1970

The General Linear Group Related Groups

J. William Beck
Eastern Illinois University

THE GENERAL LINEAR GROUP

—

RELATED GROUPS

(TITLE)

BY

J. William Beck

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

IN THE GRADUATE SCHOOL, EASTERN ILLINOIS UNIVERSITY
CHARLESTON, ILLINOIS

1970

YEAR

I HEREBY RECOMMEND THIS THESIS BE ACCEPTED AS FULFILLING THIS PART OF THE GRADUATE DEGREE CITED ABOVE

8/14/70

DATE

ADVISER

3 September 1970

DATE

DEPARTMENT HEAD

[redacted]

ACKNOWLEDGEMENT

The student wishes to thank Dr. Jon M. Laible for his friendly and invaluable guidance.

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

It is the purpose of this paper to study some of the properties of the general linear group and its subgroups and quotient groups.

The general linear group will be considered as the group of linear transformations of a vector space onto itself under composition of mappings and as the group of nonsingular matrices under matrix multiplication (chapter I). Several notations are used to denote the general linear group. They include: GL(m,F), (Rotman, 1965, p. 155); GLH(m,q), (Dickson, 1958, p. 76); and L(F,m), (Schenkman, 1965, p. 116).

In chapter II, the general linear group is discussed in more detail. Some of its normal subgroups such as its center and its commutator subgroup are introduced. The special linear group is then discussed in more detail since the quotient group of this group by its center is a source of simple groups of finite order. The orders of these groups are determined in the case where the underlying field is finite. Various notations used to denote the special linear group are: SL(m,F), (Rotman, 1965, p. 157); SLH(m,q), (Dickson, 1958, p. 82); and S(F,m), (Schenkman, 1965, p. 116).

The quotient group of the special linear group by its center, called the projective unimodular group, is then shown to be simple for all but two cases (chapter III). The projective unimodular group is, in some cases, not isomorphic to other known simple groups such as the alternating groups. Several notations are used to denote the projective unimodular group as well. They include PSL(m,F), (Rotman, 1965, p. 161);

LF(m,q), (Dickson, 1958, p. 87); and P(F,m), (Schenkman, 1965, p. 116).

Although all of the results of this paper are known, some of the proofs are original, e.g., theorem 12. Those proofs which are not original have been modified by the author in an attempt to make them more readible. In addition to the theory which is developed in the text of the paper, there are three tables. These tables, using the nonsingular matrices associated with the linear transformations, display the elements of the general linear groups of orders 6 and 48 and the projective unimodular group of order 12, and note some of the characteristics of these groups.

The following group theoretic notation will be used where convenient.

$H \Delta G$ shall mean that H is a normal subgroup of G.

G/H shall be the quotient group of G by H where $H \Delta G$.

[G:H] shall be the index of a subgroup H of G in G.

$|G|$ shall be the order of G.

Standard set theoretic notation will be used throughout.

$\delta_{ij} = 1$ if $i = j$, $\delta_{ij} = 0$ if $i \neq j$.

CHAPTER I

LINEAR TRANSFORMATIONS AND MATRICES

In this chapter, we will develop the fundamental concepts on which the rest of the work is based. We will show that under proper restrictions on the underlying vector space and under appropriate definitions for addition, multiplication, and scalar multiplication, the set of linear transformations forms an algebra. We then define corresponding operations for matrices and note that the set of m by m matrices also forms an algebra. We then show the existence of an isomorphism between these two algebras. In this way, we can, depending on which approach is more convenient, develop the rest of the work by looking at the general linear group as a group of linear transformations or as a group of square matrices under matrix multiplication.

Definition 1. Let U and V be vector spaces over a field F. A mapping f of U into V is a linear transformation of U into V if and only if f satisfies the following:

$$(x + y)f = xf + yf \quad \text{for all } x \in U \text{ and } y \in U,$$

$$(ax)f = a(xf) \quad \text{for all } a \in F \text{ and } x \in U.$$

Denote by L(U,V) the set of all linear transformations of U into V.

We may define addition of two elements of L(U,V) by:

$$x(f + g) = xf + xg \quad \text{for all } x \in U. \tag{1}$$

We may also define scalar multiplication of an element f of L(U,V) by an element a of F by:

(2) $x(af) = a(xf)$ for all $x\varepsilon U$.

Lemma 1.1. Let U and V be vector spaces over a field F. L(U,V) is a vector space under the operations defined above.

Proof: Let f and g be in L(U,V). If $x,y\varepsilon U$, then

$$(x + y)(f + g) = (x + y)f + (x + y)g = xf + yf + xg + yg$$
$$= xf + xg + yf + yg = x(f + g) + y(f + g).$$

The preceeding equalities follow directly from (1) and from definition 1.

Let f and g be in L(U,V). If $a\varepsilon F$ and $x\varepsilon U$, then

$$(ax)(f + g) = (ax)f + (ax)g = a(xf) + a(xg)$$
$$= a(xf + xg) = a[x(f + g)].$$

The above equalities follow from (2) and definition 1. Therefore $(f+g)\varepsilon L(U,V)$. L(U,V) forms an abelian group under +. The identity is $0\varepsilon L(U,V)$ (defined by $x0 = 0$ for every $x\varepsilon U$) since $x(f + 0) = xf + x0 = xf$ and $x(0 + f) = x0 + xf = xf$. The additive inverse for $f\varepsilon L(U,V)$ is $-f$ (defined by $x(-f) = -(xf)$ for all $x\varepsilon U$) since for $x\varepsilon U$, $x[f + (-f)] = xf + x(-f) = xf - xf = 0$. Associativity and commutativity for L(U,V) follow from the corresponding properties in V.

The following arguments which complete the proof use properties (1), (2) and definition 1. We have $a(f + g) = af + ag$ for all $a\varepsilon F$ and $f,g\varepsilon L(U,V)$ since for each $x\varepsilon U$,

$$x[a(f + g)] = a[x(f + g)] = a(xf + xg)$$
$$= a(xf) + a(xg) = x(af) + x(ag) = x(af + ag).$$

Also $(a + b)f = af + bf$ for all a and b in F and $f\varepsilon L(U,V)$ since for $x\varepsilon U$,

$$x[(a + b)f] = (a + b)(xf)$$

$$= a(xf) + b(xf) = x(af + bf).$$

Further, $(ab)f = a(bf)$ for all $a,b \in F$ and every $f \in L(U,V)$ since if $x \in U$,

$$x[(ab)f] = (ab)(xf) = a[b(xf)]$$

$$= a[x(bf)] = x[a(bf)].$$

Finally, $x(1f) = 1(xf) = xf$. Thus $L(U,V)$ is a vector space over F.

