Annali di Matematica 180, 359–372 (2001)

DOI (Digital Object Identifier) 10.1007/s102310100016

Giampiero Chiaselotti

Some presentations for the special linear groups on finite fields

Received: March 16, 1998; in final form: November 3, 2000
Published online: October 2, 2001 – © Springer-Verlag 2001

Abstract. We simplify the Steinberg presentation of $SL_n(\mathbf{F}_d)$, where $n \geq 1$ and $\mathbf{F}_d$ is any finite field with d elements. That presentation has the elementary matrices $e_{ij}(r)$, with $i, j \in \{1, \dots, n\}, i \neq j$ and $r \in \mathbf{F}_d$, as generators, and (E1)–(E3), described at the opening of this work, as relations. The presentation that we shall obtain reduces the number of generators $e_{ij}(r)$ and relations (E1)–(E3). In particular, relations (E3) are considerably reduced.

Mathematics Subject Classification (2000). 20F05

Key words. Steinberg presentation – elementary matrices

Introduction

In this paper we study some presentations of the special linear groups $SL_n(\mathbf{F}_d)$, on a finite field $\mathbf{F}_d$, where $n \geq 3$ and $d = p^m$, with $m \geq 1$ and p an odd prime. A presentation of $SL_n(\mathbf{F}_d)$, obtained by determining an isomorphism among these groups and the Steinberg's ones $St_n(\mathbf{F}_d)$, is described in [2]. Our work has been devoted to simplifying and remarkably reducing in number the relations of $SL_n(\mathbf{F}_d)$ for the group presentations described in [2]. We notice that, obviously, the presentations of $SL_n(\mathbf{F}_d) \cong SL(V)$, where V is a vector space of dimension n on $\mathbf{F}_d$, depend upon the choice of a basis for V. In [1] and [4] suitable presentations for the special linear groups and for the Steinberg's groups are determined and these do not depend upon the choice of a basis for V. In [2] it is proved that the group $SL_n(\mathbf{F}_d)$ has a presentation with abstract generators $x_{ij}(r)$ (where $i, j \in \{1, \dots, n\}$, $i \neq j$ and $r \in \mathbf{F}_d$) and relations (E1)–(E3) are given at the beginning of that paper. The abstract generator $x_{ij}(r)$ corresponds to the elementary matrix $e_{ij}(r)$, which has r in the (i, j) entry, 1 on the whole principal diagonal and 0 in the other places. Then, the obtained presentation simplifies and remarkably reduces the previous relations, in particular (E3). In fact, if $i, j, k \in \{1, \dots, n\}$ are fixed and distinct, the number of relations in (E3) (after a reduction of the generators) is p^{2m}; we reduce such a number to m^2. Such results are described in Proposition 3.

Let us fix the notation for the following: p will denote an odd prime, m an integer ≥ 1, and n an integer ≥ 3. Moreover, we shall set $d = p^m$.

G. Chiaselotti: Dipartimento di matematica, Università degli studi della Calabria, cap 87036, Arcavacata Di Rende (CS), Italy

$\mathbf{F}_d$ will denote a finite field with d elements.

In [2] it has been proved that

$$SL_n(\mathbf{F}_d) \cong St_n(\mathbf{F}_d). \tag{1}$$

Let us recall that $St_n(\mathbf{F}_d)$ is an abstract group having generators $x_{ij}(r)$, where $r \in \mathbf{F}_d$, $i, j \in \{1, \dots, n\}$ and $i \neq j$, with the following relations:

(E1) $x_{ij}(r)x_{ij}(s) = x_{ij}(r+s)$;

(E2) $\left[x_{ij}(r), x_{kl}(s)\right] = 1$ if $j \neq k$ and $i \neq l$;

(E3) $\left[x_{ij}(r), x_{jk}(s)\right] = x_{ik}(rs)$ if i, j and k are distinct.

In the isomorphism (1) every generator $x_{ij}(r)$ of the abstract group $St_n(\mathbf{F}_d)$ corresponds, in $SL_n(\mathbf{F}_d)$, to the elementary matrix $e_{ij}(r)$. Consequently, we can consider the generator $x_{ij}(r)$ just as the matrix $e_{ij}(r)$, and use all the matrix calculus rules valid in $SL_n(\mathbf{F}_d)$.

The field $\mathbf{F}_d$ is a vector space of dimension m over the field $\mathbf{F}_p$, and it has a basis having the form $\{1, \alpha, \dots, \alpha^{m-1}\}$; so all elements of $\mathbf{F}_d$ can be written in the form

$$\lambda_0 + \lambda_1\alpha + \cdots + \lambda_{m-1}\alpha^{m-1}, \tag{2}$$

where the coefficients $\lambda_0, \dots, \lambda_{m-1}$ are integers uniquely determined mod p.

Let now $i, j \in \{1, \dots, n\}$ be fixed, with $i \neq j$. If $r \in \mathbf{F}_d$ is a generic element expressed in the form (2), by relation (E1) one immediately has that

$$x_{ij}(r) = x_{ij}(1)^{\lambda_0} x_{ij}(\alpha)^{\lambda_1} \dots x_{ij}(\alpha^{m-1})^{\lambda_{m-1}}, \tag{3}$$

and also

$$x_{ij}(r)^p = x_{ij}(0) = 1. \tag{4}$$

Obviously, (4) follows from the fact that the characteristic of $\mathbf{F}_d$ is p.

By (3) it follows that all the generators $x_{ij}(r)$ of $SL_n(\mathbf{F}_d)$ are contained in the subgroup generated by $x_{ij}(1), x_{ij}(\alpha), \dots, x_{ij}(\alpha)^{m-1}$; then all generators $x_{ij}(r)$ with $r \notin \{1, \alpha, \dots, \alpha^{m-1}\}$ can be eliminated from the presentation of $SL_n(\mathbf{F}_d)$ given in (1).

Now, we ask ourselves what relations (among (E1)–(E3)) remain between the generators $x_{ij}(1), x_{ij}(\alpha), \dots, x_{ij}(\alpha^{m-1})$, after we have eliminated the unnecessary ones.

