# On conjugacy and order structure of certain classes of finite groups

**Article** *in* International Journal of Pure and Applied Mathematics · March 2014

DOI: 10.12732/ijpam.v91i4.2



**2 authors**, including:

Maurice Owino Oduor
University of Kabianga
**33** PUBLICATIONS **50** CITATIONS

SEE PROFILE

**International Journal of Pure and Applied Mathematics**
**Volume 91 No. 4 2014, 435-458**
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
**url:** http://www.ijpam.eu
**doi:** http://dx.doi.org/10.12732/ijpam.v91i4.2


# ON CONJUGACY AND ORDER STRUCTURE OF CERTAIN CLASSES OF FINITE GROUPS

Osango E.O. Hesbon[1] §, Owino Maurice Oduor[2]

[1]Department of Mathematics
Egerton University
P.O. Box 536, Egerton, KENYA
[2]Department of Mathematics and Computer Science
University of Kabianga
P.O. Box 2030-20200, Kericho, KENYA

**Abstract:** The classification of finite groups still remains an open problem. 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 conjugacy and order structures of general linear groups, $GL(n, q)$ and special linear groups, $SL(n, q)$ with some restrictions on $n$. We have also established the special cases of conjugacy classes of $GL(n, q)$ splitting in $SL(n, q)$ and given the conditions of splitting or not splitting.

**AMS Subject Classification:** 20E45, 20H30
**Key Words:** conjugacy classes, finite groups

## 1. Introduction

It is well known that simple groups have been classified. But the classification of all finite groups still remain an open problem. The structures of conjugacy and order of elements in finite groups have proved to be powerful tools towards the classification of these groups. In this case, we have classified the $GL(n, q)$ and its subgroup, $SL(n, q)$ when $n = 2, 3$ and $q \leq 5$. Earlier work began with Lipchurtz, who used group field concepts to say that the order of $F$ be $q$ and

Received: October 23, 2013



§Correspondence author

is paramount to general linear groups. These are multiplicative groups of all $n \times n$ invertible matrices over $F$. Moori and Basheer [8] studied the properties and structure of the general linear group $GL(n, F)$ and some of its subgroups if $F$ is finite with $q$ elements.

## 2. The Conjugacy and Order Structure of $GL(2, q)$

Let $F$ be a finite field with $q$ elements, where $q = p^r$, for some prime $p$. Using a well known result that matrices with the same Jordan form are similar and hence conjugate. The normalizer of $A$ in $G$, $N_G(A)$, includes all matrices of the form

$$\alpha_0 I + \alpha_1 A + \alpha_2 A^2 + \cdots + \alpha_{n-1} A^{n-1}.$$

**Theorem 2.1.1.** *If the eigenvalues of the minimal polynomial $m(x)$ of a matrix $A \in G$ are distinct, then $N_G(A)$ contains only the matrices of the form*

$$\alpha_0 I + \alpha_1 A + \alpha_2 A^2 + \cdots + \alpha_{n-1} A^{n-1}.$$

*Proof.* Let $A$ be a matrix whose eigenvalues are $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that $\lambda_i \neq \lambda_j,\ i, j = 1, 2, \ldots, n$. Consider all the matrices that commute with $A$, i.e.

$$N_G(A) = \{B :\ BA = AB\}.$$

We show that $B$ is of the form

$$\alpha_0 I + \alpha_1 A + \alpha_2 A^2 + \cdots + \alpha_{n-1} A^{n-1}.$$

Let $Av = \beta v$ where $\beta = \lambda_i,\ i = 1, 2, \ldots, n$. Then

$$B(Av) = B(\beta v) \quad \Rightarrow A(Bv) = \beta(Bv).$$

This implies that $Bv$ is an eigenvector of $A$ corresponding to the eigenvalue $\beta$.

Since eigenvectors of distinct eigenvalues are linearly independent, $Bv$ must be a multiple of $v$, hence $Bv_i = \mu_i v_i$ where $v_i$ is an eigenvector corresponding to the eigenvalue $\lambda_i$. $B$ is determined by the scalars $(\mu_1, \mu_2, \ldots, \mu_n)$, where $\mu_i$ are not necessarily distinct.

Now, let $B_1, B_2, \ldots, B_m$ be a basis for $N_G(A)$. Then each $B_i$ is determined by scalars $\mu_1, \mu_2, \ldots, \mu_n$, where the $\mu_i$ are not necessarily distinct.

Since $B_1, B_2, \ldots, B_m$ are linearly independent if and only if the set of vectors $\mu_{i1}, \mu_{i2}, \ldots, \mu_{in}\ , i = 1, 2, \ldots, m$ in $F_n$ are linearly independent and $F_n$ has dimension $n$, then $m \leq n$. Now since matrices of the form

$$\alpha_0 I + \alpha_1 A + \alpha_2 A^2 + \cdots + \alpha_{n-1} A^{n-1},\ \alpha_j \in F,\ j = 1, 2, \ldots, n-1$$

are also in $N_G(A)$ and $\{I, A, A^2, \ldots, A^{n-1}\}$ are linearly independent and $A$ cannot satisfy a polynomial of degree less than $n$ in $F$, then the set $\{I, A, A^2, \ldots, A^{n-1}\}$ span a vector space of dimension $n$. Therefore $B$ is of the form

$$\alpha_0 I + \alpha_1 A + \alpha_2 A^2 + \cdots + \alpha_{n-1} A^{n-1}. \qquad \square$$

We use the above result together with the minimal polynomial and the corresponding Jordan forms of elements of $GL(2, q)$ to determine the conjugacy classes of the elements of $GL(2, q)$.

The following are all the possible forms of characteristic polynomials obtainable from the elements of $G$:

1. $p(x) = (x - a)^2$
2. $p(x) = (x - a)(x - b), \quad a \neq b$
3. $p(x) = x^2 + ax + b, \quad b \neq 0$, which is irreducible over $F$.

By considering the possible minimal polynomials in each case and letting a class representative of each $A \in G$ which is similar to the Jordan form, we have:-

**Case 1: when** $p(x) = (x - a)^2$ **and** $m(x) = x - a.$, then $A$ is similar to the Jordan form

$$J = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad a \neq 0.$$

Then $J$ is a scalar matrix and so commutes with each element in $G$, hence $N_G(A) = G$. The number of conjugates of $A$ is $|G : N_G(A)| = 1$. Thus each scalar matrix has only one conjugate.

The number of such matrices $J$ is $q - 1$, hence there are $q - 1$ conjugacy classes each with one element.

