralnick, stated in Section 3: the maximal subgroups of $\mathrm{SL}_n(q)$ that are not of maximal rank cover a proportion of the group that tends to 0 [FG03, Theorem 3.2] (in [FG12, Theorem 7.3]: the maximal subgroups containing no maximal torus), while the conjugates of the regular diagonal matrices cover a proportion about $1/n!$ [FG03, Section 4]. So almost every regular diagonal matrix lies only in maximal subgroups of maximal rank; for $\mathrm{SL}_n(q)$ these are reducible, imprimitive or extension field subgroups (as indicated at the end of [FG03, Section 4]), and the last ones contain no diagonal matrix whose r -th power is regular. Neither paper mentions diagonal matrices, Levchuk or the Notebook. Specialists will regard Theorem 1.1 as a corollary of these theorems, and we claim no priority for it. What this note adds is the deduction, written out in full in Sections 3 to 5, which to our knowledge is not stated anywhere, and the complete answer for $n = 2$ (Theorem 1.2, Proposition 6.3), which follows from Dickson's classification of the subgroups of $\mathrm{PSL}_2(q)$ [Dic01]. A second proof, through all classes of Aschbacher's theorem [Asc84], is described in Section 7.

Levchuk's work of 1973 on $n = 2, 3$ [Lev73] was not available to us. The subgroups of GL_n and SL_n that contain the *whole* diagonal group were described, in terms of nets, by Borevich [Bor76], by Vavilov in a series of five papers (1985–1993) beginning with [Vav85], and by King [Kin90]. Containing

T is a much stronger condition on a subgroup than containing one element $d \in T$ (an overgroup of T contains every $d \in T$, not conversely), so these descriptions do not answer Problem 7.27. Testerman and Zalesski [TZ15] determine, under certain restrictions, the maximal closed connected subgroups of simple algebraic groups that contain a regular torus (a torus with abelian centralizer); this analogue for algebraic groups concerns neither finite groups nor single elements.

2 Preliminaries

Let $\overline{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}_q$, $V = \overline{\mathbb{F}}^n \supseteq V_0$ and $\mathbf{G} = \mathrm{SL}_n(\overline{\mathbb{F}})$. We write F for the Frobenius map that raises the coordinates of vectors and the entries of matrices (in the standard basis) to the q -th power. It is a bijection of V and a ring automorphism of the matrix ring $M_n(\overline{\mathbb{F}})$, it satisfies $F(\lambda x) = \lambda^q F(x)$ and $F(gv) = F(g)F(v)$, and its fixed points are V_0 , $M_n(\mathbb{F}_q)$ and $\mathbf{G}^F = \mathrm{SL}_n(q)$. We write Z for the centre of $\mathrm{SL}_n(q)$, the group of scalar matrices of determinant 1.

Lemma 2.1. *Let K be a field and $x = \mathrm{diag}(x_1, \dots, x_n) \in \mathrm{GL}_n(K)$ with pairwise distinct x_i .*

- (a) *Every matrix commuting with x is diagonal.*
- (b) *Every x -invariant subspace of K^n is spanned by the standard basis vectors that it contains.*

Proof. (a) If $xy = yx$ then $x_i y_{ij} = y_{ij} x_j$, so $y_{ij} = 0$ for $i \neq j$. (b) Let U be invariant and $u = \sum_i c_i e_i \in U$. The vectors $x^k u = \sum_i c_i x_i^k e_i$, $0 \leq k < n$, lie in U , and since the Vandermonde matrix (x_i^k) is invertible, each $c_i e_i$ is a linear combination of them. Hence $e_i \in U$ whenever $c_i \neq 0$. $\square$

Lemma 2.2. *Let $W \subseteq V$ be a subspace with $F(W) = W$. Then W is spanned by $W_0 = W \cap V_0$, and $\dim_{\mathbb{F}_q} W_0 = \dim W$.*

Proof. The rows of the reduced row echelon matrix whose row space is W form a basis of W that is determined by W . Applying F entrywise gives the reduced row echelon matrix of $F(W) = W$, so the matrix is fixed by F and its entries lie in $\mathbb{F}_q$. The coordinates of a vector of W in this basis are its entries in the pivot columns, so W_0 is the $\mathbb{F}_q$ -span of the basis. $\square$

Lemma 2.3. *Assume that $(n, q) \notin \{(2, 2), (2, 3)\}$ and let $\pi: \mathrm{SL}_n(q) \rightarrow \mathrm{PSL}_n(q)$ be the quotient map.*

- (a) *Every maximal subgroup M of $\mathrm{SL}_n(q)$ contains Z , and $M \mapsto M/Z$ is a bijection from the maximal subgroups of $\mathrm{SL}_n(q)$ onto those of $\mathrm{PSL}_n(q)$.*
- (b) *For every set $\mathcal{M}$ of maximal subgroups of $\mathrm{PSL}_n(q)$, the union $\bigcup_{\bar{M} \in \mathcal{M}} \pi^{-1}(\bar{M})$ is the preimage of $\bigcup_{\bar{M} \in \mathcal{M}} \bar{M}$, and its proportion in $\mathrm{SL}_n(q)$ equals the proportion of $\bigcup_{\bar{M} \in \mathcal{M}} \bar{M}$ in $\mathrm{PSL}_n(q)$.*

Proof. (a) Under the assumption, $\mathrm{SL}_n(q)$ is perfect [Hup67]. If M is maximal and $Z \not\leq M$, then $MZ = \mathrm{SL}_n(q)$; so M is normal (it is normalized by M and by the central subgroup Z), and $\mathrm{SL}_n(q)/M \cong Z/(Z \cap M)$ is abelian, which forces $M = \mathrm{SL}_n(q)$, a contradiction. The bijection is the correspondence theorem. (b) Preimages commute with unions, and every subset X of $\mathrm{PSL}_n(q)$ satisfies $|\pi^{-1}(X)| = |Z||X|$. $\square$

3 The density theorems of Fulman and Guralnick

We state the two theorems as they are formulated in [FG12, FG03].

Theorem 3.1 (Fulman and Guralnick [FG12, Theorem 7.3]). *Let G be an almost simple group whose socle S is a Chevalley group of fixed rank r defined over $\mathbb{F}_q$, and assume that G is contained in the group of inner-diagonal automorphisms of S . Let $\mathcal{M}(G)$ be the set of maximal subgroups of G that do not contain a maximal torus of S . Then the proportion of $\bigcup_{M \in \mathcal{M}(G)} M$ in G tends to 0 as $q \rightarrow \infty$.*

The theorem states only this limit. The rate is in its proof: the proportion is $O(\log \log q/q)$, and $O(1/q)$ once the subfield subgroups are treated separately. The proof starts from the description of the maximal subgroups in [FG03], which is the next theorem.

Theorem 3.2 (Fulman and Guralnick [FG03, Section 3 and Theorem 3.2]). *Fix a type of simple algebraic group of rank r , of any isogeny type. For a prime p let X be the simple algebraic group of this type over $\overline{\mathbb{F}}_p$, and let σ be an endomorphism of X whose group of fixed points $X(q) = X_\sigma$ is finite. Every maximal subgroup H of $X(q)$ is of one of the following types:*

- (1) $|H| < N$, for a number N that depends only on the type;
- (2) $H = N_{X(q)}(X(q'))$ for a subgroup $X(q')$ defined over a subfield, twisted forms included;
- (3) $H = Y_\sigma$ for a proper σ -stable semisimple closed subgroup Y of X of rank less than r ;
- (4) $H = Y_\sigma$ for a proper σ -stable closed subgroup Y of X of rank r .

