The first part of this work has already appeared as a Preprint of the *Università degli Studi di Milano* (1992, N.12). However since the second part heavily depends on the first one, we decided to reproduce it here for reader's convenience. Using this opportunity we corrected some minor inaccuracies in it.

(2,3)-GENERATION OF SL(n, q). I. CASES n = 5, 6, 7

Lino Di Martino * and **Nikolai Vavilov** **

Dipartimento di Matematica
Università degli Studi di Milano
via C.Saldini 50
20133, Milano, Italia

and

Department of Mathematics and Mechanics
University of Sanct Petersburg
Petrodvorets, 198904, Russia

Abstract. In this paper we prove that the groups $\mathrm{SL}(n, q)$, $q = p^m$, are factors of the modular group $\mathrm{PSL}(2, \mathbb{Z})$ when $n = 5, 6, 7$ and $p \neq 2$, $q \neq 9$.

Introduction

There is growing evidence that most finite simple groups (and closely related groups) appear as factor-groups of the classical modular group $\mathrm{PSL}(2, \mathbb{Z})$. It is well known that $\mathrm{PSL}(2, \mathbb{Z})$ is isomorphic to the free product of the groups of orders 2 and 3 and thus a group appears as a factor-group of $\mathrm{PSL}(2, \mathbb{Z})$ if and only if it is generated by an involution and an element of order 3. Such groups are often called (2,3)-*generated.*

---

* The first-named author was supported by the *Ministero dell'Università e della Ricerca Scientifica e Tecnologica* (M.U.R.S.T.)

** The second-named author gratefully acknowledges the financial support of the *Consiglio Nazionale delle Ricerche* (C.N.R.) and the hospitality of the *Università degli Studi di Milano* during the preparation of this work.

AMS 1991 Subject Classification: 20G40, 20F05
Keywords: special linear group, root subgroups, (2,3)-generation.

The following groups are known to be (2,3)-generated:

– The alternating groups A_n, $n \neq 6, 7, 8$ (this was proven by A.Miller in 1901, see references in [DiMT]);

– The projective special linear groups $\mathrm{PSL}(2, q)$, $q \neq 9$ ([Mb]);

– The projective special linear groups $\mathrm{PSL}(3, q)$, $q \neq 4$ ([Ga], [Co]);

– The special linear groups $\mathrm{SL}(n, q)$, $n \geq 25$ ([T1]);

– The Chevalley groups $G_2(q)$ of type G_2 and the twisted groups ${}^2G_2(q)$ ([Ma1],[Ma2]);

– The projective symplectic groups $\mathrm{PSp}(4, q)$,$q = p^m$, $p \neq 2, 3$ ([CD]);

– The special linear groups $\mathrm{SL}(4, q)$, $q = p^m$, $p \neq 2$ ([TV]);

– All sporadic simple groups apart from M_{11}, M_{22}, M_{23} and McL ([Wo]).

For some of the excluded cases, like, for example, for the groups $\mathrm{PSL}(2, 9)$ and $\mathrm{PSL}(3, 4)$ and the sporadics it is known that they are *not* (2,3)-generated, while most of the other exceptions are basically due to the methods used in the proofs of these results.

The proofs for the cases $\mathrm{PSL}(2, q)$, $\mathrm{PSL}(3, q)$, $\mathrm{PSp}(4, q)$ and $G_2(q)$ rely on explicit knowledge of the subgroup structure (in [Co] it is claimed that the groups $\mathrm{PSU}(3, q)$ are also (2,3)-generated but the proof there contains an error). In turn the remarkable proof of the (2,3)-generation of large special linear groups due to M.Ch.Tamburini ([T1]) is essentially permutational and relies on techniques developed in [TW]. This proof based on the analysis of the corresponding alternating groups A_n does not carry over easily to the smaller dimensions.

In this paper we propose an alternative approach to the proof of the (2,3)-generation of finite linear groups which works also when the dimension is small. This approach is based on the classification of finite irreducible linear groups generated by root subgroups ([Mc]). Starting from dimension 9 our generators are essentially the same as in [T1], the element of order 3 being monomial and the involution being monomial times a transvection. The generators are "periodic modulo 6" so that the proof depends essentially only on the congruence class of n modulo 6.

The purpose of this first part is to show how the strategy works giving the full details of the proofs for the cases $n = 5, 6, 7$ (the case $n = 4$, requiring somewhat more complicated generators is treated in a similar way in [TV]). On one side these cases are already quite complicated giving a full flavour of how the method works in general, on the other side the low dimensional groups seem to require a separate case by case treatment anyway, since the shapes of the 3-element in some of the dimensions ≤ 8 are slightly different, and their analysis leads to equations depending on the dimension (not just on its congruence class modulo 6).

§1. Statement of results

In this section we construct the generators of orders 2 and 3, state the main theorem and discuss the general plan of its proof.

1°. Notation. Most of our notation is quite standard. For a primary number $q = p^m$ (where p is a rational prime and m a natural number) we denote by $\mathbb{F}_q$ the field of q elements. A generator of the cyclic group $\mathbb{F}_q^*$ will be called a *primitive element* of $\mathbb{F}_q$, while a generator of $\mathbb{F}_q$ as an algebra over $\mathbb{F}_p$ will be called a *field generator* or a *defining element of* $\mathbb{F}_q$ (see [LN]). We will write $\mathbb{F}_q = \mathbb{F}_p[\lambda]$ to denote that λ is a defining element of $\mathbb{F}_q$ and we will always assume that a defining element is non-zero if the field is prime.

Let G be any group. For two elements $x, y \in G$ we denote by $[x, y] = xyx^{-1}y^{-1}$ their commutator and by $x^y = y^{-1}xy$ the conjugate of x by y. We write $H \leq G$ when H is a subgroup of G (as opposed to $X \subseteq G$ when X is an arbitrary subset). For a subset $X \subseteq G$ we denote by $\langle X \rangle \leq G$ the subgroup of G generated by X and by $\langle X \rangle^G \trianglelefteq G$ the normal subgroup of G generated by X, i.e. the normal closure of $\langle X \rangle \leq G$ in G. For two subgroups F and H of G we write $F \sim_G H$ — or simply $F \sim H$ when the group G is clear from the context — to denote that F and H are conjugated by an element of G.

For any field K and any natural number n we denote by $\mathrm{GL}(n, K)$ and $\mathrm{SL}(n, K)$ the general and the special linear groups respectively ([HO'M] and [KL] are our general references for linear groups where one can find definitions of all the notions we use here and many further references). In particular, $K^* = \mathrm{GL}(1, K)$ is the group of non-zero elements of K. For the case $K = \mathbb{F}_q$ we use the shortcuts $\mathrm{GL}(n, q)$ and $\mathrm{SL}(n, q)$.

By e_n — or simply by e if the order is clear from the context — we denote the identity matrix of order n. We will usually write simply 1 instead of e_1. For a fixed n and $1 \leq i, j \leq n$ we denote by e_{ij} the corresponding standard matrix unit, i.e. the matrix which has 1 in position (i, j) and zeros elsewhere. We denote by $a_1 \oplus \ldots \oplus a_t$ the *direct sum* of the matrices $a_1, \ldots, a_t$, i.e. the block matrix which has blocks $a_1, \ldots, a_t$ along the principal diagonal and zeros elsewhere. Sometimes $a_1 \oplus \ldots \oplus a_t$ is called the *diagonal sum* and denoted $\mathrm{diag}(a_1, \ldots, a_t)$.

We denote the matrix entry of a matrix x in position (i, j) by x_{ij}, so that $x = (x_{ij})$. The inverse of a matrix $x \in \mathrm{GL}(n, K)$ is denoted by $x^{-1} = (x'_{ij})$ and the transpose by x^t.

The groups $\mathrm{GL}(n, K)$ and $\mathrm{SL}(n, K)$ act on the left on the n-dimensional column space $V = K^n$. We denote by $v_1, \ldots, v_n$ the standard base of the space V, i.e. v_i is a column which has 1 as its i-th coordinate, while all other coordinates are zeros. The dual space $V^* = \mathrm{Hom}(V, K)$ is the n-dimensional row space, which will be denoted by ${}^nK$.

2^0. Construction of the generators. Here we describe the general strategy of constructing an involution $x = x_n$ and an element of order three $y = y_n$ which generate $\mathrm{SL}(n, K)$, $n \geq 5$. This construction follows the same idea as in [TW], [T1], [Wi]. Our generators tend to be close to monomial matrices: actually y will be monomial in most cases while x will differ from a monomial matrix only by a transvection. In most cases they will be constructed as diagonal sums of blocks of degree ≤ 3.

Let π be any permutation. Denote by (π) the corresponding permutation matrix, i.e. a matrix, whose entry in the position (i, j) equals $\delta_{i,\pi(j)}$. For any field K the map $\pi \mapsto (\pi)$ is a monomorphism of the symmetric group S_n in the monomial group $N = N(n, K)$. The image of the long cycle $(1, \ldots, n)$ under this map will be denoted by cox_n and called *Coxeter matrix.* Actually in this work we will only use it in the cases $n = 2, 3$. Here are the matrices cox_2 and cox_3:

$$\mathrm{cox}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathrm{cox}_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Many authors use the notation w_{12} and w_{123} for these matrices which is convenient when you embed them in a large group $\mathrm{GL}(n, K)$ on prescribed positions (say w_{ij} or w_{ijh}). But here we use them almost exclusively as summands of direct sums, so we stick to the notation cox_n.

Our involution x will be basically a direct sum of blocks of type ± 1 and cox_2, the summands of the form -1 being introduced to make the determinant of the resulting matrix equal to 1. However since our 3-element will be monomial in most cases, we have to introduce in our involution at least one block which is not monomial (since otherwise x and y would generate a subgroup of $N(n, K)$). As the only non-monomial block we will take the following matrix

$$\mathrm{fun}_2(t) = \begin{pmatrix} 1 & 0 \\ t & -1 \end{pmatrix},$$

which obviously is an involution.

In most cases our 3-element y will be a direct sum of blocks of type 1 and cox_3. However in dimensions 5 and 8 we introduce a summand of a different shape, namely the matrix

$$\mathrm{fan}_2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},$$

which obviously has order 3 and determinant 1.

An obvious necessary condition for the group $G = \langle x, y\rangle$ to be irreducible is that it should not have proper invariant subspaces generated by the base vectors v_i. With this end in mind we will assemble the blocks cox_2 and cox_3 in such a way that the corresponding transpositions and 3-cycles act transitively on the set $\{1, \dots, n\}$ of indices (or have one invariant point in the exceptional cases when fan_2 is present).

3^0. Main theorem. The purpose of this first part of the work is to prove the following result.

Theorem 1. *Let $\mathbb{F}_q$ be a finite field of characteristic not 2, $q \neq 9$ and $n = 5, 6, 7$. Then the group $\mathrm{SL}(n, q)$ is $(2, 3)$-generated.*

Here is the list of possible generators $x = x_n$ and $y = y_n$, where n refers to the degree of the matrices (when the degree is defined by the context we will usually write simply x and y):

$$\begin{aligned} x_5 &= 1 \oplus \mathrm{cox}_2 \oplus \mathrm{fun}_2(t), & y_5 &= \mathrm{fan}_2 \oplus \mathrm{cox}_3; \\ x_6 &= e_2 \oplus \mathrm{cox}_2 \oplus \mathrm{fun}_2(t), & y_6 &= \mathrm{cox}_3 \oplus \mathrm{cox}_3; \\ x_7 &= \mathrm{cox}_2 \oplus (-1) \oplus \mathrm{cox}_2 \oplus \mathrm{fun}_2(t), & y_7 &= 1 \oplus \mathrm{cox}_3 \oplus \mathrm{cox}_3. \end{aligned}$$

Actually these elements generate the whole group $\mathrm{SL}(n, q)$ only if the parameter t does not satisfy some polynomial equations and the value of some other polynomial in t is a defining element of $\mathbb{F}_q$ (for the excluded values of t these elements may generate a proper subgroup of $\mathrm{SL}(n, q)$, say, a reducible one). Of course we must take $t \neq 0$. Here are the conditions on t:

$$\begin{aligned} n = 5&: \quad t^3 - 2t + 4 \neq 0; \;\; t^2 + 2t + 4 \neq 0; \;\; \mathbb{F}_q = \mathbb{F}_p\left[2t^3(t-2)\right]; \\ n = 6&: \quad t^3 \neq 8; \;\; t^3 \neq -4; \;\; \mathbb{F}_q = \mathbb{F}_p\left[4t^3\right]; \\ n = 7&: \quad t \neq 1, -1, -2; \;\; \mathbb{F}_q = \mathbb{F}_p\left[8t^3(t+2)\right]; \end{aligned}$$

Corollary. *Under the assumptions of theorem the group $\mathrm{SL}(n, K)$ is generated by three conjugate involutions.*

Proof. Take the involution x and its conjugates yxy^{-1}, y^2xy^{-2}. They generate a normal subgroup of G which has index at most 3. Thus it should coincide with G.

One may note that it is possible to adapt the method of [T1] to some of the smaller dimensions. E.g. it is easily seen that this applies to the dimensions 13, 16, 19, 22, 24. Also with that method one does not have to exclude the case when $\mathrm{char} K = 2$, so that the groups $\mathrm{SL}(n, q)$, $n = 13$, 16, 19, 22, 24 are (2,3)-generated for all values of q.

Sections 2 and 3 below contain somewhat more preliminary results than is strictly necessary to prove theorem 1. This material will be used in the next part of the paper.

4^0. Plan of the proof. For all cases the proof proceeds according to the following four steps.

Step 1. Like in [T1] a direct calculation shows that some power z^r of the commutator $z = [x, y]$ is a nontrivial transvection. In our cases $r = 4, 8$ or 12 (in some cases the value of r was calculated by hand but at the final stage we used calculations with "Mathematica"). Then $yz^r y^{-1}$ is another transvection and a direct calculation shows that it is *opposite* to z^r (see §3). Now by Dickson's theorem these two transvections usually generate the group $\mathrm{SL}(2, q)$ — a necessary condition for this is that some polynomial in t (something like, say, $2t^3(t-2)$ or $4t^3$) is a *defining element* of $\mathbb{F}_q$. Thus we may conclude that G contains the whole *root subgroup* X consisting of all transvections with the same *centre* and the same *axis* as z^r.

Consider the group $G = \langle x, y\rangle$ generated by x and y and the normal closure $H = \langle X\rangle^G$ of the root subgroup X in G.

Step 2. An analysis of G-invariant subspaces based on the fact that x is an involution shows that apart from a few values of t the group G is irreducible. If G is primitive, then H is irreducible. If it is not, then considering the action of x and y on the *homogeneous components* of H we can get a contradiction with the fact that H contains a transvection.

Thus we may apply to H the classification of irreducible linear groups generated by root subgroups (see §2). The classification says that either H coincides with $\mathrm{SL}(n, q)$, or n is even and H is conjugate to $\mathrm{Sp}(n, q)$.

Step 3. The symplectic case is excluded since then G should preserve a nondegenerate symplectic form *up to similarity*. A direct check shows that — again apart from very few values of t — this is not the case.

This implies that — when t satisfies the imposed restrictions, which say that t is not a root of certain polynomials and, moreover, the value of some other polynomial in t is a defining element of $\mathbb{F}_q$ — one has $H = \mathrm{SL}(n, q)$.

Step 4. It remains only to check that in all cases it is possible to find $t \in \mathbb{F}_q$ satisfying the above conditions.

The realization of this plan is systematic for large n since both the patterns for z^r and $yz^r y^{-1}$ and the equations which arise in the analysis of irreducibility of G and H etc. do not depend on n but, as we mentioned in the Introduction, only on $n \bmod (6)$. Small values of n require a separate case by case treatment.

§2. Generalities on linear groups

In this section we describe the background material used in our proof.

1°. Clifford's theorem. The groups $\mathrm{GL}(n,K)$ and $\mathrm{SL}(n,K)$ act on the left on the n-dimensional column space $V = K^n$. Let G be a subgroup of $\mathrm{GL}(n,K)$. Recall that a subspace $U \subseteq V$ is called *invariant with respect to* G (or simply G*-invariant* or just *invariant* if the group G is clear from the context) if $gu \in U$ for any $g \in G$ and $u \in U$. A subspace $U \subseteq V$ is called *proper* if it is distinct from V and 0. A subgroup G of $\mathrm{GL}(n,K)$ is called *irreducible* if there are no proper G-invariant subspaces in V, i.e. if any G-invariant subspace which contains a non-zero vector coincides with V.

A direct sum decomposition $V = U_1 \oplus \ldots \oplus U_t$ is called an *imprimitivity system* for the group G if G permutes the summands U_i (for every element $g \in G$ and for every $i, 1 \leq i \leq t$, there exists a $j, 1 \leq j \leq t$, such that $gU_i \subseteq U_j$). The summands U_i themselves are then called *blocks of imprimitivity* of the group G. Every group admits the trivial imprimitivity system $V = V$ with one summand. Recall that G is called *primitive* if it does not admit a nontrivial imprimitivity system and *imprimitive* otherwise.

If a group G is irreducible but imprimitive then all the blocks of an imprimitivity system of G have the same dimension s and G permutes them transitively. In particular, $n = st$.

We will make use of a basic tool of representation theory, namely *Clifford's theorem.* Recall that if V is a completely reducible H-module and W is its irreducible submodule, then the *homogeneous component* U of V containing W is the sum of all H-submodules of V isomorphic to W. What we actually need of Clifford's theorem is embodied in the following lemma.

Lemma 1. *If G is irreducible and $H \trianglelefteq G$ is a normal subgroup of G, then*

i) *V is completely reducible as an H-module;*

ii) *The representatives $W_1, \ldots, W_t$ of the isomorphism classes of irreducible H-submodules are G-conjugate;*

iii) *Denote by U_i the homogeneous component of V, containing W_i. Then $U_1, \ldots, U_t$ form an imprimitivity system for G;*

iv) *In particular, if G is both irreducible and primitive then with respect to an appropriate base of V any element x of H has the form $a(x) \oplus \ldots \oplus a(x)$ for some matrix $a(x) \in \mathrm{GL}(s,K)$.*

2°. Normalizers of classical groups. As usual if $n = 2l$ is even we denote by $\mathrm{Sp}(n,K)$ the symplectic group of degree n over K. The group $\mathrm{Sp}(n,K)$ is defined in terms of a nondegenerate symplectic form $(\ ,\ )$

on the space V and consists of all the matrices $g \in \mathrm{GL}(n, K)$ such that $(gu, gv) = (u, v)$ for all $u, v \in V$. Since up to equivalence there is only one nondegenerate symplectic form we will always assume that this group is considered with respect to the following Gram matrix

$$F = \begin{pmatrix} & & & & & 1 \\ & & & & \cdot^{\cdot^{\cdot}} & \\ & & & 1 & & \\ & & -1 & & & \\ & \cdot^{\cdot^{\cdot}} & & & & \\ -1 & & & & & \end{pmatrix}.$$

If K is a field with involution then for any n we will consider also the special unitary group $\mathrm{SU}(n, K)$ corresponding to the hermitian form $(\ ,\ )$ *of the maximal Witt index.* In other words the Gram matrix of this form in an appropriate base has the following shape

$$f = \begin{pmatrix} & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & \end{pmatrix}.$$

Then $\mathrm{SU}(n, K)$ consists of all matrices $g \in \mathrm{GL}(n, K)$ such that $(gu, gv) = (u, v)$ for all $u, v \in V$ *and* $\det(x) = 1$. If the field $K = \mathbb{F}_q$ is finite this is again the only possibility for the group. As before we will use the shorthand notation $\mathrm{Sp}(n, q)$ and $\mathrm{SU}(n, q)$.