When $p(x) = m(x) = (x - a)^2$, then $A$ is similar to the Jordan form

$$J = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$$

We now determine the matrices which commute with $J$. Let

$$B = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in N_G(A) \text{ then}$$

$$BJ = JB \quad \Leftrightarrow \quad \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

$$\begin{aligned}
&\Leftrightarrow \quad \begin{pmatrix} ra & r+sa \\ ta & t+ua \end{pmatrix} = \begin{pmatrix} ar+t & as+u \\ at & au \end{pmatrix} \\
&\Rightarrow \quad ra = ar + t \quad \Rightarrow t = 0 \\
&\text{and} \quad r + sa = as + u \quad \Rightarrow \quad r = u.
\end{aligned}$$

Hence matrix $B$ must be of the form $B = \begin{pmatrix} r & s \\ 0 & r \end{pmatrix}$, $r \neq 0$. Since $s$ is arbitrary, we have the number of such matrices to be $q(q-1)$. Hence the number of conjugates of $A$ is

$$\frac{|GL(2,q)|}{q(q-1)} = \frac{(q^2-1)q(q-1)}{q(q-1)} = q^2 - 1.$$

The number of such matrices $J$ is $q-1$. Hence the number of conjugacy classes is $q-1$ and the number of elements in this case is $(q-1)(q^2-1)$.

**Case 2: when** $p(x) = (x-a)(x-b)$, $a \neq b$**.** Clearly $p(x) = m(x) = (x-a)(x-b)$ and $A$ is similar to the Jordan form

$$J = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

Next we determine the matrices that commute with $J$.

$$\begin{aligned}
\text{Let} \quad B = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in N_G(A), \quad &\text{then } BJ = JB \\
\Leftrightarrow \quad &\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} a & o \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix} \\
\Leftrightarrow \quad &\begin{pmatrix} ra & sb \\ ta & ub \end{pmatrix} = \begin{pmatrix} ar & as \\ bt & bu \end{pmatrix} \\
\Rightarrow \quad &ra = ar \quad \Rightarrow \quad r = r \text{ since } a \neq 0 \\
&sb = as \quad \Rightarrow \quad s = 0 \text{ since } a \neq b \\
&ta = bt \quad \Rightarrow \quad t = 0 \text{ since } a \neq b \\
&ub = bu \quad \Rightarrow \quad u = u \text{ since } b \neq 0
\end{aligned}$$

Hence $B$ must be of the form $B = \begin{pmatrix} r & 0 \\ 0 & u \end{pmatrix}$, $r, u \neq 0$. The number of such matrices is $(q-1)(q-1)$. Hence the number of conjugates of $A$ is

$$\frac{|GL(2,q)|}{(q-1)^2} = \frac{(q^2-1)(q^2-q)}{(q-1)^2} = q(q+1).$$

Thus each matrix with the Jordan form $J$ will have $q^2+q$ conjugates. The number of such matrices $J$ is

$$^{q-1}C_2 = \frac{1}{2}(q-1)(q-2)$$

Hence the number of conjugacy classes in this case is $\frac{1}{2}(q-1)(q-2)$ and the total number of elements is $\frac{1}{2}(q^2+q)(q-1)(q-2)$.

**Case 3: when $p(x) = x^2+ax+b$, which is irreducible over $F$.** Let $A \in G$ with $p(x) = x^2+ax+b$. Then $p(x)$ has two distinct roots over the quadratic extension field $E$ of $F$. Hence the matrices that commute with $A$ are of the form $a_0I + a_1A$. The set

$$\{a_0I + a_1A : a_0, a_1 \in F\}$$

form a ring $R$ isomorphic to $E = F[x]/\langle p(x)\rangle$ (see [3], pg 384) and that any two finite fields having the same number of elements are isomorphic.

Clearly the elements of the set $\{a_0I + a_1A : a_0, a_1 \in F\}$ belong to $G$ except $0I + 0A$. Hence the number of elements that commute with $A$ i.e. $|N_G(A)| = q^2-1$, since $|E^*| = q^2-1$. Now the number of conjugates of $A$ is

$$\frac{|GL(2,q)|}{(q^2-1)} = \frac{(q^2-1)(q^2-q)}{(q^2-1)} = q(q-1).$$

Thus every $2\times 2$ matrix with an irreducible characteristic polynomial has $q(q-1)$ conjugates. We now determine the number of such matrices.

Let $p(x) = x^2+ax+b$, $b \neq 0$ be the characteristic polynomial of an element in $GL(2,q)$. The number of such polynomials is clearly $q(q-1)$. To get the irreducible ones we subtract all reducible ones from $q(q-1)$. Thus

$$q(q-1) - (q-1) - \frac{(q-1)(q-2)}{2} = \frac{q(q-1)}{2}$$

Hence the total number of irreducible characteristic polynomials is $\frac{1}{2}q(q-1)$.

So the number of conjugacy classes is $\frac{1}{2}q(q-1)$ and the total number of elements in this case is $\frac{1}{2}q(q-1)q(q-1) = \frac{1}{2}q^2(q-1)^2$.

Observe that the total number of elements in the three cases is

$$\begin{aligned}(q-1) + (q-1)(q^2-1) + \frac{1}{2}(q^2+q)(q-1)(q-2) & \\ + \frac{1}{2}q^2(q-1)^2 &= q^4 - q^3 - q^2 + q \\ &= (q^2-1)(q^2-q)\end{aligned}$$

$$= |GL(2,q)|$$

Also the total number of conjugacy classes for $G$ is

$$2(q-1) + \frac{1}{2}(q-1)(q-2) + \frac{1}{2}q(q-1) = q^2 - 1.$$

In summary we have got the following results:

| The polynomial of $A \in GL(2,q)$ | Length of the conjugacy class containing $A$ |
|---|---|
| (a) $p(x) = x^2 + ax + b$ (irreducible) | $q^2 - q = q(q-1)$ |
| (b) $p(x) = (x-a)(x-b), a \neq b$ | $q^2 + q = q(q+1)$ |
| (c) $p(x) = m(x) = (x-a)^2$ | $q^2 - 1$ |
| (d) $p(x) = (x-a)^2,\ m(x) = x - a$ | 1 |

## 3. The Conjugacy Structure of $SL(2,q)$

Here we consider the subgroup $SL(2,q)$ of $GL(2,q)$ with elements (representatives) which have determinant one. We realize that some of these conjugacy classes in $G = GL(2,q)$ split into two in $H = SL(2,q)$, for some $q$. We show when this happens and the conditions of splitting.

### 3.1. Splitting of Conjugacy Classes of $GL(2,q)$ in $SL(2,q)$

Let $H = SL(2,q)$ and $G = GL(2,q)$. If $A \in H$ is a representative of a conjugacy class in $G$, then the splitting of the conjugacy class of $A$ in $H$ will occur only if the index of the normalizer of $A$ in $G$ ($|G : N_G(A)|$) is not equal to the index of the normalizer of $A$ in $H$ ($|H : N_H(A)|$).