For the fixed type, the union of all maximal subgroups of types (1)–(3) forms a proportion of $X(q)$ that tends to 0 as $q \rightarrow \infty$; only the type is fixed, so the characteristic p may vary with q .

For classical groups, [FG03] calls the description by these four types well known and refers to Aschbacher’s theorem [Asc84]. Theorem 3.2 of [FG03] is stated without a rate, for groups of a fixed type of which “only the field size is varying” ([FG03, Section 3]). We apply Theorem 3.2 to the simply connected type A_{n-1} , of rank $r = n - 1$, that is, with $X = \mathrm{SL}_n$ over $\overline{\mathbb{F}}_p$ for every prime p and with $\sigma = F$, so that $X(q) = \mathrm{SL}_n(q)$ for every prime power q . A maximal subgroup of $\mathrm{SL}_n(q)$ of type (4) is said to be of *maximal rank*. If $M = Y^F$ is of maximal rank and $g \in \mathrm{SL}_n(q)$, then $gMg^{-1} = (gYg^{-1})^F$ is again of maximal rank, because $F(g) = g$. Hence the union $\mathcal{U}_q$ of all maximal subgroups of $\mathrm{SL}_n(q)$ that are not of maximal rank is a union of conjugacy classes, and since these subgroups are of types (1)–(3), Theorem 3.2 gives

$$\varepsilon_n(q) := \frac{|\mathcal{U}_q|}{|\mathrm{SL}_n(q)|} \rightarrow 0 \quad (q \rightarrow \infty), \quad (1)$$

where here and below q runs through all prime powers.

The second ingredient is the proportion of elements conjugate to diagonal matrices with regular powers. In [FG03, Section 4] it is shown that the regular semisimple elements conjugate into a maximal torus T_w form a proportion that tends to $1/|C_W(\sigma w)|$; for the diagonal torus of $\mathrm{SL}_n(q)$ this is $1/n!$. We need the following explicit version. For $N \geq 1$ let

$$R_N = \{d \in T : d^e \text{ is regular for } 1 \leq e \leq N\}.$$

Lemma 3.3. *Let $G = \mathrm{SL}_n(q)$ and $N \geq 1$.*

- (a) $|T \setminus R_N| \leq n(n-1)N^2 |T|/(q-1)$.
- (b) *If $d \in T$ is regular, then $C_G(d) = T$, and the conjugacy class of d meets T exactly in the $n!$ matrices obtained from d by permuting its diagonal entries.*
- (c) *Let Ω_N be the union of the conjugacy classes of the elements of R_N . Then $|\Omega_N|/|G| = |R_N|/(n!|T|) \geq \frac{1}{n!}(1 - n(n-1)N^2/(q-1))$, and every union $\mathcal{U}$ of conjugacy classes of G satisfies $|R_N \cap \mathcal{U}| \leq n!|T||\mathcal{U}|/|G|$.*

Proof. (a) For $i \neq j$ the map $\varphi_{ij}: T \rightarrow \mathbb{F}_q^*$, $d \mapsto l_i/l_j$, is a homomorphism. Its image has index at most 2 in $\mathbb{F}_q^*$: for $n \geq 3$ it is surjective (use the diagonal matrix with entries w at i , w^{-1} at some $k \notin \{i, j\}$ and 1 elsewhere, w a generator of $\mathbb{F}_q^*$), and for $n = 2$ it is the group of squares. So every fibre of φ_{ij} has at most $2|T|/(q-1)$ elements. Now $d \notin R_N$ if and only if $\varphi_{ij}(d)$ has order at most N for some $i < j$, and $\mathbb{F}_q^*$ has at most $\sum_{e \leq N} e \leq N^2$ elements of order at most N . Summing over the $n(n-1)/2$ pairs gives (a).

(b) $C_G(d) = T$ by Lemma 2.1(a). If $g \in G$ and $d' = g d g^{-1} \in T$, then $d'(ge_i) = g d e_i = l_i ge_i$, so ge_i is an eigenvector of d' for the eigenvalue l_i . The diagonal matrix d' has the same distinct eigenvalues as d , and its eigenspaces are coordinate lines, so $ge_i \in \mathbb{F}_q^* e_{\pi(i)}$ for a permutation π , and d' has the entry l_i at position $\pi(i)$. Conversely, d is conjugate to each of these $n!$ matrices, which are distinct, by the monomial matrix $P_\pi \text{diag}(\text{sgn } \pi, 1, \dots, 1)$ of determinant 1, where P_π is the permutation matrix.

(c) By (b), each conjugacy class contained in Ω_N has $|G|/|T|$ elements and meets T in $n!$ elements, all of them in R_N (a set closed under permutations of the entries); distinct classes meet T in disjoint sets, and every element of R_N lies in one of them. So Ω_N consists of $|R_N|/n!$ classes, and $|\Omega_N| = |R_N| |G|/(n! |T|)$; the inequality follows from (a). If $\mathcal{U}$ is a union of classes, then $R_N \cap \mathcal{U}$ is the union of the intersections with T of the classes contained in $\Omega_N \cap \mathcal{U}$, whence $|R_N \cap \mathcal{U}| = n! |T| |\Omega_N \cap \mathcal{U}|/|G| \leq n! |T| |\mathcal{U}|/|G|$. $\square$

Remark 3.4. For large q , Theorem 3.1 applied to $G = S = \text{PSL}_n(q)$ expresses the same fact as (1). A maximal torus of S is the image of a maximal torus $\mathbf{T}^F$ of $\text{SL}_n(q)$; the scalar matrices of $\mathbf{G}$ lie in every maximal torus, so $Z \leq \mathbf{T}^F$, and by Lemma 2.3 a maximal subgroup of $\text{SL}_n(q)$ contains $\mathbf{T}^F$ if and only if its image contains the image of $\mathbf{T}^F$. A maximal subgroup $M = Y^F$ of maximal rank contains a maximal torus of $\text{SL}_n(q)$: by the Lang–Steinberg theorem [Ste68], Y° contains an F -stable maximal torus $\mathbf{S}$, which has dimension $n-1$, and $\mathbf{S}^F \leq M$. Conversely, for large q every maximal subgroup M containing a maximal torus $\mathbf{T}^F$ is of maximal rank: otherwise all conjugates of M lie in $\mathcal{U}_q$, while they contain the regular semisimple elements conjugate into $\mathbf{T}^F$, which form a proportion tending to $1/|C_W(w)| \geq 1/n!$ by [FG03, Section 4] ($W = S_n$, w the type of $\mathbf{T}$), against (1). So for large q the union in Theorem 3.1 is the image of $\mathcal{U}_q$, and the proof of [FG12, Theorem 7.3] gives $\varepsilon_n(q) = O(\log \log q/q)$. We use Theorem 3.2 below because its conclusion, “of maximal rank”, is the hypothesis of Lemma 4.1.

