

$SL_n(F)$ Equals its Own Derived Group

Jorge Maciel

BMCC-The City University of New York, CUNY
199 Chambers street, New York, NY 10007, USA
maciel@cims.nyu.edu

Abstract. We prove that $SL_n(F_q)$ is equal to its own commutator group except when $n = 2$ and $q = 2$ or $q = 3$, by using the fact that every element in the center Z of $SL_n(F_q)$ can be written in a commutator form $[A, B]$, where $A, B \in SL_n(F_q)$.

Mathematics Subject Classification: Primary 20H20, 15A04

Keywords: Central extension, Commutator group, General group, Projective special linear group, Special linear group

INTRODUCTION

Definition 1.1. A group extension

$$F \xrightarrow{i} E \xrightarrow{j} G$$

of a group G by a group F consists of a group E , an injective homomorphism $i : F \rightarrow E$, and a surjective homomorphism $j : E \rightarrow G$, such that $\mathbf{Im} i = \mathbf{Ker} j$.

Group extensions need only be constructed up to isomorphism. In detail, an equivalence of group extensions

$$F \xrightarrow{i} E \xrightarrow{j} G$$

$$F \xrightarrow{i'} E' \xrightarrow{j'} G$$

of G by F is an isomorphism $\theta : E \rightarrow E'$ such that the diagram

$$\begin{array}{ccccc} F & \xrightarrow{i} & E & \xrightarrow{j} & G \\ & & \downarrow \theta & & \\ F & \xrightarrow{i'} & E' & \xrightarrow{j'} & G \end{array}$$

commutes, that is, $\theta \circ i = i'$ and $j' \circ \theta = j$.

Definition 1.2. *An extension*

$$F \xrightarrow{i} E \xrightarrow{j} G$$

is called **central** if the image $i(F)$ is contained in the center of E . This is possible only if F is Abelian.

Definition 1.3. *An element ζ of a field F is said to be a **root of unity** if there exists an integer $n > 0$ such that $\zeta^n = 1$; for every integer $n > 0$ such that $\zeta^n = 1$, ζ is called an n -th root of unity.*

It amounts to say that the roots of unity are the elements of finite order of the multiplicative group F^* of non-zero elements of F . The roots of unity form a subgroup $\mu_\infty(F)$ of F^* , the n -th roots form a subgroup $\mu_n(F)$ of $\mu_\infty(F)$. We have $\mu_\infty(F) = \bigcup_{n \geq 1} \mu_n(F)$ and $\mu_n(F) \subset \mu_m(F)$ if m divides n . For every root of unity ζ there exists a least integer $n \geq 1$ such that ζ belongs to $\mu_n(F)$, namely the order of ζ in the group F^* .

Definition 1.4. *An n -th root of unity is said to be **primitive** if it is of order n .*

If there exists a primitive n -th root of unity ζ in F , the group $\mu_n(F)$ is of order n and is generated by ζ .

Let F be a field and n be a positive integer. We denote by $M_n(F)$ the ring of square matrices of order n over F . By an $n \times n$ **determinant** we shall mean a mapping

$$\mathbf{det} : M_n(F) \rightarrow F$$

which, when viewed as a function of the column vectors A^1, \dots, A^n of a matrix A , is multilinear alternating, and such that $\mathbf{det}(I) = 1$. It is shown that if determinants exist, they are unique. If A^1, \dots, A^n are the column vectors of dimension n , of the matrix $A = (a_{ij})$, then

$$\mathbf{det}(A^1, \dots, A^n) = \sum_{\sigma} \epsilon(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}$$

where the sum is taken over all permutations σ of $\{1, \dots, n\}$, and $\epsilon(\sigma)$ is the sign of the permutation.

