ON THE ORDER STRUCTURE OF CYCLIC AND DIHEDRAL SUBGROUPS EMBEDDED IN GL(N,Q)

OSANGO HESBON E. O.[*]

ABSTRACT

The concept of conjugacy provides an insight on the structure of finite groups. It is an equivalence relation which provides a neat algebraic description of the size of each conjugacy class in a finite group. We set to examine the order structure of cyclic and dihedral subgroups embedded in GL(n,q) for n = 2, 3. We strived to determine all possible orders of various elements of GL(n,q) and their divisors by looking at their characteristic and minimal polynomials and using the fact that matrices with the same Jordan form are similar and hence conjugate under certain conditions.

keywords: Jordan Canonical Form, Extension field, conjugacy, order structure

[*] Mathematics Department, Egerton University, P.O. Box 536, Egerton-Njoro, Kenya

1. INTRODUCTION

We denote the cyclic group of order n by C_n and it is that group generated by an element x such that $\{ x^0, x^1, x^2, \ldots, x^{n-1}\}$. Similarly, a dihedral group, D_n, is a group of symmetries of an n-gon generated by two elements, say A and B such that

$D_n = \{A, B : A^n = I, \ B^2 = I \text{ and } BAB = A^{-1}\}$ and $|D_n| = 2n$.

2. CYCLIC SUBGROUPS OF GL(2,q)

We need to identify all the possible orders of the elements of G = GL(2,q).These orders will determine the possible cyclic subgroups of G, so we consider all the possible Jordan forms of elements of G.

Remark 2.1. If A ∈ G with the characteristic polynomial, p(x) = (x- a)(x – b), then the Jordan form of A is $J = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ and the order of A is equal to the L.C.M $|a|, |b|$.

Remark 2.2: If A ∈ G with p(x) = m(x) = $(x – a)^2$, then the Jordan form of A is

$J = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$ and $J^m = \begin{bmatrix} a^m & ma^{m-1} \\ & a^m \end{bmatrix}$, $m \in \mathbb{Z}^+$. The order of A is equal to the L.C.M $(|a|, p)$ which is clearly a divisor of p(q – 1).

The following are all the possible characteristic polynomials of elements of G:

(a) $p(x) = (x – a)^2$

(b) p(x) = (x –a)(x – b), a ≠ b.

(c) $p(x) = x^2 + bx + c$, which is irreducible in F.

In case (a) above, there are two possible minimal polynomials, m(x) = x – a or m(x) = $(x – a)^2$.

When m(x) = x – a, and A ∈ G, then the Jordan form of A is J = $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ and that $J^m = a^m \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $m \in \mathbb{Z}^+$, hence the order of A is equal to the order of a, which is a divisor of q – 1. Hence G contains cyclic subgroups of order k where $k \mid q-1$.

When m(x) = p(x) = $(x - a)^2$, then the Jordan form of A ∈ G is J = $\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$ and that $J^m = \begin{bmatrix} a^m & ma^{m-1} \\ & a^m \end{bmatrix}$, $m \in \mathbb{Z}^+$,hence the order of A is a divisor of the L.C.M $(|a|, p)$ which is p(q - 1) (see remark 2.2). Hence G contains cyclic subgroup of order k, where $k \mid p(q-1)$.

In case (b), if A ∈ G with p(x) = (x – a)(x – b), then the Jordan form of A is $J = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, so the order of A is equal to the L.C.M $|a|, |b|$ (see remark 2.1) which is q – 1. Hence G contains cyclic subgroups of order k, where $k \mid q-1$.

In case (c), let A ∈ G with p(x) = x^2 + bx + c which is irreducible in F, then p(x) has roots in the quadratic extension field E of F. The Jordan form of A is $J = \begin{bmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{bmatrix}$, where $\alpha \in E$ and $\overline{\alpha}$ is its conjugate. Clearly the order of A is equal to the order of α, which divides q^2 – 1. Hence G contains cyclic subgroups of order k, where $k \mid q^2 - 1$.

Hence we observe that the only possible orders of elements of G are p(q – 1), q^2 – 1 and their divisors.

Theorem 2.3. A cyclic subgroup of G has order dividing either p(q – 1) or q^2 – 1.

Proof: As outlined above. □

Example 2.4. Let G =GL(2,2). Then $|G| = 6$. The only orders of elements of G are 1, 2 and 3. This implies that G contains cyclic subgroups of orders 1, 2, 3 since 2 = p(q-1) and 3 = q^2 – 1, hence obeying Theorem 2.3.