If $i, j \in \{1, \dots, n\}$ and $i \neq j$, let us denote by ϵ_{ij} the matrix having 1 in the place (i, j) and 0 elsewhere. The matrices ϵ_{ij} verify the following identities:

$$\epsilon_{ij}\epsilon_{kl} = \begin{cases} 0, & \text{if } i \neq j; \\ \epsilon_{il}, & \text{if } j = k. \end{cases} \tag{5}$$

We now set

$$A(i, j) = \{\, I + r\epsilon_{ij} \mid r \in \mathbf{F}_d \,\},$$

where I is the identity matrix of order n.

Proposition 1. *$A(i, j)$ is a subgroup of $SL_n(\mathbf{F}_d)$, which is generated by the elements $x_{ij}(1)$, $x_{ij}(\alpha), \ldots, x_{ij}(\alpha^{m-1})$; moreover it is isomorphic to the direct product $\mathbf{Z}_p^m = \underbrace{\mathbf{Z}_p \times \cdots \times \mathbf{Z}_p}_{m\ =\text{times}}$.*

Proof. Since $I + r\epsilon_{ij} = x_{ij}(r)$, by relations (E1) it follows at once that $A(i, j)$ is a subgroup of $SL_n(\mathbf{F}_d)$; it is generated by $x_{ij}(1), x_{ij}(\alpha), \ldots, x_{ij}(\alpha^{m-1})$ by virtue of (3). A presentation for $\mathbf{Z}_p^m$ is

$$\mathbf{Z}_p^m \cong \big\langle y_0, \ldots, y_{m-1} \mid y_0^p = y_1^p = \cdots = y_{m-1}^p = 1,\\ [y_r, y_s] = 1 \qquad \text{if} \quad r, s \in \{0, 1, \ldots, m-1\}\big\rangle. \tag{6}$$

By relations (E1), it follows at once that the elements $x_{ij}(1), \ldots, x_{ij}(\alpha^{m-1})$ verify the relations given in (6); therefore the correspondence $y_0 \mapsto x_{ij}(1)$, $y_1 \mapsto x_{ij}(\alpha)$, $\ldots$, $y_{m-1} \mapsto x_{ij}(\alpha^{m-1})$ induces an epimorphism from $\mathbf{Z}_p^m$ into the group $A(i, j)$. But $A(i, j)$ has order p^m and $p^m = |\mathbf{Z}_p^m|$, therefore $A(i, j) \cong \mathbf{Z}_p^m$. □

Now, using the isomorphism established in Proposition 1 and the presentation of $\mathbf{Z}_p^m$ given in (6), and using the standard properties of subgroup presentations (see, e.g., [3]), we can replace all relations (E1) (those which involve only the generators $x_{ij}(1), \ldots, x_{ij}(\alpha^{m-1})$) by the following ones:

(E1′) $x_{ij}(1)^p = x_{ij}(\alpha)^p = \cdots = x_{ij}(\alpha^{m-1})^p$,
(E1″) $\big[x_{ij}(\alpha^r), x_{ij}(\alpha^s)\big] = 1 \qquad \text{if} \quad r, s \in \{0, 1, \ldots, m-1\}$.

Since i and j are generic, relations (E1′) and (E1″) replace relations (E1) for all pairs of indices $i, j \in \{1, \ldots, n\}$, with $i \neq j$.

Let us point out that relations (E2) amount to the following ones:

(E2′) $[x_{ij}(\alpha^r), x_{kl}(\alpha^s)] = 1 \qquad \text{if} \quad j \neq k \quad \text{and} \quad i \neq l$,

where $r, s \in \{0, 1, \ldots, m-1\}$. In fact, if ρ, σ are two generic elements of $\mathbf{F}_d$, we have $\rho = \lambda_0 + \lambda_1 + \cdots + \lambda_{m-1}\alpha^{m-1}$, $\sigma = \mu_0 + \mu_1\alpha + \cdots + \mu_{m-1}\alpha^{m-1}$, for suitable integer coefficients $\lambda_0, \ldots, \lambda_{m-1}, \mu_0, \ldots, \mu_{m-1}$ considered mod p; hence, by (3) it follows that

$$\begin{aligned}[x_{ij}(\rho), x_{kl}(\sigma)] &= \big[x_{ij}(\lambda_0 + \lambda_1\alpha + \cdots + \lambda_{m-1}\alpha^{m-1}),\\ &\qquad x_{kl}(\mu_0 + \mu_1\alpha + \cdots + \mu_{m-1}\alpha^{m-1})\big]\\ &= \big[x_{ij}(1)^{\lambda_0} x_{ij}(\alpha)^{\lambda_1} \ldots x_{ij}(\alpha^{m-1})^{\lambda_{m-1}},\\ &\qquad x_{kl}(1)^{\mu_0} x_{kl}(\alpha)^{\mu_1} \ldots x_{kl}(\alpha^{m-1})^{\mu_{m-1}}\big].\end{aligned} \tag{7}$$

Then, if relations (E2′) hold, it is clear that all powers and all possible products made by combining the elements $x_{ij}(1)$, $x_{ij}(\alpha)$, …, $x_{ij}(\alpha^{m-1})$, $x_{kl}(1)$, $x_{kl}(\alpha)$, …, $x_{kl}(\alpha^{m-1})$ commute with each other. Consequently, relations (E2′) and (7) imply that $[x_{ij}(\rho), x_{kl}(\sigma)] = 1$, for all $\rho, \sigma \in \mathbf{F}_d$. Therefore, (E2) are a consequence of (E2′).