The **general linear group** $\mathrm{GL}_n(F)$ of invertible elements of $M_n(F)$ is just the inverse image under the mapping $\mathbf{det} : M_n(F) \rightarrow F$ of the multiplicative group F^* of invertible elements of F . The mapping $\mathbf{det} : M_n(F) \rightarrow F$ is moreover surjective and therefore so is the homomorphism $\mathbf{det} : \mathrm{GL}_n(F) \rightarrow F^*$, since for all $\lambda \in F$,

$$\mathbf{det}(\mathbf{diag}(\lambda, 1, \dots, 1)) = \lambda.$$

The kernel of the surjective homomorphism $\mathbf{det} : \mathrm{GL}_n(F) \rightarrow F^*$ is a normal subgroup of $\mathrm{GL}_n(F)$; it is denoted by $\mathrm{SL}_n(F)$ and is called the **special linear group** of square matrices of order n over F .

We note that if a matrix M commutes with every element of $\mathrm{SL}_n(F)$, then it must be a scalar matrix. Indeed, just the commutation with elementary matrices

$$E_{ij}(1) = I_n + 1_{ij}$$

show that M commutes with all matrices 1_{ij} (having 1 in the ij -component, 0 otherwise), so M commutes with all matrices, and is a scalar matrix. Taking the determinant shows that the center consists of $\mu_n(F)I_n$.

Definition 1.5. *Let Z be the center of $\mathrm{SL}_n(F)$, that is the group of scalar matrices such that the scalar is an n -th root of unity. We define the **projective special linear group** of square matrices of order n over F by the quotient group*

$$\mathrm{PSL}_n(F) = \mathrm{SL}_n(F)/Z.$$

2. THE GROUP $\mathrm{SL}_n(F)$ AS A CENTRAL EXTENSION

Let F be a field and let μ be a primitive p^n -th root of unity in F .

Note that $\mathrm{SL}_n(F)$ is a central group extension of $\mathrm{PSL}_n(F)$ by $\mu_n(F)$. Indeed, we have the central extension

$$\mu_n(F) \xrightarrow{i} \mathrm{SL}_n(F) \xrightarrow{j} \mathrm{PSL}_n(F)$$

where i is the injective homomorphism defined by $i(\mu) = \mu I_n$, j is the surjective homomorphism defined by $j(A) = \bar{A}$, and $\mathbf{Im} i = \mathbf{Ker} j$.

Theorem 2.1. *Let n be divisible by p^m where p is prime. Then the scalar matrix μI_n can be written in a commutator form $[A, B] = ABA^{-1}B^{-1}$, where $A, B \in \mathrm{SL}_n(F)$.*

Proof. We have the following possibilities:

1. Let p be an odd prime and A, B be two square matrices of order p^m over the field F such that $A = (a_{i,j}) = (\delta_{i,j}\mu^{i-1})$, and $B = (b_{i,j})$ with $b_{i+1,i} = b_{1,p^m} = 1$, and $b_{i,j} = 0$ otherwise. Then A and B belong to $\mathrm{SL}_{p^m}(F)$, and $[A, B] = ABA^{-1}B^{-1} = \mu I_{p^m}$.
2. If $p = 2$ and $n = 1$, then the matrices $A = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$, where $a^2 + b^2 = -1$, and $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ satisfy the required condition. Indeed, $[A, B] = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -a & -b \\ -b & a \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. For a finite field F_q , with q odd, such a and b always exist. If $F = F_q$ and $q = 4k + 1$ then -1 is a square and we can take $a = i$, where $i^2 = -1$, and $b = 0$. If $q = 4k + 3$ then the set of all elements of the form $x^2 + y^2$ coincides with F_q . Indeed, it contains all

quadratic residues x^2 , and it is invariant under the multiplication by an arbitrary element z^2 , where $z \in F_q$. Therefore, if it contains at least one non-quadratic element, then it coincides with F_q . If not, then quadratic residues form an additive subgroup in F_q . However, F_q does not have an additive subgroup of index 2 for odd q . Therefore, F_q is the set of elements of the form $x^2 + y^2$. In particular, there are a and b such that $a^2 + b^2 = -1$, and they provide entries for A .