So in order to be able to show where splitting or non-splitting occurs, we shall compare $|G : N_G(A)|$ with $|H : N_H(A)|$.

Since the normalizer of a class representative and hence its conjugacy class length in H can be easily determined in a straight forward manner from Section 3, we tabulate the results without showing any computations.

**Example 3.1.1.** Let $H = SL(2,2)$ and $G = GL(2,2)$,we have $|H| = |G| = q(q^2-1) = 6$. It is clear that $H$ is isomorphic to $G\,(H \cong G)$, hence the conjugacy structure of $H$ is the same as that of $G$. Clearly in this case there is no splitting of the conjugacy classes.

**Example 3.1.2.** Let $H = SL(2,3)$ and $G = GL(2,3)$, then we have $|H| = 24$. Let $A \in H$ be a representative of a conjugacy class in $G$. We shall get its characteristic and minimal polynomials, $p(x)$ and $m(x)$ respectively, normalizer of $A$ in $H$, $N_H(A)$ and the index of the normalizer of $A$ in $G$ and of $A$ in $H$. We then compare $|G : N_G(A)|$ with $|H : N_H(A)|$ in table 1 below.

| Class representative $(A)$ | $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ | $\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$ | $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ | $\begin{pmatrix}2 & 1\\ 0 & 2\end{pmatrix}$ | $\begin{pmatrix}0 & 2\\ 1 & 0\end{pmatrix}$ |
|---|---|---|---|---|---|
| $p(x)$ | $(x-1)^2$ | $(x-2)^2$ | $(x-1)^2$ | $(x-2)^2$ | $x^2-2$ |
| $m(x)$ | $x-1$ | $x-2$ | $(x-1)^2$ | $(x-2)^2$ | $x^2-2$ |
| $N_H(A)$ | 24 | 24 | 6 | 6 | 4 |
| $\|H : N_H(A)\|$ | 1 | 1 | 4 | 4 | 6 |
| $\|G : N_G(A)\|$ | 1 | 1 | 8 | 8 | 6 |

Table 1: Comparison of $|G : N_G(A)|$ with $|H : N_H(A)|$ when $G = GL(2,3)$ and $H = SL(2,3)$

Comparing the $5^{\text{th}}$ and $6^{\text{th}}$ rows, we observe that a conjugacy class in $GL(2,3)$ splits into two in $SL(2,3)$ only when;

$$p(x) = m(x) = (x-a)^2.$$

Similarly, when $H = SL(2,4)$ and $G = GL(2,4)$ we have $|H| = 60$. We then find that the conjugacy class lengths in $G$ is the same as that in $H$. Hence no splitting of the conjugacy classes of $GL(2,4)$ in $SL(2,4)$ in this case.

Finally let $H = SL(2,5)$ and $G = GL(2,5)$ then we have $|H| = 120$. Let $A \in H$ be a representative of a conjugacy class in $G$. We compare $|G : N_G(A)|$ with $|H : N_H(A)|$ and show the results in Table 2 below:

Comparing the $5^{\text{th}}$ and $6^{\text{th}}$ columns, we observe once again that splitting has occurred only in the cases when $p(x) = m(x) = (x-a)^2$.

### 3.2. Conditions for Splitting of Conjugacy Classes of $GL(2,q)$ in $SL(2,q)$

In this section we state a theorem which generalizes the conditions for splitting or non-splitting of conjugacy classes of $G = GL(2,q)$ in $H = SL(2,q)$. But before this we have,

| Class representative $(A)$ | $p(x)$ | $m(x)$ | $N_H(A)$ | $\|G : N_G(A)\|$ | $\|H : N_H(A)\|$ |
|---|---|---|---|---|---|
| $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ | $(x-1)^2$ | $x-1$ | 120 | 1 | 1 |
| $\begin{pmatrix}4 & 0\\0 & 4\end{pmatrix}$ | $(x-4)^2$ | $x-4$ | 120 | 1 | 1 |
| $\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$ | $(x-1)^2$ | $(x-1)^2$ | 10 | 24 | 12 |
| $\begin{pmatrix}4 & 1\\0 & 4\end{pmatrix}$ | $(x-4)^2$ | $(x-4)^2$ | 10 | 24 | 12 |
| $\begin{pmatrix}0 & 4\\1 & 0\end{pmatrix}$ | $(x-2)(x+2)$ | $(x-2)(x+2)$ | 4 | 30 | 30 |
| $\begin{pmatrix}0 & 4\\1 & 1\end{pmatrix}$ | $x^2-x-4$ | $x^2-x-4$ | 6 | 20 | 20 |
| $\begin{pmatrix}0 & 4\\1 & 4\end{pmatrix}$ | $x^2-4x-4$ | $x^2-4x-4$ | 6 | 20 | 20 |

Table 2: Comparison of $|G : N_G(A)|$ with $|H : N_H(A)|$ when $G = GL(2,5)$ and $H = SL(2,5)$

**Theorem 3.2.1.** *Let $q = p^r$ ($p$ is prime) and $A \in H$ with an irreducible minimal polynomial over $F$. Then*

$$|N_H(A)| = |N_G(A) \cap H| = \frac{q^n - 1}{q - 1}$$

*Proof.* (See [5], Theorem 7.3). □

**Theorem 3.2.2.** *Let $A \in H$ with $p(x)$ and $m(x)$ as its characteristic and minimal polynomials respectively. Then*

(a) *If $p(x) = (x-a)^2$ and $m(x) = x - a$, then the conjugacy class of $A$ in both $G$ and $H$ are the same.*

(b) *If $p(x) = m(x) = (x-a)^2$, then the conjugacy class of $A$ in $G$ remains the same in $H$ when $q \equiv 0 \,(mod\ 2)$ but splits into two when $q \equiv 1 \,(mod\ 2)$.*

(c) *If $p(x) = (x-a)(x-b)$, $a \neq b$, then the conjugacy class of $A$ in both $G$ and $H$ are the same.*

(d) *If $p(x) = x^2 + ax + b$, $b \neq 0$, and $p(x)$ is irreducible over $F$, then the conjugacy class of $A$ in both $G$ and $H$ are the same.*

*Proof.* (a) Matrix $A$ is contained in a singleton conjugacy class in $G$ (see Section 2, case 1). Clearly $A$ is also in its own conjugacy class in $H$.

(b) The number of conjugates of $A$ in $G$ is

$$q^2 - 1 \text{ (from Section 2 case 1).} \tag{1}$$

We denote from the same section that the elements of $N_H(A)$ are of the form $\begin{pmatrix} x & w \\ 0 & x \end{pmatrix}$, $x^2 = 1$.