If $f \in L(U,V)$ and $g \in L(V,W)$ where U, V, and W are vector spaces over F, then we define:

(3) $\qquad x(fg) = (xf)g$ for all $x \in U$, and

(4) $\qquad (ax)fg = [(ax)f]g$ for all $a \in F$.

Then for $x,y \in U$,

$$(x + y)fg = [(x + y)f]g$$

$$= (xf + yf)g = x(fg) + y(fg).$$

So that $fg \in L(U,W)$ by (1), (3) and definition 1. Also if $a \in F$ and $x \in U$, then for every $f \in L(U,V)$ and $g \in L(V,W)$, by definition 1, (3) and (4),

$$(ax)fg = [(ax)f]g = [a(xf)]g$$

$$= a[(xf)g] = a[x(fg)].$$

Hence the composition mapping fg is also a linear transformation of U into W.

Theorem 1. If U is a vector space over a field F, $L(U,U)$ is an algebra over F where the addition and scalar multiplication are defined as in lemma 1.1 and the multiplication of two elements f and g of $L(U,U)$ is defined in (3) above.

Proof: By lemma 1.1, $L(U,U)$ is a vector space over F. Associativity for multiplication follows directly from (3), while the distributive property of composition of mappings over addition holds due to (3) and (1). If $x \epsilon U$, then for all $a \epsilon F$ and $f,g \epsilon L(U,U)$, using (2) and (3); $x[a(fg)] = a[x(fg)] = (xf)(ag) = x[f(ag)]$. Similarly $x[a(fg)] = x[(af)g]$, by (2), (3) and definition 1. Hence $L(U,U)$ is an algebra over F.

Corollary 1.1. If U and V are finite dimensional vector spaces with $\dim U = m$ and $\dim V = n$, then $\dim L(U,V) = mn$. In particular, $\dim L(U,U) = m^2$.

For a proof of the corollary see Herstein (1964, p. 145). We remark only that if $u_1, u_2, \ldots, u_m$ is a basis for U and $v_1, v_2, \ldots, v_n$ is a basis for V, then f_{ij} such that $u_i f_{ij} = v_j$ and $u_k f_{ij} = 0$ for i, $1 \leq i \leq m$ and j, $1 \leq j \leq n$, $k \neq i$, is the corresponding basis for $L(U,V)$.

Let M_{mn} be the set of all m by n matrices (a_{ij}) where the entries are elements of a field F. We shall define the sum of two elements (a_{ij}) and (b_{ij}) of M_{mn} by:

(5) $$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}).$$

If $a \epsilon F$ and (a_{ij}) is in M_{mn}, then we shall define scalar multiplication as follows:

(6) $$a(a_{ij}) = (aa_{ij}).$$

The following lemma and theorem follow from these definitions using m by n matrices E_{ij} having zeros for all entries except the $ij^{\underline{th}}$ entry which is 1, as the basis.

Lemma 2.1. M_{mn} is a vector space of dimension mn over F.

We may also define multiplication for matrices. If (a_{ij}) is in M_{mn} and (b_{ij}) is in $M_{n\ell}$, the product is defined by:

$$(a_{ij})(b_{jk}) = (c_{ik}) \text{ where } c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}. \tag{7}$$

Note that the product of an m by n matrix and an n by ℓ matrix is an m by ℓ matrix.

Theorem 2. If $m = n$, M_{mn} is an algebra over F where addition and scalar multiplication are as in (5) and (6) and multiplication is as defined in (7).

Theorem 3. Let U be a vector space of dimension m over a field F. M_{mm} and L(U,U) are isomorphic as algebras over F. These algebras are isomorphic in many ways, however there is a unique isomorphism defined relative to a fixed basis for U.

Proof: Let $u_1, u_2, \ldots, u_m$ be a basis for U. Let $f \varepsilon L(U,U)$ and $x = \sum_{i=1}^{m} b_i u_i$ be any element in U. Then $xf = (\sum_{i=1}^{m} b_i u_i)f = \sum_{i=1}^{m} b_i (u_i f)$. Thus the action of f on U is uniquely determined by the action of f on the basis $u_1, u_2, \ldots, u_m$. If $f \varepsilon L(U,U)$, $u_i f = \sum_{j=1}^{m} a_{ij}u_j$, $1 \le i \le m$, $a_{ij} \varepsilon F$. Define a mapping from L(U,U) to M_{mm} by $\emptyset : f \to (a_{ij})$. This mapping is onto since if $(a_{ij}) \varepsilon M_{mm}$, then there exists an $f \varepsilon L(U,U)$ such that $u_i f = \sum_{j=1}^{m} a_{ij}u_j$, $1 \le i \le m$ where the $a_{ij} \varepsilon F$ are uniquely determined by the basis and f. $\emptyset(f + g) = \emptyset(f) + \emptyset(g)$ since if (a_{ij}) is the matrix associated with f relative to $u_1, u_2, \ldots, u_m$ and if (b_{ij}) is the matrix associated with g relative to the same basis, then for each i, $1 \le i \le m$,

$$u_i(f + g) = u_i f + u_i g = \sum_{j=1}^{m} a_{ij}u_j + \sum_{j=1}^{m} b_{ij}u_j = \sum_{j=1}^{m} (a_{ij} + b_{ij})u_j.$$

If $a \varepsilon F$, then $\emptyset(af) = a\emptyset(f)$ since for each i, $1 \leq i \leq m$,

$$u_i(af) = a(u_i f) = a\sum_{j=1}^{m} a_{ij}u_j = \sum_{j=1}^{m} (aa_{ij})u_j.$$

To see that multiplication is also preserved under $\emptyset$,

$$(u_i)fg = (u_i f)g = (\sum_{j=1}^{m} a_{ij}u_j)g = \sum_{j=1}^{m} a_{ij}(\sum_{k=1}^{m} b_{jk}u_k) = \sum_{k=1}^{m} (\sum_{j=1}^{m} a_{ij}b_{jk})u_k.$$

Thus $\emptyset(fg) = \emptyset(f)\emptyset(g)$ by (7). We conclude that $\emptyset$ is a homomorphism of $L(U,U)$ onto M_{mm}. The unique determination of f by the a_{ij}, $1 \leq i \leq m$, $1 \leq j \leq m$ assures that $\emptyset$ is one-to-one and is an isomorphism.