4 Maximal subgroups of maximal rank

In the language of Aschbacher’s theorem [Asc84, KL90], the next lemma says that a maximal subgroup of $\text{SL}_n(q)$ of maximal rank lies in a member of one of the classes $\mathcal{C}_1$ (reducible subgroups), $\mathcal{C}_2$ (imprimitive subgroups) or $\mathcal{C}_3$ (extension field subgroups); this is also indicated at the end of [FG03, Section 4]. We use three standard facts on linear algebraic groups, see [Bor91, Hum75]: (F1) a unipotent subgroup of $\text{GL}(V)$ fixes a non-zero vector of V ; (F2) a connected reductive group H with a maximal torus $\mathbf{S}$ is generated by $\mathbf{S}$ and its root subgroups with respect to $\mathbf{S}$, and its set of roots is closed under $\alpha \mapsto -\alpha$; (F3) if α is a root of $\mathbf{G}$ with respect to a maximal torus $\mathbf{S}$, then the root subgroup U_α is the only closed connected $\mathbf{S}$ -stable subgroup of $\mathbf{G}$ whose Lie algebra is the root space $\mathfrak{g}_\alpha$.

Lemma 4.1. *Let Y be a closed subgroup of $\mathbf{G}$ with $F(Y) = Y$ and $Y \neq \mathbf{G}$, whose identity component Y° contains a maximal torus of $\mathbf{G}$, and let $M = Y^F$. Then at least one of the following holds:*

- (i) M stabilizes a subspace U_0 of V_0 with $0 \neq U_0 \neq V_0$;
- (ii) M permutes the summands of a decomposition $V_0 = U_1 \oplus \dots \oplus U_t$ with $t \geq 2$ and all $U_j \neq 0$;

(iii) for some prime r dividing n , M normalizes a subfield E of the ring $\text{End}_{\mathbb{F}_q}(V_0)$ with q^r elements that contains the scalar matrices; that is, M is contained in the group $\Gamma\text{L}_{n/r}(q^r)$ of the $\mathbb{F}_{q^r}$ -semilinear maps for the $\mathbb{F}_{q^r}$ -vector space structure on V_0 defined by E .

Proof. Step 1. Suppose that the unipotent radical U of Y° is non-trivial. It is normal in Y , and $F(U) = U$, because F maps Y° onto $F(Y)^\circ = Y^\circ$ and closed connected normal unipotent subgroups onto subgroups of the same kind and dimension. By (F1) the space W of vectors fixed by U is non-zero, and $W \neq V$. It is invariant under Y , and $F(W) = W$ since $F(uv) = F(u)F(v)$. By Lemma 2.2, $U_0 = W \cap V_0$ is an M -invariant subspace with $0 \neq U_0 \neq V_0$: case (i).

Step 2. Let Y° be reductive and $\mathbf{S} \leq Y^\circ$ a maximal torus of $\mathbf{G}$. Its weights $\varepsilon_1, \dots, \varepsilon_n$ on V are distinct; let $b_1, \dots, b_n$ be weight vectors, E_{ij} the matrix units for this basis, and $U_{ij} = \{1 + cE_{ij} : c \in \mathbb{F}\}$ ($i \neq j$) the root subgroups of $\mathbf{G}$. A root of Y° is a weight of $\mathbf{S}$ on the Lie algebra of Y° , hence a root $\varepsilon_i - \varepsilon_j$ of $\mathbf{G}$, and by (F3) its root subgroup is U_{ij} . Let R be the set of pairs (i, j) with $i = j$ or $U_{ij} \leq Y^\circ$. By (F2), Y° is generated by $\mathbf{S}$ and the U_{ij} with $(i, j) \in R$, $i \neq j$, and R is symmetric; by the commutator formula $[1 + aE_{ij}, 1 + bE_{jk}] = 1 + abE_{ik}$ (i, j, k distinct) it is transitive. Let $c_1, \dots, c_k$ be its classes and W_s the span of the b_i with $i \in c_s$. If $k = 1$, then Y° contains all U_{ij} , which generate $\mathbf{G}$, so $Y = \mathbf{G}$, which is excluded; hence $k \geq 2$. The linear span of $\mathbf{S}$ is the algebra of the matrices that are diagonal in the basis (b_i) , since distinct characters are linearly independent, and the span of U_{ij} contains E_{ij} ; so the linear span A of Y° is the algebra of the endomorphisms of V preserving every W_s . The primitive idempotents of its centre are the projections π_s onto W_s along the other summands. Conjugation by $y \in Y$ and the map F are ring automorphisms of A (F maps Y° onto Y° and $\mathbb{F}$ -spans onto $\mathbb{F}$ -spans), so they permute the π_s and hence the subspaces $W_s = \pi_s V$.

Step 3. Let $O_1, \dots, O_m$ be the orbits of F on $\{W_1, \dots, W_k\}$ and $U^{(j)}$ the sum of the members of O_j . By Lemma 2.2, $U_0^{(j)} = U^{(j)} \cap V_0$ spans $U^{(j)}$, and $V_0 = U_0^{(1)} \oplus \dots \oplus U_0^{(m)}$. Every $g \in M$ permutes the W_s and commutes with F , so it permutes the orbits and the $U_0^{(j)}$; if $m \geq 2$ this is case (ii). Let $m = 1$ and number the W_s so that $F(W_s) = W_{s+1}$ (indices modulo k). Then $F(\pi_s) = \pi_{s+1}$, the W_s have equal dimension, and $k \mid n$. The F -fixed elements of the centre of A form the set $E' = \{\sum_s a_s \pi_s : a_{s+1} = a_s^q \text{ for all } s\}$, and $a \mapsto \sum_s a^{q^{s-1}} \pi_s$ is a ring isomorphism from $\mathbb{F}_{q^k}$ onto E' ; the elements of E' are matrices with entries in $\mathbb{F}_q$, and E' contains the scalar matrices. Every $g \in M$ normalizes A , hence its centre, and commutes with F , so it normalizes E' and therefore its subfield E with q^r elements, for a prime $r \mid k$. This is case (iii). $\square$

Lemma 4.2. *Let r be a prime dividing n , let E be a subfield of $\text{End}_{\mathbb{F}_q}(V_0)$ with q^r elements containing the scalar matrices, and let $d \in T$ be such that d^r is regular. Then d does not normalize E .*

Proof. Suppose that d normalizes E . Conjugation by d induces an automorphism of the field E that fixes the scalar matrices, and the automorphism group of E over $\mathbb{F}_q$ has order r ; so d^r centralizes E . Choose $z \in E$ that is not scalar; since r is prime, $E = \mathbb{F}_q[z]$, and the minimal polynomial of z over $\mathbb{F}_q$ is irreducible of degree $r \geq 2$. But z commutes with the diagonal matrix d^r , whose entries are distinct, so z is diagonal by Lemma 2.1(a), and the minimal polynomial of a diagonal matrix over $\mathbb{F}_q$ is a product of linear factors. This is a contradiction. $\square$

Lemma 4.3. *Let $d \in T$ be such that d^e is regular for all $e \leq n!$, and suppose that d permutes the summands of a decomposition $V_0 = U_1 \oplus \dots \oplus U_t$ with $t \geq 2$ and all $U_j \neq 0$. Then d fixes every U_j , and every U_j is a coordinate subspace.*