3. DIHEDRAL SUBGROUPS IN GL(2,q)

Lemma 3.1. Let $A \in G = GL(n,q)$ with $p(x) = x^n + a_n x^{n-1} + \ldots + a_2 x + a_1$, then the characteristic polynomial of $A^{-1} \in G$ is $a_1 x^n + a_2 x^{n-1} + \ldots + a_{n-1} x^2 + a_n x + 1$, with the coefficients of p(x) reversed.

Thus from the definition of dihedral subgroup, A and A^{-1} have the same Jordan form, so their minimal polynomials are equal.

The characteristic polynomials of the elements of G = GL(2,q) are of the form p)x) = $x^2 + ax + b$. So the characteristic polynomials of the inverses of elements of G will have the form

$$h(x) = bx^2 + ax + 1 \quad \text{(lemma 3.1)}$$

$$\Leftrightarrow \quad h(x) = x^2 + \frac{a}{b}x + \frac{1}{b}.$$

And two cases do arise.

Case 1(a), when b = -1 and p≠2. a = -a $\Rightarrow$ a = 0 and $p(x) = x^2 - 1$.

Let $A \in G$ with $p(x) = x^2 - 1$, then the Jordan form of A is $J = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Clearly $J^2 = I$. We choose a matrix X such that $X^2 = I$ and $X^{-1}JX = J^{-1}$.

Let $X = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, then $X^2 = I$ and $X^{-1}JX = J^{-1} = J$.

Hence we get Klein's 4-group $C_2 \times C_2$ which is sometimes regarded as a dihedral group of order 4, which is D_2.

Case 1(b), when b = -1 and p = 2 and $p(x) = (x - 1)^2$, so there are two possible minimal polynomials to consider.

When m(x) = x – 1 and let $A \in G$, then the Jordan form of A is $J = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$. Then $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ satisfies the conditions $X^2 = I$ and $X^{-1}JX = J^{-1}$. In this case we get cyclic subgroup C_2.

On the other hand, if p(x) = m(x) = $(x-1)^2$ and A ∈ G, then the Jordan form of A is $J = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, a ≠ 0, 1, then X satisfies the conditions $X^2 = I$ and $X^{-1}JX = J^{-1}$. Hence we get D_2, so G contains dihedral subgroup D_2.

Case 2: When b = 1, a = a and p(x) = $x^2 + ax + 1$.

From these the characteristic polynomial, p(x) can be

(a) reducible with distinct roots (b) irreducible (c) reducible with repeated roots.

For case 2(a), the roots of the characteristic polynomial p(x) = $x^2 + ax + 1$ must be of the form b and b^{-1} for $bb^{-1} = 1$. Hence p(x) = $(x-b)(x-b^{-1})$.

Let A ∈ G with this p(x), then the Jordan form of A is $J = \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}$. We choose a matrix X ∈ G such that $X^2 = I$ and $X^{-1}JX = J^{-1}$. Let X = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $X^2 = I$ and $X^{-1}JX = J^{-1}$. The order of J equals the order of b which can be q – 1 or its divisors (F_q has no zero divisors). Hence G contains D_k where k ≥ 2 and $k \mid q-1$.

For case 2(b), when p(x) = $x^2 + ax + 1$ is irreducible in F. Then p(x) has two distinct roots in the quadratic extension field E of F. So p(x) = $(x - \alpha)(x - \overline{\alpha})$ where $\alpha \in E,\ \alpha\overline{\alpha} = 1 = Norm(\alpha)$ since roots in the quadratic extension are conjugate.

The Jordan form of A is $J = \begin{bmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{bmatrix}$ and $J^{-1} = \begin{bmatrix} \overline{\alpha} & 0 \\ 0 & \alpha \end{bmatrix}$. We find that $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ satisfy the conditions $X^2 = I$ and $X^{-1}JX = J^{-1}$. Clearly the order of J equals the order of ∝. But the elements ∝ of norm 1 form a subgroup of E* which is the kernel of the mapping

$$\tau : E^* \rightarrow F^*$$

defined by $\tau(\beta) = norm(\beta),\quad \beta \in E^*,\ \tau$ is an onto homomorphism. By First Isomorphism Theorem,

$$F^* \cong E^*/K, \text{ where K is the kernel of } \tau.$$

So

$$|K| = \frac{|E^*|}{|F^*|} = q+1.$$

Hence the order of $\propto$ is q + 1 or its divisors. Therefore G contains D_k where $k \geq 2$ and $k \mid q+1$.

For case 2(c), when $p(x) = x^2 + ax + 1$ with repeated roots.

Here $a = \pm 2$, so we have two cases to consider.