CHAPTER II

THE GENERAL LINEAR GROUP AND RELATED GROUPS

We now begin our discussion of the general linear group and certain of its subgroups and quotient groups. When the field is finite, we will determine the order of these groups and the characteristics and order of their centers. We also include some of the interesting theorems relating these groups.

<u>Definition 2</u>. Let U be a finite dimensional vector space over a field F. $f \in L(U,U)$ is <u>nonsingular</u> (or regular) if and only is f is invertible, i.e., there exists $g \in L(U,U)$ such that $fg = gf = I$.

It is clear that the set of all nonsingular linear transformations actually form a group under composition.

<u>Definition 3</u>. Let U be a vector space of dimension m over F. The <u>general linear group</u>, denoted GL(m,F) is the group of nonsingular elements of L(U,U) under multiplication as defined in (6).

The matrix $\emptyset(f)$ where f is a nonsingular linear transformation and $\emptyset$ is an isomorphism described in theorem 3 is also called nonsingular. The image of GL(m,F) in M_{mm} is thus the group of nonsingular matrices. We will frequently identify GL(m,F) with this group of m by m nonsingular matrices over F.

<u>Theorem 4</u>. An element of M_{mm} is nonsingular if and only if its determinant is nonzero.

<u>Proof</u>: If $A \varepsilon M_{mm}$ is nonsingular, then there exists a $B \varepsilon M_{mm}$ such that $A \cdot B = I$. Thus $\det(A \cdot B) = \det I$ or $\det A \cdot \det B = \det I = 1$. We conclude $\det A \neq 0$. If $\det A \neq 0$, a standard proceedure allows the computation of a matrix B such that $AB = I$. See Shields (1968, p. 145) for the details.

When F is of finite order $q = p^{\alpha}$, $\alpha > 1$, the notation generally used for the general linear group is $GL(m,q)$. Examples of $GL(2,q)$ for $q = 2$ and 3, using the nonsingular matrices associated with the linear transformations are given in tables 1 and 2.

For the remainder of this chapter, we shall be primarily concerned with general linear groups over finite fields.

<u>Theorem 5</u>. The order of $GL(m,q)$ is $\prod_{i=0}^{m-1} (q^m - q^i)$.

<u>Proof</u>: Let U be an m dimensional vector space over a field F of order q. Consider the basis $e_1 = (1,0,\ldots,0)$, $e_2 = (0,1,0,\ldots,0),\ldots, e_m = (0,0,\ldots,1)$ for U. Let $u_1,u_2,\ldots,u_m$ be another basis for U. Then $u_i = \sum_{j=1}^{m} a_{ij}e_j = (a_{i1},a_{i2},\ldots,a_{im})$ for each i, $1 \leq i \leq m$; this representation is unique. Hence there is associated with every change of basis for U a linear transformation. Further, since we are mapping a basis to a basis, the linear transformation is nonsingular. Conversely every nonsingular linear transformation applied to $e_1,e_2,\ldots,e_m$ yields a basis for U, since for $i = 1,\ldots,m$ $u_i = \sum_{j=1}^{m} a_{ij}e_j$ is a basis for U. In order to obtain the order of $GL(m,q)$ we need only count the number of possible bases for U. In constructing

a basis $u_1, u_2, \ldots, u_m$ for U, there are $q^m - 1$ possible vectors to choose for u_1 since we must exclude the zero vector. Having chosen u_1, u_2 must be chosen so that it does not lie in the linear span of u_1, so as to be independent of u_1. Thus there are $q^m - q$ choices for u_2. Next, u_3 must be chosen such that it does not lie in the linear span of u_1 and u_2. So a total of q^2 vectors must be excluded, leaving $q^m - q^2$ choices for u_3. In general, when picking the basis element u_i, there are $q^m - q^{i-1}$ choices. Thus there are $(q^m - 1)(q^m - q)\cdots(q^m - q^{m-1})$ possible bases for U. Correspondingly, the order of GL(m,q) is $(q^m - 1)(q^m - q)\cdots(q^m - q^{m-1})$. For example, $|GL(3,2)| = 168$ and $|GL(2,49)| = (49^2 - 1)(49^2 - 49) = 5{,}644{,}800$.

An element $A \varepsilon M_{mm}$ which has determinant 1 is said to be unimodular. The set of these unimodular matrices forms a subgroup of GL(m,F) since if $A,B \varepsilon M_{mm}$ where A and B are unimodular, then $\det AB = \det A \cdot \det B = 1$. If B is unimodular, then $\det BB^{-1} = \det B \cdot \det B^{-1} = 1$ and $\det B^{-1} = (\det B)^{-1} = 1$. Hence $\det AB^{-1} = \det A \cdot \det B^{-1} = 1$. This argument establishes that the set of unimodular matrices form a subgroup of GL(m,F).

<u>Definition 4</u>. The multiplicitive group of all m by m unimodular matrices over a field F is the <u>special linear group</u>, denoted SL(m,F).

<u>Theorem 6</u>. SL(m,F) Δ GL(m,F).

<u>Proof</u>: Consider the following mapping, let $\Phi(x) = \det x$ for all $x \varepsilon GL(m,F)$. Φ is clearly a homomorphism of GL(m,F) onto the nonzero

elements of F since for any square matrices A and B, det AB = det A·det B. The kernel of Φ is SL(m,F) since SL(m,F) consists of all the unimodular matrices. Thus SL(m,F) Δ GL(m,F).

Corollary 6.1. The order of SL(m,q) = $\dfrac{\prod_{i=0}^{m} q^m - q^i}{q-1}$.

Proof: Recall the mapping Φ of GL(m,q) onto the multiplicative group of the nonzero elements of F described in theorem 6. This group has order q - 1 when F is finite. So [SL(m,q):GL(m,q)] = q - 1 and $|SL(m,q)| = (\prod_{i=0}^{m} q^m - q^i)/(q-1)$.

Definition 5. Let λ be a nonzero element of F and i $\neq$ j integers between 1 and m. A transvection $B_{ij}(\lambda) = E_{ij}(\lambda) + I$ where $E_{ij}(\lambda)$ is an m by m matrix with λ as its ij$^{\underline{th}}$ entry and zero elsewhere and I is the identity matrix.