Clearly the number of solutions of $x^2 = 1$ in $F^*$ is $(2, q-1)$, the G.C.D of 2 and $q-1$.

$$(2, q-1) = \begin{cases} 1 & \text{if} \quad q \equiv 0 \,(\text{mod } 2) \\ 2 & \text{if} \quad q \equiv 1 \,(\text{mod } 2) \end{cases}$$

and we have

$$|N_H(A)| = \begin{cases} q & \text{if} \quad q \equiv 0 \,(\text{mod } 2) \\ 2q & \text{if} \quad q \equiv 1 \,(\text{mod } 2) \end{cases}$$

Thus the number of conjugates of A in H is

$$|H : N_H(A)| = \begin{cases} q^2 - 1 & \text{if} \quad q \equiv 0 \,(\text{mod } 2) \\ \frac{q^2-1}{2} & \text{if} \quad q \equiv 1 \,(\text{mod } 2) \end{cases} \tag{2}$$

Now comparing (1) and (2) above we find that the conjugacy class of $A$ in $G$ remains the same in $H$ when $q \equiv 0 \,(\text{mod } 2)$ but splits into two when $q \equiv 1 \,(\text{mod } 2)$.

(c) The number of conjugates of $A$ in $G$ is

$$q(q+1), \text{ (see case 2 of Section 2)} \tag{3}$$

We deduce from the same section that the elements of $N_H(A)$ are of the form;

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, \quad xy = 1 \quad \Rightarrow x = y^{-1}.$$

If $q \equiv 0 \,(\text{mod } 2)$, then $x \neq y$, except when $x = y = 1$. When $x \neq y$, there is a contribution of two elements to the set $N_H(A)$, for fixed $x$ and $y$. These are;

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \text{ and } \begin{pmatrix} y & 0 \\ 0 & x \end{pmatrix}$$

When $x = y = 1$, there is a contribution of only one element, which is , $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. So $|N_H(A)|$ in this case is $\frac{2(q-2)}{2} + 1 = q - 1$.

Hence,

$$\text{the number of conjugates of } A \text{ in this case is } q(q+1) \tag{4}$$

If $q \equiv 1 \pmod 2$, then $x \neq y$ except when $x = y = 1$ and $x = y = -1$. As before when $x \neq y$ there is a contribution of two elements to $N_H(A)$ for fixed $x$ and $y$. When $x = y$ there is also a contribution of two elements to $N_H(A)$, these are $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ so $|N_H(A)|$ in this case $\frac{2(q-3)}{2} + 2 = q - 1$

Hence,

$$\text{the number of conjugates of } A \text{ in this case is } q(q+1) \tag{5}$$

Now comparing (3) with (4) and (5), we find that the conjugacy class of $A$ remains the same in $H$. Thus there is no splitting.

(d) The number of conjugates of $A$ in $G$ is

$$q(q-1) \quad \text{(see Section 2, case 3)} \tag{6}$$

Now from Theorem 3.2.1, $|N_H(A)| = q + 1$.

Therefore,

$$\text{the number of conjugates of } A \text{ in } H \text{ is } q(q-1) \tag{7}$$

Comparing (6) and (7) we find that the conjugacy class of $A$ in $G$ remains the same in $H$. Hence there is no splitting.

□

**Theorem 3.2.3.** *A matrix* $\begin{pmatrix} b & c \\ d & e \end{pmatrix} \in H$ *with* $p(x) = m(x) = (x-a)^2$ *will be conjugate to a matrix* $\begin{pmatrix} a & \lambda \\ 0 & a \end{pmatrix}$ *if* $c$ *and* $-d$ *belong to the same square class with* $\lambda$.

*Proof.* Let $B = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in H$ so that $\det B = 1$, then we have

$$\begin{aligned} B^{-1}\begin{pmatrix} a & \lambda \\ 0 & a \end{pmatrix} B &= \begin{pmatrix} u & -s \\ -t & r \end{pmatrix}\begin{pmatrix} a & \lambda \\ 0 & a \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix} \\ &= \begin{pmatrix} ua & \lambda u - as \\ -at & ar - \lambda t \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix} \\ &= \begin{pmatrix} aur + t(\lambda u - as) & aus + u(\lambda u - as) \\ -atr + t(ar - \lambda t) & -ast + u(ar - \lambda t) \end{pmatrix} \\ &= \begin{pmatrix} a(ur - ts) + \lambda tu & aus - aus + \lambda u^2 \\ -atr + atr - \lambda t^2 & a(ur - st) - \lambda ut \end{pmatrix} \end{aligned} \tag{8}$$

Since $ru - st = 1$, (8) becomes

$$\begin{pmatrix} a + \lambda tu & \lambda u^2 \\ -\lambda t^2 & a - \lambda ut \end{pmatrix}$$

Now if $A = \begin{pmatrix} b & c \\ d & e \end{pmatrix}$ is conjugate to $\begin{pmatrix} a & \lambda \\ 0 & a \end{pmatrix}$ then

$$\begin{pmatrix} b & c \\ d & e \end{pmatrix} = \begin{pmatrix} a + \lambda tu & \lambda u^2 \\ -\lambda t^2 & a - \lambda ut \end{pmatrix}$$

Clearly $b$ and $e$ are arbitrary whereas $-d = \lambda t^2$ and $c = \lambda u^2$, since $t^2$, $u^2 \in F^{*2} \Rightarrow c$ and $-d$ must be in the same square class with $\lambda$. □

## 4. The Conjugacy and Order Structure of $GL(3, q)$

### 4.1. Conjugacy Classes of $GL(3, q)$

Let $G = GL(3, q)$. Then we have $|G| = (q^3 - 1)(q^3 - q)(q^3 - q^2)$. The following are all the possible forms of characteristic polynomials of elements of $G$:

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

4. $p(x) = (x-a)(x^2+bx+c)$, where $x^2+bx+c$ is an irreducible quadratic polynomial.

5. $p(x) = x^3 + ax^2 + bx + c$, is an irreducible cubic polynomial.

Now we will determine the number of conjugacy classes and the class lengths by considering each of the above polynomials one at a time in terms of cases.

**Case 1:** $p(x) = (x-a)^3$

In this case there are 3 possible minimal polynomials, namely:

(a) $m(x) = x - a$

(b) $m(x) = (x-a)^2$

(c) $p(x) = m(x) = (x-a)^3$

**Case 1 (a)** $m(x) = x - a$

Let $A \in G$ with $m(x) = x - a$. Then the Jordan form of $A$ is

$$J = \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$$

This is a scalar matrix and hence a central element of $G$. Hence $N_G(A) = G$. Therefore the number of conjugates of $A$ in $G$ is $|G : G| = 1$. Thus, all the scalar matrices belong to a singleton conjugacy class and the number of such matrices is $q-1$.