Let $(\ ,\ )$ be a symplectic or hermitian form as above. Then along with $\mathrm{Sp}(n, K)$ and $\mathrm{SU}(n, K)$ we will consider the corresponding *general* groups $\mathrm{GSp}(n, K)$ and $\mathrm{GU}(n, K)$ which consist of all *symplectic/unitary similarities*. This means that $\mathrm{GSp}(n, K)$ and $\mathrm{GU}(n, K)$ consist of all the matrices $g \in \mathrm{GL}(n, K)$ such that for all $u, v \in V$ one has $(gu, gv) = \lambda(g)(u, v)$ for some scalar $\lambda(g) \in K^*$ which depends on g but not on u, v. This scalar $\lambda(g)$ is called the *multiplier* corresponding to g.

The following fact seems to be a common knowledge (and referred to as such in some works of R.Dye and O.King) though we could not find it stated plainly anywhere before [KL].

Lemma 2. *Let* $\Gamma = \mathrm{Sp}(n, K)$ *or* $\mathrm{SU}(n, K)$. *Then the normalizer of* Γ *in* $\mathrm{GL}(n, K)$ *coincides with* $\mathrm{GSp}(n, K)$ *or* $\mathrm{GU}(n, K)$ *respectively.*

Following Dye we denote the intersections of $\mathrm{GSp}(n, K)$ and $\mathrm{GU}(n, K)$ with $\mathrm{SL}(n, K)$ by $\mathrm{SGSp}(n, K)$ and $\mathrm{SGU}(n, K)$ respectively. These groups are precisely the normalizers of $\mathrm{Sp}(n, K)$ and $\mathrm{SU}(n, K)$ in $\mathrm{SL}(n, K)$.

3°. Transvections. Recall that the rank of the matrix $x-e$ is called the *residue* of $x \in \mathrm{GL}(n,K)$ and denoted $\mathrm{res}(x)$. We will use the following obvious properties of $\mathrm{res}(x)$ in our proofs:

$$\mathrm{res}(xy) \leq \mathrm{res}(x) + \mathrm{res}(y),$$

$$\mathrm{res}(x^{-1}) = \mathrm{res}(x),$$

$$\mathrm{res}(yxy^{-1}) = \mathrm{res}(x)$$

(see [HO'M] where one can find also many further related results).

The matrices of the form $t_{ij}(\xi) = e + \xi e_{ij}$ are called *elementary transvections.* A matrix x is called a *transvection* if it is conjugate in $\mathrm{GL}(n,K)$ to an elementary transvection. This is equivalent to saying that x is *unipotent* (i.e. all of its eigenvalues are equal to 1) and *one-dimensional*, i.e. its residue $\mathrm{res}(x)$ equals 1. The order of a transvection is equal to p if $p = \mathrm{char} K$ is finite and is infinite if $\mathrm{char} K = 0$.

The general form of a one-dimensional transformation is $x_{ca}(\xi) = e + c\xi a$, where $c = (c_1, \ldots, c_n)^t \in K^n$ is a column of height n, $a = (a_1, \ldots, a_n) \in {}^nK$ is a row of length n and $\xi \in K$ is a scalar. The letters c and a here should suggest the geometric terminology: c is a generator of the *centre* of $x_{ca}(\xi)$, while the hyperplane in K^n orthogonal to a is the *axis* of $x_{ca}(\xi)$. The transformation $x_{ca}(\xi)$ is a transvection if and only if $ac = 0$, i.e. the centre lies on the axis.

To see that these two definitions coincide, take an elementary transvection $t_{ij}(\xi)$ and a matrix $g \in \mathrm{GL}(n,K)$. Then

$$x = g t_{ij}(\xi) g^{-1} = g(e + \xi e_{ij}) g^{-1} = e + c\xi a,$$

where $c = (g_{1i}, ..., g_{ni})^t$ is the i-th column of g and $a = (g'_{j1}, ..., g'_{jn})$ is the j-th row of g^{-1}. Since $i \neq j$ one has $ac = 0$. Conversely, for any unimodular column c and any unimodular row a *over a field* such that $ac = 0$, there exists an invertible matrix g such that c is the first column of g, while a is the second row of g^{-1}, so that $x_{ca}(1)$ is conjugated to $t_{12}(1)$.

If x is a transvection, then the corresponding a and c are defined in general only up to scalar multiples. We normalize them in the following canonical way. First we set $\xi = 1$. Then we can multiply a by a non-zero scalar and c by the inverse of this scalar. If $x \neq e$ then both a and c are nonzero. We will almost always assume that the first non-zero coordinate of a equals 1 (in some cases though it is more convenient to assume that the first non-zero coordinate of c equals 1). The corresponding vectors a and c will be denoted by $a(x)$ and $c(x)$ respectively. Thus $x = x_{c(x),a(x)}(1)$.

Note that an elementary transvection $t_{ij}(\xi)$ may be written in the form $x_{v_i,v_j^t}(\xi) = x_{\xi v_i,v_j^t}(1)$ (we refer to the latter form in the proof of Lemma 10). The same calculation as above shows that for any transvection $x = x_{ca}(\xi)$ and any matrix $g \in \mathrm{GL}(n,K)$ one has

$$gx_{ca}(\xi)g^{-1} = x_{gc,ag^{-1}}(\xi).$$

Thus in particular $a(gxg^{-1}) = a(x)g^{-1}$ and $c(gxg^{-1}) = gc(x)$.

The group $X = \{x_{ca}(\xi) \mid \xi \in K\}$ is called a *one-parameter* group of transvections or, sometimes, a *root subgroup* of $\mathrm{SL}(n,K)$. It is isomorphic to the additive group K^+. In particular, the subgroups $X_{ij} = \{t_{ij}(\xi) \mid \xi \in K\}$ are called the *elementary root subgroups*. Every nontrivial transvection x is contained in a unique root subgroup, namely $X = \left\{x_{c(x),a(x)}(\xi) \mid \xi \in K\right\}$.

4°. Groups generated by transvections. Our proofs are based on the results on linear groups generated by transvections. The following striking fact was first proven by L.E.Dickson and is often called *Dickson's lemma* (see [Go] for a proof).

Lemma 3. *Let $K = \mathbb{F}_q$ be a finite field such that* $\mathrm{char}K \neq 2$ *and* $q \neq 9$. *Further, let λ be a defining element of K. Then*

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \right\rangle = \mathrm{SL}(2,K).$$

The following remarkable result due to J.McLaughlin [Mc] was later generalized in many directions. It is essentially the main instrument in our proof.

Lemma 4. *Let K be any field distinct from the field $\mathbb{F}_2$ of two elements and G be an irreducible linear group generated by root subgroups. Then one of the following holds:*

i) $G = \mathrm{SL}(n,K)$;

ii) $n = 2l$ *is even and* $G \sim \mathrm{Sp}(n,K)$.

Our original proofs were based on the following generalization of the above result, which was proven independently in [Wa] and [ZS].

Lemma 5. *Let* $\mathrm{char}K \neq 2$ *and G be an irreducible finite linear group generated by transvections. Then one of the following holds:*

i) $G \sim \mathrm{SL}(n,p^h)$ *for some h such that $\mathbb{F}_{p^h}$ is contained in K;*

ii) $n = 2l$ *is even and* $G \sim \mathrm{Sp}(n,p^h)$ *for some h such that $\mathbb{F}_{p^h}$ is contained in K;*

iii) $G \sim \mathrm{SU}(n, p^{2h})$ *for some* h *such that* $\mathbb{F}_{p^{2h}}$ *is contained in* K.

It should be noted that the conclusion of the lemma does not hold when $\mathrm{char}K = 2$, since in this case there are some additional possibilities for such a group G, like, say, the orthogonal groups and some of the alternating and symmetric groups (J.McLaughlin and H.Pollatsek have obtained a definitive list).

Since $\mathrm{res}(x) = 1$ for a transvection $x \neq e$, and

$$\mathrm{res}(a_1 \oplus \ldots \oplus a_t) = \mathrm{res}(a_1) + \ldots + \mathrm{res}(a_t)$$

there is no way to present a nontrivial transvection as a direct sum $a \oplus \ldots \oplus a$ with more than one summand. Thus lemma 1–iv implies that if G is a *primitive* irreducible group which contains a nontrivial transvection x, then the normal closure $H = \langle x \rangle^G$ of x in G is *irreducible*.

§3. Some preliminary results

Here we collect several elementary general observations which will be used in the proof of the main theorem.

1^0. Eigenspaces of elements of orders 2 and 3. In this subsection we assume that $\mathrm{char}K \neq 2$. Let x be an involution from $SL(n, K)$ and y be an element of order 3. In the sequel we denote by V^+ and V^- the eigenspaces of x corresponding to the eigenvalues $+1$ and -1 respectively. If ω is a cubic root of 1, then we denote the corresponding eigenspace by V^ω. The fact that $\mathrm{char}K \neq 2$ implies the direct decomposition $V = V^+ \oplus V^-$.

Lemma 6. *If* U *is an* x*-invariant subspace of* V, *then* $U = (U \cap V^+) \oplus (U \cap V^-)$.

Proof. Every $u \in U$ can be written in the form $u = (e - x)u/2 + (e + x)u/2$.

Lemma 7. *If* x *preserves a nondegenerate hermitian/symplectic form up to similarity with multiplier* $\lambda(x)$, *then at least one of the following holds:*

i) $\lambda(x) = 1$;

ii) $\dim(V^+) = \dim(V^-)$.

Proof. Since x is an involution, one has $\lambda(x) = \pm 1$. Suppose $\lambda(x) = -1$. Then for any $u, v \in V^\varepsilon$ for $\varepsilon = \pm 1$ one has $(u, v) = (xu, xv) = -(u, v)$, which means that both V^+ and V^- are totally isotropic. If $\dim(V^+) \neq \dim(V^-)$ then the form is degenerate.

Lemma 8. *If y preserves a nondegenerate hermitian/symplectic form up to similarity with multiplier $\lambda(y)$, then at least one of the following holds:*

i) $\lambda(y)=1$;

ii) $\dim(V^1)=\dim(V^\omega)$, *where* $\lambda(y)=\omega$

Proof. Since y has order 3, one has $\lambda(y)^3=1$. Suppose $\lambda(y)=\omega\neq 1$ (this can happen only if $\mathrm{char}K\neq 3$ and K actually contains a cubic root of 1). Let $\lambda\mapsto\overline{\lambda}$ be the involution on K. One has two possibilities: either $\overline{\omega}=\omega$ or $\overline{\omega}=\omega^2$.

If $\overline{\omega}=\omega$, then $(u,v)=(yu,yv)=\omega(u,v)$ if $u,v\in V^1$ or if $u\in V^\omega$ and $v\in V^{\omega^2}$. Moreover $\omega^2(u,v)=(yu,yv)=\omega(u,v)$ if $u,v\in V^\omega$ or if $u\in V^1$ and $v\in V^{\omega^2}$. This shows that V^{ω^2} is orthogonal to V^ω and V^1 and, moreover, V^ω and V^1 are totally isotropic. If $\dim(V^\omega)\neq\dim(V^1)$, then the inner product is degenerate.

The other possibility $\overline{\omega}\neq\omega$ may happen only if the inner product is hermitian. Then $\omega(u,v)=(yu,yv)=\overline{(yv,yu)}=\overline{\omega(v,u)}=\omega^2\overline{(v,u)}=\omega^2(u,v)$, which shows that the inner product should be identically zero.

2°. Geometry of transvections. In this subsection we describe our chief tool for getting a root subgroup inside H. Recall first, that $B(n,K)$ denotes the group of upper triangular matrices (the *standard Borel subgroup* of the general linear group $\mathrm{GL}(n,K)$). The group $B(n,K)$ is a semidirect product of the group $D(n,K)$ of diagonal matrices and the group $U(n,K)$ of upper unitriangular (=triangular unipotent) matrices. *Bruhat decomposition* asserts that

$$\mathrm{GL}(n,K)=B(n,K)N(n,K)B(n,K),$$

where $N(n,K)$ is the subgroup of monomial matrices.

Consider two transvections $x=x_{c(x),a(x)}(1)$ and $y=x_{c(y),a(y)}(1)$. The following fact is fundamental for our purposes. It was noted first in a paper by M.Aschbacher and G.Seitz, and extensively used in the “geometry of root subgroups” by B.Cooperstein. Here we reproduce a proof from [Va], where one can find further references.

Lemma 9. *Any pair (x,y) of transvections is simultaneously conjugated to a pair of elementary transvections. In other words, there exists $g\in\mathrm{GL}(n,K)$ such that*

$$gxg^{-1}=t_{ij}(\xi),\qquad gyg^{-1}=t_{hk}(\zeta),$$

for some $1\leq i,j,h,k\leq n$; $i\neq j$; $h\neq k$; $\xi,\zeta\in K$.

Proof. We know that every transvection is conjugate to an elementary one. Since all nontrivial elementary transvections are conjugated, we may from the very start think that $x = t_{1n}(1)$. Then, of course, y is conjugated to $t_{1n}(1)$ by some $z \in \mathrm{GL}(n, K)$. Consider the Bruhat decomposition of z with respect to the standard Borel subgroup: $z = b_1 w b_2$, where $b_1, b_2 \in B(n, K)$, $w \in N(n, K)$. Since $t_{1n}(1)$ lies in the centre of $U(n, K)$, one has $b_2 t_{1n}(1) b_2^{-1} = t_{1n}(\eta)$ for some $\eta \in K$. On the other side, $w t_{1n}(\eta) w^{-1} = t_{hk}(\zeta)$ for some $1 \leq h, k \leq n$; $h \neq k$; $\zeta \in K$. This means that our pair (x, y) is simultaneously conjugated to the pair $(t_{1n}(1), b_1 t_{hk}(\zeta) b_1^{-1})$. In turn, this pair is conjugated to the pair $(b_1^{-1} t_{1n}(1) b_1, t_{hk}(\zeta))$. Again since $t_{1n}(1)$ lies in the centre of $U(n, K)$, one has $b_1^{-1} t_{1n}(1) b_1 = t_{1n}(\xi)$ for some $\xi \in K$, which proves the lemma.

Usually this lemma is stated in the following form: *every pair (X, Y) of root subgroups is simultaneously conjugated to a pair of elementary root subgroups.* Now for a pair (X, Y) of elementary root subgroups $X = X_{ij}$, $Y = X_{hk}$ there are very few possibilities (corresponding to the interrelations of roots in the root system of type A_{n-1}):

– The indices i, j, h, k are all distinct, in which case the subgroups are called *orthogonal*. For $n \geq 4$ there is just one orbit of pairs of orthogonal root subgroups under conjugation.

– There are 3 distinct indices among i, j, h, k. This case branches in two cases each of which in turn branches in two subcases. Either $i \neq k$, $j \neq h$, or $i \neq h$, $j \neq k$. In the first case the root subgroups are called *commuting* (it corresponds to the angle $\pi/3$). For $n \geq 3$ there are two orbits of commuting root subgroups with representatives (X_{12}, X_{13}) and (X_{21}, X_{31}) respectively. In the second case the root subgroups are called *non-commuting* (it corresponds to the angle $2\pi/3$). Actually in this case the relative commutator $[X, Y]$ is again a root subgroup. There are two orbits of such pairs with representatives (X_{12}, X_{23}) and (X_{23}, X_{12}) respectively.

– Finally, if there are just 2 distinct indices among i, j, h, k, then either $(i, j) = (h, k)$ in which case the subgroups coincide, or — which is the most interesting case — $(i, j) = (k, h)$, when the subgroups are called *opposite*. Every pair of opposite root subgroups is conjugated to the pair (X_{12}, X_{21}).

Consider again two transvections $x = x_{c(x),a(x)}(1)$, $y = x_{c(y),a(y)}(1)$. We call them *orthogonal, commuting, non-commuting* or *opposite* if the (unique) root subgroups in which they are contained are orthogonal, commuting, non-commuting or opposite respectively.

It remains only two establish, how the mutual position of their root subgroups $X = \left\{x_{c(x),a(x)}(\xi) \mid \xi \in K\right\}$ and $Y = \left\{x_{c(y),a(y)}(\xi) \mid \xi \in K\right\}$ is expressed in terms of $a(x)$, $c(x)$, $a(y)$ and $c(y)$. For this we have to recall that under conjugation the axis and the centre behave as follows: $a(gxg^{-1}) = a(x)g^{-1}$ and $c(gxg^{-1}) = gc(x)$. This means in particular that if $(x', y') = (gxg^{-1}, gyg^{-1})$, then the products $a(x)c(y)$ and $a(y)c(x)$ remain invariant, i.e $a(x')c(y') = a(x)c(y)$ and $a(y')c(x') = a(y)c(x)$. Of course, another thing which is preserved by simultaneous conjugation is collinearity of $a(x)$ and $a(y)$ or, respectively, of $c(x)$ and $c(y)$: the rows $a(x')$ and $a(y')$ are proportional if and only if the rows $a(x)$ and $a(y)$ are and the same applies to columns $c(x')$ and $c(y')$. Since the mutual position of two elementary root subgroups is expressible in terms of the products and the collinearity, we have the following:

Lemma 10. *A necessary and sufficient condition for a pair of transvections x and y to be opposite is that both $\xi = a(x)c(y)$ and $\zeta = a(y)c(x)$ are distinct from zero. In this case the pair (x, y) is conjugate to the pair $(t_{12}(\zeta), t_{21}(\xi))$.*

Proof. For all pairs (x', y') of elementary transvections apart from $(t_{ij}(\lambda), t_{ji}(\mu))$ one has either $a(x')c(y') = 0$, or $a(y')c(x') = 0$. After conjugation by a monomial matrix we may assume that $(i, j) = (1, 2)$. Since the products $a(x)c(y)$ and $a(y)c(x)$ remain invariant under conjugation, the pair (x, y) is conjugated to $(x', y') = (x_{\zeta v_1, v_2^t}(1), x_{\xi v_2, v_1^t}(1)) = (t_{12}(\zeta), t_{21}(\xi))$.