Theorem 7. SL(m,F) is generated by the set of transvections.

Proof: Every element x of GL(m,F) can be written x = UD(μ) where U is a product of transvections and D(μ) is the diagonal matrix with diagonal entries 1,1,...,1,μ (Rotman, 1965, p. 158). If x ε SL(m,F), det x = det [UD(μ)] = det U·det D(μ) = μ so that if x is unimodular, D(μ) = D(1) = I and so x = U is a product of transvections.

Theorem 8. The commutator subgroup G' of GL(m,q) is SL(m,q) when m $\geq$ 3 or m = 2 and q $\geq$ 3.

Proof: G' is generated by elements of the form $x^{-1}y^{-1}xy$, where $x,y \in GL(m,q)$. Using the determinant map Φ of theorem 6, $\Phi(x^{-1}y^{-1}xy) = (\det x)^{-1}(\det y)^{-1}\det x \det y = 1$. So that $G' \subset SL(m,q)$. To show that $SL(m,q) \subset G'$, we need only show that every transvection is contained in G' since $SL(m,q)$ is generated by transvections by theorem 7.

Case I. $m = 2$. Let a,b,λ be nonzero elements of F. Then

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{-1}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & ab^{-1}\lambda - \lambda \\ 0 & 1 \end{pmatrix}.$$

So that all transvections $B_{12}(\alpha) = B_{12}[(ab^{-1} - 1)\lambda]$ can be generated in G' as long as there exist a and b in F such that $ab^{-1} - 1 \neq 0$, i.e., $a \neq b$. Clearly this is true for all fields of order greater than 2. $B_{21}(\alpha)$ can be realized in a similar manner. Since the transvections are contained in G', $SL(2,q) \subset G'$ for $q \geq 3$ so that $SL(2,q) = G'$. The commutator subgroup for $GL(2,2)$ is not $SL(2,2)$. See table 1.

Case II. $m \geq 3$. For E_{ij} and E_{st}, $E_{ij}E_{st} = \delta_{js}E_{it}$. The following is true:

$$\begin{aligned}
&B_{ij}(\mu)B_{jk}(\lambda)B_{ij}(\mu)^{-1}B_{jk}(\lambda)^{-1} = B_{ij}(\mu)B_{jk}(\lambda)B_{ij}(-\mu)B_{jk}(-\lambda) \\
&= [I + E_{ij}(\mu)][I + E_{jk}(\lambda)][I + E_{ij}(-\mu)][I + E_{jk}(-\lambda)] \\
&= [I + E_{ij}(\mu) + E_{jk}(\lambda) + E_{ik}(\mu\lambda)][I + E_{ij}(-\mu) + E_{jk}(-\lambda) + E_{ik}(\mu\lambda)] \\
&= I + E_{ij}(-\mu) + E_{jk}(-\lambda) + E_{ik}(\mu\lambda) + E_{ij}(\mu) + 0 + E_{ik}(-\mu\lambda) \\
&+ 0 + E_{jk}(\lambda) + 0 + 0 + 0 + E_{ik}(\mu\lambda) + 0 + 0 + E_{ik}(\mu^2\lambda^2) \\
&= E_{ik}(\mu^2\lambda^2).
\end{aligned}$$

So that any transvection $B_{ik}(\alpha) = I + E_{ik}(\alpha)$ can be realized by a commutator of appropriate transvections. Hence $SL(m,q) \subset G'$ for $m \geq 3$ and $SL(m,q) = G'$.

Theorem 9. The center of GL(m,q) is of order q − 1 and consists of scalar multiples of the identity matrix.

For a proof of this theorem, see Rotman (1965, p. 158).

Corollary 9.1. The center of SL(m,F), which we denote Z_o, consists of all scalar matrices kI with $k^m = 1$.

Proof: Since SL(m,F) Δ GL(m,F), Z_o = SL(m,F) $\cap$ Z, where Z is the center of GL(m,F). Thus $x \varepsilon Z_o$ must be a scalar multiple of the identity matrix. Since every x ε SL(m,F) must be unimodular, it follows immediately that $k^m = 1$.

Corollary 9.2. If Z_o is the center of SL(m,q) then $|Z_o| = d$, where d = (m,q-1).

Proof: By corollary 9.1 we must determine the number of elements x ε F such that $x^m = 1$. Let ρ be a primitive element of F. Then ρ has order q-1. Define $\tau = \rho^{(q-1)/d}$, where d = (m,q-1). There are exactly d distinct powers of τ and $(\tau^i)^m = 1$ for each i, since

$$(\tau^i)^m = [\rho^{i(q-1)/d}]^m = \rho^{(q-1)im/d}$$

$$(\rho^{q-1})^{im/d} = (1)^{ic} = 1$$

where cd = m.

We shall now prove that if $(\rho^t)^m = 1$, then ρ^t is a power of τ. Since (m/d, q-1/d) = 1, there are integers a and b with am/d + b(q-1)/d = 1.

Then since $\tau = \rho^{(q-1)/d}$ and $[\rho^{(q-1)i/d}]^m = 1$,

$$\tau^{im} = \rho^{(q-1)im/d}$$

$$(\tau^{im})^{am/d + b(q-1)/d} = [\rho^{(q-1)im/d}]^1$$

$$\tau^{iam^2/d} \cdot \tau^{(q-1)imb/d} = \rho^{(q-1)im/d}$$

In particular if $i = d$, $\tau^{iam^2/d} = (\tau^{ma})^m = 1$. Substituting $t = (q-1)im/d$ we have $\tau^{bt} = \rho^t$. So there are exactly $d = (m, q-1)$ elements in Z_o.

The next group to be introduced is the quotient group of SL(m,F) by its center Z_o. This is a group of considerable interest. We shall discuss its properties in more detail in chapter III.

Definition 6. The projective unimodular group PSL(m,F) is the group $SL(m,F)/Z_o$.

Theorem 10. $|PSL(m,q)| = \prod_{i=0}^{m} q^m - q^i/d(q - 1)$, where $d = (m, q-1)$.

Proof: The theorem follows directly from definition 6.
$|PSL(m,q)| = |SL(m,q)|/|Z_o| = \prod_{i=0}^{m} q^m - q^i/d(q-1)$.