So in this case we have $q-1$ conjugacy classes each with a single element. Hence the total number of elements in this case is $q-1$.

**Case 1 (b)** $m(x) = (x-a)^2$

Let $A \in G$ with $m(x) = (x-a)^2$, then the Jordan form of $A$ is

$$J = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}.$$

We now find the matrices that commute with $J$. But first we have

$$J = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} = \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Let $T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Clearly any matrix that commutes with $T$ commutes with $J$. Now let $B = \begin{pmatrix} r & s & t \\ u & v & w \\ x & y & z \end{pmatrix} \in N_G(J)$, then by definition, $BT = TB$ to give $B = \begin{pmatrix} r & s & t \\ 0 & r & 0 \\ 0 & y & z \end{pmatrix}$, $r, z \neq 0$

Since $t, s$ and $y$ are arbitrary, the number of such matrices is $q^3(q-1)^2$. Hence the number of conjugates of $A$ is

$$\frac{|G|}{q^3(q-1)^2} = (q^3-1)(q+1)$$

The number of matrices of the same form as $J$ is $q-1$. Thus we have $q-1$ conjugacy classes each with $(q^3-1)(q+1)$ elements, and the total number of elements in this case is $(q-1)(q^3-1)(q+1)$.

**Case 1 (c)** $p(x) = m(x) = (x-a)^3$**.**

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

$$J = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}$$

We have $J = \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. We then find the matrices that commute with $J$.

Let $B = \begin{pmatrix} r & s & t \\ u & v & w \\ x & y & z \end{pmatrix} \in N_G(J)$. Then we find that $B = \begin{pmatrix} r & s & t \\ 0 & r & s \\ 0 & 0 & r \end{pmatrix}$, $r \neq 0$.

Since $s$ and $t$ are arbitrary, the number of such matrices is $q^2(q-1)$. Hence $|N_G(A)| = q^2(q-1)$ Therefore the number of conjugates of $A$ is

$$\frac{|G|}{|N_G(A)|} = \frac{|G|}{q^2(q-1)} = q(q^2-1)(q^3-1).$$

The number of matrices of the same form as $J$ is $q-1$. Hence we have $q-1$ conjugacy classes each with $q(q^2-1)(q^3-1)$ elements, and the total number of elements in this case is $q(q-1)(q^2-1)(q^3-1)$.

**Case 2:** $p(x) = (x-a)(x-b)^2$

There are two possible minimal polynomials here:

(a) $m(x) = (x-a)(x-b)$

(b) $m(x) = (x-a)(x-b)^2$

We consider each subcase.

(a) when $m(x) = (x-a)(x-b)$.

Let $A \in G$ with $m(x) = (x-a)(x-b)$, then the Jordan form of $A \in G$ is

$$J = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & b \end{pmatrix}$$

which commute with $B = \begin{pmatrix} r & 0 & 0 \\ 0 & v & w \\ 0 & y & z \end{pmatrix}$, where $r \neq 0$ and $\begin{pmatrix} v & w \\ y & z \end{pmatrix} \in GL(2,q)$.

Hence the number of matrices which commute with $J$ is $(q-1)(q^2-1)(q^2-q)$ and the number of conjugates of $A$ is

$$\frac{|G|}{(q-1)(q^2-1)(q^2-q)} = q^2(q^2+q+1).$$

The number of matrices with $m(x) = (x-a)(x-b)$ is $(q-1)(q-2)$, since $a \neq b$. Hence there are $(q-1)(q-2)$ conjugacy classes each with $q^2(q^2+q+1)$ elements and the total number of elements in this case is

$$q^2(q-1)(q-2)(q^2+q+1).$$

(b) When $m(x) = (x-a)(x-b)^2$. Let $A \in G$. Then the Jordan form of $A$ is

$$J = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 1 \\ 0 & 0 & b \end{pmatrix}$$

and the matrix $B = \begin{pmatrix} r & 0 & 0 \\ 0 & v & w \\ 0 & 0 & v \end{pmatrix} \in N_G(J)$, $r, v \neq 0$, commute with $J$.

Since $w$ is arbitrary, the number of matrices which commute with $J$ is $q(q-1)^2$.

Hence the number of conjugates of $A$ is

$$\frac{|G|}{q(q-1)^2} = q^2(q^3-1)(q+1).$$

The number of matrices with $m(x) = (x-a)(x-b)^2$ is $(q-1)(q-2)$. Thus the number of conjugacy classes is $(q-1)(q-2)$, each with $q^2(q^3-1)(q+1)$ elements. Hence the total number of elements in this case is $q^2(q-2)(q^2-1)(q^3-1)$.

**Case 3:** $p(x) = (x-a)(x-b)(x-c),\ a \neq b \neq c$.
Here $p(x) = m(x)$ and $A \in G$. Then the Jordan form of $A$ is

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

and the matrices which commute with $J$ are of the form $B = \begin{pmatrix} r & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & z \end{pmatrix}$, $r, v, z \neq 0$, $B \in N_G(J)$.

Hence the number of matrices which commute with $J$ is $(q-1)^3$. Therefore the number of conjugates of $A$ is

$$\frac{|G|}{(q-1)^3} = q^3(q^2+q+1)(q+1).$$

The number of matrices with $p(x) = (x-a)(x-b)(x-c)$ is

$$\binom{q-1}{3} = \frac{1}{6}(q-1)(q-2)(q-3).$$

Hence there are $\frac{1}{6}(q-1)(q-2)(q-3)$ conjugacy classes each with $q^3(q^2+q+1)(q+1)$ elements, and the total number of elements in this case is $\frac{1}{6}q^3(q^2+q+1)(q^2-1)(q-2)(q-3)$

**Case 4:** $p(x) = (x-a)(x^2+bx+c)$**, where** $x^2+bx+c$ **is an irreducible polynomial.**

Clearly $p(x) = m(x) = (x-a)(x^2+bx+c)$. Let $A \in G$ with $p(x) = (x-a)(x^2+bx+c)$, then $A$ has distinct eigenvalues. So, $A$ commutes with elements of the form $\alpha_0 I + \alpha_1 A + \alpha_2 A^2$, where $\alpha_0,\ \alpha_1,\ \alpha_2 \in F$ (see Theorem 2.1.1). The elements

$$\{\alpha_0 I + \alpha_1 A + \alpha_2 A^2 \ :\ \alpha_0,\ \alpha_1,\ \alpha_2 \in F\}$$

form a ring $R$ which is isomorphic to

$$\frac{F[x]}{(x-a)(x^2+bx+c)}.$$

By Primary Decomposition Theorem (see [6], page 225) we have

$$\frac{F[x]}{(x-a)(x^2+bx+c)} \approx \frac{F[x]}{x-a} \oplus \frac{F[x]}{x^2+bx+c} = F \oplus E$$

where $E$ is the quadratic extension field of $F$.