3. If $p = 2$ and $m > 1$, we select $A = \sigma_1 X$ and $B = Y \sigma_2$ where X and Y are diagonal matrices and σ_1, σ_2 are commuting permutation matrices. In this case

$$\begin{aligned} [A, B] &= ABA^{-1}B^{-1} \\ &= \sigma_1 XY \sigma_2 X^{-1} \sigma_1^{-1} \sigma_2^{-1} Y^{-1} \\ &= \sigma_1 XY \sigma_2 X^{-1} \sigma_2^{-1} \sigma_1^{-1} Y^{-1} \end{aligned}$$

since σ_1 and σ_2 commute. Therefore the equations

$$(2.1) \quad ABA^{-1}B^{-1} = \mu I$$

and

$$(2.2) \quad XY(\sigma_2 X^{-1} \sigma_2^{-1})(\sigma_1^{-1} Y^{-1} \sigma_1) = \mu I$$

are equivalent, we note also that the matrices X , Y , $(\sigma_2 X^{-1} \sigma_2^{-1})$, and $(\sigma_1^{-1} Y^{-1} \sigma_1)$ are diagonal.

Suppose now that σ_1 has order 2^k and σ_2 has order 2^{m-k} , where $k \geq 1$ and $m - k \geq 1$. Then the corresponding linear space has a special coordinate system $z_{i,j}$, where $1 \leq i \leq 2^k$ and $1 \leq j \leq 2^{m-k}$ with the property that σ_1 cyclically permutes coordinates $z_{i,j}$ with the same index i and σ_2 cyclically permutes coordinates $z_{i,j}$ with the same index j .

Therefore, if we denote by $x_{i,j}$ and $y_{i,j}$ the diagonal elements of the matrices X and Y respectively, then equation (2.2) becomes equivalent to a series of equations

$$(2.3) \quad x_{i,j} y_{i,j} x_{i+1(\text{mod } 2^k),j}^{-1} y_{i,j+1(\text{mod } 2^{m-k})}^{-1} = \mu$$

for the diagonal elements. If we denote by

$$u_{i,j} =: x_{i,j} x_{i+1(\text{mod } 2^k),j}^{-1}$$

and

$$v_{i,j} =: y_{i,j} y_{i,j+1(\text{mod } 2^{m-k})}^{-1},$$

then

$$\prod_i u_{i,j} = \prod_j v_{i,j} = 1.$$

Equation (2.3) above becomes

$$u_{i,j} = \mu v_{i,j}^{-1}$$

and hence we have obtained equations only for the parameters $u_{i,j}$.

Thus our initial matrix equation (2.1) has been reduced to equations for $u_{i,j}$:

$$\prod_i u_{i,j} = 1, \quad \prod_j u_{i,j} = \mu^{2^{m-k}}.$$

These parameters $u_{i,j}$ define the complementary set of parameters $v_{i,j}$. Notice that for any $u_{i,j}$ and $v_{i,j}$ satisfying $\prod_i u_{i,j} = \prod_j v_{i,j} = 1$, we can find $x_{i,j}$ and $y_{i,j}$ so that

$$u_{i,j} = x_{i,j} x_{i+1(\text{mod } 2^k),j}^{-1}, \quad v_{i,j} = y_{i,j} y_{i,j+1(\text{mod } 2^{m-k})}^{-1},$$

and hence we can obtain solutions of the equation (2.1). Thus there are many matrix pairs A, B that satisfy equation (2.1).

4. If n is divisible by p^m , then matrices \mathbf{A} and \mathbf{B} , consisting of n/p^m diagonal blocks of matrices A and B respectively, also satisfy the relation

$$[\mathbf{A}, \mathbf{B}] = \mathbf{A} \mathbf{B} \mathbf{A}^{-1} \mathbf{B}^{-1} = \mu I_n.$$

The Theorem follows. □

This fact appeared previously in [BM].