Let us now examine relations (E3). By virtue of (3), relations (E3) take the following form:

$$\left[x_{ij}(1)^{\lambda_0}x_{ij}(\alpha)^{\lambda_1}\dots x_{ij}(\alpha^{m-1})^{\lambda_{m-1}}, x_{jk}(1)^{\mu_0}x_{jk}(\alpha)^{\mu_1}\dots x_{jk}(\alpha^{m-1})^{\mu_{m-1}}\right] = \\ = x_{ik}(1)^{l_0}x_{ik}(\alpha)^{l_1}\dots x_{ik}(\alpha^{m-1})^{l_{m-1}}, \qquad (8)$$

if i, j, k are distinct. Here λ_0, λ_1, …, λ_{m-1}, μ_0, μ_1, …, μ_{m-1}, l_0, l_1, …, l_{m-1} are integers considered mod p and l_0, l_1, …, l_{m-1} are uniquely determined by condition

$$(\lambda_0+\lambda_1\alpha+\dots+\lambda_{m-1}\alpha^{m-1})(\mu_0+\mu_1\alpha+\dots+\mu_{m-1}\alpha^{m-1}) = \\ = l_0+l_1\alpha+\dots+l_{m-1}\alpha^{m-1}. \qquad (9)$$

In other terms, the left-hand side in (9) is an element of $\mathbf{F}_d$ and consequently, as such, can be written uniquely in the form $l_0+l_1\alpha+\dots+l_{m-1}\alpha^{m-1}$ where l_0, l_1, …, l_{m-1} are integers considered mod p.

Notice that, for each fixed $i, j, k \in \{1,\dots,n\}$, with i, j, k distinct, the number of relations (8) which involve $x_{ij}(1)$, …, $x_{ij}(\alpha^{m-1})$, $x_{jk}(1)$, …, $x_{jk}(\alpha^{m-1})$, $x_{ik}(1)$, …, $x_{ik}(\alpha^{m-1})$ is p^{2m}.

Now let $i, j, k \in \{1,\dots n\}$ be fixed and distinct; let us consider the following $3m$ elements:

$$x_{ij}(\alpha^s), \quad x_{ik}(\alpha^s), \quad x_{jk}(\alpha^s), \qquad (10)$$

where $s = 0, 1, \dots, m-1$.

The relations that involve only elements in (10) are:

$$x_{ij}(1)^p = \dots = x_{ij}(\alpha^{m-1})^p = x_{ik}(1)^p = \dots = x_{ik}(\alpha^{m-1})^p = 1, \qquad (11)$$

$$[x_{ij}(\alpha^r), x_{ij}(\alpha^s)] = [x_{ik}(\alpha^r), x_{ik}(\alpha^s)] = 1, \qquad (12)$$

if $r, s \in \{0, 1, \dots m-1\}$;

$$[x_{ij}(\alpha^r), x_{ik}(\alpha^s)] = 1, \qquad (13)$$

if $r, s \in \{0, 1, \dots m-1\}$;

$$x_{jk}(1)^p = \dots = x_{jk}(\alpha^{m-1})^p = 1, \qquad (14)$$

$$[x_{jk}(\alpha^r), x_{jk}(\alpha^s)] = 1, \qquad (15)$$

if $r, s \in \{0, 1, \dots m-1\}$; finally,

$$[x_{ik}(\alpha^r), x_{jk}(\alpha^s)] = 1, \qquad (16)$$

if $r, s \in \{0, 1, \dots m-1\}$;

$$\left[x_{ij}(1)^{\lambda_0}\dots x_{ij}(\alpha^{m-1})^{\lambda_{m-1}}, x_{jk}(1)^{\mu_0}\dots x_{jk}(\alpha^{m-1})^{\mu_{m-1}}\right] = \\ = x_{ik}(1)^{l_0}\dots x_{ik}(\alpha^{m-1})^{l_{m-1}}, \qquad (17)$$

where

$$(\lambda_0 + \lambda_1\alpha + \cdots + \lambda_{m-1}\alpha^{m-1})(\mu_0 + \mu_1\alpha + \cdots + \mu_{m-1}\alpha^{m-1}) = \\ l_0 + l_1\alpha + \cdots + l_{m-1}\alpha^{m-1},$$

and $\lambda_0, \ldots, \lambda_{m-1}, \mu_0, \cdots, \mu_{m-1}$ are integers considered mod p which uniquely determine the elements $l_0, \cdots, l_{m-1}$ in $\mathbf{F}_p$.

Our next aim is to prove that the subgroup of $SL_n(\mathbf{F}_d)$ generated by the elements in (10) is isomorphic to a suitable semidirect product. After we have proved the existence of such an isomorphism, we shall proceed to a substantial reduction of relations (17), corresponding (for i, j, k fixed and distinct) to relations (E3) which involve the elements in (10) only. Notice that relations (11) and (12) are part of relations (E1′) and (E1″), just as (14) and (15) are. Relations (13) and (16) are part of relations (E2′).

Let i, j, k be fixed and distinct elements of $\{1, \ldots, n\}$, and let

$$P(i, j, k) = \{ I + x\epsilon_{ij} + y\epsilon_{ik} + z\epsilon_{jk} \mid x, y, z \in \mathbf{F}_d \}. \tag{18}$$

$P(i, j, k)$ is the set of matrices of $SL_n(\mathbf{F}_d)$ that have 1 on the principal diagonal and 0 in the other places, except in the places (i, j), (j, k), and (i, k): in all such places the elements in $\mathbf{F}_d$ can be chosen freely.

Proposition 2. *$P(i, j, k)$ is a subgroup of $SL_n(\mathbf{F}_d)$ which has order $d^3 = p^{3m}$ and is generated by the elements $x_{ij}(1)$, $x_{ij}(\alpha)$, $\ldots$, $x_{ij}(\alpha^{m-1})$, $x_{ik}(1)$, $x_{ik}(\alpha)$, $\ldots$, $x_{ik}(\alpha^{m-1})$, $x_{jk}(1)$, $x_{jk}(\alpha)$, $\ldots$, $x_{jk}(\alpha^{m-1})$.*

Proof. If $I + r\epsilon_{ij} + s\epsilon_{ik} + t\epsilon_{jk} \in P(i, j, k)$, by (5) it follows that

$$\begin{aligned} I &+ r\epsilon_{ij} + s\epsilon_{ik} + t\epsilon_{jk} \\ &= (I + r\epsilon_{ij})\big(I + (s - rt)\epsilon_{ik}\big)(I + t\epsilon_{jk}) \\ &= x_{ij}(r)x_{ik}(s - rt)x_{jk}(t). \end{aligned} \tag{19}$$