The number of invertible elements in $R$ is seen to be $(q-1)(q^2-1)$. So the number of conjugates of $A$ is

$$\frac{|G|}{(q-1)(q^2-1)} = q^3(q^3-1).$$

The number of matrices with $p(x) = (x-a)(x^2+bx+c)$ is $\frac{1}{2}(q-1)(q^2-q)$, for $a \neq 0$, and the number of irreducible quadratic polynomials is $\frac{1}{2}q(q-1)^2$. Hence there are $\frac{1}{2}q(q-1)^2$ conjugacy classes, each with $q^3(q^3-1)$ elements and the total number of elements in this case is $q^4(q-1)^2(q^3-1)$.

**Case 5: $p(x) = x^3 + ax^2 + bx + c$, irreducible over $F$.**

Let $A \in G$ with $p(x) = x^3 + ax^2 + bx + c$. Then $A$ has distinct eigenvalues in the cubic extension field $E$ of $F$. Hence $A$ commutes with elements of the form $\alpha_0 I + \alpha_1 A + \alpha_2 A^2$, where $\alpha_0$, $\alpha_1$, $\alpha_2 \in F$ (see Theorem 2.1.1).

The elements $\{\alpha_0 I + \alpha_1 A + \alpha_2 A^2 : \alpha_0, \alpha_1, \alpha_2 \in F\}$ form a ring $R$ which is isomorphic to $F[x]/\langle p(x)\rangle = E$.

All these elements of $R$ are invertible except $0I + 0A + 0A^2$. Hence the number of elements that commute with $A$ is $|E'| = q^3 - 1$. Hence the number of conjugates of $A$ is

$$\frac{|G|}{q^3-1} = q^3(q^2-1)(q-1)$$

We now find the number of conjugacy classes in this case. This is obtained by subtracting the number of all characteristic polynomials of the elements of $G$ with at least one root in $F^*$ from the total number of possible characteristic polynomials of the elements of $G$. In general a characteristic polynomial of an element of $G$ is of the form $x^3 + ax^2 + bx + c$, where $c \neq 0$, so the total number of such polynomials is $q^2(q-1)$, and the number of irreducible ones is

$$q^2(q-1) - \left(\frac{1}{2}q(q-1)^2 + \frac{1}{6}(q-1)(q-2)(q-3) + (q-1)(q-2) + (q-1)\right)$$

$$= q^2(q-1) - \frac{1}{2}q(q^2-2q+1) - \frac{1}{6}(q^3-6q^2+11q-6) - (q^2-3q+2) - q + 1$$
$$= \frac{1}{6}(6q^3 - 6q^2 - 3q^3 + 6q^2 - 3q - q^3 + 6q^2 - 11q + 6 - 6q^2$$
$$+ 18q - 12 - 6q + 6)$$
$$= \frac{1}{6}(2q^3 - 2q) = \frac{1}{3}q(q^2-1)$$

Hence there are $\frac{1}{3}q(q^2-1)$ conjugacy classes, each with $q^3(q^2-1)(q-1)$ elements. The total number of elements in this case is $\frac{1}{3}q^4(q-1)(q^2-1)^2$.

We observe that:

(a) The total number of elements in the five cases is

$$\begin{aligned}
&\big((q-1) + (q-1)(q^2-1)(q+1)(q-1)(q^3-1)(q^3-q)\big)\\
&+ \big(q^2(q-1)(q-2)(q^2+q+1) + q^2(q-2)(q^2-1)(q^3-1)\big)\\
&+ \left(\frac{1}{6}\,q^3(q-2)(q-3)(q^2-1(q^2+q+1)\right)\\
&+ \left(\frac{1}{2}\,q^4(q^3-1)(q-1)^2\right)\\
&+ \left(\frac{1}{3}\,q^4(q-1)(q^2-1)^2\right),
\end{aligned}$$

which on simplification reduces to

$$q^9 - q^8 - q^7 + q^5 + q^4 - q^3 = (q^3-1)(q^3-q)(q^3-q^2) = |G|$$

as expected.

(b) The total number of conjugacy classes of $G$ is

$$3(q-1)+2(q-1)(q-2)+\frac{1}{6}(q-1)(q-2)(q-3)+\frac{1}{2}\,q(q-1)^2+\frac{1}{3}\,q(q^2-1)$$
$$= q^3 - q = q(q^2-1).$$

The following is the summary of the results we have obtained in this section. The following table shows the nature of the minimal polynomial of the elements of a conjugacy class and the length of the conjugacy class.

| The nature of the minimal polynomial, m(x) | Length of the conjugacy class |
|---|---|
| $x-a$ | 1 |
| $(x-a)^2$ | $(q^3-1)(q+1)$ |
| $(x-a)^3$ | $(q^3-1)(q^3-q)$ |
| $(x-a)(x-b)$ | $q^2(q^2+q+1)$ |
| $(x-a)(x-b)^2$ | $q^2(q^3-1)(q+1)$ |
| $(x-a)(x-b)(x-c)$ | $q^3(q^2+q+1)(q+1)$ |
| $(x-a)(x^2+bx+c)$ | $q^3(q^3-1)$ |
| $x^3+ax^2+bx+c$ | $q^3(q^2-1)(q-1)$ |

Table 3: The nature of the minimal polynomial and the length of the conjugacy class

## 5. The Conjugacy Structure of $SL(3,q)$

Like in Section 3, we have investigated the cases when a conjugacy class $G = GL(3,q)$ splits or does not split in $H = SL(3,q)$. As before, this is achieved by comparing $|G : N_G(A)|$ with $|H : N_H(A)|,\ A \in H$.

### 5.1. Conditions for Splitting of Conjugacy Classes of $GL(3,q)$ in $SL(3,q)$

The following theorem generalizes the conditions for splitting or not splitting of conjugacy classes of $G = GL(3,q)$ in $H = SL(3,q)$.