Since the pair $(t_{12}(\zeta), t_{21}(\xi))$ is conjugate to the pair $(t_{12}(1), t_{21}(\xi\zeta))$ by a diagonal matrix, this lemma together with Dickson's lemma provides us with the following tool:

Lemma 11. *Let $K = \mathbb{F}_q$ be a finite field with $\mathrm{char}(K) \neq 2$ and $q \neq 9$. Suppose that x and y are such transvections that the product $\xi\zeta$, where $\xi = a(x)c(y)$ and $\zeta = a(y)c(x)$, is a defining element of the field K. Then the subgroup $\langle x, y\rangle$ contains a root subgroup $X \cong K^+$.*

Actually we may even conclude that $\langle x, y\rangle$ contains a subgroup isomorphic to $\mathrm{SL}(2, K)$, but when $\langle x, y\rangle$ is irreducible (which is the only interesting case), this automatically follows from the fact that $\langle x, y\rangle$ contains a subgroup isomorphic to K^+.

3^0. Irreducibility of H. In this subsection we consider a subgroup G of $\mathrm{SL}(n, K)$ generated by an involution x and an element y of order 3. Suppose some power z^r of the commutator $z = [x, y]$ is a transvection, and let H be the normal subgroup of G generated by z^r. Our aim here is to produce criteria which allow us to conclude that if G is irreducible, then H is also irreducible.

We start with the following lemma, which is an obvious consequence of the fact that the only permutations which appear in the Bruhat decomposition of transvections are transpositions. Since it is elementary we prefer to give a direct proof.

Lemma 12. *Consider a block-monomial matrix of the shape*

$$z = \begin{pmatrix} & a_1 & & \\ & & \ddots & \\ & & & a_{l-1} \\ a_l & & & \end{pmatrix},$$

where $l \geq 2$ and $a_1, \ldots, a_l \in \mathrm{GL}(m, K)$, $m \geq 2$. Then no power of z is a non-trivial transvection.

Proof. Consider z^r. If r is not divisible by l, then z^r is a block-monomial matrix which is not block-diagonal. Thus its residue is at least m. On the other side z^l is a block-diagonal matrix of the form

$$a_1 a_2 \ldots a_{l-1} a_l \,\oplus\, a_2 a_3 \ldots a_l a_1 \,\oplus\, \ldots \,\oplus\, a_l a_1 \ldots a_{l-2} a_{l-1}.$$

Since the summands are all conjugate , the residue of any power z^r where $l \mid r$ is divisible by l. This shows that z^r can never be a non-trivial transvection.

The following two propositions save us a lot of calculations later.

Proposition 1. *Let G be a subgroup of $\mathrm{SL}(n, K)$ generated by an involution x and an element y of order 3. Suppose some power z^r of the commutator $z = [x, y]$ is a non-trivial transvection and let $H = \langle z^r \rangle^G \trianglelefteq G$ be the normal subgroup of G generated by z^r. Suppose G is irreducible and let $V = U_1 \oplus \ldots \oplus U_l$ be a direct decomposition of V into H-homogeneous components. Denote by ϱ and σ the images of x and y in the action of G on the set $I = \{U_1, \ldots, U_l\}$ of components. Then:*

i) *If $l = 1$, then H is irreducible;*

ii) *$l \neq n$;*

iii) *$l \neq 2$;*

iv) *If z^r acts non-trivially on some $U_i \in I$, then $[\varrho, \sigma]\, U_i = U_i$.*

Proof. i) Here V is H-homogeneous. If it is not H-irreducible, then any matrix in H is conjugate to a matrix of the form $a \oplus \ldots \oplus a$ for some $a \in \mathrm{GL}(m, K)$, $m \mid n$, $m \neq n$, which makes it impossible for H to contain a transvection (see the remark after Lemma 4).

ii) If $l = n$, then H is diagonalizable, so it cannot contain a transvection.

iii) If $l = 2$, then the summands should be invariant with respect to y. Since G is irreducible x should transpose U_1 and U_2. In other words in a base of the space V which is a join of bases of U_1 and U_2 the matrices x and y have the following block shape

$$x = \begin{pmatrix} 0 & x_1 \\ x_2 & 0 \end{pmatrix}, \qquad y = \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix}$$

Since x is an involution one has moreover $x_2 = x_1^{-1}$. Now $z = [x, y]$ has block shape $z_1 \oplus z_2$, where $z_1 = x_1 y_2 x_1^{-1} y_1^{-1}$ and $z_2 = x_1^{-1} y_1 x_1 y_2^{-1}$. Notice that z_2 is conjugated by x_1 to z_1^{-1}. Of course the same is true for any powers z_2^r and z_1^{-r}. Thus by the properties of residues recalled in §2–3 the residue of z^r is always even, which contradicts the fact that z^r is a transvection.

iv) We may assume $l < n$. Since G is irreducible, the group $\Pi = \langle \varrho, \sigma \rangle \leq S_l$, generated by ϱ and σ acts transitively on I. Let a subspace U_i be contained in an orbit of cardinality s with respect to the commutator $[\varrho, \sigma]$ and W be the sum of the subspaces U_j from this orbit. Then it follows from Lemma 12 that the residue of any power z^r is divisible by s. This means that if z^r is a transvection, it should act trivially on W when $s \geq 2$, i.e. when U_i is not $[\varrho, \sigma]$-invariant.

Proposition 2. *Let G be a subgroup of $\mathrm{SL}(n, K)$ generated by an involution x and an element y of order 3. Suppose some power z^r of the commutator $z = [x, y]$ is a non-trivial transvection and its conjugate yz^ry^{-1} is a transvection opposite to z^r. Let $H = \langle z^r \rangle^G \trianglelefteq G$ be the normal subgroup of G generated by z^r. If G is irreducible then H is also irreducible.*

Proof. Keep the notation of Proposition 1. We may assume $2 < l < n$. Let U_i be the subspace on which z^r acts non-trivially. Then by Proposition 1 the subspace U_i is $[\varrho, \sigma]$-invariant. Notice that this subspace cannot be σ-invariant (if it were, then either U_i or $U_i \oplus xU_i$ would form a G-invariant subspace of V which is impossible since $l > 2$). But then the transvection yz^ry^{-1} acts nontrivially on some subspace U_j for some j distinct from i and thus is orthogonal to z^r and not opposite, a contradiction.

4^0. Values of polynomials over a finite field. Here we discuss the restrictions imposed in §1 on a finite field.

Lemma 13. *Let $K = \mathbb{F}_q$, $q = p^m$, be a finite field, $f(t) \in K[t]$ be a polynomial of degree $d > 0$ over K, and $X \subseteq K$ be a subset of cardinality s. Suppose one of the following holds:*

i) $m = 1$ *and* $p > d + s$;
ii) $m = 2$ *and* $p > d, s$;
iii) $m = 3$ *and* $p > \sqrt{d + s}$;
iv) $m \geq 4$ *and* $p > \sqrt{d},\ \sqrt[m-2]{s}$.
Then at least one value of $f(t)$ *on* $K \backslash X$ *is a defining element of* K.

Proof. Since each of the polynomials $f(t) - \mu$, $\mu \in K$, has at most d distinct roots, there are no more, than d distinct elements $\lambda \in K$ such that $f(\lambda) = \mu$. This shows that $f(t)$ assumes at least $(p^m - s)/d$ distinct values on $K \backslash X$.

If $m = 1$, any nonzero element of K suits us as the value of $f(t)$. Thus the condition is that $(p - s)/d$ should be > 1.

If $m = 2$ or 3, then there are p elements of K which are not defining, so that $(p^m - s)/d$ should be greater than p. This holds whenever $p^2 > pd + s$ or $p^3 > pd + s$ respectively.

If $m = 4$, then then there are precisely p^2 elements which are not defining and if $m \geq 5$ then there are no subfields of orders p^{m-1} and p^{m-2} in K and thus an extremely crude estimate shows that there are at most

$$p^{m-3} + p^{m-4} + \ldots + p = \frac{p^{m-2} - p}{p - 1} \leq p^{m-2}$$

elements which are not defining. Thus $(p^m - s)/d$ should be greater than p^{m-2}.

In the cases which appear in §1–3 we have $s \leq 7$ and $d = 3$ or $s \leq 6$ and $d = 4$. Thus the conditions of the lemma are not satisfied only when $q = 3, 5, 7, 9, 25, 27, 49$ (remember that $\mathrm{char} K \neq 2$). However the cases $q = 27, 49$ are excluded by considering the inequalities given in the proof. The remaining cases have to be checked separately.

§4. The case n = 5

In this section we prove the theorem for $n = 5$. Recall that in

$$x = \begin{pmatrix} 1 & . & . & . & . \\ . & . & 1 & . & . \\ . & 1 & & . & . \\ . & . & . & 1 & . \\ . & . & . & t & -1 \end{pmatrix}, \qquad y = \begin{pmatrix} . & 1 & . & . & . \\ -1 & -1 & . & . & . \\ . & . & . & . & 1 \\ . & . & 1 & . & . \\ . & . & . & 1 & . \end{pmatrix}$$

and $G = \langle x, y \rangle$. We follow the general scheme described in §1.

1^0. Root subgroup. Set $z=[x,y]$. Then a direct calculation shows that

$$z^4=\begin{pmatrix} 1 & . & . & . & . \\ t^2 & 1 & . & -t^2 & . \\ -t^2 & . & 1 & t^2 & . \\ . & . & . & 1 & . \\ -2t & . & . & 2t & 1 \end{pmatrix}, \; y^{-1}z^4y=\begin{pmatrix} 1-t^2 & -t^2 & . & . & -t^2 \\ t^2 & 1+t^2 & . & . & t^2 \\ 2t & 2t & 1 & . & 2t \\ t^2 & t^2 & . & 1 & t^2 \\ . & . & . & . & 1 \end{pmatrix}$$

are transvections. Denote by H the normal closure of z^4 in G. One has $a(z^4)=(1,0,0,-1,0)$, $c(z^4)=(0,t^2,-t^2,0,-2t)^t$, $a(yz^4y^{-1})$=$(1,1,0,0,1)$ and $c(yz^4y^{-1})=(-t^2,t^2,2t,t^2,0)^t$, so that by Lemma 11 the subgroup H contains a root subgroup if $a(z^4)c(yz^4y^{-1})a(yz^4y^{-1})c(z^4)=-2t^3(t-2)$ is a defining element of $\mathbb{F}_q$.

2^0. Irreducibility of H. The eigenspaces V^+ and V^- of x are

$$V^+=\{\,(a,b,b,c,\frac{t}{2}c)^t \mid a,b,c\in \mathbf{F}_q\},$$

$$V^-=\{(0,a,-a,0,b)^t \mid a,b\in \mathbf{F}_q\},$$

respectively. First, let U be a G-invariant subspace which is not contained in V^+. Then there is $u\in V$ such that $0\neq(x-1)u\in V^-\cap U$. Thus we may assume that there is a non-zero vector $(0,a,-a,0,b)^t\in U$. If $a=0$, then $b\neq 0$ and thus $v_5\in U$. Since y cyclically permutes v_3, v_4 and v_5, x interchanges v_2 and v_3 and y^2 sends v_2 to v_1, we conclude that $U=V$. Thus we may assume $a\neq 0$. In that case we have $u=(0,1,-1,0,b)^t\in V^-\cap U$ for some b. Consider the vectors

$$v=(x-e)yu=(0,b+1,-(b+1),0,-t)^t\in V^-\cap U,$$

$$w=(x-e)y^2u=(0,0,0,0,tb+2)^t\in V^-\cap U.$$

Then the necessary conditions for the space $\langle u,v,w\rangle$ to be 1-dimensional are $b^2+b+t=0$ and $tb+2=0$, which are satisfied simultaneously only if $t^3-2t+4=0$. Thus if $t^3-2t+4\neq 0$ the space $\langle u,v,w\rangle$ is 2-dimensional and must coincide with V^-. This means that $U\supseteq V^-$ and again $v_5\in U$.

So it remains only to prove that there are no proper G-invariant subspaces U contained in V^+. Let $u=(a,b,b,c,\frac{t}{2}c)^t\in U$, $u\neq 0$. Then also $yu=(b,-a-b,\frac{t}{2}c,b,c)^t$ and $y^2u=(-a-b,a,c,\frac{t}{2}c,b)^t$ must belong to V^+. This is possible only if $t^2+2t+4=0$.

Thus G — and hence by the proposition 1 from §3 also H — is irreducible, provided $t^3-2t+4\neq 0$ and $t^2+2t+4\neq 0$.

3^0. **Invariant forms.** There are no nondegenerate symplectic forms in dimension 5.

4^0. **Equations.** The roots of the equation $t^3-2t+4=0$ are -2, $1\pm i$; while the roots of the equation $t^2+2t+4=0$ are $-1\pm\sqrt{-3}$. Thus we have to choose $t\in\mathbb{F}_q$ which is not one of these roots and such that moreover $\mathbb{F}_q=\mathbb{F}_q[f(t)]$ where $f(t)=2t^3(t-2)$. By Lemma 13 the choice is certainly possible when $q\neq 3,5,7,9,25$.

Let $\mathbb{F}_{25}=\mathbb{F}_5[\tau]$, where $\tau^2+\tau+1=0$. The roots of the first equation are -2 (twice) and 4. Since τ is not a root of the second equation and $f(\tau)=2(\tau-2)$ is a field generator the choice $t=\tau$ will do.

If $q=7$, then the the first equation has just the root -2 and the second equation has the roots 1 and 4. Thus we may take $t=3$, (recall that we want $2t^3(t-2)\neq 0$).

If $q=5$ then the roots of the first equation are -2 (twice) and 4, while the second equation has no roots so that $t=1$ will do.

For $q=3$ the elements x and y generate a reducible subgroup of $\mathrm{SL}(5,3)$ if $t=\pm 1$, but a direct check with "CAYLEY" shows that they generate the whole group $\mathrm{SL}(5,3)$ when $t=0$ (notice that in this case y is *not* monomial).

§5. The case n = 6

In this section we prove the theorem for $n=6$. Recall that

$$x=\begin{pmatrix} 1 & . & . & . & . & . \\ . & 1 & . & . & . & . \\ . & . & . & 1 & . & . \\ . & . & 1 & . & . & . \\ . & . & . & . & 1 & . \\ . & . & . & . & t & -1 \end{pmatrix}, \qquad y=\begin{pmatrix} . & . & 1 & . & . & . \\ 1 & . & . & . & . & . \\ . & 1 & . & . & . & . \\ . & . & . & . & . & 1 \\ . & . & . & 1 & . & . \\ . & . & . & . & 1 & . \end{pmatrix}$$

and $G=\langle x,y\rangle$. We follow the general scheme described in §1.

1^0. **Root subgroup.** Set $z=[x,y]$. Then a direct calculation shows that

$$z^4=\begin{pmatrix} 1 & . & . & . & . & . \\ . & 1 & . & . & . & . \\ t^2 & . & 1 & . & -t^2 & . \\ -t^2 & . & . & 1 & t^2 & . \\ . & . & . & . & 1 & . \\ -2t & . & . & . & 2t & 1 \end{pmatrix}, \; yz^4y^{-1}=\begin{pmatrix} 1 & t^2 & . & . & . & -t^2 \\ . & 1 & . & . & . & . \\ . & . & 1 & . & . & . \\ . & -2t & . & 1 & . & 2t \\ . & -t^2 & . & . & 1 & t^2 \\ . & . & . & . & . & 1 \end{pmatrix}$$

are transvections. Denote by H the normal closure of z^4 in G. One has $a(z^4) = (1,0,0,0,-1,0)$, $c(z^4) = (0,0,t^2,-t^2,0,-2t)^t$, $a(yz^4y^{-1}) = (0,1,0,0,0,-1)$ and $c(yz^4y^{-1}) = (t^2,0,0,-2t,-t^2,0)^t$. By Lemma 11 the subgroup H contains a root subgroup if $a(z^4)c(yz^4y^{-1})a(yz^4y^{-1})c(z^4) = 4t^3$ is a defining element of $\mathbb{F}_q$.

2^0. Irreducibility of H. The eigenspaces V^+ and V^- of x are

$$V^+ = \{\,(a,b,c,c,d,\frac{t}{2}d)^t \mid a,b,c,d \in \mathbf{F}_q\},$$

$$V^- = \{(0,0,a,-a,0,b)^t \mid a,b \in \mathbf{F}_q\},$$

respectively. Let first U be a G-invariant subspace which is not contained in V^+. Then there is a $u \in V$ such that $0 \neq (b-1)u \in V^- \cap U$. Thus we may assume that there is a non-zero vector $(0,0,a,-a,0,b)^t \in U$. If $a = 0$, then $b \neq 0$ and thus $v_6 \in U$. Since y cyclically permutes v_4, v_5 and v_6; x interchanges v_3 and v_4 and y cyclically permutes v_1, v_2 and v_3, we conclude that $U = V$. Thus we may assume that $a \neq 0$. In that case we have $u = (0,0,1,-1,0,b)^t \in V^- \cap U$ for some b. Consider the vectors

$$v = (x-e)yu = (0,0,b,-b,0,-t)^t \in V^- \cap U,$$

$$w = (x-e)y^2u = (0,0,0,0,0,tb+2)^t \in V^- \cap U.$$

Then the necessary conditions for the space $\langle u,v,w\rangle$ to be 1-dimensional are $b^2+t=0$ and $tb+2=0$, which are satisfied simultaneously only if $t^3+4=0$. Thus if $t^3+4\neq 0$ the space $\langle u,v,w\rangle$ is 2-dimensional and must coincide with V^-. This means that $U \supseteq V^-$ and again $v_6 \in U$.

So it remains only to prove that there are no proper G-invariant subspaces U contained in V^+. Let $u = (a,b,c,c,d,\frac{t}{2}d)^t \in U$, $u \neq 0$. Then also $yu = (c,a,b,\frac{t}{2}d,c,d)^t$ and $y^2u = (b,c,a,d,\frac{t}{2}d,c)^t$ must belong to V^+. This is possible only if $a = d$, $b = \frac{t}{2}d$, $d = \frac{t}{2}c$ and $c = \frac{t^2}{4}d$. Now if $d = 0$ then $u = 0$ which contradicts our choice of u. So $d \neq 0$ and thus $t^3 = 8$.