Let us observe that $x_{ij}(r) \in A(i, j)$, $x_{ik}(s - rt) \in A(i, k)$, $x_{jk}(t) \in A(j, k)$; then, by Proposition 1 and (19) it follows that $P(i, j, k)$ is generated by $x_{ij}(1), \ldots, x_{ij}(\alpha^{m-1}), x_{ik}(1), \ldots, x_{ik}(\alpha^{m-1}), x_{jk}(1), \ldots, x_{jk}(\alpha^{m-1})$. □

Suppose now that the $m - 1$ elements of $\mathbf{F}_d$, $\alpha^m, \alpha^{m+1}, \ldots, \alpha^{2m-2}$ are written as linear combinations of the basis $1, \alpha, \ldots, \alpha^{m-1}$ as follows:

$$\alpha^{m+s} = a_{0,m+s} + a_{1,m+s}\alpha + \cdots + a_{m-1,m+s}\alpha^{m-1}, \tag{20}$$

where $s = 0, 1, \ldots, m-2$, and a_{ij} are suitable integers uniquely determined mod p. If k is an integer ≥ 1, we shall denote by $\mathbf{Z}_p^k$ the direct product of k copies of $\mathbf{Z}_p$.

Let us consider now the abelian groups $\mathbf{Z}_p^m$ and $\mathbf{Z}_p^m \times \mathbf{Z}_p^m$. By $\operatorname{Aut}(\mathbf{Z}_p^m \times \mathbf{Z}_p^m)$ we shall denote the group of automorphisms of the group $\mathbf{Z}_p^m \times \mathbf{Z}_p^m$. In the following we shall identify each matrix $A \in GL_{2m}(\mathbf{Z}_p)$ with the induced automorphism $f_A \in \operatorname{Aut}(\mathbf{Z}_p^m \times \mathbf{Z}_p^m)$ and we shall misuse the notations by writing $A \in \operatorname{Aut}(\mathbf{Z}_p^m \times \mathbf{Z}_p^m)$ instead of $f_A \in \operatorname{Aut}(\mathbf{Z}_p^m \times \mathbf{Z}_p^m)$. Notice that, if $A, B \in GL_{2m}(\mathbf{Z}_p)$, then the product AB corresponds to the composition $f_B \circ f_A$; therefore, if we have to verify some relation concerning the automorphisms f_A, it suffices to examine the corresponding relation between matrices with the usual row-by-column product. Now, given the abelian group $\mathbf{Z}_p^m$, let $\Delta = \{e_1, \ldots, e_m\}$ be the set of its canonical generators, namely $e_1 = (1, 0, \ldots, 0), \ldots, e_m = (0, 0, \ldots, 0, 1)$. Consider the correspondence

$$\varphi : \Delta \longrightarrow \operatorname{Aut}\bigl(\mathbf{Z}_p^m \times \mathbf{Z}_p^m\bigr)$$

such that

$$e_1 \mapsto A_0 = \begin{pmatrix} I & B_0 \\ 0 & I \end{pmatrix}, e_2 \mapsto A_1 = \begin{pmatrix} I & B_1 \\ 0 & I \end{pmatrix}, e_m \mapsto A_{m-1} = \begin{pmatrix} I & B_{m-1} \\ 0 & I \end{pmatrix},$$

where I is the identity $m \times m$ matrix, 0 is the zero matrix of order m and $B_0, \ldots, B_{m-1}$ are the following $m \times m$ blocks:

$$B_0 = I,$$

$$B_1 = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_{0m} \\ 1 & 0 & \ldots & 0 & a_{1m} \\ 0 & 1 & \ldots & 0 & a_{2m} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{m-1,m} \end{pmatrix},$$

$$B_2 = \begin{pmatrix} 0 & \ldots & 0 & a_{0,m} & a_{0,m+1} \\ 0 & \ldots & 0 & a_{1,m} & a_{1,m+1} \\ 1 & \ldots & 0 & a_{2,m} & a_{2,m+1} \\ \vdots & & \vdots & \vdots & \vdots \\ 0 & \ldots & 1 & a_{m-1,m} & a_{m-1,m+1} \end{pmatrix},$$

$$B_{m-1} = \begin{pmatrix} 0 & a_{0m} & a_{0,m+1} & \ldots & a_{0,2m-2} \\ 0 & a_{1m} & a_{1,m+1} & \ldots & a_{0,2m-2} \\ 0 & a_{2m} & a_{2,m+1} & \ldots & a_{0,2m-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{m-1,m} & a_{m-1,m+1} & \ldots & a_{m-1,2m-2} \end{pmatrix}.$$

In other terms, block B_1 is built starting from $B_0 = I$, by eliminating the first column of B_0 and inserting, as the last column, the m-coefficients in (20) which determine α^m as linear combination of the basis $\{1, \alpha, \ldots, \alpha^{m-1}\}$. The block B_2 is built starting from B_1, by eliminating the first column of B_1 and inserting, as the last column, the m-coefficients in (20) which determine α^{m+1} as linear combination of the basis $\{1, \alpha, \ldots, \alpha^{m-1}\}$, and so on until we arrive at B_{m-1}.

Notice that all the matrices $A_0, \ldots, A_{m-1}$ have order $2m \times 2m$ and determinant 1; consequently, they are contained in $SL_{2m}(\mathbf{F}_p)$ and induce m automorphisms of the group $\mathbf{Z}_p^m \times \mathbf{Z}_p^m$.