When $a = 2$ and $p \neq 2$, then $p(x) = (x+1)^2$. Let $A \in G$ then the Jordan form of A is either

$$J = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \text{ or } J = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}.$$

Suppose $J = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, the order of J is 2 and $X = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ satisfies the conditions $X^2 = I$ and $X^{-1}JX = J^{-1}$. So G contains D_2.

Similarly, if $J = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$ and $J^p = -I$ and $J^{2p} = I$. Then the order of J is 2p.

Let $X = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, then this matrix satisfies the set conditions. Hence G contains D_k, where $k \mid 2p$ and $k \geq 2$.

Also when $a = 2$ and $p = 2$, $p(x) = (x+1)^2$. Let $A \in G$ with this p(x), then the Jordan form of A is either $J = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ which is similar to 1(b), or $J = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, then $J^p = I$ hence $o(J) = p$.

Matrix $X = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ will satisfy the conditions $X^2 = I$ and $X^{-1}JX = J^{-1}$. Hence G contains D_p.

In case 2, G contains both D_{2p} and D_p.

The above results are summed up in the following theorem.

Theorem 3.2: The general linear group GL(2,q) contains a dihedral subgroup D_k, where $k \geq 2$ and k divides either $q + 1$, $q - 1$ or $2p$.

Proof: As explained above.

□

Example: In GL(2,7) the only dihedral subgroups are of the type D_{14}, D_8, D_7, D_6, D_4, D_3, and D_2 (by Theorem 3.2).

4. Cyclic Subgroups in GL(3,q)

Again, we consider all the possible orders of the elements of G = GL(3,q) by considering all the possible Jordan forms of the elements of G.

The following are all the possible characteristic polynomials of the elements of G:

(a) $p(x) = (x - a)^3$ (b) $p(x) = (x - a)(x - b)^2$, $a \neq b$.

(c) $p(x) = (x - a)(x - b)(x - c)$, $a \neq b \neq c$

(d) $p(x) = (x - a)(x^2 + bx + c)$, $(x^2 + bx + c)$ is irreducible in F.

(e) $p(x) = x^3 + ax^2 + bx + c$, irreducible in F.

Case (a) Suppose $A \in G$ with $p(x) = (x - a)^3$, then the Jordan form of A is either of the form:

$$\text{(i)} \begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix} \quad \text{(ii)} \begin{bmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix} \text{ or } \text{(iii)} \begin{bmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{bmatrix}.$$

For (i) all elements are contained in a cyclic subgroups of G of order q – 1. Hence G contains a cyclic subgroup of order k, where $k \mid q-1$.

For (ii) if $J = \begin{bmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix}$ then $J^m = \begin{bmatrix} a^m & ma^{m-1} & 0 \\ 0 & a^m & 0 \\ 0 & 0 & a^m \end{bmatrix}$, $m \in \square^+$. Clearly the order of J is equal to the L.C.M $(|a|, p)$ (see section 2, Remark 2.2). Hence every element of the form J is contained in a cyclic subgroup of G of order p(q – 1). Hence G contains a cyclic subgroup of order k, where k ≥ 2 and $k \mid p(q-1)$.

For (iii), when $J = \begin{bmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{bmatrix}$, then $J^m = \begin{bmatrix} a^m & ma^{m-1} & \frac{m(m-1}{2}a^{m-2} \\ 0 & a^m & ma^{m-1} \\ 0 & 0 & a^m \end{bmatrix}$, $m \in \square^+$.

When p ≠ 2, o(J) = L.C.M $(|a|, p)$ (see section 2, Remark 2.2). Hence every element of the form J has order dividing p(q – 1). So G contains a cyclic subgroup of order k, where $k \mid p\ q-1$.

When p = 2 to get zeros for entries a_{12}, a_{13} and a_{23} in the matrix J^m above, m(m – 1) must be a multiple of 4, hence the order of J is equal to the L.C.M $|a|, 4 = |a|, p^2$. Hence G contains a cyclic subgroup of order k, where $k \mid p^2(q-1)$.

Case (b) when $p(x) = (x-a)(x-b)^2$, $a \neq b$.

Let A∈G with this p(x), then the Jordan form of A is either of the form

(i) $J = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & b \end{bmatrix}$ or (ii) $J = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 1 \\ 0 & 0 & b \end{bmatrix}$.

For $J = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & b \end{bmatrix}$, the order of J is a divisor of the L.C.M $|a|, |b|$ which is q – 1. Hence G contains cyclic subgroups of order k, where $k \mid q-1$.