This shows that G — and thus by proposition 2 also H — is irreducible provided $t^3 \neq 8,-4$.

3^0. Invariant forms. We have to prove that there exists no nondegenerate symplectic form on V which is invariant under the action of G *up to similarity.* This is true whenever $t \neq 0$. First observe that it follows from the Lemma 7 that $\lambda(x) = 1$. (since $\dim V^+ = 2 \neq 4 = \dim V^-$). Let now $(\ ,\ )$ be an invariant form. Then $(v_i,v_5) =_x (v_i,v_5) + t(v_i,v_6)$ for $i = 1,2$ and, since $t \neq 0$ we have $(v_1,v_6) = (v_2,v_6) = 0$. Of course this implies that

$(v_1, v_5) =_y (v_3, v_4) =_y (v_2, v_6) = 0$ and $(v_2, v_4) =_y (v_3, v_5) =_y (v_1, v_6) = 0$ Then since $(v_2, v_4) =_x (v_2, v_3)$ also $(v_3, v_1) =_y (v_1, v_2) =_y (v_2, v_3) = 0$ and since $(v_4, v_1) =_x (v_3, v_1)$, also $(v_6, v_3) =_y (v_5, v_2) =_y (v_4, v_1) = 0$ By reflexivity this means that all of the inner products (v_i, v_j) are 0 if at least one of the indices i,j is ≤ 3 and $i \neq j$. Since the inner product is symplectic v_1, v_2 and v_3 are in the radical, so that the product is degenerate.

4^0. Equations. Here the equations are $t^3 = 8$ and $t^3 = -4$. Thus we have to choose $t \in \mathbb{F}_q$ which is not a root of these equations and such that moreover $\mathbb{F}_q = \mathbb{F}_q[f(t)]$ where $f(t) = 4t^3$. By Lemma 13 the choice is certainly possible when $q \neq 3, 5, 7, 9, 25$.

Let $q = 25$. Then the inequality $p^2 > pd + s$ is clearly satisfied since $d = 3$ and $s \leq 7$.

For $q = 7$ the roots of the equation are just 1,2 and 3, while the second one has no roots. Thus any $t \neq 0$, 1, 2, 3 will do.

For $q = 5$ only 1 and 2 are roots of the above equations, so that $t = 3$ or 4 will do.

When $q = 3$ the equations reduce to $t^3 = 2$. Thus we may take $t = 1$.

§6. The case n = 7

In this section we prove the theorem for $n = 7$. Recall that

$$x = \begin{pmatrix} . & 1 & . & . & . & . & . \\ 1 & . & . & . & . & . & . \\ . & . & -1 & . & . & . & . \\ . & . & . & . & 1 & . & . \\ . & . & . & 1 & . & . & . \\ . & . & . & . & . & 1 & . \\ . & . & . & . & . & t & -1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & . & . & . & . & . & . \\ . & . & . & 1 & . & . & . \\ . & 1 & . & . & . & . & . \\ . & . & 1 & . & . & . & . \\ . & . & . & . & . & . & 1 \\ . & . & . & . & 1 & . & . \\ . & . & . & . & . & 1 & . \end{pmatrix}$$

and $G = \langle x, y \rangle$. We follow the general scheme described in §1.

1^0. Root subgroup. Set $z = [x, y]$. Then a direct calculation shows that

$$z^8 = \begin{pmatrix} 1 & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . \\ . & . & 1 & . & . & . & . \\ -2t^2 & 2t^2 & -2t^2 & 1 & . & 2t^2 & -4t \\ -2t^2 & 2t^2 & -2t^2 & . & 1 & 2t^2 & -4t \\ . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & 1 \end{pmatrix},$$

$$yz^8y^{-1} = \begin{pmatrix} 1 & . & . & . & . & . & . \\ -2t^2 & 1 & 2t^2 & -2t^2 & -4t & . & 2t^2 \\ . & . & 1 & . & . & . & . \\ . & . & . & 1 & . & . & . \\ . & . & . & . & 1 & . & . \\ -2t^2 & . & 2t^2 & -2t^2 & -4t & 1 & 2t^2 \\ . & . & . & . & . & . & 1 \end{pmatrix}$$

are transvections. Denote by H the normal closure of z^8 in G. In this case we prefer to normalize a and c in such a way that the first non-zero component of c equals 1 (before we always normalized them so that the first non-zero component of a was 1). Then $a(z^8) = (-2t^2, 2t^2, -2t^2, 0, 0, 2t^2, -4t)$, $c(z^8) = (0,0,0,1,1,0,0)^t$, $a(yz^8y^{-1}) = (-2t^2, 0, 2t^2, -2t^2, -4t, 0, 2t^2)$ and $c(yz^8y^{-1}) = (0,1,0,0,0,1,0)^t$. Thus by Lemma 11 the subgroup H contains a root subgroup if $a(z^8)c(yz^8y^{-1})a(yz^8y^{-1})c(z^8) = -8t^3(t+2)$ is a defining element of $\mathbb{F}_q$.

2^0. Irreducibility of H. The eigenspaces V^+ and V^- of x are

$$V^+ = \{\,(a, a, 0, b, b, c, \frac{t}{2}c)^t \mid a, b, c \in \mathbf{F}_q\},$$

$$V^- = \{(a, -a, b, c, -c, 0, d)^t \mid a, b, c, d \in \mathbf{F}_q\},$$

respectively. Let first U be a G-invariant subspace which is not contained in V^-. Then there is $u \in V$ such that $0 \neq (b+1)u \in U \cap V^+$. Thus we may assume that there is a non-zero vector $u = (a, a, 0, b, b, c, \frac{t}{2}c)^t \in U$. Consider the vectors

$$v = (x+1)yu = (a+b, a+b, 0, \frac{t}{2}c, \frac{t}{2}c, 2b, tb)^t \in U \cap V^+;$$

$$w = (x+1)y^2u = (a, a, 0, a+c, a+c, \frac{t}{2}c, \frac{t^2}{2}c)^t \in U \cap V^+.$$

Suppose first that u and v are linearly dependent and $c = 0$. Then $b = 0$, so that $u = (a, a, 0, 0, 0, 0, 0)^t$, which implies $v_1 + v_2 \in U \cap V^+$.

Applying x and y to $v_1 + v_2$ we check that $v_4 + v_5 \in U$ and $v_6 - v_7 \in U$. Hence $v_6 + (t+1)v_7 \in U$ and therefore $(t+2)v_7 \in U$. If $t \neq -2$ this implies that $v_7 \in U$ and thus all the base vectors belong to U, i.e. $U = V$.

Thus if u and v are dependent we may assume that $c \neq 0$ (which in turn implies that $a \neq 0$ if $t \neq 1$). Now suppose that u and w are also linearly dependent. Then $a \neq 0$ implies that $c = 0$ so that we get a contradiction. This means that we may assume that $\dim(U \cap V^+) \geq 2$ and thus U must contain a vector of the form $u = (1,1,0,b,b,0,0)^t$. But then $(x+1)y^2(1,1,0,b,b,0,0)^t = (1,1,0,1,1,0,0)^t$ also belongs to U, so we may take $u = (1,1,0,1,1,0,0)^t$. The vectors u, $v = (x+1)yu = (2,2,0,0,0,2,t)^t$ and $w = (x+1)y^2v = (2,2,0,4,4,2t,t^2)^t$ all belong to $U \cap V^+$ and are linearly independent if $t \neq -1$. Then $U \geq V^+$ and the proof finishes as before.

The only case not yet considered is when $U \leq V^-$. But it is immediate to see that if u, yu, y^2u all belong to V^-, then necessarily $u = 0$.

Thus G — and hence by proposition 1 also H — is irreducible provided $t \neq 1, -1, -2$.

$\mathbf{3^0}$. **Invariant forms.** There are no non-degenerate symplectic forms in dimension 7.

$\mathbf{4^0}$. **Equations.** Here t has to be distinct from 0, 1, -1 and -2. Thus we have to choose $t \in \mathbb{F}_q$ which is not one of these elements and such that moreover $\mathbb{F}_q = \mathbb{F}_q[f(t)]$ where $f(t) = 8t^3(t+2)$. By Lemma 13 the choice is certainly possible when $q \neq 3, 5, 7, 9, 25$.

If $q = 25$, then the inequality $p^2 > pd + s$ is clearly satisfied since $d = 4$ and $s = 4$.

If $q = 7$, then for all $t \neq 0$, 1, -1, -2 the value of $f(t)$ is not zero.

For $q = 5$ the value $t = 2$ will do.

For the case $q = 3$ the elements x_7 and y_7 given in §1 always generate a reducible subgroup, but a direct check with "CAYLEY" shows that the elements x_7 for $t = -1$ and $y_7 + e_{12} - e_{13}$ generate the whole group $\mathrm{SL}(7,3)$.

Final remarks.

1. The results listed in the introduction together with the evidence provided by work currently under way indicate that most finite simple groups appear as factor-groups of $\mathrm{PSL}(2,\mathbb{Z})$. This is in sharp contrast with the normal structure of $\mathrm{PSL}(n,\mathbb{Z})$, $n \geq 3$, which is essentially controlled by the congruence subgroups, so that its finite simple factors are just the groups $\mathrm{PSL}(n,p)$, p prime. Originally this was discovered by J.Mennicke [Me] and H.Bass — M.Lazard — J.-P.Serre [BLS]. Of course it follows also from the subsequent results of H.Bass, J.S.Wilson, I.Z.Golubchik, L.N.Vaserstein and others on the normal structure of linear groups over rings. Actually from these results it follows that $\mathrm{PSL}(n,\mathbb{Z})$ has $\aleph_0$ normal subgroups when $n \geq 3$, while $\mathrm{PSL}(2,\mathbb{Z})$ has $2^{\aleph_0}$ normal subgroups [Ms]. As another illustration of how rich in normal subgroups $\mathrm{PSL}(2,\mathbb{Z})$ is one could mention the following result: every finitely generated group can be embedded in an infinite simple group with generators of orders 2 and 3 respectively, whose product has infinite order [Sch], [MP].

2. In general one could ask for which values $m \geq 3$ a finite simple group is generated by an involution and an element of order m. But the question of the (2,3)-generation is particularly interesting because it is related to the classical problem of Hurwitz generation. Let us recall that a group is called a *Hurwitz group* if it can be generated by an involution and an element of order 3 whose product has order 7, i.e. if it appears as a factor-group of the triangle group

$$\langle\, x, y \mid x^2 = y^3 = (xy)^7 = 1 \,\rangle .$$

There are dozens of papers dedicated to the study of Hurwitz groups. It is known for example that almost all alternating groups, almost all groups of types G_2 and ${}^2\mathrm{G}_2$, some of the sporadic groups and most of the groups $\mathrm{PSL}(2,q)$ for $q = p$ or p^3, p prime, are Hurwitz (see the surveys [Con], [DiMT] for references and further related results). It is our belief though that the large finite simple groups of Lie type are *never* Hurwitz. Actually J.Cohen has shown that all of the groups $\mathrm{PSL}(3,q)$, $q \neq 2$ are not Hurwitz (of course $\mathrm{PSL}(3,2) \cong \mathrm{PSL}(2,7)$ *is* Hurwitz), while M.Ch.Tamburini and S.Vassallo have shown that $\mathrm{PSL}(4,q)$ and $\mathrm{PSU}(4,q^2)$ are *never* Hurwitz (at the end of their paper they state a result which says that many of the groups $\mathrm{PSL}(n,q)$ for $n = 5,6,7,8,9,10,11,16$ are not Hurwitz either).

3. Recently M.Ch.Tamburini has discovered a remarkable method to "duplicate" the generators of $\mathrm{SL}(n,q)$ which allows in most cases (at least when the involution has a large eigenspace corresponding to the eigenvalue 1) to construct a pair of (2,3)-generators of the even dimensional classical groups $\mathrm{Sp}(2n,q)$, $\Omega^+(2n,q)$ and $\mathrm{SU}(2n,q^2)$ from a pair of (2,3)-generators of $\mathrm{SL}(n,q)$ [T2]. We believe that a combination of her and our methods is sufficient to prove that all the even dimensional classical groups are (2,3)-generated at least when the dimension is ≥ 10 and the characteristic of the ground field is distinct from 2 and 3.

Using a variation of this construction we were able to produce a pair of elements a and b of orders 2 and 3 respectively in the Chevalley group of type E_6 which generate a subgroup acting irreducibly on the 27-dimensional module and such that the 12-th power of their commutator $[a, b]$ is a unipotent root element. We think there is strong evidence that these elements actually generate the whole group $E_6(q)$. Actually to find the commutator $[a, b]$ and its powers we used symbolic calculation with "Mathematica". We have not yet fully implemented analogous programs for the Chevalley groups of types E_7 and E_8 since the explicit symbolic calculations in the Chevalley groups of these types require enormous computer time, but we propose to do this in the near future.

4. Let us mention another obvious consequence of the (2,3)-generation. As we have seen in §1, any (2,3)-generated *simple* group can be generated by three *conjugate* involutions. It is known that all non-abelian finite simple groups are generated by a set of three (not necessarily conjugate) involutions with the only exception of $\mathrm{PSU}(3, 3^2)$ (see the survey [DiMT] and the recent paper [MSW]).

5. The most intriguing problem here is of course whether the group $\mathrm{SL}(n, \mathbb{Z})$ — or even the group $\mathrm{PSL}(n, \mathbb{Z}[t])$ — is (2,3)-generated. The authors have opposite opinions as to whether this is plausible. Of course, this result would imply the results of this paper as well as a lot of other things.

Bibliography

[BLS] Bass H., Lazard M., Serre J.-P. Sous-groupes d'indice fini dans $\mathrm{SL}(n, \mathbb{Z})$. – *Bull. Amer. Math. Soc.* – 1964. – **70**. – P.385–392.

[CD] Cazzola M., Di Martino L. (2,3)-generation of $\mathrm{PSp}(4, q)$, $q = p^m$, $p \neq 2, 3$. – *in preparation.*

[Co] Cohen J. On non-Hurwitz groups. – *Glasgow Math. J.* – 1981. – **22**. – P.1–7.

[Con] Conder M.D.E. Hurwitz groups: a brief survey. – *Bull. Amer. Math. Soc.* – 1990. – **23**, N.2. – P.359–370.

[DiMT] Di Martino L, Tamburini M.Ch. 2-Generation of finite simple groups and some related topics. – in *Generators and Relations in Groups and Geometries*, A.Barlotti et al. (eds.), Kluwer Acad. Publ. – 1991. – P.195–233.

[Ga] Garbe D. Über eine Klasse von arithmetisch definierbaren Normalteilern der Modulgruppe. – *Math. Ann.* – 1978. – **235**. – S.195–215.

[Go] Gorenstein D. *Finite groups.* – Harper & Row Publishers: N.Y.–London. – 1968. – 527P.

[HO'M] Hahn A.J., O'Meara O.T. *The classical groups and K-theory.* – Springer: Berlin et al. – 1989. – 576P.

[KL] Kleidman P., Liebeck M. *The subgroup structure of the finite classical groups.* – LMS Lecture Note Series. – 1990. – **129**.

[LN] Lidl R., Niederreiter H. *Finite fields.* – Encyclopedia of Math. and Appl. – Addison Wesley P.C.: London et al. – 1983. – **20**.

[Mb] Macbeath A.W. Generators of linear fractional groups. – *Proc. Symp. Pure Math.* – 1967. – **12**. – P.14–32.

[Ma1] Malle G. Exceptional groups of Lie type as Galois groups. – *J. reine angew. Math.* – 1988. – **392**. - S.70–109.

[Ma2] Malle G. Hurwitz groups and G_2. – *Canad. Math. Bull.* – 1990. – **33**, N.3. – P.349–357.

[MSW] Malle G., Saxl J., Weigel Th. – Generation of classical groups. – *submitted.*

[Ms] Mason A.W. Nonstandard, normal subgroups and nonnormal, standard subgroups of the modular group. – *Canad. Math. Bull.* – 1989. – **32**, N.1. – P.109–113.

[MP] Mason A.W., Pride S.J. Normal subgrous of prescribed order and zero level of the modular group and related groups. – *J. London. Math. Soc.* – 1990. – **42**. – P.465–474.

[Mc] McLaughlin J.E. Some groups generated by transvections. – *Arch. Math.* – 1967. – **18**. – P.364–368.

[Me] Mennicke J. Finite factor groups of the unimodular group. – *Ann. Math.* – 1965. – **81**. – P.31–37.

[Sch] Schupp P.E. Embeddings into simple groups. – *J. London Math. Soc.* – 1976. – **13**. – P.90–94.

[T1] Tamburini M.Ch. Generation of certain simple groups by elements of small order. – *Rend. Ist. Lomb. Sci.* – 1987. – **A121** – P.21–27.

[T2] Tamburini M.Ch. *in preparation.*

[TV] Tamburini M.Ch., Vassallo S. (2,3)-generazione di $SL(4, q)$ in caratteristica dispari e problemi collegati. – *in preparation.*

[TW] Tamburini M.Ch., Wilson J.S. On the generation of finite simple groups by pairs of subgroups. – *J. Algebra.* – 1988. – **116**, N.2. – P.316–333.

[Va] Vavilov N.A. Geometry of long root subgroups in the Chevalley groups – *Vestnik Leningrad. Univ., Math.* – 1988. – N.1. – P.5–10.

[Wa] Wagner A. Groups generated by elations. – *Abh. Semin. Math.Univ. Hamburg.* – 1974. – **41**. – P.199–205.

[We] Weigel Th. Generation of exceptional groups of Lie-type. – *submitted.*

[Wi] Wilson J.S. A residual property of free groups. - *J. Algebra.* – 1991. – **138**, N.1. – P.36–47.

[Wo] Woldar A.J. On Hurwitz generation and genus action of sporadic groups. – *Illinois Math . J .* – 1989. – **33**. – P.416–437.

[ZS] Zalesskii A.E., Serezhkin V.N. Linear groups generated by transvections. – *Math. USSR Izvestija.* – 1976. – **40**. – P.25–46.

(2,3)-GENERATION OF SL$(\mathbf{n}, \mathbf{q})$. II. CASES $\mathbf{n} \geq 8$

Lino Di Martino * and **Nikolai Vavilov** **

Dipartimento di Matematica
Università degli Studi di Milano
via C.Saldini 50
20133, Milano, Italia

and

Department of Mathematics and Mechanics
University of Sanct-Petersburg
Petrodvorets, 198904, Russia

and

Fakultät für Mathematik
Universität Bielefeld
4800 Bielefeld 1, Deutschland

Introduction

There is growing evidence that most finite simple groups (and closely related groups) appear as factor-groups of the classical modular group $\mathrm{PSL}(2, \mathbf{Z})$. It is well known that $\mathrm{PSL}(2, \mathbf{Z})$ is isomorphic to the free product

* The first-named author was supported by the *Ministero dell'Università e della Ricerca Scientifica e Tecnologica* (M.U.R.S.T.)

