ISSN: 1991-8941

The Projective Special Linear Group 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 GF(pr) and deals with canonical form which represents the conjugacy class of the groups with dimension 4 over a field GF(2).

Keywords: Projective , Special , Linear Group , 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 PSL(2,q) and independently by WIMAN(1899). The subgroups of PSL(3,q) were found by MITHELL(1911) while KHALF(1993) determined the subgroups of PSL(7,2a). The present work investigates the linear groups over a field 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 Pn elements where p is prime, is called a GALOIS Field of order Pn and is denoted by GF(pn).

3. Definition: A polynomial is an expression of the form

f(t)=antn+an-1tn-1+…+a1t+a0, where a0,a1,a2,…,an are real numbers. If an≠0 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 β be a bilinear form on n-dimensional vector space over a field F. We say that β is non-singular if it satisfies the condition:

β(x,y)=0 ∀ y ∈ V, then x=0.

A pair (V, β) is called a non-singular space if β 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 GL(n,F), where n denotes the dimension of V. If F is a finite field with q elements then GL(n,F) is denoted by GL(n,q).

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

7. Remark: The order of the classical group:

$|GL(n,q)|=qn(n-1)/2 \prod_{i=1}^{n}(q^i-1)$.

$|SL(n,q)|=|PGL(n,q)|=qn(n-1)/2 \prod_{i=2}^{n}(q^i-1)$.

|PSL(n,q)|=[1/(n,q)].|SL(n,q)|. [3]

8. Definition: A polynomial f(x) in F[x] is said to be irreducible over a field F, if whenever f(x)=a(x).b(x) with a(x),b(x) ∈ F[x] then one of a(x) or b(x) has zero degree, otherwise f(x) is called reducible. [4]

9. Remark: Irreducibilty depends on the field; for instance the polynomial x2+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) ┼ 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 ┼ P ∀ r>s∈ Z+ such that n|2s-1. [4]

12. Corollary: Let n|P, then c(x) is irreducible if for some r>s∈ Z+ n|2s-1.[4]

13. Definition: The number of irreducible polynomials

Let P(x) be the a polynomial of degree r where r>0, then we can write

$$r=\prod_{i=1}^{k} p_i^{a_i}$$

(pi distinct primes, ai positive integers.

The Mobius function is defined by:

$$m(r)=\begin{cases}1 & r=1\\ 0 & \prod_{i=1}^{k} a_i \rangle 1\\ (-1)^k & otherwise\end{cases}$$

If p prime μ(p)=-1 and if q is prime also then μ(pq)=1 while μ(p2)=0,

Hence the number of irreducible polynomials over F2 of degree r is given by

$$\Psi(r)=\frac{1}{r}\sum_{d/r} 2^d\, m(r/d)$$

where the sum extended over all positive divisor d of r. [2]

14. Definition: Let f(x)=a0+a1x+a2x2+…+anxn be any polynomial over F where an≠ 0. The following n×n matrix

$$\begin{bmatrix} 0 & 0 & \dots & 0 & -\frac{a_0}{a_n}\\ 1 & 0 & \dots & 0 & -\frac{a_1}{a_n}\\ 0 & 1 & \dots & 0 & -\frac{a_2}{a_n}\\ \vdots & \vdots & \dots & \vdots & \vdots\\ 0 & 0 & \dots & 1 & -\frac{a_{n-1}}{a_n}\end{bmatrix}$$

is called the Companion Matrix of the polynomial f(x) and is denoted by c(f). [13]

Note: when f(x)=a0+x then c(f)=[-a0].

15. Remark: Let g(x)=b0+b1x+b 2x2+…+bt-1xt-1+btxt be a polynomial over F where bt≠0 and f(x)=[g(x)]r then the companion matrix is the tr×tr matrix.

$$c(f)=\begin{bmatrix} c(g) & A & \dots & 0 & 0\\ 0 & c(g) & \dots & 0 & 0\\ \vdots & \vdots & \cdots & \vdots & \vdots\\ 0 & 0 & \dots & c(g) & A\\ 0 & 0 & \dots & 0 & c(g)\end{bmatrix}$$

Where A is t×t zero matrix except (t,1) of A is equal 1 and 0 is the zero matrix. [5]

16. Theorem: If T∈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:

$$\begin{bmatrix} c(f(x)^{e_1}) & 0 & \dots & 0 & 0\\ 0 & c(f(x)^{e_2}) & \dots & 0 & 0\\ \vdots & \vdots & \dots & \vdots & \vdots\\ 0 & 0 & \dots & 0 & c(f(x)^{e_r})\end{bmatrix}$$

where e =e1≥ e2 ≥… ≥ er. [5]