Proof. Let $\tau \in S_t$ be the permutation of the summands induced by d ; its order o divides $t!$, so $o \leq n!$. Then d^o fixes every U_j , and since d^o is diagonal with distinct entries, every U_j is a coordinate subspace by Lemma 2.1(b). A diagonal matrix fixes every coordinate subspace, so τ is the identity. $\square$

5 Proof of Theorem 1.1

Fix $n \geq 2$, put $N = n!$, and let $\mathcal{U}_q$ and $\varepsilon_n(q)$ be as in (1). Put $\mathcal{G}'_q = R_N \setminus \mathcal{U}_q$. Since $\mathcal{U}_q$ is a union of conjugacy classes, Lemma 3.3(a) and (c) give

$$|T \setminus \mathcal{G}'_q| \leq |T \setminus R_N| + |R_N \cap \mathcal{U}_q| \leq \left(\frac{n(n-1)(n!)^2}{q-1} + n! \varepsilon_n(q) \right) |T|.$$

By (1) the right-hand side is $o(|T|)$ as $q \rightarrow \infty$. We show that every $d \in \mathcal{G}'_q$ has property $P(d)$. Since $\mathcal{G}'_q \subseteq R_N \subseteq T^{\text{reg}}$, this gives $\mathcal{G}'_q \subseteq \mathcal{G}_q$, and hence $|\mathcal{G}_q|/|T^{\text{reg}}| \geq |\mathcal{G}_q|/|T| \geq |\mathcal{G}'_q|/|T| \rightarrow 1$, which proves Theorem 1.1.

Let $d \in \mathcal{G}'_q$ and let H be a proper irreducible subgroup of $\text{SL}_n(q)$ containing d . Choose a maximal subgroup M of $\text{SL}_n(q)$ with $H \leq M$. Since $d \in M$ and $d \notin \mathcal{U}_q$, the subgroup M is of maximal rank: $M = Y^F$ for a proper F -stable closed subgroup Y of $\mathbf{G}$ whose identity component contains a maximal torus of $\mathbf{G}$. We apply Lemma 4.1. Case (i) is impossible, since a subspace stabilized by M is stabilized by the irreducible group H . Case (iii) is impossible by Lemma 4.2, since $d \in M$ and d^r is regular ($r \leq n \leq N$). So case (ii) holds: M , and therefore H , permutes the summands of a decomposition $V_0 = U_1 \oplus \cdots \oplus U_t$ with $t \geq 2$. By Lemma 4.3, applied to $d \in H$, every U_j is a coordinate subspace. As H is irreducible, it permutes the U_j transitively, so they have the same dimension n/t . This is $P(d)$. $\square$

Remark 5.1. Since $\varepsilon_n(q)$ is not explicit (the proof of [FG12, Theorem 7.3] gives $\varepsilon_n(q) = O(\log \log q/q)$, see Remark 3.4), neither is $q_1(n)$. For small q the set $R_{n!}$ may be empty even if $q > n$: for $n = 4$ and $q = 64$ two of the four exponents of the entries with respect to a generator of $\mathbb{F}_{64}^*$ agree modulo 3, so some ratio l_i/l_j has order dividing 21. For $n = 2$, $q_1(2) = 13$ by Theorem 1.2.

6 The case $n = 2$

In this section $n = 2$, $q = p^f$, $d = \text{diag}(l, l^{-1})$ with $l \in \mathbb{F}_q^*$, and $\mathbb{P}^1$ is the set of the $q+1$ lines of $V_0 = \mathbb{F}_q^2$. We write $z \in \mathbb{F}_q$ for the line spanned by $(z, 1)^T$ and ∞ for the line $\mathbb{F}_q e_1$; so $\mathbb{F}_q e_2$ is the point 0, and d acts on $\mathbb{P}^1$ by $z \mapsto l^2 z$. Put $k = \gcd(2, q-1)$; bars denote images in $\text{PSL}_2(q) = \text{SL}_2(q)/Z$, where $Z = \{\pm I\} \cap \text{SL}_2(q)$, and $\text{PSL}_2(q)$ acts faithfully on $\mathbb{P}^1$. Let m be the order of l^2 . Since $d^j \in Z$ if and only if $l^{2j} = 1$, m is the order of $\bar{d}$; it divides $(q-1)/k$, and $p \nmid m$.

Lemma 6.1. *A subgroup H of $\text{SL}_2(q)$ is irreducible and not block-monomial if and only if every orbit of H on $\mathbb{P}^1$ has at least three points. If $l^4 \neq 1$, every block-monomial subgroup containing d permutes the lines $\mathbb{F}_q e_1$ and $\mathbb{F}_q e_2$.*

Proof. H is reducible if and only if it fixes a point of $\mathbb{P}^1$, and block-monomial if and only if it preserves a set $\{L_1, L_2\}$ of two distinct lines, that is, if it has an orbit of size 2 or two fixed points. If $l^4 \neq 1$, then $\bar{d} \neq 1$ fixes exactly 0 and ∞ , and if it interchanges two points $z \neq z'$ then $l^4 z = z'$, which is impossible; so $\{0, \infty\}$ is the only pair of points preserved by d . $\square$

For $q \geq 4$ the group $\text{SL}_2(q)$ is perfect, so a subgroup H is proper if and only if $\bar{H}$ is proper (as in Lemma 2.3), and H and $\bar{H}$ have the same orbits. Call a proper subgroup K of $\text{PSL}_2(q)$ all of whose orbits on $\mathbb{P}^1$ have at least three points a *witness*. By Lemma 6.1, if some witness contains $\bar{d}$ then $P(d)$ fails, whether the blocks are arbitrary or coordinate subspaces (if irreducibility is meant absolutely, the preimage of the witness must also be absolutely irreducible; see the proof of Theorem 1.2), and if $l^4 \neq 1$ the converse holds as well.

Lemma 6.2. *Let $q \geq 4$ and $m \geq 3$. Every element $y \in \text{PSL}_2(q)$ of order m generates a conjugate of $\langle \bar{d} \rangle$, and fixes exactly two points of $\mathbb{P}^1$.*

Proof. Let $\hat{y} \in \mathrm{SL}_2(q)$ be a preimage of y . Its order (m or $2m$, and m if $p = 2$) is prime to p , so $\hat{y}$ is diagonalizable over $\mathbb{F}_{q^2}$, with eigenvalues $\lambda^{\pm 1}$, and $y^j = 1$ if and only if $\lambda^{2j} = 1$; so λ^2 has order m . If $\lambda \notin \mathbb{F}_q$, then $\lambda^q = \lambda^{-1}$, hence $\lambda^{q+1} = 1$ and m divides $(q+1)/k$; together with $m \mid (q-1)/k$ this gives $m = 1$, because $(q-1)/k$ and $(q+1)/k$ are coprime. So $\lambda \in \mathbb{F}_q$, and $\hat{y}$ is conjugate in $\mathrm{GL}_2(q)$ to $\mathrm{diag}(\lambda, \lambda^{-1})$; it is conjugate in $\mathrm{SL}_2(q)$ as well, since the diagonal matrices, which centralize $\mathrm{diag}(\lambda, \lambda^{-1})$, have every determinant. As λ^2 and l^2 generate the same subgroup of $\mathbb{F}_q^*$, $\lambda^2 = l^{2j}$ with $\gcd(j, m) = 1$, so $\lambda = \pm l^j$ and y is conjugate to $\bar{d}^j$, a generator of $\langle \bar{d} \rangle$. Finally $\bar{d}^j$ fixes exactly 0 and ∞ . $\square$

Hence, for $m \geq 3$: $P(d)$ fails if and only if some witness contains an element of order m ; and a subgroup that normalizes a cyclic subgroup $\langle y \rangle$ of order $m \geq 3$ is not a witness, since it permutes the two fixed points of y .