** The second-named author gratefully acknowledges the support of the *Consiglio Nazionale delle Ricerche* (C.N.R.) and the *Alexander von Humboldt-Stiftung* and the hospitality of the *Università degli Studi di Milano* and the *Universität Bielefeld* during the preparation of this work.

AMS 1991 Subject Classification: 20G40, 20F05
Keywords: special linear group, root subgroups, (2,3)-generation.

of the groups of orders 2 and 3 and thus a group appears as a factor-group of $\mathrm{PSL}(2,\mathbf{Z})$ if and only if it is generated by an involution and an element of order 3. Such groups are often called (2,3)-*generated.*

The following quasisimple groups are known to be (2,3)-generated:

– The alternating groups A_n, $n \neq 6,7,8$ (this was proven by A.Miller in 1901, see references in [DiMT]);

– The projective special linear groups $\mathrm{PSL}(2,q)$, $q \neq 9$ ([Mb]);

– The projective special linear groups $\mathrm{PSL}(3,q)$, $q \neq 4$ ([Ga], [Co]);

– The special linear groups $\mathrm{SL}(n,q)$, $n \geq 25$ ([T1]);

– The Chevalley groups $\mathrm{G}_2(q)$ of type G_2 and the twisted groups ${}^2\mathrm{G}_2(q)$ ([Ma1], [Ma2]);

– The projective symplectic groups $\mathrm{PSp}(4,q)$, $q = p^m$, $p \neq 2,3$ ([CD]);

– The special linear groups $\mathrm{SL}(4,q)$, $q = p^m$, $p \neq 2$ ([TV]);

– The special linear groups $\mathrm{SL}(n,q)$, $n = 5,6,7$, $q = p^m$, $p \neq 2$, $q \neq 9$ ([DiMV]);

– The groups $\mathrm{PSp}(2n,q)$ and $\mathrm{PSU}(2n,q^2)$, $n \geq 37$, $q = p^m$, $p \neq 2$ ([TWG]);

– The groups $\mathrm{P}\,\Omega^+(2n,q)$, $n \geq 37$ ([TWG]);

– All sporadic simple groups apart from M_{11}, M_{22}, M_{23} and McL ([Wo]).

For some of the excluded cases, like, for example, for the alternating groups, the groups $\mathrm{PSL}(2,9)$, $\mathrm{PSL}(3,4)$ and $\mathrm{PSL}(4,2) \cong \mathrm{A}_8$ and the sporadics it is known that they are *not* (2,3)-generated, while most of the other exceptions are basically due to the methods used in the proofs of these results.

In this paper, which is a continuation of [DiMV], we carry on the analysis of the (2,3)-generation of the groups $\mathrm{SL}(n,q)$. The purpose of this part is to prove that the groups $\mathrm{SL}(n,q)$, $q = p^m$, are (2,3)-generated whenever $p \neq 2$, $q \neq 9$. These restrictions on the ground field arise due to the fact that – as in [DiMV] – our proof relies on Dickson's lemma and the classification of irreducible subgroups of $\mathrm{GL}(n,K)$ generated by root subgroups.

§1. Statement of results

In this section we state the main theorem and describe the strategy of its proof.

1°. Notation. Most of our notation is quite standard. For a primary number $q = p^m$ (where p is a rational prime and m a natural number) we denote by $\mathbf{F}_q$ the field of q elements. A generator of the cyclic group $\mathbf{F}_q^*$ will be called a *primitive element* of $\mathbf{F}_q$, while a generator of $\mathbf{F}_q$ as an algebra over $\mathbf{F}_p$ will be called a *field generator* or a *defining element of* $\mathbf{F}_q$ (see [LN]). We will write $\mathbf{F}_q = \mathbf{F}_p[\lambda]$ to denote that λ is a defining element of $\mathbf{F}_q$ and we will always assume that a defining element is non-zero if the field is prime.

Let G be any group. For two elements $x, y \in G$ we denote by $[x, y] = xyx^{-1}y^{-1}$ their commutator. We write $H \leq G$ when H is a subgroup of G (as opposed to $X \subseteq G$ when X is an arbitrary subset). For a subset $X \subseteq G$ we denote by $\langle X \rangle \leq G$ the subgroup of G generated by X and by $\langle X \rangle^G \trianglelefteq G$ the normal subgroup of G generated by X, i.e. the normal closure of $\langle X \rangle \leq G$ in G. For two subgroups F and H of G we write $F \sim_G H$ — or simply $F \sim H$ when the group G is clear from the context — to denote that F and H are conjugate in G. By $G \times H$ we denote the direct product of the groups G and H, while $G.H$ denotes some extension of G by H (the action of G on H will be clear from the context).

For any field K and any natural number n we denote by $\mathrm{GL}(n, K)$ and $\mathrm{SL}(n, K)$ the general and the special linear groups of degree n over K respectively ([HO'M] and [KL] are our general references for linear groups where one can find definitions of all the notions we use here and many further references). In particular, $K^* = \mathrm{GL}(1, K)$ is the group of non-zero elements of K. For the case $K = \mathbf{F}_q$ we use the shorthand $\mathrm{GL}(n, q)$ and $\mathrm{SL}(n, q)$.

By e_n — or simply by e if the order is clear from the context — we denote the identity matrix of order n. We will usually write simply 1 instead of e_1. For a fixed n and $1 \leq i, j \leq n$ we denote by e_{ij} the corresponding standard matrix unit, i.e. the matrix which has 1 in position (i, j) and zeros elsewhere. We denote by $a_1 \oplus \ldots \oplus a_t$ the *direct sum* of the matrices $a_1, \ldots, a_t$, i.e. the block matrix which has blocks $a_1, \ldots, a_t$ along the principal diagonal and zeros elsewhere. Sometimes $a_1 \oplus \ldots \oplus a_t$ is called the *diagonal sum* and denoted $\mathrm{diag}(a_1, \ldots, a_t)$.

We denote the matrix entry of a matrix x in position (i, j) by x_{ij}, so that $x = (x_{ij})$. The inverse of a matrix $x \in \mathrm{GL}(n, K)$ is denoted by $x^{-1} = (x'_{ij})$ and the transpose by x^t.

The groups $\mathrm{GL}(n, K)$ and $\mathrm{SL}(n, K)$ act on the left on the n-dimensional column space $V = K^n$. We denote by $v_1, \ldots, v_n$ the standard base of the space V, i.e. v_i is a column which has 1 as its i-th coordinate, while all other coordinates are zeros. The dual space $V^* = \mathrm{Hom}(V, K)$ is the n-dimensional row space, which will be denoted by ${}^nK$.

2^0. Main theorem. The purpose of this work is to prove the following result:

Theorem. *Let $\mathbf{F}_q$ be a finite field of characteristic not 2, $q \neq 9$ and*

$n \geq 2$. *Then the group* $\mathrm{SL}(n, q)$ *is* $(2, 3)$*-generated.*

For the degrees up to 7 this result is already known (see [Mb], [Co], [Ga], [DiMV], [TV]). Therefore we may – and will – assume that $n \geq 8$. As already mentioned in the Introduction, for $n \geq 25$ this result was proven by a different method by M.C.Tamburini [Ta] without any restrictions on q whatsoever. As was noted in [DiMV] the method of [Ta] can only be applied to *some* of the dimensions ≤ 24. Our proof in this paper is based on entirely different ideas and is independent of [Ta]. Although our treatment of small dimension (up to 11 inclusive) involves a considerable amount of case by case analysis, the method of proof itself is very uniform and does not depend of the dimension. In particular, we give another proof of the results of [Ta] under the restrictions $p \neq 2$, $q \neq 9$.

It is obvious that the theorem implies the following

Corollary. *Under the assumptions of Theorem the group* $\mathrm{SL}(n, K)$ *is generated by three conjugate involutions.*

It is known that all finite simple groups with the only exception of $\mathrm{PSU}(3, 3^2)$ are generated by three involutions (see [DiMT], [MSW] and [We]). It is however an open problem to classify the finite simple groups generated by three *conjugate* involutions.

3^0. About the proof. The proof in this paper closely follows the general plan proposed in [DiMV]. Namely we construct an involution x and a element y of order three such that:

i) Some power z^r of the commutator $z = [x, y]$ is a transvection (actually $r = 12$ in most cases and $r = 8, 24$ in a few exceptional ones);

ii) The conjugate $yz^r y^{-1}$ of this transvection by y is a transvection *opposite* to z^r;

iii) The group $G = \langle x, y\rangle$ is irreducible.

Then, by Proposition 2 of [DiMV], the normal closure $H = \langle z^r\rangle^G$ of z^r in G is irreducible, and contains a root subgroup by Dickson's lemma (provided some parameter related to the construction of x is a defining element of $\mathbf{F}_q$). Thus we can apply the classification of irreducible subgroups generated by root subgroups and conclude that either $G = \mathrm{SL}(n, \mathbf{F}_q)$, or possibly, $n = 2l$ is even, and up to conjugacy $\mathrm{Sp}(n, \mathbf{F}_q) \leq G \leq \mathrm{SGSp}(n, \mathbf{F}_q)$. So only the symplectic case remains to be excluded.

However in this second part there are two major innovations which simplify and shorten the proof considerably. One of them is the use of the transvection z^r to prove that G is irreducible (instead of considering the eigenspaces V^+ and V^- of x as we did in [DiMV]). Namely, let U be a

G-invariant subspace in V. We have the following alternative: either U contains the centre of z^r or U is contained in the axis of z^r. Using the explicit form of the generators and their transitivity on the standard base of V it is easy to show that $U = V$ in the first case and $U = 0$ in the second one.

The second innovation is that we can from the very start exclude the symplectic case using the fact that G actually contains *three* pair-wise opposite transvections, namely z^r, $yz^r y^{-1}$ and $y^{-1}z^r y$. To make use of this fact we develop in §3 some more 'geometry of transvections' (compare in this context [Coo], [Va2], [BH]). Namely we give a criterion – stated in terms of centres and axes – when the subgroup generated by three pair-wise opposite transvections contains two non-commuting root subgroups (angle $2\pi/3$). This criterion turns out to be satisfied by the transvections z^r, $yz^r y^{-1}$, $y^{-1}z^r y$, so that the symplectic case is ruled out. Indeed, due to the relative positions of long roots in a root system of type C_l any two distinct long root subgroups of the symplectic group are either orthogonal or opposite.

Our standing restrictions $p \neq 2$ and $q \neq 9$ have their explanation in the fact that we use Dickson's lemma to conclude that our group $G = \langle x, y \rangle$ contains a root subgroup. This breaks down irreparably in characteristic 2 since in this case a transvection is an involution and the group $\mathrm{SL}(2, K)$ only *very* seldom happens to be dihedral.

§2. Construction of the generators

In this section we explicitly construct the generators x and y.

1^0. Preliminary remarks. Here we describe the general strategy of constructing an involution $x = x_n$ and an element of order three $y = y_n$ which generate $\mathrm{SL}(n, K)$, $n \geq 5$. This construction follows the same idea as in [TW], [Ta], [Wi], [DiMV] (compare also [TWG]). Our generators will be constructed as diagonal sums of blocks of size ≤ 3. They tend to be close to monomial matrices: in fact x will differ from a monomial matrix only in one block of size 2, whereas y will be monomial in most cases (differing from a monomial matrix only in one block of size 2 for $n \equiv 2 (\mathrm{mod} 3)$, and exceptionally in two blocks of size two when $n = 10$).

Let π be any permutation. Denote by (π) the corresponding permutation matrix, i.e. a matrix, whose entry in the position (i, j) equals $\delta_{i,\pi(j)}$. For any field K the map $\pi \mapsto (\pi)$ is a monomorphism of the symmetric group S_n in the monomial group $N = N(n, K)$. The image of the long cycle $(1, \dots, n)$ under this map will be denoted by cox_n and called *Coxeter* *matrix*. Actually in this work we will only use it in the cases $n = 2, 3$. Here are the matrices cox_2 and cox_3:

$$\mathrm{cox}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathrm{cox}_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Many authors use the notation w_{12} and w_{123} for these matrices, which is convenient when you embed them in a group $\mathrm{GL}(n, K)$ of large degree on prescribed positions (say w_{ij} or w_{ijh}). But here we use them almost exclusively as summands of direct sums, so we stick to the notation cox_n.

Our involution x will be a direct sum of blocks of type ± 1 and cox_2 (the summands of the form -1 being introduced to make the determinant of the resulting matrix equal to 1) plus a single non-monomial block, namely:

$$\mathrm{fun}_2(t) = \begin{pmatrix} 1 & 0 \\ t & -1 \end{pmatrix},$$

which obviously is an involution.

In most cases our 3-element y will be a direct sum of blocks of type 1 and cox_3. However in dimensions congruent to 2 modulo 3 and in dimension 10 it is convenient to introduce a summand of a different shape, namely the matrix

$$\mathrm{fan}_2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},$$

which obviously has order 3 and determinant 1.

An obvious necessary condition for the group $G = \langle x, y \rangle$ to be irreducible is that it should not have proper invariant subspaces generated by the base vectors v_i. With this end in mind we will assemble the blocks cox_2 and cox_3 in such a way that the corresponding transpositions and 3-cycles act transitively on the set $\{1, \ldots, n\}$ of indices (or have one invariant point when fan_2 is present).

2^0. Construction in the general case. Here is the list of possible generators $x = x_n$ and $y = y_n$, where n refers to the degree of the matrices (when the degree is defined by the context we will usually write simply x and y). Apart from the three exceptional cases $n = 8, 10, 11$, the generators are in a sense 'periodic modulo 6'. In all cases the expression for x ends with the same matrix of degree 8, which we call the 'tail'. Namely:

$$\mathrm{tail} = (-1) \oplus \mathrm{cox}_2 \oplus 1 \oplus \mathrm{cox}_2 \oplus \mathrm{fun}_2(\mathrm{t}).$$

Since our proof of the irreducibility of the subgroup G generated by x and y exploits the action of the tail on columns and rows, we reproduce the matrix form of it for the reader's convenience:

$$\mathrm{tail} = \begin{pmatrix} -1 & . & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & 1 & . & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . \\ . & . & . & . & . & 1 & . & . \\ . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & t & -1 \end{pmatrix}.$$

Now, if $n = 3l$, $n \geq 9$, we set

$$x_n = 1 \oplus 1 \oplus \mathrm{cox}_2 \oplus \ldots \oplus 1 \oplus \mathrm{cox}_2 \oplus \epsilon \oplus \mathrm{cox}_2 \oplus \mathrm{tail},$$
$$y_n = \mathrm{cox}_3 \oplus \ldots \oplus \mathrm{cox}_3,$$

where $\epsilon = -1$ if l is even (i.e. if n is congruent to 0 modulo 6) and $\epsilon = 1$ if l is odd (i.e. if n is congruent to 3 modulo 6). For $n = 9$ this has to be understood as $x_9 = 1 \oplus \mathrm{tail}$, and when ε appears in later computations, it has to be taken $= 1$.

If $n = 3l + 1$, $n \geq 13$, we set

$$x_n = \mathrm{cox}_2 \oplus 1 \oplus \mathrm{cox}_2 \oplus \ldots \oplus 1 \oplus \mathrm{cox}_2 \oplus \epsilon \oplus \mathrm{cox}_2 \oplus \mathrm{tail},$$
$$y_n = 1 \oplus \mathrm{cox}_3 \oplus \ldots \oplus \mathrm{cox}_3,$$

where $\epsilon = -1$ if l is odd (i.e. if n is congruent to 4 modulo 6) and $\epsilon = 1$ if l is even (i.e. n is congruent to 1 modulo 6).

Finally, if $n = 3l + 2$, $n \geq 14$ we set

$$x_n = (-1) \oplus \mathrm{cox}_2 \oplus \ldots \oplus (-1) \oplus \mathrm{cox}_2 \oplus \mathrm{tail},$$
$$y_n = \mathrm{fan}_2 \oplus \mathrm{cox}_3 \oplus \ldots \oplus \mathrm{cox}_3.$$

(Here, when ε appears in later computations it has to be taken $= -1$). In this last case the choice of generators differs slightly from the one we announced in [DiMV], since y is *not* monomial, but it is better in the following respect: in contrast to the other cases it does not depend on the residue class of n modulo 6 and it leads to essentially the same transvection as in the other cases. This makes uniform and substantially shortens the analysis of the irreducibility of the subgroup G generated by x and y.

The proposed x and y do in fact generate the whole group $\mathrm{SL}(n, q)$ only if the parameter t fails to satisfy some polynomial equations and the value of another polynomial in t is a defining element of $\mathbf{F}_q$ (for the excluded values of t these elements may generate a proper subgroup of $\mathrm{SL}(n,q)$, say, a reducible one). Of course, when y is monomial or the field is not prime, we *must* take $t \neq 0$. Moreover, the restriction $t \neq 0$ is crucial in getting the desired transvection in G. So we generally assume $t \neq 0$. Here are the other conditions on t in the general case:

$$t^3 \neq -1, -9, \qquad \mathbf{F}_q = \mathbf{F}_p[t^3].$$

As we shall see in § 6 for all finite fields of characteristic not 2 it is always possible to find an element t satisfying these conditions.