And for $J=\begin{bmatrix} a & 0 & 0 \\ 0 & b & 1 \\ 0 & 0 & b \end{bmatrix}$, then $J^m=\begin{bmatrix} a^m & 0 & 0 \\ 0 & b^m & mb^{m-1} \\ 0 & 0 & b^m \end{bmatrix}$, $m \in \square^+$ and every element of J has order dividing p(q – 1) (see section2, remark 2.2). Hence G contains cyclic subgroups of order k, where $k \mid p(q-1)$.

Case (c): when p(x) =(x – a)(x – b)(x – c), a ≠ b ≠ c.

Suppose A∈G with this p(x), then the Jordan form of A is $J=\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}$. Clearly the o(J)=L.C.M $|a|,|b|,|c|$ and every element of the form J is contained in a cyclic subgroup of order q – 1. Hence G contains s=cyclic subgroups of order k, where $k \mid q-1$.

Case (d): when p(x) = (x – a)(x² + bx + c, where x²+bx+c is irreducible in F.

Suppose A∈G with this p(x), then p(x) has 3 distinct roots, 2 of which are in the quadratic extension field of F. If these roots are a, α and $\overline{\alpha}$, then the Jordan form of A is

$$J=\begin{bmatrix} a & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \overline{\alpha} \end{bmatrix}.$$

In this case the o(J) = L.C.M $|a|,|\alpha|$ and every element of the form J is contained in a cyclic subgroup of order q² – 1. Hence G contains cyclic subgroups of order k, where $k \mid q^2-1$.

Case (e): when p(x) = x³+ax²+bx +c, which is irreducible in F.

Suppose A∈G with p(x) as given, then p(x) has 3 distinct roots in the cubic extension field of F. If these roots are α, β and γ, then the Jordan form of A is

$$J=\begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{bmatrix}.$$

The order of J is equal to the L.C.M $|\alpha|,|\beta|,|\gamma|$. Thus every element of the form J is contained in a cyclic subgroup of order $q^3 - 1$. Hence G contains cyclic subgroups of order k, where $k \mid q^3 - 1$.

The following theorem summarizes our results.

Theorem 4.1:

(a) If $p = 2$, a cyclic subgroup of G has order dividing either $q^3 - 1$, $q^2 - 1$ or $p^2(q - 1)$.

(b) If $p > 2$, a cyclic subgroup of G has order dividing $q^3 - 1$, $q^2 - 1$ or $p(q - 1)$.

Proof: As outlined above in section 4.

□

The following two examples confirm the above results:

Example 4.2: Let $G = GL(3,2)$. Then the only orders of the elements of G are 1, 2, 3, 4 and 7.Clearly these orders are divisors of either 3, 4 or 7. Also observe that $3 = q^2 - 1$, $4 = p^2(q-1)$. Hence theorem 4.1 is obeyed.

Example 4.3: Let $G = GL(3,3)$. Then the only orders of elements of G are 1, 2, 3, 4, 6, 8, 13 and 26. Clearly these orders are divisors of either 6, 8 or 26. Observe that $6 = p(q-1) = 3(2)$, $8 = q^2 - 1 = 3^2 - 1$ and $26 = q^3 - 1$. Hence Theorem 4.1 is obeyed.

5. Dihedral Subgroups in GL(3,q)

Similar to section 3, we consider elements with the same characteristic polynomials as their inverses in $G = GL(3,q)$.

Generally the characteristic polynomial of an element A in G is of the form

$$x^3 + ax^2 + bx + c \qquad (5.1)$$

The characteristic polynomial of the inverse of A in G has the coefficients of (5.1) reversed, hence it is of the form

$$cx^3 + bx^2 + ax + 1 \quad \text{(see Lemma 3.1)}$$

$$\Leftrightarrow \quad x^3 + \frac{b}{c}x^2 + \frac{a}{c}x + \frac{1}{c} \qquad (5.2)$$

Since A is conjugate to A^{-1}, (5.1) and (5.2) are equal. Hence

$$a = \frac{b}{c}, \quad b = \frac{a}{c} \quad and \quad c = \frac{1}{c} \quad \Rightarrow \quad c = \pm 1.$$

Now when c = 1, b = a and $p(x) = x^3 + ax^2 + ax + 1 = (x - 1)(x^2 + (a - 1)x + 1)$.

And when c = -1, b = -a and $p(x) = x^3 + ax^2 - ax - 1 = (x - 1)(x^2 + (a + 1)x + 1)$.

Clearly these polynomials do not include the cubic irreducible ones. Hence p(x) can be with:

(a) reducible quadratic polynomials

(b) two repeated roots

(c) three distinct roots

(d) three repeated roots .