Remark. Let us consider now $\mathbf{F}_d$ as a vector space V of dimension m on $\mathbf{F}_p$, having basis $\mathcal{X} = \{1, \alpha, \dots, \alpha^{m-1}\}$. Let us define the application

$$f_\alpha : V \longrightarrow V$$

such that

$$f_\alpha(x) = \alpha x,$$

for each $x \in V$. Therefore $f_\alpha \in GL(V)$ and $f_\alpha^k = \underbrace{f_\alpha \circ \cdots \circ f_\alpha}_{k \text{ times}}$ is such that

$$f_\alpha^k(x) = \alpha^k x, \qquad \text{if} \quad k \geq 1. \tag{$*$}$$

Immediately we can easily verify that

$$\mathrm{Mat}_{\mathcal{X}}(f_\alpha) = B_1.$$

Then, since $\mathrm{Mat}_{\mathcal{X}} : GL(V) \longrightarrow GL_m(\mathbf{F}_p)$ is a group isomorphism, we get

$$\mathrm{Mat}_{\mathcal{X}}(f_\alpha^k) = B_1^k,$$

for each integer $k \geq 1$.

On the other hand, by (20) and ($*$) it follows that:

$$\mathrm{Mat}_{\mathcal{X}}(f_\alpha^k) = B_k, \qquad \text{if} \quad 1 \leq k \leq m-1.$$

Hence

$$B_1^k = B_k, \qquad \text{if} \quad 1 \leq k \leq m-1.$$

□

The group $\mathbf{Z}_p^m$ is a direct product of m copies of $\mathbf{Z}_p$; thus we have the following presentation:

$$\mathbf{Z}_p^m \cong \big\langle z_0, \dots, z_{m-1} \;\big|\; z_0^p = \cdots = z_{m-1}^p = 1, [z_i, z_j] = 1 \quad \text{if} \quad i, j \in \{0, \dots, m-1\}\big\rangle. \tag{21}$$

We can assume that

$$z_0 \longleftrightarrow e_1, \qquad \dots, \qquad z_{m-1} \longleftrightarrow e_m \tag{22}$$

under the isomorphism in (21). By matrix calculations we can easily verify that the matrices $A_0, \dots, A_{m-1}$ satisfy the relations of the groups $\mathbf{Z}_p^m$, as given in (21). So, the application φ extends uniquely to a group morphism (which we denote by φ again)

$$\varphi : \mathbf{Z}_p^m \longrightarrow \mathrm{Aut}\big(\mathbf{Z}_p^m \times \mathbf{Z}_p^m\big). \tag{23}$$

Now let us consider the semidirect product S of $\mathbf{Z}_p^m$ and $(\mathbf{Z}_p^m \times \mathbf{Z}_p^m)$ with respect to the action φ:

$$S = \mathbf{Z}_p^m \ltimes_\varphi \big(\mathbf{Z}_p^m \times \mathbf{Z}_p^m\big).$$

The direct product $(\mathbf{Z}_p^m \times \mathbf{Z}_p^m)$ has the following presentation (see [3] for details):

$$\begin{aligned} &\mathbf{Z}_p^m \times \mathbf{Z}_p^m \cong \\ &\qquad \big\langle x_0, \ldots, x_{m-1}, y_, \ldots, y_{m-1} \mid x_0^p = \cdots = x_{m-1}^p = y_0^p = \cdots = y_{m-1}^p = 1; \\ &\qquad\quad [x_i, x_j] = 1 \qquad \text{if} \quad i, j \in 0, \ldots, m-1; \\ &\qquad\quad [y_i, y_j] = 1 \qquad \text{if} \quad i, j \in 0, \ldots, m-1; \\ &\qquad\quad [x_i, y_j] = 1 \qquad \text{if} \quad i, j \in 0, \ldots, m-1 \big\rangle. \end{aligned} \tag{24}$$

We can obviously assume that generators x_i, y_j correspond under the isomorphism (24) to elements X_i and Y_j, respectively, where the last ones are given by the following $2m$-uples:

$$X_0 = (1, 0, \ldots, 0, 0, \ldots, 0), \ldots, X_{m-1} = (0, 0, \ldots, 0, \underset{\substack{\uparrow\\ \text{place}\\ \text{m}-\text{th}}}{1}, 0, \ldots, 0),$$

$$\begin{aligned} Y_0 &= (0, 0, \ldots, 0, 0, \ldots, \underset{\substack{\uparrow\\ \text{place}\\ (\text{m}+1)-\text{th}}}{1}, 0, \ldots, 0), \ldots, Y_{m-1} \\ &= (0, 0, \ldots, 0, 0, \ldots, 0, \underset{\substack{\uparrow\\ \text{place}\\ 2\text{m}-\text{th}}}{1}). \end{aligned}$$

Using the presentations of $\mathbf{Z}_p^m$ and $\mathbf{Z}_p^m \times \mathbf{Z}_p^m$ established in (21) and (24), respectively, we see that S is isomorphic to the abstract group Ω given by the following presentation:

$$\begin{aligned} \Omega = \big\langle & z_0, \ldots, z_{m-1}, x_0, \ldots, x_{m-1}, y_0, \ldots, y_{m-1} \mid \\ & z_0^p = \cdots = z_{m-1}^p = 1 && (25) \\ & [z_r, z_s] = 1 \qquad \text{se} \quad r, s \in \{0, 1, \ldots, m-1\} && (26) \\ & x_0^p = \cdots = x_{m-1}^p = y_0^p = \cdots = y_{m-1}^p = 1 && (27) \\ & [y_r, y_s] = [x_r, x_s] = 1 \qquad \text{se} \quad r, s \in \{0, 1, \ldots, m-1\}, && (28) \\ & [y_r, x_s] = 1 \qquad \text{se} \quad r, s \in \{0, 1, \ldots, m-1\}, && (29) \\ & z_s x_r^{z_s} = x_r z_s \qquad \text{se} \quad r, s \in \{0, 1, \ldots, m-1\}, && (30) \\ & z_s y_r^{z_s} = y_r z_s \qquad \text{se} \quad r, s \in 0, 1, \ldots, m-1\} \big\rangle. && (31) \end{aligned}$$

