The Projective Special Linear Group $\text{PSL}(4,2)$.

Alaa Adnan Auad          Muthana A. Mahmood  
University of Anbar - College of Education for pure science  
Received:28/10/2008 Accepted:15/6/2009

Abstract: The present study deals with conjugacy classes for the projective linear group. The study of conjugacy classes has a great and important role; in hand it is an introductory step to study the general linear group and also the maximal subgroup in it. We introduce the investigation of the canonical form which represent each class for the linear group of dimension 4 over a field $\text{GF}(pr)$ and deals with canonical form which represents the conjugacy class of the groups with dimension 4 over a field $\text{GF}(2)$.

Keywords: Projective, Special, Linear Group, $\text{PSL}(4,2)$.

Introduction

The subgroups of 2 and 3 dimensional linear groups over a field of characteristic $p>0$ have been known for some times. MOORE (1893) had given detailed account of the subgroups of $\text{PSL}(2,q)$ and independently by WIMAN(1899). The subgroups of $\text{PSL}(3,q)$ were found by MITHELL(1911) while KHALF(1993) determined the subgroups of $\text{PSL}(7,2a)$. The present work investigates the linear groups over a field $\text{GF}(2)$.

1. Definition: A field $F$ which has a finite number of elements is called a Finite Field. [5]
2. Remark: A finite field $F$ with $p^n$ elements where $p$ is prime, is called a GALOIS Field of order $p^n$ and is denoted by $\text{GF}(p^n)$. [6]
3. Definition: A polynomial is an expression of the form $f(t)=a_n t^n+a_{n-1}t^{n-1}+\ldots+a_1 t+a_0$, where $a_n,a_{n-1},\ldots,a_0$ are real numbers. If $a_n\neq0$ then $f(t)$ is said to have the degree $n$. [2]
4. Definition: Let $F$ be a subfield of a field $E$. If a polynomial $f(x)$ has no root in $F$ but it has a root in $E$, then $E$ is called an Extension field. [3]
5. Definition: Let $\beta$ be a bilinear form on an $n$-dimensional vector space over a field $F$. We say that $\beta$ is non-singular if it satisfies the condition: $\beta(x,y)=0 \forall y \in V$, then $x=0$. A pair $(V, \beta)$ is called a non-singular space if $\beta$ is non-singular. [3]
6. Definition: The set of all non-singular linear transformations of $V$ into itself forms a group called the General Linear Group and denoted by $\text{GL}(n,F)$, where $n$ denotes the dimension of $V$. If $F$ is a finite field with $q$ elements then $\text{GL}(n,F)$ is denoted by $\text{GL}(n,q)$.

The center $Z$ of $\text{GL}(n,q)$ is set of all non-singular scalar matrices, hence we may form the factor group $\text{GL}(n,q)/Z(\text{GL}(n,q))$ called the Projective Linear Group and is denoted by $\text{PGL}(n,q)$. $\text{GL}(n,q)$ has a normal subgroup, consisting of all matrices of determinant 1 called Special Linear Group denoted by $\text{SL}(n,q)$. The image of $\text{SL}(n,q)$ under the mapping $M: \text{GL}(n,q) \rightarrow \text{PGL}(n,q)$ is the Projective Special Linear Group and is denoted by $\text{PSL}(n,q)$. [6]

7. Remark: The order of the classical group: $|\text{SL}(n,q)|=|\text{PGL}(n,q)|=q^n(n-1)/2 \prod_{i} (q^i-1)$.
8. Definition: A polynomial $f(x)$ in $\text{F}[x]$ is said to be irreducible over a field $F$, if whenever $f(x)=a(x).b(x)$ with $a(x),b(x) \in \text{F}[x]$ then one of $a(x)$ or $b(x)$ has zero degree, otherwise $f(x)$ is called reducible. [4]
9. Remark: Irreducibility depends on the field; for instance the polynomial $x^2+1$ is irreducible over the real field but it is not over the complex field. [4]
10. Theorem: if $c(x)$ is irreducible then $f(x)|c(x)$ and $n|P$ or $f(x)\nmid c(x)$ or $n+P$ then $c(x)$ is reducible. [4]
11. Theorem: Let $n|P$ then $c(x)$ irreducible if and only if 2s-1 $\nmid P$ $\forall s>\in Z^+$ such that $n|2s-1$. [4]
12. Corollary: Let $n|P$, then $c(x)$ is irreducible if for some $r>\in Z^+$ $n|2s-1$. [4]
13. Definition: The number of irreducible polynomials
Let \( P(x) \) be the a polynomial of degree \( r \) where \( r \neq 0 \), then we can write
\[
\begin{align*}
\Psi(r) &= \frac{1}{r} \sum_{d \mid r} 2^d \mu(r/d) \\
\text{where the sum extended over all positive divisor } d \text{ of } r. \quad [2]
\end{align*}
\]