We use Dickson's classification [Dic01] (see also [Hup67]): every subgroup of $\mathrm{PSL}_2(q)$ is isomorphic to one of the following groups: (D1) an elementary abelian p -group; (D2) a cyclic group of order z dividing $(q \pm 1)/k$; (D3) a dihedral group of order $2z$, z as in (D2); (D4) A_4 ; (D5) S_4 ; (D6) A_5 ; (D7) a semidirect product of an elementary abelian group of order p^a by a cyclic group of order t , where $t \mid p^a - 1$ and $t \mid (q-1)/k$; (D8) $\mathrm{PSL}_2(q_0)$ with $\mathbb{F}_{q_0} \subseteq \mathbb{F}_q$, or $\mathrm{PGL}_2(q_0)$ with $\mathbb{F}_{q_0^2} \subseteq \mathbb{F}_q$. Moreover $\mathrm{PSL}_2(q)$ contains subgroups isomorphic to A_4 if $p > 2$ or f is even, to S_4 if $q^2 \equiv 1 \pmod{16}$, and to A_5 if $p = 5$ or $q^2 \equiv 1 \pmod{5}$.

Proposition 6.3. *Let $q \geq 4$. Then $P(d)$ holds if and only if either*

- (a) $m = 3$ and $q = 4$; or
- (b) $m \geq 6$, and m divides none of the numbers $(q_0 \pm 1)/\gcd(2, q_0 - 1)$ for subfields $\mathbb{F}_{q_0} \subsetneq \mathbb{F}_q$ with $q_0 \geq 3$, and none of the numbers $q_0 \pm 1$ for subfields $\mathbb{F}_{q_0^2} \subseteq \mathbb{F}_q$ with $q_0 \geq 3$.

Proof. The case $m \leq 2$. Identify V_0 with $\mathbb{F}_{q^2}$, let λ generate the subgroup of order $q+1$ of $\mathbb{F}_{q^2}^*$, and let $s \in \mathrm{SL}_2(q)$ be multiplication by λ (its determinant is the norm $\lambda^{q+1} = 1$). An eigenvalue of s^j in $\mathbb{F}_q$ would satisfy $\lambda^{j(q-1)} = 1 = \lambda^{j(q+1)}$, so that $s^j = \pm I$; hence $\langle \bar{s} \rangle$, of order $(q+1)/k \geq 3$, acts semiregularly on $\mathbb{P}^1$ and is a witness containing $\bar{d} = 1$ if $m = 1$. If $m = 2$, then $l^2 = -1$ and $q \equiv 1 \pmod{4}$. Let u be the map $x \mapsto cx^q$ with $c^{q+1} = -1$; as $x \mapsto x^q$ and multiplication by c both have determinant -1 , $u \in \mathrm{SL}_2(q)$, and $usu^{-1} = s^{-1}$, $u^2 = -I$. So $\langle \bar{s}, \bar{u} \rangle$ has order at most $q+1$, its orbits are unions of $\langle \bar{s} \rangle$ -orbits of size $(q+1)/2 \geq 3$, and it is a witness containing the involution $\bar{u}$. Every involution of $\mathrm{PSL}_2(q)$ is conjugate to $\bar{d}$: a preimage g satisfies $g^2 = -I$ (an element $g \neq \pm I$ of $\mathrm{SL}_2(q)$ has $g^2 \neq I$), so its eigenvalues are $\pm l \in \mathbb{F}_q$ and g is conjugate to d as in the proof of Lemma 6.2.

Dickson's list, $m \geq 3$. Groups of type (D1) have no element of order m . In a group of type (D2) or (D3), an element y of order $m \geq 3$ lies in the cyclic subgroup of index at most 2, so $\langle y \rangle$ is normal and the group is not a witness. A non-trivial p -element of $\mathrm{PSL}_2(q)$ is the image of a unipotent matrix $\neq I$ and fixes exactly one point; a p -subgroup $P \neq 1$ lies in a Sylow p -subgroup, a conjugate of the image of the upper unitriangular group, so it has exactly one fixed point, which every group normalizing P fixes. So groups of type (D7) with $a \geq 1$, and A_4 if $p = 2$, are not witnesses. Let p be odd. A point stabilizer $\bar{B}$, the image of a group of upper triangular matrices, has a normal p -subgroup with cyclic quotient; A_4 has no non-trivial normal p -subgroup and is not cyclic, so $A_4 \not\leq \bar{B}$; and A_4 has no subgroup of index 2, hence no orbit of size 2. So A_4 is a witness. So is S_4 (which forces q odd): it fixes no point since A_4 does not, and an orbit of size 2 would give its subgroup A_4 a fixed point. A_5 fixes no point ($\bar{B}$ is solvable) and has no subgroup of index 2; it is a witness unless $q \in \{4, 5\}$, where it is not proper. Elements of A_4 , S_4 and A_5 have order at most 5. Elements of $\mathrm{PSL}_2(q_0)$ of order prime to p have orders dividing $(q_0 \pm 1)/\gcd(2, q_0 - 1)$, those of $\mathrm{PGL}_2(q_0)$ orders dividing $q_0 \pm 1$, and all these orders occur; for $q_0 = 2$ all element orders are at most 3.

Subfield subgroups. Let $q_0 \geq 3$, let K_0 be the image of $\mathrm{SL}_2(q_0)$, and if $\mathbb{F}_{q_0^2} \subseteq \mathbb{F}_q$ let $K_1 \supseteq K_0$ be the image of $\mathrm{GL}_2(q_0)$, which lies in $\mathrm{PSL}_2(q)$ because the elements of $\mathbb{F}_{q_0}$ are squares in $\mathbb{F}_q$. Both are witnesses: $\mathbb{P}^1(\mathbb{F}_{q_0})$ is a K_0 -orbit of size $q_0 + 1$; for $z \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$, an element $g \neq 1$ of $\mathrm{PGL}_2(q_0)$ fixing z commutes with $x \mapsto x^{q_0}$, so it fixes $z^{q_0} \neq z$ and hence, fixing at most two points, no point of $\mathbb{P}^1(\mathbb{F}_{q_0})$; so the stabilizer of z acts semiregularly on $\mathbb{P}^1(\mathbb{F}_{q_0})$, has at most $q_0 + 1$ elements, and the K_0 -orbit of z has at least $q_0(q_0 - 1)/\gcd(2, q_0 - 1) \geq 3$ points.