17.Corollary: If T∈GL(n,F) has as minimal polynomial $m(x)=f_1(X)^{r_1}+f_2(X)^{r_2}+\cdots+f_n(X)^{r_n}$ in F[x] where fi(x),i=1,2,…,n are irreducible distinct polynomials in F[x] then there exists a basis for V such that T has the following matrix representation:

$$\begin{bmatrix} R_1 & 0 & \dots & 0 & 0\\ 0 & R_2 & \dots & 0 & 0\\ \vdots & \vdots & \dots & \vdots & \vdots\\ 0 & 0 & \dots & R_{n-1} & 0\\ 0 & 0 & \dots & 0 & R_n\end{bmatrix}$$

where

$$R_i=\begin{bmatrix} c(f(x)^{e_{i_1}}) & 0 & \dots & 0 & 0\\ 0 & c(f(x)^{e_{i_2}}) & \dots & 0 & 0\\ \vdots & \vdots & \dots & \vdots & \vdots\\ 0 & 0 & \dots & c(f(x)^{e_{i_{n-1}}}) & 0\\ 0 & 0 & \dots & 0 & c(f(x)^{e_{i_n}})\end{bmatrix}$$

where $e_i=e_{i_1}\geq e_{i_2}\geq\cdots\geq e_{i_n}$ and 0 denotes the zero matrix. [13]

18. Conjugacy Classes of PSL(4,pr)

PSL(4,pr) contains an element whose characteristic determinate;

$\Delta(x)=$ x4-a1x3 –a2x2 –a3x –a4 .

The coefficient a1, a2, a3 and a4 ∈ GF(pr), a4≠ 0.

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.

11. Four distinct linear factors.

Let q=p^r and let a, b, g, l be a primitive roots of GF(q), GF(q^2), GF(q^3) and GF(q^4) respectively such that $a = b^{q+1} = g^{q^2+q+1} = l^{q^3+q^2+q+1}$. Then according to the above cases each element of PSL(4,q) is similar to a matrix of one of the following types:

Table [2-2]

Type	Symbol	**Canonical form**	Notes
Case1	(4)	$\begin{bmatrix} l_4 & 0 & 0 & 0 \\ 0 & l_4^q & 0 & 0 \\ 0 & 0 & l_4^{q^2} & 0 \\ 0 & 0 & 0 & l_4^{q^3} \end{bmatrix}$	$l_4, l_4^q, l_4^{q^2}, l_4^{q^3}$ $\in$GF(q^4) but $\notin$GF(q^3)
Case2	(3,1)	$\begin{bmatrix} g_3 & 0 & 0 & 0 \\ 0 & g_3^q & 0 & 0 \\ 0 & 0 & g_3^{q^2} & 0 \\ 0 & 0 & 0 & g_1 \end{bmatrix}$	$g_3, g_3^q, g_3^{q^2}, g_1$ $\in$GF(q^3) but $\notin$GF(q^2)
Case3	(2,2)	$\begin{bmatrix} b_2 & 0 & 0 & 0 \\ 0 & b_2^q & 0 & 0 \\ 0 & 0 & m_2 & 0 \\ 0 & 0 & 0 & m_2^q \end{bmatrix}$	b_2, b_2^q, m_2, m_2^q $\in$GF(q^2) but $\notin$GF(q)
Case4	(2^2)	$\begin{bmatrix} b_2 & 0 & 0 & 0 \\ 0 & b_2^q & 0 & 0 \\ 0 & 0 & b_2 & 0 \\ 0 & 0 & 0 & b_2^q \end{bmatrix}, \begin{bmatrix} b_2 & 1 & 0 & 0 \\ 0 & b_2^q & 0 & 0 \\ 0 & 0 & b_2 & 0 \\ 0 & 0 & 0 & b_2^q \end{bmatrix}, \begin{bmatrix} b_2 & 1 & 0 & 0 \\ 0 & b_2^q & 0 & 0 \\ 0 & 0 & b_2 & 1 \\ 0 & 0 & 0 & b_2^q \end{bmatrix}$	$b_2, b_2^q,$ $\in$GF(q^2) but $\notin$GF(q)
Case5	($2,1^2$)	$\begin{bmatrix} b_2 & 0 & 0 & 0 \\ 0 & b_2^q & 0 & 0 \\ 0 & 0 & b_1 & 0 \\ 0 & 0 & 0 & b_1 \end{bmatrix}, \begin{bmatrix} b_2 & 0 & 0 & 0 \\ 0 & b_2^q & 0 & 0 \\ 0 & 0 & b_1 & 1 \\ 0 & 0 & 0 & b_1 \end{bmatrix}$	b_1, b_2, b_2^q $\in$GF(q^2) but $\notin$GF(q)
Case6	(2,1,1)	$\begin{bmatrix} b_2 & 0 & 0 & 0 \\ 0 & b_2^q & 0 & 0 \\ 0 & 0 & b_1 & 0 \\ 0 & 0 & 0 & m_1 \end{bmatrix}$	b_1, m_1, b_2, b_2^q $\in$GF(q^2) but $\notin$GF(q)
Case7	(1^4)	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_1 & 0 \\ 0 & 0 & 0 & a_1 \end{bmatrix}, \begin{bmatrix} a_1 & 1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_1 & 0 \\ 0 & 0 & 0 & a_1 \end{bmatrix}, \begin{bmatrix} a_1 & 1 & 0 & 0 \\ 0 & a_1 & 1 & 0 \\ 0 & 0 & a_1 & 0 \\ 0 & 0 & 0 & a_1 \end{bmatrix}$ $, \begin{bmatrix} a_1 & 1 & 0 & 0 \\ 0 & a_1 & 1 & 0 \\ 0 & 0 & a_1 & 1 \\ 0 & 0 & 0 & a_1 \end{bmatrix}$	a_1 $\in$GF(q)
Case8	(1^3,1)	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_1 & 0 \\ 0 & 0 & 0 & a_2 \end{bmatrix}, \begin{bmatrix} a_1 & 1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_1 & 0 \\ 0 & 0 & 0 & a_2 \end{bmatrix}, \begin{bmatrix} a_1 & 1 & 0 & 0 \\ 0 & a_1 & 1 & 0 \\ 0 & 0 & a_1 & 0 \\ 0 & 0 & 0 & a_2 \end{bmatrix}$	a_1, a_2 $\in$GF(q)
Case9	(1^2,1^2)	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_2 \end{bmatrix}, \begin{bmatrix} a_1 & 1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_2 \end{bmatrix}, \begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 1 \\ 0 & 0 & 0 & a_2 \end{bmatrix},$	a_1, a_2 $\in$GF(q)