At this point let us note an interesting relationship between PSL(m,q) and the following group of mappings of the field F.

Definition 7. If F is a field, LF(F) is the group of all unimodular linear transformations $x \to (ax + b)/(cx + d)$ under composition of mappings where $a,b,c,d \in F$ and $ad - bc = 1$.

<u>Theorem 11</u>. $PSL(2,F) \simeq LF(F)$.

<u>Proof</u>: If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \varepsilon\ SL(2,F)$, define a mapping θ as follows:

$$\theta \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \{x \to (ax + b)/(cx + d)\}.$$

If $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ are elements of $SL(2,F)$, then

$$\theta\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix}\right] = \theta \begin{pmatrix} aA + bC & aB + bD \\ cA + cC & cB + dD \end{pmatrix}$$

$$= [(aA + bC)x + aB + bD]/[(cA + cC)x + cB + dD]$$

$$= \theta \begin{pmatrix} a & b \\ c & d \end{pmatrix} \theta \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Thus θ is a homomorphism. It is onto since for any $f \varepsilon LF(F)$, the pre-image of $f(x) = (ax + b)/(cx + d)$ is the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The kernel of θ is $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \varepsilon\ SL(2,F) : \theta \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \{x \to x\}\right\}$. But this means $(ax + b)/(cx + d) = x$ so that $a = d$ and $c = b = 0$. So that we have elements of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ which by corollary 9.1 is Z_o. Then by the first isomorphism theorem, $PSL(2,F) \simeq SL(2,F)/Z_o \simeq LF(F)$.

CHAPTER III

THE SIMPLICITY OF THE PROJECTIVE UNIMODULAR GROUP

In this chapter, we will be concerned mainly with the simplicity of the projective unimodular group. We begin by showing that PSL(2,F) is simple for those cases when the order of F is greater than 3. We then show that PSL(3,F) is simple as the first step for an induction proof that PSL(m,F) is simple for all $m \geq 3$.

The following lemma can be proved using the method of theorem 8.

<u>Lemma 12.1</u>. If a normal subgroup H of SL(2,F) contains a transvection $B_{ij}(\lambda)$, then H = SL(2,F).

<u>Theorem 12</u>. The group PSL(2,F) is simple except when $|F| \leq 3$.

<u>Proof</u>: Since $|PSL(2,2)| = 6$ and $|PSL(2,3)| = 12$, and there are no simple groups of order less than 60, these groups are not simple

Let H be a normal subgroup of SL(2,F) which contains a matrix not in Z_o, the center of SL(2,F). By the correspondence theorem, it suffices to show that H = SL(2,F), since if we let π:SL(2,F) $\rightarrow$ SL(2,F)/Z_o where π is the natural map, π defines a one-to-one correspondence between the set of those subgroups of SL(2,F) containing Z_o and the set of all subgroups of SL(2,F)/Z_o.

Suppose H contains a matrix $A = \begin{pmatrix} r & o \\ s & t \end{pmatrix}$ where $r \neq \pm 1$.

If $S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, then due to the fact that $H \Delta SL(2,F)$, H also contains

$$(SAS^{-1})A^{-1} = \begin{pmatrix} 1 & 0 \\ 1 - t^2 & 1 \end{pmatrix}.$$

Since $\det A = 1 = rt$, $t \neq \pm 1$ and $1 - t^2 \neq 0$. This last matrix is thus a transvection and so $H = SL(2,F)$ by lemma 12.1.

To complete the proof, we have only to produce a matrix in H whose first row is $(r\ 0)$ where $r \neq \pm 1$.

H contains an element M not in Z_o of the form

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \; ad - bc = 1.$$

If $b = 0$, $a = d = 1$, $c \neq 0$, then M is a transvection. If $b = 0$, $a = d = -1$, $c \neq 0$, them M^2 is a transvection. If $b = 0$, $a = d = \pm 1$, $c = 0$, then $M \varepsilon Z_o$ contrary to assumption.

If $b \neq 0$, then

$$\begin{pmatrix} 1 & 0 \\ a/b & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -a/b & 1 \end{pmatrix} = \begin{pmatrix} 0 & b \\ -1/b & a + b \end{pmatrix} = C$$

so that $C \varepsilon H$. Let $T = \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix}$, then H contains

$$U = TCT^{-1}C^{-1} = \begin{pmatrix} \alpha^{-2} & 0 \\ -(a + d)(\alpha^2 - 1)/b & \alpha^2 \end{pmatrix}.$$

U will be the desired matrix if $\alpha^{-2} \neq \pm 1$. This is equivalent to $\alpha^4 \neq 1$. If $|F| > 5$ or F is infinite, such a nonzero α does exist since $\alpha^4 - 1$ has at most 4 roots. If $|F| = 4$, then every $\alpha \varepsilon F$ satisfies $\alpha^4 = \alpha$, so that if $\alpha \neq 1$, then $\alpha^4 \neq 1$. For $|F| = 5$, $\alpha^4 = 1$ is true for all $\alpha \neq 0$ so that $\alpha^2 = 1$ or $\alpha^2 = -1$. Choose α such that $\alpha^2 = -1$. Then $U = \begin{pmatrix} -1 & 0 \\ \lambda & -1 \end{pmatrix}$ where $\lambda = -(a + d)(\alpha^2 - 1)/b \neq 0$. Since $U \varepsilon H$, then U^2 is also in H, but $U^2 = \begin{pmatrix} 1 & 0 \\ -2\lambda & 1 \end{pmatrix}$ and U^2 is a transvection.

<u>Lemma 13.1</u>. Let $H \triangle SL(m,F)$, and let $A \varepsilon H$. If A is similar to

$$C = \begin{pmatrix} & & & b_1 \\ & & & b_2 \\ & C' & & \cdot \\ & & & \cdot \\ & & & \cdot \\ a_1 & a_2 & \cdots & y \end{pmatrix},$$

Where C' is an $(m - 1)$ by $(m - 1)$ matrix, then there is a nonzero $\mu \varepsilon F$ such that H contains

$$C' = \begin{pmatrix} & & & \mu^{-1}b_1 \\ & & & \mu^{-1}b_2 \\ & C' & & \cdot \\ & & & \cdot \\ & & & \cdot \\ \mu a_1 & \mu a_2 & \cdots & y \end{pmatrix}.$$

For proof of the lemma see Rotman (1965, p. 159).