Conclusion. If $m = 3$ and p is odd, A_4 is a witness with elements of order 3. If $m = 3$, $p = 2$ and $q \neq 4$, then f is even, $q \geq 16$, and $K_0 \cong A_5$ for $q_0 = 4$ is such a witness. If $q = 4$, the groups in the list with elements of order 3 are of types (D2)–(D4) and (D7), the whole group $A_5 \cong \mathrm{PSL}_2(4)$, and $\mathrm{PSL}_2(2) \cong S_3$, which is dihedral; so $P(d)$ holds. If $m = 4$, then $q \equiv 1 \pmod{8}$, so $q^2 \equiv 1 \pmod{16}$ and S_4 is a witness with elements of order 4. If $m = 5$, then $q \equiv 1 \pmod{5}$, so $q \geq 11$ and A_5 is a proper witness with elements of order 5. If $m \geq 6$, only subgroups of type (D8) with $q_0 \geq 3$ can be witnesses with an element of order m ; such an element exists if and only if m divides one of the numbers in (b), and then K_0 or K_1 is such a witness. $\square$

Proof of Theorem 1.2. Let $q \geq 13$ and $l = w$ a generator of $\mathbb{F}_q^*$. Then $m = (q - 1)/k \geq 6$. Every subfield $\mathbb{F}_{q_0}$ in (b) has $q_0 \leq \sqrt{q}$, and $(q - 1)/2 > \sqrt{q} + 1$ for $q > 9$, so $m > q_0 + 1$ and (b) holds; so $P(d)$ holds. For $q = 4$ and l of order 3, (a) holds. For $q = 8$ and $l \neq 1$, $m = 7$ and the only proper subfield is $\mathbb{F}_2$, so (b) holds. For $q = 5, 7, 9, 11$ the possible values of m are $\{1, 2\}$, $\{1, 3\}$, $\{1, 2, 4\}$, $\{1, 5\}$, so $P(d)$ fails for every d by Proposition 6.3. More precisely, the full preimages in $\mathrm{SL}_2(q)$ of a subgroup A_4 ($q = 5$), S_4 ($q = 7, 9$) or A_5 ($q = 11$) of $\mathrm{PSL}_2(q)$ are witnesses, by the proof of Proposition 6.3; they contain Z , a conjugate of every $\bar{d}$ of order $m \geq 3$ (Lemma 6.2) and, for $q \equiv 1 \pmod{4}$, a conjugate of every involution. They are non-abelian, hence absolutely irreducible: an irreducible subgroup of $\mathrm{GL}_2(q)$ that is not absolutely irreducible fixes a line L of V and the line $F(L) \neq L$, so it is diagonal in a basis of V and abelian. For $q = 3$ the quaternion group Q_8 generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ contains $\pm I$; its image, of order 4, acts regularly on the four points of $\mathbb{P}^1$, so Q_8 is irreducible and not block-monomial (it is primitive over $\mathbb{F}_3$, although monomial over $\mathbb{F}_9$; block-monomial is meant over $\mathbb{F}_q$, as in Section 1), and it is non-abelian. For $q = 2$, the group of order 3 generated by $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ permutes the three points of $\mathbb{P}^1$ cyclically; it is irreducible over $\mathbb{F}_2$ and not block-monomial, and it contains I . It is not absolutely irreducible, and no proper subgroup of $\mathrm{SL}_2(2) \cong S_3$ is, since all of them are abelian. $\square$

Table 1 lists witnesses computed by closure in $\mathrm{SL}_2(q)$ (part (E) of the program in Section 8); Table 2 lists, for $q \leq 64$, the orders of l for which $P(d)$ holds. The latter table was computed twice, from Proposition 6.3 and by direct generation using the following lemma, which does not use Dickson's list; the results agree.

Lemma 6.4. *Let $q \geq 4$ and $l^4 \neq 1$. Then $P(d)$ holds if and only if $\langle d, x \rangle = \mathrm{SL}_2(q)$ for every $x \in \mathrm{SL}_2(q)$ that is neither upper triangular, nor lower triangular, nor antidiagonal.*

Proof. Such an x moves both 0 and ∞ and does not interchange them. If $\langle d, x \rangle$ is proper, an orbit of size at most 2 would be invariant under $\bar{d}$, so it would be $\{0\}$, $\{\infty\}$ or $\{0, \infty\}$ (Lemma 6.1), which x does not preserve; so $\langle \bar{d}, x \rangle$ is a witness and $P(d)$ fails. Conversely, let $\bar{H}$ be a witness containing $\bar{d}$, and H its preimage. As H does not preserve $\{0, \infty\}$, some $z \in H$ maps it to another set. If z fixes neither point, $x = z$ will do. Otherwise, say, z fixes ∞ and not 0, so z is upper triangular and not diagonal. Since H does not fix ∞ , some $y \in H$ moves ∞ . If y is neither lower triangular nor antidiagonal, $x = y$ will do. If y is antidiagonal, replace it by $yz y^{-1}$, which is lower triangular and not diagonal. If y is lower triangular and not diagonal, then $x = zy$ has non-zero entries in both off-diagonal positions and in position (2, 2), so it is neither triangular nor antidiagonal. The case where z fixes 0 is symmetric. In all cases $\langle d, x \rangle \leq H$ is proper. $\square$

q	diagonal matrices	witness H (image in $\mathrm{PSL}_2(q)$)	orbits on $\mathbb{P}^1$
2	I	cyclic of order 3 (irreducible over $\mathbb{F}_2$ only)	3
3	$\pm I$	Q_8 (image $C_2 \times C_2$), $ H = 8$	4
5	all four	$\mathrm{SL}_2(3)$ (image A_4), $ H = 24$	6
7	all six	image S_4 , $ H = 48$	8
9	all eight	image S_4 , $ H = 48$	4 + 6
11	all ten	$\mathrm{SL}_2(5)$ (image A_5), $ H = 120$	12

Table 1: For $q \leq 11$, $q \notin \{4, 8\}$, every diagonal matrix of $\mathrm{SL}_2(q)$ lies in a proper subgroup H that is irreducible and not block-monomial; for $q \geq 3$ the witnesses are non-abelian, hence absolutely irreducible. The groups were computed by closure in $\mathrm{SL}_2(q)$, with explicit generators, in part (E) of the program.

q	ord(l) with $P(d)$	q	ord(l) with $P(d)$	q	ord(l) with $P(d)$
4	3	19	9, 18	41	20, 40
5	—	23	11, 22	43	7, 14, 21, 42
7	—	25	24	47	23, 46
8	7	27	13, 26	49	24, 48
9	—	29	7, 14, 28	53	13, 26, 52
11	—	31	15, 30	59	29, 58
13	12	32	31	61	12, 15, 20, 30, 60
16	15	37	9, 12, 18, 36	64	21, 63
17	16				

Table 2: The orders of l (equal to the order of d) for which $d = \mathrm{diag}(l, l^{-1}) \in \mathrm{SL}_2(q)$ has property $P(d)$, $4 \leq q \leq 64$; for all other divisors of $q - 1$, $P(d)$ fails. Computed from Proposition 6.3 and, independently, by direct generation (Lemma 6.4); the two computations agree.