Example 2.2. Let F_q be a field and let μ be a primitive p^n -th root of unity in F_q , where $n > 1$ and $4 \mid q - 1$. We decompose 2^n coordinates into two groups of order 2^{n-1} and take the diagonal matrix $X = \mathbf{diag}([1, 1, \dots, i], [1, 1, \dots, -i])$, where brackets show the boundaries of each block. The element i , with $i^2 = -1$, is contained in F_q since, by our assumption, 4 divides $q - 1$. Similarly, take the diagonal matrix $Y = \mathbf{diag}([1, \mu, \dots, \mu^{2^{n-1}-1}], [\mu, \mu^2, \dots, \mu^{2^{n-1}}])$. Let σ_1 be the permutation which permutes variables cyclically within each block, and σ_2 be the permutation of order 2 which interchanges these two blocks of variables. Recall that $\mu^{2^{n-1}} = -1$. Then

$$X(\sigma_2 X^{-1} \sigma_2^{-1}) = \mathbf{diag}([-1, 1, \dots, 1], [-1, 1, \dots, 1])$$

and

$$Y(\sigma_1^{-1}Y^{-1}\sigma_1) = \mathbf{diag}([-\mu, \mu, \dots, \mu], [-\mu, \mu, \dots, \mu])$$

and hence

$$XY(\sigma_2X^{-1}\sigma_2^{-1})(\sigma_1^{-1}Y^{-1}\sigma_1) = \mu I.$$

If we take $A = \sigma_1X$, $B = Y\sigma_2 \in \mathrm{SL}_{2n}(F)$, then $[A, B] = ABA^{-1}B^{-1} = \mu I_{2n}$.

Example 2.3. Let F_q be a field and let μ be a p^n -th root of unity in F_q of order m . If $p = 2$ and $n = 2$, consider the permutation matrices

$$\sigma_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

of the group $\mathrm{SL}_4(F_q)$. Since σ_1 and σ_2 commute, it is seen that, for every pair of diagonal matrices

$$X = \begin{pmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} y_1 & 0 & 0 & 0 \\ 0 & y_2 & 0 & 0 \\ 0 & 0 & y_3 & 0 \\ 0 & 0 & 0 & y_4 \end{pmatrix}$$

in $\mathrm{SL}_4(F_q)$, the commutator

$$[X\sigma_1, Y\sigma_2]$$

is a diagonal matrix in $\mathrm{SL}_4(F_q)$. Taking account of this, it is immediately seen that the scalar matrix μI_4 can be expressed in the form of commutator $[X\sigma_1, Y\sigma_2]$ for some diagonal matrices $X, Y \in \mathrm{SL}_4(F_q)$. For, the definition of product of matrices gives

$$[X\sigma_1, Y\sigma_2] = \begin{pmatrix} x_1y_2x_3^{-1}y_1^{-1} & 0 & 0 & 0 \\ 0 & x_2y_1x_4^{-1}y_2^{-1} & 0 & 0 \\ 0 & 0 & x_3y_4x_1^{-1}y_3^{-1} & 0 \\ 0 & 0 & 0 & x_4y_3x_2^{-1}y_4^{-1} \end{pmatrix}$$

Then necessarily

$$(2.4) \quad x_1 y_2 x_3^{-1} y_1^{-1} = \mu$$

$$(2.5) \quad x_2 y_1 x_4^{-1} y_2^{-1} = \mu$$

$$(2.6) \quad x_3 y_4 x_1^{-1} y_3^{-1} = \mu$$

$$(2.7) \quad x_4 y_3 x_2^{-1} y_4^{-1} = \mu$$

Multiplying conditions (2.4) and (2.5) gives

$$x_1 x_2 (x_3 x_4)^{-1} = \mu^2.$$

Similarly, multiplying (2.6) and (2.7) gives

$$x_3 x_4 (x_1 x_2)^{-1} = \mu^2.$$

Note that the additional hypothesis

$$\mathbf{det} X = x_1 x_2 x_3 x_4 = 1$$

implies that

$$(x_1 x_2)^2 = \mu^2 \quad \text{and} \quad (x_3 x_4)^2 = \mu^2.$$

Then the above three relations show that

$$x_1 x_2 = \pm \mu \quad \text{and} \quad x_3 x_4 = \pm \mu$$

when $\mu^2 = 1$ and

$$x_1 x_2 = \pm \mu \quad \text{and} \quad x_3 x_4 = \mp \mu$$

when $\mu^2 = -1$.