Cases (a), (b) and (c)

Since $c = \pm 1$, the matrix $A \in G$ has the general form $\begin{bmatrix} \mp 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{bmatrix}$ which gives the required characteristic polynomials.

In determining the dihedral subgroups embedded in G, we find that cases (a), (b) and (c) of p(x) above are treated in the same way as in Section 3. Since in the general matrix above what matters is the 2 x 2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dealt with in section 3. In each case the matrix Y such that $Y^2 = I_3$ and $Y^{-1}JY = J^{-1}$ is of the form

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & j & k \\ 0 & l & m \end{bmatrix}, \quad where \quad \begin{bmatrix} j & k \\ l & m \end{bmatrix} = X \text{ is as in section 3.}$$

So from these cases, G contains dihedral subgroups D_k, where $k \geq 2$ and k divides either $q - 1$, $q + 1$ or $2p$.

Case (d): When p(x) has three repeated roots.

When $p \neq 2$, there are two possibilities, namely $p(x) = (x - 1)^3$ and $p(x) = (x + 1)^3$.

Let $A \in G$ with $p(x) = (x - 1)^3$, then the Jordan form of A is either

$$J = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad J = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad or \quad J = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

The first two forms of J were dealt with in case (d) in section 4. Hence G contains D_p.

And when $J = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$, we have $(J - I_3)^p = 0$ since $p \geq 3 \Rightarrow J^p = I_3$. Hence order of J is p.

We now find a matrix Y such that $Y^2 = I_3$ and $Y^{-1}JY = J^{-1}$.

The general form of Y is $Y = \begin{bmatrix} rs & t & 0 \\ 0 & s & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and since $Y^2 = I_3$, we have

$$Y^2 = \begin{bmatrix} (rs)^2 & st(r+1) & 0 \\ 0 & s^2 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$\Rightarrow \quad (rs)^2 = 1 \quad$ and $\quad s^2 = 1.$

To get Y satisfying the above conditions, we choose r and s to be elements of order 2 in F*. Clearly $r + 1 = 0$ since $r^2 = 1$. Thus $r = 1$ or -1, but since $p \geq 3$, $r \neq 1$, hence $r + 1 = 0$.

To get t, we use the equation $Y^{-1}JY = J^{-1}$.

Finally, let $A \in G$ with $p(x) = (x + 1)^3$, then the Jordan form A will either be

$$J=\begin{bmatrix}-1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{bmatrix}, \qquad J=\begin{bmatrix}-1 & 1 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{bmatrix} \quad or \quad J=\begin{bmatrix}-1 & 1 & 0\\ 0 & -1 & 1\\ 0 & 0 & -1\end{bmatrix}.$$

The first two forms of J have been dealt with in a similar way to those of section 3 case (c).

When $J=\begin{bmatrix}-1 & 1 & 0\\ 0 & -1 & 1\\ 0 & 0 & -1\end{bmatrix}$, we have $(J + I_3)^p = 0$. Since $p \geq 3$, $\Rightarrow J^p = -I_3 \quad \Leftrightarrow J^{2p} = I_3$.

So the order of J is 2p. By the method described in (d), we get $Y \in G$ such that $Y^2 = I_3$ and $Y^{-1}JY = J^{-1}$. Hence G contains dihedral subgroups D_k, where $k \geq 2$ and $k \mid 2p$.

Having considered all the possible forms of elements of G with the same characteristic polynomials as their inverses, we sum-up the results in the following theorem:

Theorem 5.1 The general linear group, GL(3,q) contains dihedral subgroups D_k, where $k \geq 2$ and k divides either $q + 1$, $q - 1$ or $2p$.

Proof: See outline above. □

Example 5.2: In GL(3,3), the only dihedral subgroups are of the type D_2, D_3, D_4 and D_6.

6. References

[1] Adan-Bante E. On Conjugacy Classes and derived length, J. Algebra, 266 : 305-319, 2003.

[2] Durbin R.J. Modern Algebra, An Introduction, 3rd Edition, John Willey and Sons Inc. NY, 1985.

[3] Fraleigh J.B. A First Course in Abstract Algebra, 6th edition. Addison-Wesley Publishing Company, London, 1999.

[4] Finkbeiner II T.D, Introduction on Matrices and Transformations, 3rd Edition, W.H. Freeman Company, San Francisco, 1978.

[5] Herstein I.N., Topics in Algebra, 2nd Edition. John Willey and Sons Inc., NY, 1975.

[6] Huppert B, Endliche grupperI, Die grundlelren der Mathematischen, Springer, Berlin, 1967.

[7] Kostrikin A.I, Bbegehue b Algebra (in Russian), Akademik Nauka Publishers, Moskva, 1978.