7 A second proof through all Aschbacher classes

Theorem 1.1 can also be proved without [FG03, FG12], through all classes of Aschbacher’s theorem [Asc84, KL90]; we only describe this proof. Call $d = \mathrm{diag}(l_1, \dots, l_n) \in T$ (B, E)-*generic* if (G) for every $\mu \in \mathbb{Z}^n \setminus \{0\}$ with $\sum_i \mu_i = 0$ and $\max_i |\mu_i| \leq B$, the element $\prod_i l_i^{\mu_i}$ has order greater than E , and (F) for every prime r with $q = q_0^r$ and all $i \neq j$, $(l_1/l_2)^{q_0} \neq l_i/l_j$. For suitable $B = B(n)$ and $E = \max(E_0(n), 6n^2 \lceil \log_2 q \rceil)$, a count of fibres of characters as in Lemma 3.3(a) shows that the elements that are not generic form a proportion $O_n((\log q)^2/\sqrt{q})$ of T . For a generic d , eigenvalue arguments exclude the members of $\mathcal{C}_3$ (as in Lemma 4.2), of $\mathcal{C}_4$ and $\mathcal{C}_7$ (a tensor product of matrices of sizes at least 2 with distinct eigenvalues has four eigenvalues at distinct positions with $\mu_1\mu_2 = \mu_3\mu_4$, against (G)), of $\mathcal{C}_5$ and the unitary part of $\mathcal{C}_8$ (against (F)), of $\mathcal{C}_6$ (order bounded modulo scalars) and of the bilinear part of $\mathcal{C}_8$ (against (G)). The class $\mathcal{S}$ is excluded by the classification of finite simple groups (bounded order for the groups not of Lie type in characteristic p , through the degrees of their projective representations) and, in defining characteristic, by Steinberg’s restriction and tensor product theorems [Ste63] and his description of the automorphisms [Ste60], with a bound for the weights of restricted modules. Aschbacher’s theorem then leaves $\mathcal{C}_1$ and $\mathcal{C}_2$, and the proof ends as in Section 5. This route gives explicit genericity conditions and the proportion $1 - O_n((\log q)^2/\sqrt{q})$, but no explicit $q_1(n)$ either. It was found together with the results of this note, and the two verification runs that examined the first write-up re-derived its steps (Section 8); we do not reproduce it, and nothing in this note depends on it.

8 Computations and reproducibility

All theorems, propositions and lemmas of this note are proved without computation. The program `check_note.py` of the reproducibility package (Python 3, standard library only; about 80 seconds; it ends with “TOTAL failures: 0”) checks: (A) the arithmetic of $\mathbb{F}_q$ for all prime powers $q \leq 256$, and the computation of orders of subgroups of $\mathrm{PGL}_2(q)$ by a stabilizer chain, against brute-force closure (700 pairs of generators); (B) the bound of Lemma 3.3(a) by exact counts for $n = 2, 3, 4$ ($q \leq 1024, 256, 128$); (C) Lemma 3.3(b) by brute force for $n = 2, q \leq 13$, and $n = 3, q \in \{4, 5\}$; (D) Table 2, from Proposition 6.3 and by direct generation through Lemma 6.4, with a checked witness for every failure, and the same comparison for the 107 pairs $(q, \mathrm{ord}(l))$ with $64 < q \leq 128$ and $\mathrm{ord}(l) \nmid 4$; (E) Table 1, by closure in $\mathrm{SL}_2(q)$; (F) $P(d)$ for $d = \mathrm{diag}(w, w^{-1})$ by direct generation for all prime powers $13 \leq q \leq 256$, and the inequalities in the proof of Theorem 1.2 for $13 \leq q \leq 20000$. With the option `--quick` it runs in about five seconds. The programs of the first two verification runs are not part of the package; those of the third, with their recorded outputs, are in the folder `independent_run_2/` of the package. The results of all three are summarized in the accompanying verification report.

Verification. The results were first obtained with the proof described in Section 7, with the observation that the answer follows from [FG03, FG12], and with programs for $n = 2$. Two independent verification runs, both AI-assisted, followed; each wrote its own programs, and neither read the other’s report. The first compared the statement with the text and the PDF of the Notebook, read [FG03] (Sections 3 and 4) and [FG12] (Section 7), wrote out the two steps of the deduction that had only been named (Lemmas 3.3 and 4.1 here), re-derived every step of the proof of Section 7, and decided $P(d)$ for $n = 2$ with its own programs: from Dickson’s list for $q \leq 256$, by direct generation for $q \leq 32$, by explicit certificates for all diagonal matrices for $q = 5, 7, 9, 11$, and by a search of all two-generated subgroups for $q = 2, 3, 4, 8$, which showed that $q = 2, 3$ fail as well. The second decided $P(d)$ for $4 \leq q \leq 64$ by direct generation with exact group orders and from Dickson’s list (identical results; Dickson’s list alone up to $q = 20000$), recomputed the counting data, tested the eigenvalue arguments for the symplectic and unitary members of $\mathcal{C}_8$ on random similitudes, re-ran the programs with which the results had been obtained (identical outputs), and checked the bibliography and the literature. Both runs found that the answer is a short corollary of [FG03, FG12], and neither found a mathematical error. All their required corrections were made; they are listed in the verification report. Among them: the result is presented as a corollary, not as new; [FG12, Theorem 7.3] is stated exactly, with the passage to $\mathrm{PSL}_n(q)$; the two steps are written out; textbooks are cited by content only; and the cases $q = 2, 3$ are included. When the note was written, the deduction was organized around [FG03, Theorem 3.2], Lemma 4.1 received the proof above, Proposition 6.3, Lemma 6.4 and the tables were added, and Table 2 was recomputed by the exact program of this note.

A further AI-assisted verification run then examined the final text and the package; its programs and outputs are in the folder `independent_run_2/` of the reproducibility package. It compared the statement again with the text and the PDF of the Notebook, read [FG03] (Sections 3 and 4) and [FG12] (Sections 1 and 7) again, re-derived the proofs of Sections 2 to 6 line by line, and wrote its own programs before re-running the program of this note from the archived package (identical output apart from running times). Its programs checked Lemma 3.3 by exact enumeration ($n = 2, 3, 4; q \leq 1024, 256, 128$) and, in parts (b) and (c), over all of $\mathrm{SL}_3(7)$ and $\mathrm{SL}_3(8)$; Lemma 4.2 on all subfields of $M_2(\mathbb{F}_q)$ with q^2 elements ($q \leq 32$), for $n = 3$ through the normalizer $\Gamma\mathrm{L}_1(q^3)$, and for $n = 4, r = 2$ by linear algebra; Lemma 4.3 for $n = 3$ on all decompositions permuted by d ; Theorem 1.2 and Table 1 for $q \leq 17$ from the definitions alone, through the whole lattice of overgroups of every diagonal element, without Dickson’s list and without Lemma 6.4, in the four readings (irreducibility over $\mathbb{F}_q$ or absolute, arbitrary or coordinate blocks), which confirms that only $q = 2$ depends on the reading;

Proposition 6.3 and Table 2 against direct generation, with a separate implementation of the Schreier–Sims algorithm, for all 288 pairs $(q, \text{ord}(l))$ with $4 \leq q \leq 128$; $P(\text{diag}(w, w^{-1}))$ for all prime powers $13 \leq q \leq 256$ and for $q \in \{289, 343, 361, 509, 512\}$; and the arithmetic of the proof of Theorem 1.2 for all prime powers up to 10^6 . It also repeated the literature search and checked the identifiers of the references. It found no mathematical error. It required that Theorem 3.2 be quoted, as in [FG03], for a fixed type with the characteristic allowed to vary, which is what Theorem 1.1 needs, and four corrections of wording (the sentence on $n = 2$ in the abstract, the overgroups of T in Section 1, the readings in Section 6, and the description of the earlier runs); all were made.