On the other hand, multiplying conditions (2.4) and (2.6) gives

$$y_2 y_4 (y_1 y_3)^{-1} = \mu^2.$$

Similarly, multiplying conditions (2.5) and (2.7) gives

$$y_1 y_3 (y_2 y_4)^{-1} = \mu^2.$$

Note that the hypothesis

$$\mathbf{det} Y = y_1 y_2 y_3 y_4 = 1$$

on $\mathbf{det} Y$ therefore implies that

$$(y_2y_4)^2 = \mu^2 \quad \text{and} \quad (y_1y_3)^2 = \mu^2.$$

Then

$$y_2y_4 = \pm\mu \quad \text{and} \quad y_1y_3 = \pm\mu$$

when $\mu^2 = 1$ and

$$y_2y_4 = \pm\mu \quad \text{and} \quad y_1y_3 = \mp\mu$$

when $\mu^2 = -1$.

In particular we derive from these results that the matrices

$$X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

satisfy the relation

$$[X\sigma_1, Y\sigma_2] = \mu I_4$$

when $m = 2$.

Similarly, the matrices

$$X = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

satisfy the relation

$$[X\sigma_1, Y\sigma_2] = \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & -\mu^2\mu & 0 & 0 \\ 0 & 0 & -\mu^2\mu & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix} = \mu I_4$$

when $m = 4$.

In conformity with the above results, we shall distinguish two cases:

(a) If $m = 2$, let A and B be two square matrices of order 4 over the field F_q which can be written in the form

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ \mu & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & \mu & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mu \\ \mu & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

with respect to the same basis. It follows from the method of calculating a determinant that $\det A = 1$ and $\det B = 1$. The definition of product of matrices gives

$$ABA^{-1}B^{-1} = \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix}$$

(b) If $m = 4$, let A and B be two square matrices of order 4 over the field F_q which can be written in the form

$$A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ \mu & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & \mu & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & \mu \\ \mu & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

with respect to the same basis. The method of calculating a determinant and the hypothesis on μ imply that $\det A = 1$ and $\det B = 1$. Now, it is immediate that A and B satisfy the desired condition

$$ABA^{-1}B^{-1} = \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix}.$$

Theorem 2.4. *Let p be a prime number and F be a finite field of order $q = p^k$. If $n \geq 3$ ($n \geq 2$ if $q \geq 5$), then $SL_n(F)$ is equal to its own commutator group.*

Proof. The commutator subgroup $SL_n^c(F) = [SL_n(F), SL_n(F)]$ is the smallest normal subgroup N of $SL_n(F)$ such that $SL_n(F)/N$ is abelian. Theorem 2.1 readily implies that the center Z of $SL_n(F)$ is a normal subgroup of $SL_n^c(F)$.

By the First Isomorphism Theorem,

$$SL_n^c(F)/Z \trianglelefteq PSL_n(F)$$

and

$$PSL_n(F)/(SL_n^c(F)/Z) \cong SL_n(F)/SL_n^c(F).$$

Since $PSL_n(F)$ is a finite simple group for every finite field F of order q and $n \geq 3$ ($n \geq 2$ if $q \geq 5$), it follows that $SL_n^c(F)$ is either Z or $SL_n(F)$.

On the other hand, a non-cyclic simple group is not solvable. Then

$$SL_n^c(F) = SL_n(F).$$

□

REFERENCES

- [1] Bourbaki N. *Elements of Mathematics, Algebra I*. Addison-Wesley publishing company (1973).
- [2] Bogomolov F. A., Maciel J., Tihomir P. *Unramified Brauer Groups of Finite Simple Groups of Lie Type A_ℓ* . American Journal of Mathematics 126 (2004), 935-949.
- [3] Grillet P. A., *Algebra*. John Wiley & sons, Inc. (1999).

Received: December 14, 2007