3^0. Generators in the exceptional cases. It remains to exhibit the generators for the cases $n = 8, 10, 11$. Namely, for $n = 8$ we take as x_8 the usual tail and

$$y_8 = \mathrm{fan}_2{}^{-1} \oplus \mathrm{cox}_3 \oplus \mathrm{cox}_3.$$

Thus, y_8 slightly differs from the usual y for n congruent to 2 modulo 3. This change is necessary in order to get the same transvection as in the other cases. For the reader's convenience we reproduce the matrix form of y_8:

$$y_8 = \begin{pmatrix} -1 & -1 & . & . & . & . & . & . \\ 1 & . & . & . & . & . & . & . \\ . & . & . & . & 1 & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . \\ . & . & . & . & . & . & . & 1 \\ . & . & . & . & . & 1 & . & . \\ . & . & . & . & . & . & 1 & . \end{pmatrix}.$$

These x and y generate $\mathrm{SL}(8,q)$ if t is subject to the following conditions:

$$t \neq 0, 1, \quad t^3 \neq -1, \quad t^2 - 2t + 2 \neq 0, \quad t^3 \neq 8$$
$$t^3 + t^2 + 2t + 4 \neq 0, \quad 3t + 5 \neq 0, \qquad \mathbf{F}_q = \mathbf{F}_p[t^3].$$

The generators for $n = 10$ are as follows:

$$x_{10} = -1 \oplus \mathrm{cox}_2 \oplus \mathrm{cox}_2 \oplus -1 \oplus \mathrm{cox}_2 \oplus \mathrm{fun}_2(\mathrm{t}),$$
$$y_{10} = \mathrm{fan}_2 \oplus \mathrm{fan}_2 \oplus \mathrm{cox}_3 \oplus \mathrm{cox}_3,$$

or, in matrix form

$$x_{10} = \begin{pmatrix} -1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & t & -1 \end{pmatrix},$$

$$y_{10} = \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -1 & -1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & -1 & -1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix}.$$

This choice of generators leads to essentially the same transvection as in the case $n = 7$ considered in [DiMV]. The conditions on t which ensure that these x and y generate $\mathrm{SL}(10, q)$ are as follows:

$$t \neq 0, \pm 1, 2, \quad t^3 \neq -8, \quad 2t^3 - t^2 - 4 \neq 0, \quad t^2 + 3t + 4 \neq 0,$$
$$9t^4 - 6t^2 + 12t - 8 \neq 0, \qquad \mathbf{F}_q = \mathbf{F}_p[t^4 - 2t^3].$$

Finally for $n = 11$ we take

$$x_{11} = (-e_2) \oplus \mathrm{cox}_2 \oplus \mathrm{cox}_2 \oplus 1 \oplus \mathrm{cox}_2 \oplus \mathrm{fun}_2(\mathrm{t}),$$
$$y_{11} = \mathrm{cox}_3 \oplus \mathrm{fan}_2 \oplus \mathrm{cox}_3 \oplus \mathrm{cox}_3.$$

or, in matrix form,

$$
x_{11} = \begin{pmatrix}
-1 & . & . & . & . & . & . & . & . & . & . \\
. & -1 & . & . & . & . & . & . & . & . & . \\
. & . & . & 1 & . & . & . & . & . & . & . \\
. & . & 1 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & 1 & . & . & . & . & . \\
. & . & . & . & 1 & . & . & . & . & . & . \\
. & . & . & . & . & . & 1 & . & . & . & . \\
. & . & . & . & . & . & . & . & 1 & . & . \\
. & . & . & . & . & . & . & 1 & . & . & . \\
. & . & . & . & . & . & . & . & . & 1 & . \\
. & . & . & . & . & . & . & . & . & t & -1
\end{pmatrix},
$$

$$
y_{11} = \begin{pmatrix}
. & . & 1 & . & . & . & . & . & . & . & . \\
1 & . & . & . & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 1 & . & . & . & . & . & . \\
. & . & . & -1 & -1 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & 1 & . & . & . \\
. & . & . & . & . & 1 & . & . & . & . & . \\
. & . & . & . & . & . & 1 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 1 \\
. & . & . & . & . & . & . & . & 1 & . & . \\
. & . & . & . & . & . & . & . & . & 1 & .
\end{pmatrix}.
$$

This choice of generators leads to essentially the same transvection as in the cases $n = 13, 16$, but with some permutation of columns and rows. The conditions on t under which x and y generate $\mathrm{SL}(11, q)$ are as follows:

$$
\begin{aligned}
&t \neq 0, -1, \quad t^2 - 2t + 2 \neq 0, \quad t^3 + t^2 + 2t + 4 \neq 0, \\
&t^3 \neq 8, \quad 3t + 5 \neq 0, \quad \mathbf{F}_q = \mathbf{F}_p[t^6].
\end{aligned}
$$

It is not true in general that in these exceptional cases such a t always exists. As a result we have to slightly modify the generators for some very small values of q, like, for example, $q = 3, 5$ or 7.

§3. Groups generated by three opposite transvections

To avoid the analysis of G-invariant symplectic forms we develop in this section some more 'geometry of transvections'. Throughout the section we assume $\mathrm{char} K \neq 2$ and $K \neq \mathbf{F}_9$.

Let z_1, z_2, z_3 be three transvections in $\mathrm{SL}(n, K)$ with corresponding centres c_1, c_2, c_3 and axes a_1, a_2, a_3 and let $G = \langle z_1, z_2, z_3 \rangle$. We are only interested in the case when z_1, z_2, z_3 are *pair-wise opposite*, i.e. when every pair (z_i, z_j), $i \neq j$, can be brought to a pair $(t_{12}(\xi), t_{21}(\zeta))$, $\xi, \zeta \in K$, by simultaneous conjugation. By Lemma 10 of [DiMV] we know that this is equivalent to saying that $a_i c_j \neq 0$ for all $i \neq j$.

In all cases which actually arise we can ensure that moreover $\xi\zeta$ is a *defining element* of $K = \mathbf{F}_q$. Then Dickson's lemma implies that G contains the whole group $\langle X_1, X_2, X_3 \rangle$, where

$$X_i = \{e + c_i \eta a_i \mid \eta \in K\}$$

is the one-parameter subgroup of transvections with axis a_i and centre c_i, $i = 1, 2, 3$. By our assumption such groups X_i are pair-wise opposite.

The possibilities for groups generated by three (long) root subgroups two of which are opposite are well-known. The classification of such groups was one of the main tools in Cooperstein's "geometry of the long root subgroups" [Coo]. We note explicitely that starting from this point up to the end of the section the field K may be arbitrary (not necessarily finite), and we state here a result which (for finite fields) can be relatively easily derived from the results of [Coo]. The group Y appearing in this lemma is defined as follows:

$$Y = \left\{ \begin{pmatrix} 1 & a & b & c \\ . & 1 & . & b \\ . & . & 1 & -a \\ . & . & . & 1 \end{pmatrix}, \quad a, b, c \in K \right\}.$$

This is precisely the unipotent radical of the standard parabolic subgroup P_1 in the symplectic group $\mathrm{Sp}(4, K)$. The action of $\mathrm{SL}(2, K)$ on Y is induced by the action of the Levi subgroup of P_1.

Lemma 1. *Let $G = \langle X_1, X_2, X_3 \rangle$, where X_1, X_2, X_3 are root subgroups in $\mathrm{SL}(n, K)$ such that X_1, X_2 are opposite. Then one of the following holds:*

i) $G \cong \mathrm{SL}(2, K)$,

ii) $G \cong \mathrm{SL}(2, K) \times K$,

iii) $G \cong \mathrm{SL}(2, K).K^2$,

iv) $G \cong (\mathrm{SL}(2, K).K^2) \times K$,

v) $G \cong \mathrm{SL}(2, K).Y$,

vi) $G \cong \mathrm{SL}(3, K)$.

However, since it is not at all easy to pin-point a place in [Coo] where the result is stated in this form, we prefer to give an independent elementary proof. The following lemma is a particular case of a result from [Va2]. Compare also [Va1], [Se], where an analogous reduction appears for an essentially equivalent problem of calculating the Bruhat decomposition of semisimple root elements in $\mathrm{SL}(n, K)$.

Lemma 2. *Let X_1, X_2, X_3 be three root subgroups of $\mathrm{SL}(n, K)$, $n \geq 5$, such that X_1 and X_2 are opposite. Then there exists $g \in \mathrm{SL}(n, K)$ such that $gX_1g^{-1}, gX_2g^{-1}, gX_3g^{-1} \leq Q$, where Q is the subgroup of degree 4 generated by X_{ij}, $1 \leq i \neq j \leq 4$, isomorphic to $\mathrm{SL}(4, K)$.*

Proof. Without loss of generality we may assume $X_1 = X_{1n}$ and $X_2 = X_{n1}$. Then X_3 has the form $X_{ca} = \{x_{ca}(\xi) = e + c\xi a \mid \xi \in K\}$ with corresponding axis $a = (a_1, \dots, a_n) \in {}^nK$ and centre $c = (c_1, \dots, c_n)^t \in K^n$. We first conjugate X_3 by a suitable matrix from the subgroup $G_1 \cong \mathrm{SL}(n-2, K)$ generated by X_{ij}, $2 \leq i \neq j \leq n-1$. Let $c' = (c_2, \dots, c_{n-1})^t$. Since the group $\mathrm{SL}(n-2, K)$ is transitive on non-zero vectors of K^{n-2}, either $c' = 0$, or there exists $g_1 \in G_1$ such that $g_1c' = (1, 0, \dots, 0)^t$. Let $X_3' = g_1X_3g_1^{-1}$. Now we conjugate X_3' by a suitable matrix from the subgroup $G_2 \cong \mathrm{SL}(n-3, K)$, generated by X_{ij}, $3 \leq i \neq j \leq n-1$. Namely, let $a' = (a_2, \dots, a_{n-1})g_1^{-1} = (a_2', \dots, a_{n-1}')$. Then as above, either $(a_3', \dots, a_{n-1}') = 0$ or there exists $g_2 \in G_2$ such that $(a_3', \dots, a_{n-1}')g_2^{-1} = (1, 0 \dots, 0)$. If we set $g = g_2g_1$, then clearly $gX_1g^{-1} = X_1$, $gX_2g^{-1} = X_2$, while gX_3g^{-1} is contained in the subgroup $G_3 \cong \mathrm{SL}(4, K)$ generated by X_{ij}, where $i, j = 1, 2, 3, n$, $i \neq j$. It remains only to conjugate this group by a permutation matrix.

In fact in [Va2] a much more general result is observed, namely that for *any* field K three long root subgroups in a Chevalley group two of which are opposite are contained up to conjugacy in a subgroup corresponding to a (possibly twisted) subsystem of the root system of type D_4.

It follows from the above lemma, that it is sufficient to prove Lemma 1 only for the case when $n = 4$.

Proof of Lemma 1. Without loss of generality we may assume $n = 4$ and $X_1 = X_{14}$, $X_2 = X_{41}$. Then $X_3 = X_{ca}$ with $c = (c_1, c_2, c_3, c_4)^t$ and $a = (a_1, a_2, a_3, a_4)$. Denote by F the normalizer of the subgroup generated by X_{14} and X_{41}.

Let first $c_1 \neq 0$. Then conjugating X_3 by the matrix $g_1 = t_{41}(-c_4/c_1)$ belonging to F we may assume $c_4 = 0$. More precisely in this case $c =$

$(c_1, c_2, c_3, 0)^t$, while $a = (a_1 + a_4c_4/c_1, a_2, a_3, a_4)$.

Now let $c_2 \neq 0$. Then conjugating $g_1X_3g_1^{-1}$ by the matrix $g_2 = t_{32}(-c_3/c_2)$ belonging to F we may assume $c_3 = 0$. More precisely, in this case $c = (c_1, c_2, 0, 0)^t$, while $a = (a_1 + a_4c_4/c_1, a_2 + a_3c_3/c_2, a_3, a_4)$.

Thus we can, without loss of generality, assume that at least one of the elements of each of the pairs (c_1, c_4) and (c_2, c_3) is zero. By symmetry reasons we may even assume $c_3 = c_4 = 0$.

First assume $c_1 = 0$. Then since $c \neq 0$ and $ac = a_1c_1 + a_2c_2 = 0$, it follows $c_2 \neq 0$, $a_2 = 0$. Thus we may assume that

$$X_3 = \{t_{21}(\xi a_1)t_{23}(\xi a_3)t_{24}(\xi a_4) \mid \xi \in K\}.$$

If $a_1 = a_4 = 0$ we fall into case ii). Assume a_1 and a_4 are not both zeros. Then, if $a_3 = 0$, we fall into case iii); if $a_3 \neq 0$ we fall into case iv).

Now assume $c_1 \neq 0$. If $a_1 \neq 0$, then necessarily a_2 and c_2 are different from 0. Conjugating X_3 by the matrix $g = t_{14}(a_4/a_1) \cdot t_{23}(a_3/a_2) \in F$ we may assume without loss of generality that $a_3 = a_4 = 0$. Then it is easily seen (by taking the commutators of X_3 with X_1 and X_2) that we are in the case vi).

It remains to consider the case $a_1 = 0$. In this case either $a_2 = 0$, or $c_2 = 0$ (or both). If $c_2 = 0$ and $a_2 = a_3 = 0$, we fall into case i). If $c_2 = 0$ and a_2 or a_3 is distinct from 0, we fall into case iii).

If $c_2 \neq 0$, then necessarily $a_2 = 0$. If moreover $a_3 = 0$, we fall into case iii). If $a_3 \neq 0$ and $a_4 = 0$ we fall into case iv). Finally if $a_3, a_4 \neq 0$, we fall into the case v). The lemma is completely proven.

Remark. Calculating in $\mathrm{SO}(8, K)$ instead of $\mathrm{SL}(4, K)$ we could in the same manner prove an analogue of Lemma 1 for all Chevalley groups. Of course in the general case two further possibilities for G arise, namely $\mathrm{SU}(3, L)$, $[L : K] = 2$, and an analogue of the group of type iv) based on v) instead of iii). This proof applies to arbitrary fields and is considerably shorter than the geometric proof from [Coo].

The groups of types ii) and iv) cannot be generated by three pair-wise opposite transvections, so these cases may be excluded from the very start. In these cases there are two commuting root subgroups (recall that in the terminology of [DiMV] *'commuting'* means commuting *and* not orthogonal), so that the corresponding groups are in any case not contained in the symplectic group.

Set $l = \dim\langle a_1, a_2, a_3\rangle$ and $m = \dim\langle c_1, c_2, c_3\rangle$. In fact, we will have to deal only with the case when $l = m = 3$. Since clearly l and m are not changed by a simultaneous conjugation, we can rule out cases i) and iii).

Indeed, in case i) one has $l = 2$ and $m = 2$, while in case iii) one has $l = 2$, $m = 3$, or $l = 3$, $m = 2$. In case iii) two non-conjugate classes of subgroups appear, with shapes

$$\begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ * & * & 1 \end{pmatrix}.$$

This shows also that there are two non-conjugate classes of subgroups of type iv) with representatives of shape

$$\begin{pmatrix} 1 & 0 & 0 & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & * & 0 \\ 0 & * & * & 0 \\ * & * & * & 1 \end{pmatrix}.$$

respectively.

On the other side in cases v) and vi) one has $l = m = 3$. We need a more delicate criterion to distinguish these cases. Such a criterion is provided by a certain bootstrip invariant.

Lemma 3. *Let X_1, X_2, X_3 be three pair-wise opposite root subgroups of $SL(n, K)$ with corresponding centres c_1, c_2, c_3 and axes a_1, a_2, a_3. Suppose that* $\dim\langle a_1, a_2, a_3\rangle = \dim\langle c_1, c_2, c_3\rangle = 3$. *If*

$$(a_1c_3)(a_2c_1)(a_3c_2) + (a_1c_2)(a_2c_3)(a_3c_1) \neq 0,$$

then $\langle X_1, X_2, X_3\rangle \cong \mathrm{SL}(3, K)$.

Proof. Clearly it suffices to show that the group $G = \langle X_1, X_2, X_3\rangle$ contains two non-commuting root subgroups (recall that by the convention of [DiMV] *'non-commuting'* means non-commuting *and* not opposite).

Every root subgroup X in the group $\langle X_1, X_2\rangle \cong \mathrm{SL}(2, K)$ generated by X_1, X_2 has axis of the form $a = \alpha a_1 + \beta a_2$, $\alpha, \beta \in K$. In order for this subgroup X not to be opposite to X_3 it suffices to have $ac_3 = (\alpha a_1 + \beta a_2)c_3 = 0$. Clearly one may take $\alpha = a_2c_3 \neq 0$, $\beta = -a_1c_3 \neq 0$.

Now look at the centre of X in the form $c = \gamma c_1 + \delta c_2$, $\gamma, \delta \in K$. The centre lies on the axis, so we must have $ac = \delta(a_2c_3)(a_1c_2) - \gamma(a_1c_3)(a_2c_1) = 0$. To satisfy this condition we may take $\gamma = (a_2c_3)(a_1c_2) \neq 0$ and $\delta = (a_1c_3)(a_2c_1) \neq 0$. But now, by assumption

$$a_3c = (a_1c_3)(a_2c_1)(a_3c_2) + (a_1c_2)(a_2c_3)(a_3c_1) \neq 0,$$

so that X and X_3 do not commute.

§4. Transvections in G

In this section we show that the group G generated by x and y above always contains two opposite transvections – and thus by Dickson's lemma (see [DiMV] for details) it contains a whole root subgroup.

1^0. Evidence for the general case. First let $n \neq 8, 10, 11$. A direct check with 'Mathematica' which we carried through for $n = 9, 12, 14, 15$ and $17 \leq n \leq 28$ shows that the twelth power of the commutator $z = [x, y]$ is a transvection of the following shape:

$$z^{12} = e_{n-7} \oplus \text{coda},$$

where 'coda' is a certain transvection of degree 7:

$$\text{coda} = \begin{pmatrix} 1 & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . \\ . & . & 1 & . & . & . & . \\ 2t^2 & 2t^2 & . & 1 & . & -2t^2 & . \\ -2t^2 & -2t^2 & . & . & 1 & 2t^2 & . \\ . & . & . & . & . & 1 & . \\ -4t & -4t & . & . & . & 4t & 1 \end{pmatrix}.$$

In other words for $n \geq 9$, $n \neq 10, 11, 13, 16$ the power z^{12} is *always* the transvection $e + vu$, where

$$a = (0, \ldots, 0, 1, 1, 0, 0, 0, -1, 0),$$
$$c = (0, \ldots, 0, 2t^2, 2t^2, 0, -4t)^t.$$

Now the transvections $yz^{12}y^{-1}$ and $y^{-1}z^{12}y$ conjugated to z^{12} by y and y^{-1} have the following axis and centres respectively:

$$a' = ay^{-1} = (0, \ldots, 0, 1, 0, 0, 0, 1, 0, 0, 0, -1),$$
$$c' = yc = (0, \ldots, 0, 2t^2, 0, 0, -4t, -2t^2, 0)^t;$$
$$a'' = ay = (0, \ldots, 0, 1, 0, 0, 0, 1, -1, 0, 0),$$
$$c'' = y^{-1}c = (0, \ldots, 0, 2t^2, 0, 0, -4t, 2t^2)^t.$$

A direct calculation shows that $ac' = 4t^2$ and $a'c = 4t$. Thus by Lemma 10 from [DiMV] the transvections z^{12} and $yz^{12}y^{-1}$ are opposite. If, moreover, $16t^3$ is a defining element of $\mathbf{F}_q$, then the subgroup generated by these two transvections contains a root subgroup by Dickson's lemma (see [DiMV], Lemmas 3 and 11). By symmetry $a'c'' = a''c = 4t^2$ and $a''c' = ac'' = 4t$, and the same applies to the pairs $yz^{12}y^{-1}$ and $y^{-1}z^{12}y$, $y^{-1}z^{12}y$ and z^{12}. Thus if t^3 is a defining element of $\mathbf{F}_q$ we may assume G contains the root subgroups X_1, X_2, X_3 with corresponding axes a_1, a_2, a_3 and centres c_1, c_2, c_3. It is obvious that when $t \neq 0$ one has $\dim\langle a_1, a_2, a_3\rangle = \dim\langle c_1, c_2, c_3\rangle = 3$. Now look at the criterion stated in Lemma 3: it asserts that if $(ac')(a'c'')(a''c) + (ac'')(a'c)(a''c') \neq 0$ then the subgroup generated by X_1, X_2, X_3 is isomorphic to $\mathrm{SL}(3, K)$. But this last condition amounts to $t^3 \neq -1$. This means that if the transvection z^{12} has the form described above, then whenever $t \neq 0$, $t^3 \neq -1$ and t^3 is a defining element of $\mathbf{F}_q$ we may assume that $\langle X_1, X_2, X_3\rangle$ is isomorphic to $\mathrm{SL}(3, K)$.