<u>Theorem 13</u>. $PSL(3,F)$ is simple for every field F.

<u>Proof</u>: Let H be a normal subgroup of $SL(3,F)$ which contains Z_o, and let $A \varepsilon H$ be a scalar matrix. There are three possible canonical forms for A:

i) a direct sum of three 1 by 1 companion matrices;

ii) a direct sum of a 2 by 2 and a 1 by 1 companion matrix;

iii) a 3 by 3 companion matrix.

Case (i). A is similar to

$$D = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix},$$

where D is nonscalar. Therefore $ac^{-1} \neq 1$. By lemma 13.1, $D \varepsilon H$. If

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

then

$$BDB^{-1}D^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 - ac^{-1} & 0 & 1 \end{pmatrix} \varepsilon H,$$

but this is a transvection, so by lemma 12.1, $H = SL(3,F)$.

Case (ii). A is similar to

$$D = \begin{pmatrix} 0 & a & 0 \\ 1 & b & 0 \\ 0 & 0 & c \end{pmatrix}.$$

If $B = B_{32}(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, then

$$M = BDB^{-1}D^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -ca^{-1} & 1 & 1 \end{pmatrix} \varepsilon H.$$

Now the characteristic polynomial of M is $(x - 1)^3$. Since $M \neq I$ and M satisfies $(x - 1)^2$, the minimum polynomial of M is $(x - 1)^2$. Since the characteristic roots of M are all equal to 1, they lie in F, so by Rotman (1965, p. 72), M is similar to its Jordan canonical form $J = \begin{pmatrix} a & 0 & 0 \\ 1 & a & 0 \\ 0 & 0 & b \end{pmatrix}$. If we write the characteristic polynomial $(x - 1)^3$ in the form $(-1)(x^3 - 3x^2 + 3x - 1)$, then the trace of J is 3 and the determinant of J is 1. Thus $a + a + b = 3$ and $aab = 1$. Solving these simultaneously yields $(a - 1)(2a^2 - a - 1) = 0$, so that $a = 1$ and $b = 1$, so that $J = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. By lemma 12.1, this transvection is in H so

$H = SL(3,F)$.

Case (iii). A is similar to a 3 by 3 companion matrix,

$C = \begin{pmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & c \end{pmatrix}$, $a \neq 0$ since A is nonsingular, and by lemma 13.1, H contains

$$C^* = \begin{pmatrix} 0 & 0 & \mu^{-1}a \\ 1 & 0 & \mu^{-1}b \\ 0 & \mu & c \end{pmatrix}.$$

Therefore, H contains the commutator

$$D = C^{*-1}B_{21}(-1)C^*B_{21}(1) = \begin{pmatrix} -ba^{-1} & 1 & 0 \\ -ca^{-1} & 0 & \mu^{-1} \\ \mu a^{-1} & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & \mu^{-1}a \\ 1 & 0 & \mu^{-1}b \\ 0 & \mu & c \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} -ba^{-1}-1 & 1 & 0 \\ -ca^{-1} & 0 & \mu^{-1} \\ \mu a^{-1} & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & \mu^{-1}a \\ 1 & 0 & \mu^{-1}b \\ \mu & \mu & c \end{pmatrix} = \begin{pmatrix} 1 & 0 & -\mu^{-1}a \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since $D \in H$, $D^{-1} = \begin{pmatrix} 1 & 0 & \mu^{-1} \\ -1 & 1 & -\mu^{-1} \\ 0 & 0 & 1 \end{pmatrix} \in H$ also.

H also contains $B_{21}(1)DB_{21}(-1)D^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\mu^{-1}a \\ 0 & 0 & 1 \end{pmatrix}$ and since $\mu \neq 0$,

this is a transvection so that $H = SL(3,F)$.

<u>Lemma 14.1</u>. Let $H \Delta SL(m,F)$ and let H contain $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, where B is a k by k matrix that is not scalar. Then H contains a matrix $\begin{pmatrix} I & 0 \\ 0 & D \end{pmatrix}$, where I is an identity matrix and D is a k by k matrix that is not scalar.

<u>Proof</u>: Since $H \Delta SL(m,F)$ we know that if $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in H$, then if B is a diagonal matrix and is not scalar, then $B = (b_1,..b_k)$, such that $b_i \neq b_j$ for some i,j, $1 \le i \le k$, $1 \le j \le k$. Since $B^{-1}B_{ij}(1)^{-1}BB_{ij}(1) = B_{ij}(1 - b_i^{-1}b_j)$ which is not scalar, we use

$$\begin{pmatrix} A^{-1} & 0 \\ 0 & B^{-1} \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & B_{ij}(1)^{-1} \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & B_{ij}(1) \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & D \end{pmatrix}$$

and $D = B^{-1}B_{ij}(1)^{-1}BB_{ij}(1)$ is not scalar

If $B = (b_{ij})$ is not diagonal, then use $D = (d_{ij})$ where $d_{ij} = 0$ if $i \neq j$, $d_{ii} \neq 0$ for each i and $d_{ii} \neq d_{jj}$ for any i,j, $1 \leq i \leq k$, $1 \leq j \leq k$. Assume $B^{-1}D^{-1}BD = xI$. Then $BD = xDB$, so that

$$BD = (c_{ih}), \quad c_{ih} = b_{ih}d_{hh};$$

$$DB = (a_{ih}), \quad a_{ih} = d_{ii}b_{ih}.$$

Therefore $BD = xDB$ if and only if $b_{ih}d_{hh} = xd_{ii}b_{ih}$ for each i,h. When $i = h$, $x = 1$, so $b_{ih}d_{hh} = d_{ii}b_{ih}$. When $i \neq h$, not all b_{ih} are zero therefore $d_{hh} = d_{ii}$ for some i,h which contradicts $d_{ii} \neq d_{hh}$ for any i,h. Therefore

$$\begin{pmatrix} A^{-1} & 0 \\ 0 & B^{-1} \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & D^{-1} \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & D \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & E \end{pmatrix}$$

and E is not scalar.

Lemma 14.2. Suppose that $PSL(m,F)$ is simple, for some fixed $m \geq 3$. If a normal subgroup H of $SL(m,F)$ contains a nonscalar matrix, then $H = SL(m,F)$.