**Theorem 5.1.1.** *Let $A \in H$. Then*

1. *the conjugacy class of A in both G and H are the same when*

   (a) $p(x) = (x-a)^3,\ m(x) = x-a$

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

   (c) $p(x) = (x-a)(x-b)^2,\ m(x) = (x-a)(x-b),\ a \neq b$

   (d) $p(x) = (x-a)(x-b)^2,\ m(x) = (x-a)(x-b)^2,\ a \neq b$

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

   (f) $p(x) = m(x) = (x-a)(x^2+bx+c)$, *where* $x^2+bx+c$ *is irreducible in F.*

   (g) $p(x) = m(x) = x^3+ax^2+bx+c$, *which is irreducible in F.*

*2. If $p(x) = m(x) = (x-a)^3$, the conjugacy class of $A$ in $G$ remains the same in $H$ when $q \equiv 0$ or $2 \pmod 3$ but splits into 3 when $q \equiv 1 \pmod 3$.*

*Proof.* **1 (a) when $p(x) = (x-a)^3$ and $m(x) = x-a$.**

From Subsection 4.1, case 1(a), $A$ is contained in a singleton conjugacy class in $G$. Therefore $A$ must be in its own conjugacy class in $H$.

**(b) when $p(x) = (x-a)^3,\ m(x) = (x-a)^2$.**

From Subsection 4.1, case 1(a),

$$\text{the length of the conjugacy class of A is } (q^3-1)(q+1) \tag{9}$$

The elements of $N_H(A)$ are of the form $\begin{pmatrix} r & s & t \\ 0 & r & 0 \\ 0 & y & z \end{pmatrix}$, where its determinant is $r^2z = 1$, we have $q-1$ choices for $r$, $q$ choices for $s$, $t$, $y$ and $z$ is dependent on $r$. Hence $|N_H(A)| = q^3(q-1)$ and so

$$|H : N_H(A)| = (q^3-1)(q+1) \tag{10}$$

Comparing (9) and (10) we find that there is no splitting in this case

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

From Subsection 4.1, case 2(a),

$$\text{the conjugacy class of } A \text{ in } G \text{ is of length } q^2(q^2+q+1) \tag{11}$$

The elements of $N_H(A)$ are of the form $\begin{pmatrix} r & 0 & 0 \\ 0 & v & w \\ 0 & y & z \end{pmatrix}$, where $\begin{pmatrix} v & w \\ y & z \end{pmatrix} \in GL(2,q)$ and $r(vz - yw) = 1$.

Since $r$ is dependent on $\begin{pmatrix} v & w \\ y & z \end{pmatrix}$ we have

$$|N_H(A)| = (q^2-1)(q^2-q) = |GL(2,q)|.$$

Therefore

$$|H : N_H(A)| = q^2(q^2+q+1). \tag{12}$$

Comparing (11) and (12), we find that there is no splitting in this case.

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

From Subsection 4.1, case 2(a),

$$\text{the conjugacy class of } A \text{ in } G \text{ is of length } q^2(q^3-1)(q+1). \tag{13}$$

We deduce from the same section that an element in $N_H(A)$ is of the form $\begin{pmatrix} r & 0 & 0 \\ 0 & v & w \\ 0 & 0 & v \end{pmatrix}$, where $rv^2 = 1$. Since $r$ depends on $v$ and there are $q-1$ choices for $v$ and $q$ choices for $w$, we have $|N_H(A)| = q(q-1)$. Hence

$$|H : N_H(A)| = q^2(q^3-1)(q+1) \tag{14}$$

. Comparing (13) and (14), we find that there is no splitting in this case.

**(e) when** $p(x) = m(x) = (x-a)(x-b)(x-c),\ a \neq b \neq c$.

From Subsection 4.1, case 3,

$$\text{the conjugacy class of } A \text{ in } G \text{ is of length } q^3(q+1)(q^2+q+1) \tag{15}$$

.

We deduce from the same section that an element in $N_H(A)$ is of the form $\begin{pmatrix} r & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & z \end{pmatrix}$, where $rvz = 1$.

Since $r$ depends on $v$ and $z$, and $v$ and $z$ each can take $q-1$ values, we have $|N_H(A)| = (q-1)^2$. Therefore

$$|H : N_H(A)| = q^3(q+1)(q^2+q+1). \tag{16}$$

Hence comparing (15) and (16) we find that there is no splitting in this case.

**(f) When** $p(x) = m(x) = (x-a)(x^2+bx+c),\ x^2+bx+c$ **is irreducible in** $F$**.**

From Subection 4.1, case 4,

$$\text{the conjugacy class of } A \text{ in } G \text{ is of length } q^3(q^3-1). \tag{17}$$

We deduce from the same section that an element of $N_H(A)$ is similar to a matrix of the form $\begin{pmatrix} r & 0 & 0 \\ 0 & s & 0 \\ 0 & 0 & t \end{pmatrix}$, where $r \in F$ and $s,\ t \in E$ (quadratic extension of $F$) and $rst = 1$. Since $s$ depends on $t$ (because they are conjugates) and $r$ depends on $s$ and $t$, we only choose $t$. Since there are $q^2-1$ choices for $t$, we have $|N_H(A)| = q^2-1$. Hence

$$|H : N_H(A)| = q^3(q^3-1). \tag{18}$$

Comparing (17) and (18), we find that there is no splitting in this case.

**(g) When $p(x) = m(x) = x^3 + ax^2 + bx + c$, which is irreducible in $F$.**
From Subsection 4.1 case 5,

$$\text{the conjugacy class of } A \text{ in } G \text{ is of length } q^3(q-1)(q^2-1). \tag{19}$$

Now from Theorem 3.2.1

$$|N_H(A)| = \frac{q^3-1}{q-1} = q^2 + q + 1.$$

So

$$|H : N_H(A)| = q^3(q-1)(q^2-1). \tag{20}$$

Hence, comparing (19) and (20), we see that there is no splitting in this case.

**2. when $p(x) = m(x) = (x-a)^3$.**
From Subsection 4.1 case 1(c), subcase (c),

$$\text{the conjugacy class of } A \text{ in } G \text{ is of length } (q^3-1)(q^3-q). \tag{21}$$

The elements of $N_H(A)$ are of the form $\begin{pmatrix} r & s & t \\ 0 & r & s \\ 0 & 0 & r \end{pmatrix}$, where $r^3 = 1$.