Relations (25) and (26) define the subgroup $\mathbf{Z}_p^m$ and relations (27), (28) and (29) define the subgroup $\mathbf{Z}_p^m \times \mathbf{Z}_p^m$ (i.e. the normal factor of the semidirect product S); finally, relations (30) and (31) define the action of the generators z_s on the generators $x_0, \ldots, x_{m-1}, y_0 \ldots, y_{m-1}$. Now, let us observe that in the isomorphism between the abstract group Ω and the semidirect product S, the elements of Ω given by

$$x_0^{z_i}, x_1^{z_i}, \ldots, x_{m-1}^{z_i}, y_0^{z_k}, y_1^{z_k}, \ldots, y_{m-1}^{z_k}$$

correspond, respectively, to the following elements of S:

$$f_{A_i}(X_0), \dots, f_{A_i}(X_{m-1}), f_{A_k}(Y_0), \dots, f_{A_k}(Y_{m-1}),$$

where $i, k = 0, 1, \dots, m-1$. Let us note that $f_{A_i}(X_j)$, $f_{A_k}(Y_r)$ are identified, respectively, with the matricial products A_iX_j and A_kY_r, where X_j and Y_r are thought of as $2m \times 1$ matrices (X_j and Y_r are the canonical generators of the group $\mathbf{Z}_p^m \times \mathbf{Z}_p^m$, as one sees from the notation introduced after the presentation (24)). By the definition of $A_0, \dots, A_{m-1}$ it follows at once that the previous elements of S are, respectively, given by:

$$\begin{aligned}
&A_0X_0 = X_0,\, A_0X_1 = X_1, \dots, A_0X_{m-1} = X_{m-1},\\
&\qquad\qquad\qquad\qquad\vdots\\
&A_{m-1}X_0 = X_0,\, A_{m-1}X_1 = X_1, \dots, A_{m-1}X_{m-1} = X_{m-1},
\end{aligned}$$

$$\begin{aligned}
&A_0Y_0 = X_0 + Y_0\\
&A_0Y_1 = X_1 + Y_1\\
&A_0Y_2 = X_2 + Y_2\\
&\qquad\quad\vdots\\
&A_0Y_{m-2} = X_{m-2} + Y_{m-2}\\
&A_0Y_{m-1} = X_{m-1} + Y_{m-1}
\end{aligned}$$

$$\begin{aligned}
&A_1Y_0 = X_1 + Y_0\\
&A_1Y_1 = X_2 + Y_1\\
&A_1Y_2 = X_3 + Y_2\\
&\qquad\quad\vdots\\
&A_1Y_{m-2} = X_{m-1} + Y_{m-2}\\
&A_1Y_{m-1} = a_{0,m}X_0 + a_{1,m}X_1 + \cdots + a_{m-1,m}X_{m-1} + Y_{m-1}
\end{aligned}$$

$$\begin{aligned}
&A_2Y_0 = X_2 + Y_0\\
&A_2Y_1 = X_3 + Y_1\\
&A_2Y_2 = X_4 + Y_2\\
&\qquad\quad\vdots\\
&A_2Y_{m-3} = X_{m-1} + Y_{m-3}\\
&A_2Y_{m-2} = a_{0,m}X_0 + a_{1,m}X_1 + \cdots + a_{m-1,m}X_{m-1} + Y_{m-2}\\
&A_2Y_{m-1} = a_{0,m+1}X_0 + a_{1,m+1}X_1 + \cdots + a_{m-1,m+1}X_{m-1} + Y_{m-1} =
\end{aligned}$$

$$\begin{aligned}
&A_{m-1}Y_0 = X_{m-1} + Y_0\\
&A_{m-1}Y_1 = a_{0,m}X_0 + a_{1,m}X_1 + \cdots + a_{m-1,m}X_{m-1} + Y_1\\
&A_{m-1}Y_2 = a_{0,m+1}X_0 + a_{1,m+1}X_1 + \cdots + a_{m-1,m+1}X_{m-1} + Y_2\\
&\qquad\quad\vdots\\
&A_{m-1}Y_{m-1} = a_{0,2m-2}X_0 + a_{1,2m-2}X_1 + \cdots + a_{m-1,2m-2}X_{m-1} + Y_{m-1}
\end{aligned}$$

By the isomorphism between the semidirect product S and the abstract group Ω, the previous identities in S correspond to identities in Ω. In fact, A_iX_j and

A_kY_r correspond in S, respectively, to the actions of z_i on x_j and of z_k on y_r in Ω.

Hence, from these last identities it follows that relations (30) take the following equivalent form in the abstract group Ω:

$$[z_s, x_r] = 1 \qquad \text{if} \quad r,\ s \in \{0, 1, \dots, m-1\}, \tag{30b}$$

since the action of z_s leaves $x_0, x_1, \dots, x_{m-1}$ fixed.

On the other hand, relations (31) take the following equivalent form:

$$\begin{aligned}
&[y_0, z_0^{-1}] = x_0^{-1},\\
&[y_1, z_0^{-1}] = x_1^{-1},\\
&\qquad\vdots\\
&[y_{m-1}, z_0^{-1}] = x_{m-1}^{-1},\\
&[y_0, z_1^{-1}] = x_1^{-1},\\
&[y_1, z_1^{-1}] = x_2^{-1},\\
&\qquad\vdots,\\
&[y_{m-2}, z_1^{-1}] = x_{m-1}^{-1},\\
&[y_{m-1}, z_1^{-1}] = x_0^{-a_{0,m}} \cdots x_{m-1}^{-a_{m-1,m}},\\
&\qquad\vdots\\
&[y_0, z_{m-2}^{-1}] = x_{m-2}^{-1},\\
&[y_1, z_{m-2}^{-1}] = x_{m-1}^{-1},\\
&[y_2, z_{m-2}^{-1}] = x_0^{-a_{0,m}} \dots x_{m-1}^{-a_{m-1,m}},\\
&\qquad\vdots\\
&[y_{m-1}, z_{m-2}^{-1}] = x_0^{-a_{0,2m-3}} \dots x_{m-1}^{-a_{m-1,2m-3}},\\
&[y_0, z_{m-1}^{-1}] = x_{m-1}^{-1},\\
&[y_1, z_{m-1}^{-1}] = x_0^{-a_{0,m}} \dots x_{m-1}^{-a_{m-1,m}},\\
&\qquad\vdots\\
&[y_{m-1}, z_{m-1}^{-1}] = x_0^{-a_{0,2m-2}} \dots x_{m-1}^{-a_{m-1,2m-2}}.
\end{aligned} \tag{31b}$$

Notice that in transforming relations (31) into (31b) we have used the fact that $x_0, \dots, x_{m-1}$ commute each other in Ω.