A direct check with 'Mathematica' shows that for the degrees $n = 13, 16$ excluded above the 24-th power of the commutator z is the *square* of the transvection above, i.e. the transvection $e + v2u$ for the same u, v as above, or, in other words, the direct sum of e_{n-7} and coda^2. This means that the conclusions of the previous paragraph still hold in these two cases.

In the next subsection we show that for large values of n the twelth power of the commutator z *always* equals $e_{n-7} \oplus \mathrm{coda}$. It is actually *very* convenient for the rest of the proof that the tail of the transvection does not change.

2^0. Proof for the general case. Here we analyse the action of z on V and prove the following result:

Lemma 4. *Let $n \geq 17$. Then $z^{12} = e_{n-7} \oplus \mathrm{coda}$.*

Proof. We consider the action of x and of $x' = yxy^{-1}$ on the standard base of V. Since in all cases x and y have the same tails of degree 10, the conjugates x' always have the same tail of degree 9 as shown below:

$$\mathrm{tail}' = \begin{pmatrix} . & . & . & . & 1 & . & . & . & . \\ . & . & . & . & . & . & . & . & . \\ . & . & -1 & . & . & . & . & . & . \\ . & . & . & . & . & . & . & 1 & . \\ 1 & . & . & . & . & . & . & . & . \\ . & . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & . & -1 & . & t \\ . & . & . & 1 & . & . & . & . & . \\ . & . & . & . & . & . & . & . & 1 \end{pmatrix},$$

the other entries in the columns and rows of x' with indices $\geq n-6$ being zeros.

Clearly the subspace $U = \langle e_{n-6}, e_{n-5}, e_{n-3}, e_{n-2}, e_{n-1}, e_n \rangle$ is invariant under the action of both x and x'. Moreover, the restrictions of x and x' to U – and, consequently, the action of $z = xx'$ on U – are always the same. As we know by direct computation in small dimensions, the 12-th power of the restriction of xx' to U is the transvection obtained from 'coda' by throwing out the third row and the third column.

Now we look at what happens to the other elements of the standard base under the action of x and x'. Since our generators are constructed according to the residue class of n modulo 3, we have to distinguish three cases.

Let first $n \equiv 0 \pmod 3$. Then x transposes v_i and v_{i+1} for $i \equiv 0 \pmod 3$ and possibly changes signs of v_i for $i \equiv 2 \pmod 3$. On the other side x' transposes v_i and v_{i+4} for $i \equiv 1 \pmod 3$ and possibly changes signs of v_i for $i \equiv 0 \pmod 3$. This shows that $z = xx'$ leaves invariant the following subspaces: $\langle v_2 \rangle$, $\langle v_1, v_5 \rangle$, $\langle v_3, v_4, v_8 \rangle$, $\langle v_6, v_7, v_{11} \rangle$, $\ldots$, $\langle v_{n-9}, v_{n-8}, v_{n-4} \rangle$. Clearly the order of the restriction of z to the first two subspaces divides 4. On each of the remaining subspaces it induces a product of two transpositions of base vectors with a possible change of signs. Such a product has order dividing 6. Thus the restriction of z to the subspace W generated by all v_i, $i \neq n-6, n-5, n-3, n-2, n-1, n$ has order dividing 12. This proves the lemma in this case.

Now let $n \equiv 1 \pmod 3$. Then x transposes v_i and v_{i+1} for $i \equiv 1 \pmod 3$ and possibly changes signs of v_i for $i \equiv 0 \pmod 3$. On the other side x' transposes v_1 and v_3, v_i and v_{i+4} for $i \equiv 2 \pmod 3$ and possibly changes signs of v_i for $i \equiv 1 \pmod 3$, $i \geq 4$. This shows that $z = xx'$ leaves invariant the following subspaces: $\langle v_1, v_2, v_3, v_6 \rangle$, $\langle v_4, v_5, v_9 \rangle$, $\langle v_7, v_8, v_{12} \rangle$, $\ldots$, $\langle v_{n-9}, v_{n-8}, v_{n-4} \rangle$. As before, on all these subspaces except the first one z induces a product of two transpositions of base vectors with a possible change of signs which has order dividing 6. On the other side on the first subspace it induces a 4-cycle with a possible change of sign. This change of sign actually appears when $x_{66} = -1$. But when $n \geq 19$ we have $x_{66} = 1$ so that z induces on $\langle v_1, v_2, v_3, v_6 \rangle$ an element conjugated to cox_4 which has order 4, and thus again the restriction of z to the subspace W has order dividing 12, which proves the lemma in this case. On the other side in the excluded cases $n = 13, 16$ one has $x_{66} = -1$ and thus z induces on the first subspace a transformation conjugated to $-e_{14} + e_{21} + e_{32} + e_{34}$, which has order 8, so that the restriction of z to W has order dividing 24.

Let, finally, $n \equiv 2 \pmod 3$. The action of x is as before, namely x transposes v_i and v_{i+1} for $i \equiv 2 \pmod 3$ and changes *all* signs of the remaining base vectors v_i, $i \equiv 1 \pmod 3$. The action of x', however, is somewhat more complicated than in the other cases, since it induces a nonmonomial transformation on the subspace generated by v_1, v_2, v_4, permutes v_i and v_{i+4} for $i \equiv 0 (\mathrm{mod}\, 3)$ and changes signs of all v_i, $i \equiv 2 (\mathrm{mod}\, 3)$. This shows that $z = xx'$ leaves invariant the following subspaces: $\langle v_1, v_2, v_3, v_4, v_7 \rangle$, $\langle v_5, v_6, v_{10} \rangle$, $\langle v_8, v_9, v_{13} \rangle$, $\ldots$, $\langle v_{n-9}, v_{n-8}, v_{n-4} \rangle$. As before on all these subspaces except the first one z induces a product of two transpositions of base vectors with a possible change of signs, which has order dividing 6. On the other hand, on the first subspace z induces the same transformation for all degrees n such that $7 < n - 6$ (i.e. $n \geq 14$). But by direct computation for small degrees we know that the order of this transformation also divides 12. Thus the lemma is completely proven.

Together with the observations made in section 1^o this lemma means that for all degrees except $8, 10, 11$ we have established that the subgroup G generated by x and y contains a root subgroup. In the next subsection we deal with the remaining cases.

3^0. Exceptional cases. Here we describe how the transvection z^r and its conjugates look for the exceptional cases $n = 8, 10, 11$. All these results were obtained using 'Mathematica'.

First, let $n = 8$. Again a direct calculation shows that the 12-th power of the commutator $z = [x, y]$ is the usual transvection $1 \oplus$ coda. The tail of y is different from that for the general case, but a direct calculation shows that this *does not* influence the products $ac', \ldots, a''c$, so that as for the general case the transvections z^{12}, $yz^{12}y^{-1}$ and $y^{-1}z^{12}y$ generate the whole group $\mathrm{SL}(3, K)$ if $t \neq 0$, $t^3 \neq -1$ and t^3 is a defining element of $\mathbf{F}_q$.

Now, let $n = 10$. Then the 8-th power of the commutator z^8 is the following transvection, which very much resembles the transvection for the case $n = 7$:

$$z^8 = \begin{pmatrix} 1 & . & . & . & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . & . & . \\ . & . & . & . & 1 & . & . & . & . & . \\ . & . & . & . & . & 1 & . & . & . & . \\ 2t^2 & . & . & -2t^2 & 2t^2 & 2t^2 & 1 & . & 2t^2 & -4t \\ 2t^2 & . & . & -2t^2 & 2t^2 & 2t^2 & . & 1 & 2t^2 & -4t \\ . & . & . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & . & . & . & 1 \end{pmatrix}.$$

In other words z^8 is the transvection with axis and centre

$$a = (2t^2, 0, 0, -2t^2, 2t^2, 2t^2, 0, 0, 2t^2, -4t),$$

$$c = (0,0,0,0,0,0,1,1,0,0)^t.$$

A direct calculation shows that the conjugates of z^8 are the transvections with corresponding axes and centres:

$$\begin{aligned}
a' &= ay^{-1} = (-2t^2, -2t^2, -2t^2, 0, 0, 2t^2, 2t^2, -4t, 0, 2t^2),\\
c' &= yc = (0,0,0,0,1,0,0,0,1,0)^t;\\
a'' &= ay = (0, 2t^2, 2t^2, 2t^2, 2t^2, 0, 2t^2, 2t^2, -4t, 0),\\
c'' &= y^{-1}c = (0,0,0,0,0,0,1,0,0,0,1)^t.
\end{aligned}$$

Then $ac' = a'c'' = a''c = 4t^2$ and $ac'' = a'c = a''c' = 2t^2 - 4t$, so that the transvections z^{24}, $yz^{24}y^{-1}$ and $y^{-1}z^{24}y$ are pair-wise opposite whenever $t \neq 0, 2$. If moreover $8t^4 - 16t^3$ is a defining element of the field $\mathbf{F}_q$, then any pair of these transvections generates $\mathrm{SL}(2, K)$ by Dickson's lemma. Finally, if $9t^4 - 6t^2 + 12t - 8 \neq 0$, these three transvections generate $\mathrm{SL}(3, K)$ by Lemma 2.

Finally, let $n = 11$. In this case a direct calculation shows that z^{24} is the following transvection (essentially the same as for dimensions $n = 13, 16$, apart from some permutation of rows and columns):

$$z^{24} = \begin{pmatrix}
1 & . & . & . & . & . & . & . & . & . & .\\
. & 1 & . & . & . & . & . & . & . & . & .\\
. & . & 1 & . & . & . & . & . & . & . & .\\
. & . & . & 1 & . & . & . & . & . & . & .\\
. & . & . & . & 1 & . & . & . & . & . & .\\
. & . & . & . & . & 1 & . & . & . & . & .\\
. & . & . & . & . & . & 1 & . & . & . & .\\
. & . & -4t^2 & -4t^2 & . & . & 4t^2 & 1 & . & . & .\\
. & . & 4t^2 & 4t^2 & . & . & -4t^2 & . & 1 & . & .\\
. & . & . & . & . & . & . & . & . & 1 & .\\
. & . & 8t & 8t & . & . & -8t & . & . & . & 1
\end{pmatrix}.$$

In other words z^{24} has axis and centre

$$\begin{aligned}
a &= (0,0,1,1,0,0,-1,0,0,0,0),\\
c &= (0,0,0,0,0,0,0,-4t^2, 4t^2, 0, 8t)^t.
\end{aligned}$$

A direct calculation shows that the conjugates of z^{24} are the transvections with corresponding axes and centres:

$$a' = ay^{-1} = (1,0,0,-1,-1,0,0,-1,0,0,0),$$

$$c' = yc = (0,0,0,0,0,-4t^2,0,0,8t,4t^2,0)^t;$$

$$a'' = ay = (0,1,0,0,1,-1,0,0,0,0,0),$$

$$c'' = y^{-1}c = (0,0,0,0,0,0,-4t^2,0,0,8t,4t^2)^t.$$

It is clear that $ac' = a'c'' = a''c = 0$ so that the transvections z^{24}, $yz^{24}y^{-1}$ and $y^{-1}z^{24}y$ are *not* opposite. On the other side $a'c = a''c' = ac'' = 4t^2$ so that when $t \neq 0$, these transvections form mutual angles $2\pi/3$. Now

$$f = [yz^{24}y^{-1}, z^{24}] = e + c'4t^2a = x_{c'a}(4t^2)$$

is a transvection with centre c' and axis a, so that it is opposite to $y^{-1}z^{24}y$. By Dickson's lemma f and $y^{-1}z^{24}y$ generate $\mathrm{SL}(2,K)$ if $64t^6$ is a defining element of the field $\mathbf{F}_q$. Then clearly z^{24}, $yz^{24}y^{-1}$ and $y^{-1}z^{24}y$ generate the whole group $\mathrm{SL}(3,K)$. So the only restrictions in this case are that $t \neq 0$ and t^6 is a defining element of $\mathbf{F}_q$.

§5. Irreducibility

In this section we prove that the subgroup G generated by x and y acts irreducibly on the vector space $V \equiv K^n$. As we know from Proposition 2 of [DiMV], this implies that the normal closure $H = \langle z^r \rangle^G$ of the transvection z^r exhibited in the previous section is irreducible.

1^0. The general case. In this subsection we assume $n \neq 8, 10, 11$. Namely, let U be a G-invariant subspace. Let g be the usual transvection contained in G, described in § 4 with axis a and centre c. If there exists a vector $u \in U$ which does not lie on the axis of the transvection, i.e. is such that $au \neq 0$, then we may conclude that $c \in U$. Since $t \neq 0$ we may even assume that

$$c = (0,\dots,0,t,-t,0,-2)^t \in U.$$

Then a direct calculation shows that

$$d = (yxy^2xy + xy + y)c = (0,\dots,0,-4,-2-t^3,-2t,-2t^2)^t \in U$$

Taking the projection of this vector in V^- we get

$$(x-e)d = (0,\dots,0,2-t^3,-2+t^3,0,2t^2)^t \in U.$$

It remains to observe that since $4 \neq 0$, this vector is *always* linearly independent from c so that one has $v_n \in U$. But now since G acts transitively on the vectors of the standard base, $U = V$.

Thus we may assume that U is contained in the axis of the transvection, in other words that all $u = (u_1, \ldots, u_n)^t \in U$ satisfy the equation $u_{n-6} + u_{n-5} - u_{n-1} = 0$. We shall prove that in this case $U = 0$ (provided t is not a solution of some cubic equations). We shall look at the picture dually. Namely the homogeneous linear equations satisfied by all vectors of U are represented by *rows* of length n, i.e. elements of ${}^nK$, on which G acts *on the right*. All such equations form a *subspace* X of ${}^nK$. Since U is G-invariant the space X is also G-invariant. By our assumption on U one has

$$a = (0, \ldots, 0, 1, 1, 0, 0, 0, -1, 0) \in X.$$

We will concentrate on the last 10 coordinates of the rows from X. A straightforward calculation shows that

$$b = ay^2(e + \epsilon x - z) = (0, \ldots, 0, t, 1 + \epsilon, 0, 0, -\epsilon t, \epsilon - 2) \in X.$$

Now

$$by^2(x - e) = (0, \ldots, 0, -3, 3, -\epsilon t^2, 2\epsilon t) \in X,$$

$$by^2(x - e)y(x - e) = (0, \ldots, 0, -\epsilon t^2, \epsilon t^2, 3t, -6) \in X.$$

If $t^3 \neq -9$ these inclusions imply that $b_1 = (0, \ldots, 0, -1, 1, 0, 0) \in X$ and $b_2 = (0, \ldots, 0, -t, 2) \in X$. Clearly if $\varepsilon = -1$ one has $b + tb_1y^2 + 2b_2 = v_n^t$. On the other side if $\varepsilon = 1$ one has $b + tb_1y^2 + 2b_1y = v_n^t$. Thus in any case $v_n^t \in X$. Again, since G acts transitively on the standard base of ${}^nK$, we may conclude that $X = {}^nK$ and thus $U = 0$. This means that G is irreducible.

2^0. The cases n=8, 11. We preserve the notation of §§ 2, 4 and follow the same plan as in the first subsection. Namely, let U be a G-invariant subspace and X be the subspace of the dual space V^* consisting of the homogeneous linear equations satisfied by elements of U. If there exists a vector $u \in U$ which does not belong to the axis of the transvection, i.e. is such that $au \neq 0$, then we may conclude that $c \in U$. Since $t \neq 0$ we may assume that

$$c = (0, \ldots, 0, t, -t, 0, -2)^t \in U.$$

Then a straightforward calculation shows that

$$d = -(y^2 + y + e)xyc = (0, \ldots, 0, 2, 2, 2, 2, t^2 + t, t^2 + t, t^2 + t)^t \in U.$$

And thus

$$(x - e)y(td - 2c) = (0, \ldots, 0, t^3 + t^2 - 2t + 4, -t^3 - t^2 + 2t - 4, 0, t^4 - t^3)^t \in U.$$

Comparing this last inclusion with the inclusion $c \in U$, we get $v_n \in U$ provided $t^2 - 2t + 2 \neq 0$ and $t^3 + t^2 + 2t + 4 \neq 0$.

On the other side, if $a \in X$, consider $b = -a(e + y^2 + y^2 x)(e + y + y^2) \in X$. A direct calculation shows that

$$b_8 = (0, 0, -2, -2, -2, t + 1, t + 1, t + 1),$$
$$b_{11} = (0, 0, 0, 0, 0, 3, 3, 3, 1, 1, 1).$$

and the vector $bx(e + y + y^2) \in X$ has one of the following forms.

$$((0, 0, t - 1, t - 1, t - 1, t^2 + t - 2, t^2 + t - 2, t^2 + t - 2),$$
$$(0, 0, 0, 0, 0, 4, 4, 4, t + 3, t + 3, t + 3).$$

If $n = 8$ and $t \neq 1$ we can divide the vector by $t - 1$. By comparing these vectors with b, we get

$$u = (0, \ldots, 0, 1, 1, 1) \in X,$$

provided $3t + 5 \neq 0$. Now

$$uxy(x - e)y(x - e) = (0, \ldots, 0, -t(t + 1), 2(t + 1)) \in X.$$

and thus if $t \neq -1$, we may assume

$$v = (0, \ldots, 0, -t, 2) \in X.$$

As before, considering the vectors v, vy and vy^2 we conclude that $v_n^t \in X$ if $t^3 \neq 8$. Now by the usual argument $X = {}^nK$ and $U = 0$.