Proof: If $PSL(m,F)$ is simple, then Z_o, the center, is a maximal normal subgroup of $SL(m,F)$. Since H and Z_o are both normal in $SL(m,F)$, then HZ_0 is the smallest subgroup of $SL(m,F)$ containing H and Z_o. But for $hz_o \in HZ_o$, $ghz_og^{-1} = ghg^{-1}z_o \in HZ_o$ for all $g \in SL(m,F)$. Hence HZ_o is a normal subgroup which contains Z_o but since Z_o is maximal, $HZ_o = SL(m,F)$.

It follows that H must contain A, a scalar multiple of a transvection

$$A = \begin{pmatrix} \alpha & \mu & 0 & 0 & \dots & 0 \\ 0 & \alpha & 0 & 0 & \dots & 0 \\ 0 & 0 & \alpha & 0 & \dots & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & 0 & \dots & \alpha \end{pmatrix},$$

and its inverse

$$A^{-1} = \begin{pmatrix} \alpha^{-1} & -\mu\alpha^{-2} & 0 & 0 & \dots & 0 \\ 0 & \alpha^{-1} & 0 & 0 & \dots & 0 \\ 0 & 0 & \alpha^{-1} & 0 & \dots & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & 0 & \dots & \alpha^{-1} \end{pmatrix}.$$

If $|F| = 2$ then A is a transvection and by Lemma 12.1 $H = SL(m,F)$. If $|F| \geq 3$ then there is a nonzero $\beta \in F$ with $-\mu\alpha^{-2} + \beta \neq 0$. Now A^{-1} is similar to B where

$$B = \begin{pmatrix} \alpha^{-1} & -\mu\alpha^{-2} + \beta & 0 & 0 & \dots & 0 \\ 0 & \alpha & 0 & 0 & \dots & 0 \\ 0 & 0 & \alpha^{-1} & 0 & \dots & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

since for

$$D = \begin{pmatrix} \begin{matrix} a & b \\ 0 & -a\mu\alpha^{-2}/(-\mu\alpha^{-2} + \beta) \end{matrix} & O \\ O & I \end{pmatrix},$$

$A^{-1}D = DB$. $\beta \in H$ by lemma 13.1 as long as $m \geq 3$. But $AB = B_{12}(\alpha\beta)$, H contains a transvection, and so $H = SL(m,F)$.

Theorem 14. $PSL(m,F)$ is simple for every field F and all $m \geq 3$.

Proof: The theorem is proved by induction on m, where $m \geq 3$. Theorem 13 completed the initial step where $m = 3$. Let $H \Delta SL(m,F)$, where $m > 3$ and H properly contains Z_o. Now H contains a nonscalar matrix A, and A is similar to a direct sum of companion matrices

$$\begin{pmatrix} C_1 & & & & \\ & C_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & C_t \end{pmatrix},$$

by lemma 13.1, this matrix lies in H if we adjust the last row and column.

If $t > 1$, then lemma 14.1 gives a matrix in H of the form $\begin{pmatrix} I & 0 \\ 0 & D \end{pmatrix}$, where D is a k by k matrix that is not scalar. We may assume that $k \geq 3$: if for example, $k = 2$, then let

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}.$$

Let S^* be the following isomorphic copy of $SL(k,F)$ in $SL(m,F)$:

$$S^* = \left\{ \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} : U \in SL(k,F) \right\}.$$

Now $S^* \cap H \Delta S^*$ and $\begin{pmatrix} I & 0 \\ 0 & D \end{pmatrix}$ is a nonscalar matrix in this intersection. Since $PSL(k,F)$ is simple, by induction, lemma 14.2 gives $S^* \cap H = S^*$ so that H contains a transvection.

The last case is when $t = 1$, i.e., the original matrix A is similar to a companion matrix. Thus H contains an adjusted companion matrix

$$C = \begin{pmatrix} 0 & 0 & \dots & 0 & a_1 \\ 1 & 0 & \dots & 0 & a_2 \\ 0 & 1 & \dots & 0 & a_3 \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ 0 & 0 & \dots & \mu & a_m \end{pmatrix},$$

where $\mu = a_1^{-1}$. Our multiplication is easier if we think of C as a linear transformation; there is a basis $\alpha_1 = 1,0,\dots,0$ $\alpha_2 = 0,1,0,\dots,0$ $\dots,$ $\alpha_m = 0,0,\dots,1$ with

$$\begin{aligned} C\alpha_1 &= \alpha_2, \\ &\vdots \\ C\alpha_{m-1} &= \alpha_m, \\ C\alpha_m &= \quad a_i\alpha_i. \end{aligned}$$

The inverse of C also lies in H; since $CC^{-1}\alpha_i = \alpha_i$, its action is given by

$$\begin{aligned} C^{-1}\alpha_1 &= -a_2\mu\alpha_1 - a_3\mu\alpha_2 - \dots - a_{m-1}\mu\alpha_{m-2} - a_m\mu\alpha_{m-1} + \mu\alpha_m, \\ C^{-1}\alpha_2 &= \alpha_1 \\ &\vdots \\ C^{-1}\alpha_{m-1} &= \alpha_{m-2} \\ C^{-1}\alpha_m &= \mu^{-1}\alpha_{m-1}. \end{aligned}$$

If B is the transvection $B_{21}(1)$, then

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & I \end{pmatrix},$$

and $B\alpha_1 = \alpha_1 + \alpha_2$ and $B\alpha_i = \alpha_i$ for $i \geq 2$. The transformation $D = BCB^{-1}C^{-1}$ acts as follows:

$$D\alpha_1 = \alpha_1 + \alpha_2 + a_2\mu\alpha_3$$

$$D\alpha_2 = \alpha_2 - \alpha_3 \ ; \ D\alpha_i = \alpha_i \text{ for } i \geq 3.$$

The matrix of D relative to the basis of α is in H, and

$$D = \begin{pmatrix} 1 & 0 & 0 & \\ 1 & 1 & 0 & 0 \\ a_2\mu & -1 & 1 & \\ & 0 & & I \end{pmatrix}.$$

If $S^* = \left\{\begin{pmatrix} U & 0 \\ 0 & I \end{pmatrix};\ U \in SL(3,F)\right\}$, then $S^* \simeq SL(3,F)$ and $H \cap S^* \Delta S^*$. Since $H \cap S^*$ contains D, a nonscalar matrix, $H \cap S^* = S^*$, by lemma 14.2. Therefore, $S^* \subset H$ and H contains a transvection.