Let us now consider the correspondence given by:

$$z_r \mapsto x_{jk}(\alpha^r), \quad x_s \mapsto x_{ik}(\alpha^s), \qquad y_t \mapsto x_{ij}(\alpha^t), \tag{32}$$

where $r, s, t = 0, 1, \dots, m-1$, from the set $\{z_0, \dots, z_{m-1}, x_0 \dots, x_{m-1}, y_0, \dots, y_{m-1}\}$ in the group $P(i, j, k)$. Let us observe that, by virtue of the previous correspondence, relations (14) correspond to (25), (15) to (26), (11) to (27), (12) to (28), (13) to (29), (16) to (30b).

Now, let us examine relations (17) in connection with relations (31b).

Choosing suitable integer exponents (considered mod p) $\lambda_0, \lambda_1, \ldots, \lambda_{m-1}, \mu_0, \mu_1, \ldots, \mu_{m-1}$ in (17) and keeping into account (20), gives at once that all relations (31b) are satisfied in $P(i, j, k)$ with $x_{ij}(\alpha^r)$ in place of y^r, with $x_{jk}(\alpha^s)$ in place of z_s and with $x_{ik}(\alpha^l)$ in place of x_l. For example, setting $\lambda_0 = \cdots = \lambda_{m-2} = 0$, $\lambda_{m-1} = 1$, $\mu_0 = 0 \cdots = \mu_{m-2} = 0$, $\mu_{m-1} = -1$, we have (by (20)):

$$(\lambda_0 + \lambda_1\alpha + \cdots + \lambda_{m-1}\alpha^{m-1})(\mu_0 + \mu_1\alpha + \cdots + \mu_{m-1}\alpha^{m-1}) = \\ -\alpha^{2m-2} = -a_{0,2m-2} - a_{1,2m-2}\alpha - \cdots - a_{m-1,2m-2}\alpha^{m-1}.$$

Hence

$$l_0 = -a_{0,2m-2}, \qquad l_1 = -a_{1,2m-2}, \qquad \ldots, \qquad l_{m-1} = -a_{m-1,m+1},$$

by which we obtain that

$$[x_{ij}(\alpha^{m-1}), x_{jk}(\alpha^{m-1})^{-1}] = x_{ik}(1)^{-a_{0,2m-2}} \ldots x_{ik}(\alpha^{m-1})^{-a_{m-1,2m-2}},$$

corresponding to the relation

$$[y_{m-1}, z_{m-1}^{-1}] = x_0^{-a_{0,2m-2}} \ldots x_{m-1}^{-a_{m-1,2m-2}}$$

given in (31b). We can proceed analogously to verify that all relations (31b) are satisfied. Consequently, by virtue of Proposition 2, there exists an epimorphism from the abstract group Ω in $P(i, j, k)$. On the other hand, Ω is isomorphic to the semidirect product $S = \mathbf{Z}_p^m \ltimes (\mathbf{Z}_p^m \times \mathbf{Z}_p^m)$, thus $|\Omega| = p^{3m} = |P(i, j, k)|$; therefore Ω is isomorphic to the subgroup $P(i, j, k)$. Hence, in relations (17) we can eliminate all those that do not appear in (31b). Then, having fixed distinct i, j, $k \in \{1, \ldots, n\}$, the relations that involve the elements in (10) are (11)–(16), as well as the following (which come from (17) after the above-mentioned reduction):

$$\begin{aligned}
&[x_{ij}(1), x_{jk}(1)^{-1}] = x_{ik}(1)^{-1},\\
&[x_{ij}(\alpha), x_{jk}(1)^{-1}] = x_{ik}(\alpha)^{-1},\\
&\qquad\vdots\\
&[x_{ij}(\alpha^{m-2}), x_{jk}(1)^{-1}] = x_{ik}(\alpha^{m-2})^{-1},\\
&[x_{ij}(\alpha^{m-1}), x_{jk}(1)^{-1}] = x_{ik}(\alpha^{m-1})^{-1},\\
&[x_{ij}(1), x_{jk}(\alpha)^{-1}] = x_{ik}(\alpha)^{-1},\\
&[x_{ij}(\alpha), x_{jk}(\alpha)^{-1}] = x_{ik}(\alpha^2)^{-1},\\
&\qquad\vdots\\
&[x_{ij}(\alpha^{m-2}), x_{jk}(\alpha)^{-1}] = x_{ik}(\alpha^{m-1})^{-1},\\
&[x_{ij}(\alpha^{m-1}), x_{jk}(\alpha)^{-1}] = x_{ik}(1)^{-a_{0,m}} \ldots x_{ik}(\alpha^{m-1})^{-a_{m-1,m}},\\
&\qquad\vdots\\
&[x_{ij}(1), x_{jk}(\alpha^{m-1})^{-1}] = x_{ik}(\alpha^{m-1})^{-1},\\
&[x_{ij}(\alpha), x_{jk}(\alpha^{m-1})^{-1}] = x_{ik}(1)^{-a_{0,m}} \ldots x_{ik}(\alpha^{m-1})^{-a_{m-1,m}},\\
&\qquad\vdots\\
&[x_{ij}(\alpha^{m-1}), x_{jk}(\alpha^{m-1})^{-1}] = x_{ik}(1)^{-a_{0,2m-2}} \ldots x_{ik}(\alpha^{m-1})^{-a_{m-1,2m-2}}
\end{aligned} \tag{E3$'$}$$

Notice that, for i, j and k fixed, there are m^2 relations (17b), whereas relations (17) are p^{2m} in number. In conclusion, we have obtained the following result:

Proposition 3. *Let n be an integer ≥ 3, m an integer ≥ 1, p an odd prime and $d = p^m$. Let $\alpha \in \mathbf{F}_d$ such that $\{1, \alpha \ldots, \alpha^{m-1}\}$ is a basis of $\mathbf{F}_d$ as a vector space over $\mathbf{F}_p$. Then, the special linear group $SL_n(\mathbf{F}_d)$ has a presentation with the following generator and relations:*

Generators :

$$x_{ij}(1), \ldots, x_{ij}(\alpha^{m-1}), \quad \textit{where } i, j \in \{1, \ldots, n\} \textit{ and } i \neq j.$$

Relations :

$$x_{ij}(1)^p = x_{ij}(\alpha)^p = \cdots = x_{ij}(\alpha^{m-1})^p = 1; \qquad \text{(E1}'\text{)}$$

$$[x_{ij}(\alpha^r), x_{ij}(\alpha^s)] = 1, \quad \textit{if } r, s \in \{0, 1, \ldots, m-1\}; \qquad \text{(E1}''\text{)}$$

$$[x_{ij}(\alpha^r), x_{kl}(\alpha^s)] = 1, \quad \textit{if } j \neq k \textit{ and } i \neq l, \qquad \text{(E2}'\text{)}$$
$$\textit{where } \; r, s \in \{0, 1, \ldots, m-1\};$$

relations given in (E3′), where i, j and k are distinct.

Example. In the case of $SL_3(\mathbf{F}_p)$ we have six generators a, b, c, d, f, which can be respectively identified with the following matrices:

$$x_{12}(1) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad x_{13}(1) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$x_{21}(1) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad x_{23}(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$x_{31}(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \qquad x_{32}(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Relations (E1′) are the following:

$$a^p = b^p = c^p = d^p = e^p = f^p = 1.$$

Relations (E1″) become superflous.

Relations (E2′) are given by:

$$ab = ba, af = fa, bd = db,$$
$$cd = dc, ce = ec, ef = fe.$$

Relations (E3), entirely written before their reduction, are $6(p-1)^2$ in number and look as follows:

$$a^r d^s a^{-r} d^{-s} = b^{rs}, \quad \text{with } 1 \leq r, \; s \leq p-1 \pmod{p}$$
$$b^r f^s b^{-r} f^{-s} = a^{rs}, \quad \text{with } 1 \leq r, \; s \leq p-1 \pmod{p}$$
$$c^r b^s c^{-r} b^{-s} = d^{rs}, \quad \text{with } 1 \leq r, \; s \leq p-1 \pmod{p}$$
$$d^r e^s d^{-r} e^{-s} = c^{rs}, \quad \text{with } 1 \leq r, \; s \leq p-1 \pmod{p}$$
$$e^r a^s e^{-r} a^{-s} = f^{rs}, \quad \text{with } 1 \leq r, \; s \leq p-1 \pmod{p}$$
$$f^r c^s f^{-r} c^{-s} = e^{rs}, \quad \text{with } 1 \leq r, \; s \leq p-1 \pmod{p}.$$

Just as in the general case of $SL_n(\mathbf{F}_d)$, with $n \geq 3$, the relations are reduced to (E3′), which are the following six:

$$\begin{aligned}
[a, d^{-1}] &= ad^{-1}a^{-1}d = b^{-1}\\
[b, f^{-1}] &= bf^{-1}b^{-1}f = a^{-1}\\
[c, b^{-1}] &= cb^{-1}c^{-1}b = d^{-1}\\
[d, e^{-1}] &= de^{-1}d^{-1}e = c^{-1}\\
[e, a^{-1}] &= ea^{-1}e^{-1}a = f^{-1}\\
[f, c^{-1}] &= fc^{-1}f^{-1}c = e^{-1}.
\end{aligned}$$

To complete the argument let us list the six subgroups $P(i, j, k)$ (with i, j, k distinct) that occur in the case of $SL_3(\mathbf{F}_p)$ and that are all isomorphic to the semidirect product $\mathbf{Z}_p \ltimes_\varphi (\mathbf{Z}_p \times \mathbf{Z}_p)$:

$$P(1, 2, 3) = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbf{F}_p \right\} = \langle a, b, d \rangle,$$

$$P(1, 3, 2) = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & z & 1 \end{pmatrix} : x, y, z \in \mathbf{F}_p \right\} = \langle a, b, f \rangle,$$

$$P(2, 1, 3) = \left\{ \begin{pmatrix} 1 & 0 & x \\ y & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbf{F}_p \right\} = \langle b, c, d \rangle,$$

$$P(2, 3, 1) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ x & 1 & y \\ z & 0 & 1 \end{pmatrix} : x, y, z \in \mathbf{F}_p \right\} = \langle c, d, e \rangle,$$

$$P(3, 1, 2) = \left\{ \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ y & z & 0 \end{pmatrix} : x, y, z \in \mathbf{F}_p \right\} = \langle a, e, f \rangle,$$

$$P(3, 2, 1) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & z & 1 \end{pmatrix} : x, y, z \in \mathbf{F}_p \right\} = \langle c, e, f \rangle.$$

Notice that, in the particular case of $SL_3(\mathbf{F}_p)$, subgroups $P(i, j, k)$ are all p-Sylow subgroups since $\left|SL_3(\mathbf{F}_p)\right| = 2p^3(p^3 - 1)(p^2 - 1)$.

Acknowledgements. I would like to thank R. Dvornicich for having pointed out this problem to me and for his suggestions.

References

1. Francis, T.A.: Presentations of the special and general linear groups. J. Algebra **169**, 943–964 (1994)
2. Hahn, A.J., O'Meara, O.T.: The Classical Groups and K-Theory. New York-Berlin: Springer 1989

3. Johnson, D.L.: Presentation of Groups. Cambridge, UK: Cambridge University Press 1976
4. van der Kallen, M.: Another presentation for Steinberg groups. Indag. Math. **39**, 304–312 (1977)