		$\begin{bmatrix} a_1 & 1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 1 \\ 0 & 0 & 0 & a_2 \end{bmatrix}$	
Case10	$(1^2,1,1)$	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_3 \end{bmatrix}, \begin{bmatrix} a_1 & 1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_3 \end{bmatrix}$	$a_1, a_2, a_3 \in GF(q)$
Case11	(1,1,1,1)	$\begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & a_3 & 0 \\ 0 & 0 & 0 & a_4 \end{bmatrix}$	$a_1, a_2, a_3, a_4 \in GF(q)$

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 [3-1]

r	2	3	4	5	6	7	8	…
$\Psi(r)$	1	2	3	6	9	18	30	…

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 [3-2]

Deg.	No. of irr. Pol.	Irreducible polynomial	Matrix form
1	1	$f_1(x)=x+1$	[1]
2	1	$f_2(x)=x^2+x+1$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
3	2	$f_3(x)=x^3+x+1$ $f_4(x)=x^3+x^2+1$	$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$
4	3	$f_5(x)=x^4+x+1$ $f_6(x)=x^4+x^3+1$ $f_7(x)=x^4+x^3+x^2+x+1$	$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

Reference

1. Al-Timimi A.H.J., The 6-Dimensional linear groups over a field of two elements, Ph.D. thesis university of Birmingham 1978.
2. Al-Timimi A.H.J. and Khalf M. K. , The irreducible subgroups of PSL(V8,2q) Iraqi society of physic and mathematics, 1994.
3. Dimartion L. and Wagner A. , The irreducible subgroups of PSL(V5,q) where q is odd resulted dermath, 1978.
4. Golomb S.W. ,Shift Register Sequences, San Francisco 1967.
5. Herstun I.N. ,Topics in Algebra, Corporation USA 1975.
6. S.S ,On the 8-dimensional linear groups over a field of characteristic two , university of Al-Mustansitiyah 1997.

الزمرة الخطية الاسقاطية الخاصة

علاء عدنان عواد مثنى عبد الواحد محمود

E.mail: scianb@yahoo.com

الخلاصة

لقد قمنا بدراسة صفوف الترافق للزمرة الخطية الاسقاطية حيث ان دراسة هذه الصفوف له اهمية عظمى ومن جهة اخرى يعتبـــر مدخلا مهما بدراسة الزمر الخطية العامة وكذلك الزمر الجزئية العظمى. لقد عرضنا في هذا البحث الصيغة القانونية التي تمثل كل صف للزمرة الخطية ذات البعد الرابع على الحقل GF(Pr) وكذلك عرض الصيغة القانونية التي تمثل صف الترافق للزمـــر ذات البعد الرابع على الحقل GF(2).