3⁰. The case n=10. We preserve the notation of §§ 2, 4 and follow the same plan as in the first subsection. Namely, let U be a G-invariant subspace. If there exists a vector $u \in U$ which does not belong to the axis of the transvection, i.e. is such that $au \neq 0$, then we may conclude that $c \in U$. Since $t \neq 0$ we may assume that

$$c = (0, 0, 0, 0, 0, 0, 1, 1, 0, 0)^t \in U.$$

Then a straightforward calculation shows that

$$(x + e)y^2 xy(y + e)xyc = (0, 0, 0, 0, 0, 0, t - 1, t - 1, 2t^2 - 2, t^3 - t)^t \in U$$

and thus clearly

$$d = (0,0,0,0,0,0,0,0,2t^2 - 2, t^3 - t)^t \in U.$$

Now consider the vectors d, yd and y^2d belonging to U. If the determinant of the matrix expressing them in terms of v_8, v_9 and v_{10} is not 0, then clearly $v_{10} \in U$. An easy calculation shows that the determinant equals $(t-1)^3(1+t)^3(t^3+8)$, so that U contains v_{10} if $t \neq \pm 1$, $t^3 \neq -8$. The proof of the equality $U = V$ is now ended in the usual manner.

The proof in the case when U is contained in the axis of z^8 is somewhat more complicated. Since $t \neq 0$ we may from the very start suppose that

$$a = (t, 0, 0, -t, t, t, 0, 0, t, -2) \in X.$$

Let us take the vectors

$$a(e + y + y^2) = (0,0,0,0,2t,2t,2t,-2+t,-2+t,-2+t) \in X$$

and

$$ay^2(x-e)(e+y+y^2) =$$
$$(0,0,0,0,-2-3t,-2-3t,-2-3t,t^2-t+2,t^2-t+2,t^2-t+2) \in X.$$

We see that if $2t^3 + t^2 - 4 \neq 0$, then $b = (0,0,0,0,0,0,0,1,1,1) \in X$. Now

$$v = b((1+t)e - xy)(x+e) = (0,0,0,0,0,0,0,0,t^2+3t+4,0) \in X,$$

which shows that $v_9^t \in X$ if $t^2 + 3t + 4 \neq 0$. The proof of equalities $X = {}^nK$, $U = 0$ is now ended as usual.

§6. Equations

In this final section we prove that in most cases we can choose an element $t \in K = \mathbf{F}_q$, $q = p^m$, which satisfies the required restrictions, and we show how to modify the generators in the remaining cases. The analysis is based on Lemma 13 from [DiMV].

1⁰. The general case. The analysis of the general case is straightforward. With the notation of [DiMV] we have $d = 3$, $s \leq 7$. If $m \geq 4$, then the condition $p > \sqrt{3}, \sqrt{7}$ of the above lemma amounts to $p > 2$. If $m = 3$, then $p > \sqrt{3+7}$ leaves only the case $q = 27$, but this case is ruled out by the inequality $p^3 > pd + s$ from the proof of Lemma 13. If $m = 2$

then $p > 3, 7$ excludes only the cases $p = 9, 25, 49$. The case $q = 9$ is excluded anyhow, while the existence of a desired t in the cases $q = 25, 49$ follows from the inequality $p^2 > pd + s$ appearing in the proof of Lemma 13. Finally, if $m = 1$, then the desired t certainly exists if $p > 7 + 3$ so that only the cases $q = 3, 5, 7$ remain to be considered. A direct check shows that 1 will do for $q = 3$ and $q = 7$, while 3 will do for $q = 5$. This finishes the proof of the theorem for all cases apart from $n = 8, 10, 11$.

2^0. The case n=8. With the same notation as above we have $d = 3$ and $s \leq 14$. If $m > 4$ then $p > \sqrt{3}, \sqrt[3]{14}$ is satisfied for all $p > 2$, while for $m = 4$ the case $p = 3$ remains to be considered. However the inequality $p^4 > dp^2 + s$ appearing in the proof of Lemma 13 from [DiMV] is clearly satisfied for $p = 3$. If $m = 3$, then the inequality $p^3 > dp + s$ is satisfied for any $p > 2$. For $m = 2$ the inequality $p^2 > dp + s$ is not satisfied only for the case $p = 5$. However for the field $\mathbf{F}_{25}$ the inequality $3t + 5 \neq 0$ merely gives $t \neq 0$; the equation $t^2 - 2t + 2 = (t - 3)(t - 4) = 0$ has both roots in the prime subfield; and the cubic equation $t^3 + t^2 + 2t - 4 = 0$ has root $t = 2$, so that it excludes at most two other elements of $\mathbf{F}_{25}$. Since t^3 has to be a defining element, the cubic roots of elements of the prime subfield are excluded which gives together with the previous condition 15 excluded values altogether. Clearly we can choose an element in $\mathbf{F}_{25}$ satisfying these restrictions. Finally if $m = 1$, any $p > 3 + 14$ will do, so that we have only to consider the cases $q = 3, 5, 7, 11, 13, 17$. For $q = 11, 13, 17$ one can take $t = 3$. For the remaining cases $q = 3, 5, 7$ there are no elements satisfying these restrictions. This leaves us with the analysis of the cases $\mathrm{SL}(8, 3)$, $\mathrm{SL}(8, 5)$ and $\mathrm{SL}(8, 7)$. But a direct analysis carried on by K.Lux from RWTH Aachen using a specialized GAP-program (see [Sch]) developed by F.Celler shows that x_8 and y_8 generate these groups when $t = 0$*.

3^0. The case n=10. In this case $d = 4$, $s \leq 16$. For $m \geq 4$ everything works precisely as in the case $n = 8$. For $m = 3$ only the case

---

* These groups were too large to be analysed by CAYLEY. For the group $\mathrm{SL}(8, 3)$ we have checked with a standard release of GAP that these elements generate the whole group also for $t = 1$. However this required about 15 hours of computer time, so that all other excluded cases were definitely out of reach. Here is an excerpt from a letter of J.Neubüser to us: ".. auch bei uns einer meiner Mitarbeiter die (2,3)-Erzeugbarkeit von $\mathrm{SL}(8, 3)$ mit den in GAP vorhandenen Funktionen mit "brute force" in einigen Stunden verifiziert hat. Die Verifikation mit den neuen Funktionen von Herrn Celler, die erst demnächst in GAP aufgenommen werden, dauerte dagegen nur ungefähr 2 Minuten für alle 6 Gruppen zusammen".

$q = 27$ remains to be considered. But actually for characteristic 3 the last equation happens to have degree 3 and not 4 and moreover $t = 1$ is one of the roots of $t^3 = -8$, so that in fact $s \leq 14$ and everything works as before. For $m = 2$ the inequality $p^2 > dp + s$ is not satisfied only in the case $q = 25$. In this case $t^2+3t+4 = (t+2)^2$ and $9t^4-6t^2+12t-8 = (t-1)(t^3+t^2+2)$. The cubic equations $2t^3 - t^2 - 4 = 0$ and $t^3 + t^2 + 2 = 0$ do not have roots in $\mathbf{F}_5$ – and thus also in $\mathbf{F}_{25}$. Thus in this case we may take as t a square root of 2. Indeed, $t^4 - 2t^3 = t - 1$ is a defining element of $\mathbf{F}_{25}$, clearly t does not belong to $\mathbf{F}_5$ and is not a root of the only remaining quadratic equation $t^2 - 2t + 4 = 0$. This leaves us, as before, only with the analysis of the prime cases. Since the roots of the polynomial $t^3(t-2)$ are already excluded, any $p > 15$ will do for $m = 1$, so that we have only to consider the cases $m = 3, 5, 7, 11, 13$. In the cases $q = 11, 13$ one can take $t = 3$, but the cases $q = 3, 5, 7$ are really exceptional in the sense that there are no t satisfying desired restrictions. This leaves us with the analysis of the cases $\mathrm{SL}(10,3)$, $\mathrm{SL}(10,5)$ and $\mathrm{SL}(10,7)$. Again a direct computer check by K.Lux using an extension of GAP developed by F.Celler showed that x_{10} and y_{10} generate these groups for $t = 0$, see the footnote at the preceding page.

4^0. The case n=11. In this case $d = 6$, $s \leq 11$. If $m \geq 4$ everything works as before. On the other side if $m = 1$, the desired t certainly exists if $q > 11$ (since the polynomial t^6 has only one root and this root is already excluded), and a direct check shows that $t = 1$ works for the cases $q = 3, 5, 11$, while $t = 5$ works for $q = 7$. If $m = 2, 3$, the inequalities given in Lemma 13 of [DiMV] leave only the cases $q = 25, 27, 49$ to be considered. If $q = 25$ all the 6-th powers lie in the prime subfield. However the conditions which garantee irreducibility can still be satisfied by an element t lying outside the prime subfield. Thus the group $G = \langle x, y\rangle$ is irreducible and contains $\mathrm{SL}(3,5)$ up to conjugacy. By the classification of the irreducible subgroups generated by transvections (see the references in [Ka], [DiMV]), G contains $\mathrm{SL}(11,5)$ up to conjugacy. But $\mathrm{SL}(11,5)$ is maximal in $\mathrm{SL}(11,25)$ and the trace of yxy equals t, so that yxy cannot lie in $\mathrm{SL}(11,5)$ up to conjugacy and G coincides with $\mathrm{SL}(11,25)$. The same argument works for $q = 49$. Finally, the case $q = 27$ is ruled out, since the only root of $t^3 - 8 = 0$ is 2; thus $s \leq 7$ in this case, and the condition $p^3 > pd + s$ is satisfied.

Conclusion

The results of §§ 4–6 completely prove our main theorem for the case $n \geq 8$. Indeed, the results of § 4 imply that under suitable restrictions on t the group G generated by the elements x and y contains a subgroup conjugate to $\mathrm{SL}(3,K)$, namely the subgroup generated by z^r, yz^ry^{-1}, $y^{-1}z^ry$ has this property. § 5 tells us that – under some additional restrictions on t – the group G is irreducible. Then the Proposition 2 of [DiMV] implies that the normal closure H of z^r in G is irreducible. Moreover this normal closure contains $\mathrm{SL}(3,K)$ in the natural representation up to conjugacy. Then the classification of irreducible subgroups generated by root subgroups implies that $H = \mathrm{SL}(n,K)$. In other words x and y generate the whole group $\mathrm{SL}(n,K)$ provided there exists an element $t \in K$ satisfying the restrictions above. Finally in § 6 we have shown that such an element t almost always exists, and that it is possible to modify the generators slightly in some small cases in which such a t does not exist. Thus the theorem is completely proven.

We believe that it should be possible to apply our method also in characteristic 2, but of course this requires a somewhat more delicate analysis. First, if we want to keep y as close to monomial as possible, the involution x has to be modified so as to ensure that its residue is large enough. Second, one is unable to ensure at an early stage that G contains a root subgroup, so that one has to refer to the classification of irreducible linear groups generated by *transvections* rather than root subgroups (see [Mc], [Po], [Ka]). Here the list is longer and there are more subgroups to be excluded. We believe that in the absence of Dickson's lemma it still should be possible to prove that G is not contained in a subgroup defined by a proper subfield by some direct argument, for example, considering traces of elements of G, as in [CDiM], [TV] and § 6 above.

The results of [DiMV] and of the present paper are instrumental in establishing (2,3)-generation of other classical groups and the groups of types E_l, $l = 6, 7, 8$, over fields of characteristic $\neq 2$. This can be achieved by the "duplication" method due to M.C.Tamburini (see, for example [TWG] for a version of this method). The corresponding results will appear in a subsequent paper by the authors.

Finally, we would like to mention that the problem posed at the very end of [DiMV] was solved in an unexpected way in [TWG]. Namely, in [DiMV] we asked whether the group $\mathrm{SL}(n,\mathbf{Z})$ – or even the group $\mathrm{SL}(n,\mathbf{Z}[t])$ – was (2,3)-generated. Using the methods of [TW] and [Ta] the authors of [TWG] succeeded in proving that for *any* finitely generated ring R the elementary group $\mathrm{E}(n,R)$ is (2,3)-generated if n is large enough with respect to the number of generators of R. More precisely, Theorem A of [TWG] says that if R is generated by $t_1,\ldots,t_d$, where t_1 is a unit of R of finite multiplicative order, then the $\mathrm{E}(n,R)$ is (2,3)-generated for all $n \geq 12d+16$. Of course, when $\mathrm{SK}_1(n,R) = 0$ (for example when $n \geq 2$ and R is semilocal or euclidean, or when $n \geq 3$ and R is a Hasse domain or a polynomial ring over one of the rings above [HO'M], [Su]), then the group $\mathrm{E}(n, R)$ coincides with $\mathrm{SL}(n, R)$. For example, the group $\mathrm{SL}(n, \mathbf{Z})$ is (2,3)-generated for $n \geq 28$ and the group $\mathrm{SL}(n, \mathbf{Z}[t])$ is (2,3)-generated for $n \geq 40$.

It would be interesting to know the exact list of values of n for which these groups are (2,3)-generated. One might note that this is not always true. For example since the group $\mathrm{PSL}(4, 2)$ is not (2,3)-generated, the group $\mathrm{SL}(4, \mathbf{Z})$ cannot be (2,3)-generated. Similarly, since the group $\mathrm{PSL}(3, 4)$ is not (2,3)-generated, the group $\mathrm{SL}(3, \mathbf{Z}[t])$ cannot be (2,3)-generated.

The authors are grateful to F.Celler, K.Lux, G.Malle and J.Neubüser for their help with GAP which lead to the solution of the 6 remaining exceptional cases.

Bibliography

[BH] Brown R., Humphries S. Orbits under symplectic transvections. I, II. – *Proc. London Math. Soc.* – 1986. – **52**. – P.517–531; P.532–556.

[CDiM] Cazzola M., Di Martino L. (2,3)-generation of $\mathrm{PSp}(4, q)$, $q = p^m$, $p \neq 2, 3$. – *submitted to Res. Math.*

[Co] Cohen J. On non-Hurwitz groups. – *Glasgow Math. J.* – 1981. – **22**. – P.1–7.

[Coo] Cooperstein B.N. The geometry of root subgroups in exceptional groups. I. – *Geom. Dedic.* – 1979. – **8**. – P.317–381.

[DiMT] Di Martino L., Tamburini M.C. 2-Generation of finite simple groups and some related topics. – in *Generators and Relations in Groups and Geometries*, A.Barlotti et al. (eds.), Kluwer Acad. Publ. – 1991. – P.195–233.

[DiMV] Di Martino L., Vavilov N.A. (2,3)-generation of $\mathrm{SL}(n, q)$. I. Cases $n = 5, 6, 7$. – *Preprint Univ. degli Studi Milano.* – 1992. – N.12. – 16P. (*submitted to Comm. Algebra.*)

[Ga] Garbe D. Über eine Klasse von arithmetisch definierbaren Normalteilern der Modulgruppe. – *Math. Ann.* – 1978. – **235**. – S.195–215.

[HO'M] Hahn A.J., O'Meara O.T. *The classical groups and K-theory.* – Springer: Berlin et al. – 1989. – 576P.

[Ka] Kantor W.M. Subgroups of classical groups generated by long root elements. – *Trans. Amer. Math. Soc.* – 1979. – **248**, N.2. – P.347–379.

[KL] Kleidman P., Liebeck M. *The subgroup structure of the finite classical groups.* – LMS Lecture Note Series. – 1990. – **129**.

[LN] Lidl R., Niederreiter H. *Finite fields.* – Encyclopedia of Math. and Appl. – Addison Wesley P.C.: London et al. – 1983. – **20**.

[Mb] Macbeath A.W. Generators of linear fractional groups. – *Proc. Symp. Pure Math.* – 1967. – **12**. – P.14–32.

[Ma1] Malle G. Exceptional groups of Lie type as Galois groups. – *J. reine angew. Math.* – 1988. – **392**. - S.70–109.

[Ma2] Malle G. Hurwitz groups and G_2. – *Canad. Math. Bull.* – 1990. – **33**, N.3. – P.349–357.

[MSW] Malle G., Saxl J., Weigel Th. – Generation of classical groups. – *submitted.*

[Mc] McLaughlin J.E. Some subgroups of $SL_n(\mathbf{F}_2)$. – *Illinois J. Math.* – 1969. – **13**. – P.108–115.

[Po] Pollatsek H. Irreducible groups generated by transvections over fields of characteristic 2. – *J. Algebra.* – 1976. – **39**. – P.328–333.

[Sch] Schönert M. et al. *GAP 3.2, Manual.* – Lehrstuhl D für Mathematik, RWTH Aachen. – Aachen, 1993. – 850P.

[Se]* Semenov A.A. Bruhat decomposition of semisimple root subgroups in the special linear group. – *J. Sov. Math.* – 1990. – **52**, N.3. – P.3178–3184.

[Su] Suslin A.A. On the structure of the general linear group over polynomial rings. – *Sov. Math. Izv.* – 1977. – **41**, N.2 – P.503–516.

[Ta] Tamburini M.C. Generation of certain simple groups by elements of small order. – *Rend. Ist. Lomb. Sci.* – 1987. – **A121** – P.21–27.

[TV] Tamburini M.C., Vassallo S. (2,3)-generazione di $SL(4,q)$ in caratteristica dispari e problemi collegati. – *submitted.*

[TW] Tamburini M.C., Wilson J.S. On the generation of finite simple groups by pairs of subgroups. – *J. Algebra.* – 1988. – **116**, N.2. – P.316–333.

[TWG] Tamburini M.C., Wilson J.S., Gavioli N. The (2,3)-generation of some classical groups and a residual property of $PSL_2(\mathbf{Z})$. – *Quaderni Sem. Mat. Brescia.* – 1993. – N.1. – 15P. (*submitted to J. Algebra.*)

[Va1] Vavilov N.A. Bruhat decomposition of two-dimensional transformations. – *Vestnik Leningr. Univ., Math.* – 1989. – **22**, N.3. – P.1–6.

* This reference was not easy to locate because in the *J. Sov. Math.* this paper is wrongly attributed to A.V.Yakovlev. The authors believe that this could never occur in the translations supervised by the A.M.S.

[Va2] Vavilov N.A. Semisimple long root elements and triples of unipotent long root subgroups in a Chevalley group. – In: *Problems in Algebra (Minsk)*. – 1989. – N.4. – P.162–173. (in Russian).

[We] Weigel Th. Generation of exceptional groups of Lie-type. – *submitted.*

[Wi] Wilson J.S. A residual property of free groups. - *J. Algebra*. – 1991. – **138**, N.1. – P.36–47.

[Wo] Woldar A.J. On Hurwitz generation and genus action of sporadic groups. – *Illinois Math. J* . – 1989. – **33**. – P.416–437.