Further investigation of PSL(m,F) shows that not only do these simple groups reproduce other simple groups, i.e., table 3 shows that $PSL(2,3) \simeq A_4$, but others such as PSL(3,4) which has order 20,160 is not isomorphic to A_8 which is also simple and of order 20,160 (Rotman, 1965, p. 172).

LIST OF REFERENCES

1. W. Burnside, Theory of Groups of Finite Order, 2nd ed., New York, 1955.

2. L. E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, New York, 1958.

3. I. N. Herstein, Topics in Algebra, New York, 1964.

4. J. J. Rotman, The Theory of Groups: An Introduction, Boston, 1965.

5. E. Schenkman, Group Theory, New York, 1965.

6. P. C. Shields, Elementary Linear Algebra, New York, 1968.

TABLE 1

GL(2,2)

Element	Order
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1
$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	2
$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	2
$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	3
$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	3
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	2

The commutator subgroup is: $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right\}$.

By noting the order of the elements, it is clear that $GL(2,2) \simeq S_3$

TABLE 2

GL(2,3)

Element	Element	Element	Element
$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&2\\2&2\end{pmatrix}$	$\begin{pmatrix}2&0\\2&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$
$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}2&2\\2&1\end{pmatrix}$	$\begin{pmatrix}1&1\\2&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\2&0\end{pmatrix}$	$\begin{pmatrix}1&2\\1&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$
$\begin{pmatrix}0&1\\2&2\end{pmatrix}$	$\begin{pmatrix}0&1\\2&1\end{pmatrix}$	$\begin{pmatrix}0&2\\2&0\end{pmatrix}$	$\begin{pmatrix}1&1\\0&2\end{pmatrix}$
$\begin{pmatrix}2&1\\2&0\end{pmatrix}$	$\begin{pmatrix}0&2\\1&1\end{pmatrix}$	$\begin{pmatrix}0&2\\2&2\end{pmatrix}$	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$
$\begin{pmatrix}0&1\\2&0\end{pmatrix}$	$\begin{pmatrix}1&2\\1&0\end{pmatrix}$	$\begin{pmatrix}2&2\\2&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&2\end{pmatrix}$
$\begin{pmatrix}0&2\\1&0\end{pmatrix}$	$\begin{pmatrix}0&2\\1&2\end{pmatrix}$	$\begin{pmatrix}2&2\\1&2\end{pmatrix}$	$\begin{pmatrix}2&0\\1&1\end{pmatrix}$
$\begin{pmatrix}1&1\\1&2\end{pmatrix}$	$\begin{pmatrix}2&2\\1&0\end{pmatrix}$	$\begin{pmatrix}2&1\\2&2\end{pmatrix}$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$
$\begin{pmatrix}2&1\\1&1\end{pmatrix}$	$\begin{pmatrix}1&0\\2&1\end{pmatrix}$	$\begin{pmatrix}2&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\0&2\end{pmatrix}$
$\begin{pmatrix}2&0\\0&2\end{pmatrix}$	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&2\end{pmatrix}$	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$
$\begin{pmatrix}2&2\\0&2\end{pmatrix}$	$\begin{pmatrix}2&0\\1&2\end{pmatrix}$	$\begin{pmatrix}0&2\\2&1\end{pmatrix}$	$\begin{pmatrix}1&0\\2&2\end{pmatrix}$
$\begin{pmatrix}2&0\\2&2\end{pmatrix}$	$\begin{pmatrix}2&1\\0&2\end{pmatrix}$	$\begin{pmatrix}1&2\\2&0\end{pmatrix}$	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$

The matrices in the first two columns have determinant 1 and are thus the group SL(2,3).

Table 3

$PSL(2,3)$

Element	Order
$Z_0 = \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}2&0\\0&2\end{pmatrix}\right\}$	Identity
$\begin{pmatrix}1&1\\0&1\end{pmatrix}Z_0 = \left\{\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}2&2\\0&2\end{pmatrix}\right\}$	3
$\begin{pmatrix}1&0\\1&1\end{pmatrix}Z_0 = \left\{\begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}2&0\\2&2\end{pmatrix}\right\}$	3
$\begin{pmatrix}0&1\\2&2\end{pmatrix}Z_0 = \left\{\begin{pmatrix}0&1\\2&2\end{pmatrix}, \begin{pmatrix}0&2\\1&1\end{pmatrix}\right\}$	3
$\begin{pmatrix}2&1\\2&0\end{pmatrix}Z_0 = \left\{\begin{pmatrix}2&1\\2&0\end{pmatrix}, \begin{pmatrix}1&2\\1&0\end{pmatrix}\right\}$	3
$\begin{pmatrix}0&1\\2&0\end{pmatrix}Z_0 = \left\{\begin{pmatrix}0&1\\2&0\end{pmatrix}, \begin{pmatrix}0&2\\1&0\end{pmatrix}\right\}$	2
$\begin{pmatrix}1&1\\1&2\end{pmatrix}Z_0 = \left\{\begin{pmatrix}1&1\\1&2\end{pmatrix}, \begin{pmatrix}2&2\\2&1\end{pmatrix}\right\}$	2
$\begin{pmatrix}2&1\\1&1\end{pmatrix}Z_0 = \left\{\begin{pmatrix}2&1\\1&1\end{pmatrix}, \begin{pmatrix}1&2\\2&2\end{pmatrix}\right\}$	2
$\begin{pmatrix}1&1\\2&0\end{pmatrix}Z_0 = \left\{\begin{pmatrix}1&1\\2&0\end{pmatrix}, \begin{pmatrix}2&2\\1&0\end{pmatrix}\right\}$	3
$\begin{pmatrix}0&1\\2&1\end{pmatrix}Z_0 = \left\{\begin{pmatrix}0&1\\2&1\end{pmatrix}, \begin{pmatrix}0&2\\1&2\end{pmatrix}\right\}$	3
$\begin{pmatrix}1&0\\2&1\end{pmatrix}Z_0 = \left\{\begin{pmatrix}1&0\\2&1\end{pmatrix}, \begin{pmatrix}2&0\\1&2\end{pmatrix}\right\}$	3
$\begin{pmatrix}1&2\\0&1\end{pmatrix}Z_0 = \left\{\begin{pmatrix}1&2\\0&1\end{pmatrix}, \begin{pmatrix}2&1\\0&2\end{pmatrix}\right\}$	3