14. Definition: Let \( f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \) be any polynomial over \( F \) where \( a_n \neq 0 \). The following \( n \times n \) matrix
\[
\begin{bmatrix}
0 & 0 & \ldots & -a_0/a_n \\
1 & 0 & \ldots & -a_1/a_n \\
0 & 1 & \ldots & -a_2/a_n \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 1 - a_{n-1}/a_n
\end{bmatrix}
\]
is called the Companion Matrix of the polynomial \( f(x) \) and is denoted by \( c(f) \). [13]

Note: when \( f(x) = a_0 + x \) then \( c(f) = [-a_0] \).

15. Remark: Let \( g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_tx^t + \ldots + b_nx^n \) be a polynomial over \( F \) where \( b_n \neq 0 \) and \( f(x) = [g(x)]r \) then the companion matrix is the \( tr \times tr \) matrix,
\[
\begin{bmatrix}
c(g) & A & \ldots & 0 & 0 \\
0 & c(g) & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & c(g) & A \\
0 & 0 & \ldots & 0 & c(g)
\end{bmatrix}
\]
Where \( A \) is \( txt \) zero matrix except \((1,1)\) of \( A \) is equal 1 and 0 is the zero matrix. [5]

16. Theorem: If \( T \in GL(n,F) \) has as minimal polynomial \( m(x) = f(x)^e \) where \( f(x) \) is an irreducible polynomial in \( F[x] \), then a basis of \( V \) over \( F \) can be found in which the matrix of \( T \) is of the form:
\[
\begin{bmatrix}
e(f(x)^e) & 0 & \ldots & 0 & 0 \\
0 & e(f(x)^e) & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & e(f(x)^e) & 0 \\
0 & 0 & \ldots & 0 & e(f(x)^e)
\end{bmatrix}
\]
where \( e = e_1 \geq e_2 \geq \cdots \geq e_s \) and 0 denotes the zero matrix. [13]

17. Corollary: If \( T \in GL(n,F) \) has as minimal polynomial \( m(x) = f_1(x)^{e_1} + f_2(x)^{e_2} + \cdots + f_n(x)^{e_n} \) in \( F[x] \) where \( f_i(x), i=1,2,\ldots,n \) are irreducible distinct polynomials in \( F[x] \) then there exists a basis for \( V \) such that \( T \) has the following matrix representation:
\[
\begin{bmatrix}
R_{e_1} & 0 & \ldots & 0 & 0 \\
0 & R_{e_2} & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & R_{e_i} & 0 \\
0 & 0 & \ldots & 0 & R_{e_s}
\end{bmatrix}
\]
where
\[
\begin{bmatrix}
e(f(x)^{e_1}) & 0 & \ldots & 0 & 0 \\
0 & e(f(x)^{e_2}) & \ldots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & e(f(x)^{e_i}) & 0 \\
0 & 0 & \ldots & 0 & e(f(x)^{e_s})
\end{bmatrix}
\]

According to the positive factorization of \( \Delta(x) \) in \( GF(pr) \) we can distinguish the cases:

1. Irreducible quadric.
2. Irreducible Cubic and linear factor.
3. Two distinct irreducible quadratics.
4. Two equal irreducible quadratics.
5. Irreducible quadratic and two equal linear factors.
6. Irreducible quadratic and two distinct linear factors.
7. Four equal linear factors.
8. Three equal linear factors and one linear factor.
9. Two equal linear factors and two equal linear factors.
10. Two equal linear factors and two distinct linear factors.
Four distinct linear factors.
Let \( q = p^l \) and let \( \alpha, \beta, \gamma, \lambda \) be a primitive roots of \( GF(q) \), \( GF(q^2) \), \( GF(q^3) \) and \( GF(q^4) \) respectively such that

\[
\alpha = \beta^{q+1} = \gamma^{q^2+q+1} = \lambda^{q^3+q^2+q+1}.
\]

Then according to the above cases each element of \( PSL(4,q) \) is similar to a matrix of one of the following types:

<table>
<thead>
<tr>
<th>Type</th>
<th>Symbol</th>
<th>Canonical form</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Case1 | (4) \( \lambda \) | \[
\begin{bmatrix}
\lambda_1 & 0 & 0 \\
0 & \lambda_1^q & 0 \\
0 & 0 & \lambda_1^{q^2}
\end{bmatrix}
\] | \( \lambda_1, \lambda_1^q, \lambda_1^{q^2}, \lambda_1^{q^3} \) but \( \in GF(q^3) \) |
| Case2 | (3,1) \( \gamma \) | \[
\begin{bmatrix}
\gamma_1 & 0 & 0 \\
0 & \gamma_1^q & 0 \\
0 & 0 & \gamma_1^{q^2}
\end{bmatrix}
\] | \( \gamma_1, \gamma_1^q, \gamma_1^{q^2}, \gamma_1^{q^3} \) but \( \in GF(q^3) \) |
| Case3 | (2,2) \( \beta \) | \[
\begin{bmatrix}
\beta_1 & 0 & 0 \\
0 & \beta_1^q & 0 \\
0 & 0 & \beta_1^{q^2}
\end{bmatrix}
\] | \( \beta_1, \beta_1^q, \beta_1^{q^2} \) but \( \in GF(q^3) \) |
| Case4 | (2') \( b \) | \[
\begin{bmatrix}
b_1 & 0 & 0 \\
0 & b_1^q & 0 \\
0 & 0 & b_1^{q^2}
\end{bmatrix}
\] | \( b_1, b_1^q, b_1^{q^2} \) but \( \in GF(q^3) \) |
| Case5 | (2,1') \( g \) | \[
\begin{bmatrix}
g_1 & 0 & 0 \\
0 & g_1^q & 0 \\
0 & 0 & g_1^{q^2}
\end{bmatrix}
\] | \( g_1, g_1^q, g_1^{q^2} \) but \( \in GF(q^3) \) |
| Case6 | (2,1,1) \( m \) | \[
\begin{bmatrix}
m_1 & 0 & 0 \\
0 & m_1^q & 0 \\
0 & 0 & m_1^{q^2}
\end{bmatrix}
\] | \( m_1, m_1^q, m_1^{q^2} \) but \( \in GF(q^3) \) |
| Case7 | (1') \( a \) | \[
\begin{bmatrix}
a_1 & 0 & 0 \\
0 & a_1^q & 0 \\
0 & 0 & a_1^{q^2}
\end{bmatrix}
\] | \( a_1 \) \( \in GF(q) \) |
| Case8 | (1',1) \( c \) | \[
\begin{bmatrix}
c_1 & 0 & 0 \\
0 & c_1^q & 0 \\
0 & 0 & c_1^{q^2}
\end{bmatrix}
\] | \( c_1, c_1^q \) \( \in GF(q) \) |
| Case9 | (1',1') \( d \) | \[
\begin{bmatrix}
d_1 & 0 & 0 \\
0 & d_1^q & 0 \\
0 & 0 & d_1^{q^2}
\end{bmatrix}
\] | \( d_1, d_1^q \) \( \in GF(q) \) |
3.1.3 Remark: By definition (3.2.3) the number of irreducible polynomials over GF(2) is given by the following table (see appendix [A.3.1]):

<table>
<thead>
<tr>
<th>r</th>
<th>Ψ(r)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>7</td>
<td>18</td>
</tr>
<tr>
<td>8</td>
<td>30</td>
</tr>
</tbody>
</table>

Where from theorems (3.3.1) & (3.3.2) the irreducible polynomials of degree n=1,2,3,4,5,6,7 and 8 over GF(2) are given in the following table (see appendix [A.3.2]):

<table>
<thead>
<tr>
<th>Deg.</th>
<th>No. of irr. Pol.</th>
<th>Irreducible polynomial</th>
<th>Matrix form</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>f₁(x)=x+1</td>
<td>[1]</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>f₂(x)=x²+x+1</td>
<td>[0 1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[1 1]</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>f₃(x)=x³+1</td>
<td>[0 0 1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>f₄(x)=x³+x²+1</td>
<td>[1 0 1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[1 0 0]</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>f₅(x)=x⁴+x³+1</td>
<td>[0 0 0 1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>f₆(x)=x⁴+x²+x³+1</td>
<td>[1 0 0 0]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[1 0 0 1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>f₇(x)=x⁴+x³+x²+x+1</td>
<td>[0 1 0 0]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[0 0 1]</td>
</tr>
</tbody>
</table>

Reference


E.mail: scianb@yahoo.com