Scope and priority. The note answers Problem 7.27 of [KM26] affirmatively for every fixed $n \geq 2$ and all sufficiently large q , without an explicit bound $q_1(n)$ for $n \geq 3$, and settles the case $n = 2$ completely; a version uniform in n is not treated. The problem is Levchuk’s; his work of 1973 on $n = 2, 3$ [Lev73] was not available to us and was not read. The density theorems are those of Fulman and Guralnick [FG03, FG12], which rest on Aschbacher’s theorem [Asc84] and further results cited there; the case $n = 2$ rests on Dickson’s classification [Dic01]; the descriptions of the overgroups of the whole diagonal group [Bor76, Vav85, Kin90] answer a different and weaker question. Specialists will regard Theorem 1.1 as a corollary of the theorems of Fulman and Guralnick. The deduction in Sections 3 to 5 is, to our knowledge, not stated anywhere, and we did not find the complete answer for $n = 2$ in print; no priority is claimed for either.

What was read: [KM26] in version 48, text and PDF (the wording in version 46 is the same); [FG03] in full and [FG12] (Sections 1 and 7) in version 1 of the arXiv preprints, whose numbering we use, the journal versions not being compared; of [TZ15] the abstract; of [Vav85] the zbMATH review; of [Bor76, Kin90] the bibliographic data. The works [Asc84, KL90, Bor91, Hum75, Hup67, Dic01, Ste68, Ste60, Ste63] are cited for standard statements, by content; the proofs of the cited theorems were not checked. The searches were made on 17 and 18 October 2026: the Notebook (Problem 7.27 has no comment, and no other problem refers to it); the arXiv API (Kourovka and Levchuk; “diagonal matrix” with “irreducible subgroup”; overgroups of regular semisimple elements and of tori; “block-monomial”; Fulman and Guralnick); zbMATH Open (the records of the authors Levchuk and Nuzhin, overgroups of semisimple elements, block-monomial groups); Crossref; OpenAlex; and six web searches. Semantic Scholar refused our requests and was not used. Judging from titles and reviews, none of Levchuk’s later papers in zbMATH Open treats the question for $n \geq 4$. No printed answer to the question was found in these sources; a search that finds nothing is not a proof of novelty.

AI-assisted tools were used to search the problem corpus and the literature, to find the arguments, to write and run the verification programs, and to help prepare this manuscript. The author has reviewed the proofs, the computations and the sources and is responsible for all claims. The note has not been peer reviewed.

References

- [Asc84] Michael Aschbacher. On the maximal subgroups of the finite classical groups. *Inventiones Mathematicae*, 76(3):469–514, 1984. doi:10.1007/BF01388470.
- [Bor76] Z. I. Borevich. Description of subgroups of the general linear group containing the group of diagonal matrices. *Zapiski Nauchnykh Seminarov LOMI*, 64:12–29, 1976. In Russian; English translation: J. Soviet Math. 17 (1981), 1718–1730, to which the DOI refers. doi:10.1007/BF01091757.
- [Bor91] Armand Borel. *Linear Algebraic Groups*, volume 126 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1991. doi:10.1007/978-1-4612-0941-6.

- [Dic01] Leonard Eugene Dickson. *Linear Groups with an Exposition of the Galois Field Theory*. B. G. Teubner, Leipzig, 1901.
- [FG03] Jason Fulman and Robert Guralnick. Derangements in simple and primitive groups. In A. Ivanov et al., editors, *Groups, Combinatorics & Geometry (Durham, 2001)*, pages 99–121. World Scientific, 2003. [arXiv:math/0208022](#), [doi:10.1142/9789812564481_0006](#).
- [FG12] Jason Fulman and Robert Guralnick. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Transactions of the American Mathematical Society*, 364(6):3023–3070, 2012. [arXiv:0902.2238](#), [doi:10.1090/S0002-9947-2012-05427-4](#).
- [Hum75] James E. Humphreys. *Linear Algebraic Groups*, volume 21 of *Graduate Texts in Mathematics*. Springer, New York, 1975. [doi:10.1007/978-1-4684-9443-3](#).
- [Hup67] Bertram Huppert. *Endliche Gruppen I*, volume 134 of *Grundlehren der mathematischen Wissenschaften*. Springer, Berlin, 1967. [doi:10.1007/978-3-642-64981-3](#).
- [Kin90] Oliver King. Subgroups of the special linear group containing the diagonal subgroup. *Journal of Algebra*, 132(1):198–204, 1990. [doi:10.1016/0021-8693\(90\)90263-N](#).
- [KL90] Peter Kleidman and Martin Liebeck. *The Subgroup Structure of the Finite Classical Groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990. [doi:10.1017/CB09780511629235](#).
- [KM26] E. I. Khukhro and V. D. Mazurov, editors. *Unsolved Problems in Group Theory. The Kourovka Notebook. No. 21*. Sobolev Institute of Mathematics, Novosibirsk, 2026. Version 48 of the arXiv preprint, 6 October 2026. [arXiv:1401.0300](#).
- [Lev73] V. M. Levchuk. Contribution to: Some problems of the theory of groups and rings. Inst. of Physics SO AN SSSR, Krasnoyarsk, 1973. In Russian; cited in the Kourovka Notebook for $n = 2, 3$; not seen by us.
- [Ste60] Robert Steinberg. Automorphisms of finite linear groups. *Canadian Journal of Mathematics*, 12:606–615, 1960. [doi:10.4153/CJM-1960-054-6](#).
- [Ste63] Robert Steinberg. Representations of algebraic groups. *Nagoya Mathematical Journal*, 22:33–56, 1963. [doi:10.1017/S0027763000011016](#).
- [Ste68] Robert Steinberg. *Endomorphisms of Linear Algebraic Groups*. Number 80 in Memoirs of the American Mathematical Society. American Mathematical Society, Providence, RI, 1968. [doi:10.1090/memo/0080](#).
- [TZ15] Donna M. Testerman and Alexandre E. Zalesski. Subgroups of simple algebraic groups containing regular tori, and irreducible representations with multiplicity 1 non-zero weights. *Transformation Groups*, 20(3):831–861, 2015. [arXiv:1403.1387](#), [doi:10.1007/s00031-015-9321-1](#).
- [ula26] ulamai. UnsolvedMath. Hugging Face dataset, <https://huggingface.co/datasets/ulamai/UnsolvedMath>, 2026. Version 1.8.0; record KOU-7.27.
- [Vav85] N. A. Vavilov. Subgroups of a special linear group, containing a group of diagonal matrices. I. *Vestnik Leningrad University. Mathematics*, 18(4):3–7, 1985. Parts II–V: 1986, 1987, 1988, 1993.