Clearly the number of solutions of $r^3 = 1$ in $F^*$ is the G.C.D of 3 and $q-1$. Now

$$(3,\, q-1) = \begin{cases} 1, & \text{if} \quad q \equiv 0 \text{ or } 2 \pmod 3 \\ 3, & \text{if} \quad q \equiv 1 \pmod 3 \end{cases}$$

So that

$$|N_H(A)| = \begin{cases} q^2, & \text{if} \quad q \equiv 0 \text{ or } 2 \pmod 3 \\ 3q^2, & \text{if} \quad q \equiv 1 \pmod 3 \end{cases}$$

since $s$ and $t$ can each take $q$ values. Hence

$$|H : N_H(A)| = \begin{cases} (q^3-1)(q^3-q), & \text{if} \quad q \equiv 0 \text{ or } 2 \pmod 3 \\ \frac{1}{3}(q^3-1)(q^3-q), & \text{if} \quad q \equiv 1 \pmod 3 \end{cases} \tag{22}$$

Now comparing (21) and (22), we find that the conjugacy class of $A$ in $G$ remains the same in $H$ when $q \equiv 0$ or $2 \pmod 3$ but splits into three when $q \equiv 1 \pmod 3$. □

From Theorem 5.1.1 above, it is clear that splitting will occur only when $p(x) = m(x) = (x-a)^3$ and $q \equiv 1 \pmod 3$. The problem we are now faced with is how to determine the conjugacy class in which an element in $H$ with $p(x) = m(x) = (x-a)^3$ and $q \equiv 1 \pmod 3$ belongs.

### 5.2. Conjugacy Class Representative in $SL(3, q)$

Here we show the three conjugacy classes in $H$ represent the three cubic classes of $F^*$. These are $F^{*3}$, $\lambda F^{*3}$ and $\lambda^2 F^{*3}$, where $\lambda \notin F^{*3}$ and each cubic class represents a conjugacy class.

We now show how to determine the conjugacy class in which an element $A \in H$ belongs among the three. We begin with a proposition.

**Proposition 5.2.1.** *Let $A \in H$ with $m(x) = (x-a)^3$ and the Jordan form, $J = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}$, then:*

*(a) If $AB = BA$, then $\det B = r^3$, $r \in F^*$.*

*(b) If $B = P^{-1}AP$ in $G$ and $\det P = r^3$, then $B$ is conjugate to $A$ in $H$.*

*(c) If $B = P^{-1}AP$ in $G$ and $\det P = \lambda r^3$, $\lambda \notin F^{*3}$ then $B$ is not conjugate to $A$ in $H$.*

*Proof.* (a) The elements that commute with $A$ are of the form $\begin{pmatrix} r & s & t \\ 0 & r & s \\ 0 & 0 & r \end{pmatrix}$ (see Subsection 4.1, case 1(c).

Hence $B$ is of this form and $\det B = r^3$.

(b) Since $\det P = r^3$, let $Q = \begin{pmatrix} r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{pmatrix}$ then $\det Q = r^3$. We have

$$\begin{aligned} QBQ^{-1} &= QP^{-1}APQ^{-1} \\ \Leftrightarrow QBQ^{-1} &= (PQ^{-1})^{-1}A(PQ^{-1}), \text{ since } Q \text{ is a scalar matrix.} \end{aligned}$$

Clearly $\det(PQ^{-1}) = 1$. Hence $B$ is conjugate to $A$ in $H$.

(c) Since $\det P = \lambda r^3$, let $Q = \begin{pmatrix} \lambda r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{pmatrix}$ then $\det Q = \lambda r^3$. We have

$$\begin{aligned} QBQ^{-1} &= QP^{-1}APQ^{-1} \\ \Leftrightarrow QBQ^{-1} &= (PQ^{-1})^{-1}A(PQ^{-1}) \end{aligned}$$

By Subsection 4.1, case 1(c), $Q$ does not commute with $B$. Hence $QBQ^{-1} \neq B$.

Clearly $\det(PQ^{-1}) = 1$. Hence $B$ is not conjugate to $A$ in $H$. □

Now let $A \in H$ with $m(x) = (x-a)^3$. Then the Jordan form of $A$ is

$$J = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}$$

To find out the conjugacy class in which $A$ belongs in $H$, we find a matrix $X$ in $G$ such that

$$X^{-1}AX = J$$

To get $X$, we find another matrix $B$, where $B = A - aI$ with $B^2 \neq 0$. We choose a vector $u$ in the standard basis such that $B^2u \neq 0$, so that

$$u \to Bu \to B^2u \to 0.$$

Then we use the new basis $\{B^2u, Bu, u\}$ to form our new matrix $X$. Thus $X = \begin{pmatrix} B^2u & Bu & u \end{pmatrix}$. We then look at the determinant of $X$ and check the cubic class in which it belongs. Now matrix $A$ belongs to the corresponding conjugacy class. ([2], page 228).

The following is a general illustration of the method discussed above.

Let $A = \begin{pmatrix} a & r & t \\ 0 & a & s \\ 0 & 0 & a \end{pmatrix}$ with $m(x) = (x-a)^3$. Then the Jordan form of $A$ is

$$J = \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}.$$

We now find $X$, such that $X^{-1}AX = J$ as explained above. Let $B = A - aI$, then we have

$$B = \begin{pmatrix} 0 & r & t \\ 0 & 0 & s \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad B^2 = \begin{pmatrix} 0 & 0 & rs \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

We choose a vector $u$ such that $B^2u \neq 0$. Clearly $u = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, and

$$\begin{matrix} u \\ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \end{matrix} \to \begin{matrix} Bu \\ \begin{pmatrix} t \\ s \\ 0 \end{pmatrix} \end{matrix} \to \begin{matrix} B^2u \\ \begin{pmatrix} rs \\ 0 \\ 0 \end{pmatrix} \end{matrix}$$

Hence $X = \begin{pmatrix} rs & t & 0 \\ 0 & s & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Thus we find that $\det X = rs^2$.

Now for $A$ to be a representative of $F^{*3}$, we must choose $r$ and $s$ such that $rs^2 \in F^{*3}$. Similarly for $A$ to be in $\lambda F^{*3}$ or $\lambda^2 F^{*3}$, we choose $r$ and $s$ such that $rs^2 \in \lambda F^{*3}$ or $rs^2 \in \lambda^2 F^{*3}$ respectively.

$s$ and $rs^2$ can easily be determined by choosing $s$ to be equal to 1, then for $A \in F^{*3}$, $r$ may be equal to 1, for $A \in \lambda F^{*3}$, $r$ may be equal to $\lambda$ and for $A \in \lambda^2 F^{*3}$, $r$ may be equal to $\lambda^2$.

Hence the general form of a class representative $A$ in each of the three conjugacy classes is:

$$(a) \quad \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix} \qquad (b) \quad \begin{pmatrix} a & \lambda & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix} \qquad (c) \quad \begin{pmatrix} a & \lambda^2 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}$$

## References


[1] R.J. Durbin, *Modern Algebra, An Introduction*, 3-rd Edition, John Willey and Sons Inc, New York (1985).

[2] T.D. Finkbeiner II, *Introduction on Matrices and Linear Transformations*, 3-rd Edition, W.H. Freeman Company, San Francisco (1978).

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

[4] I.N. Herstein, *Topics in Algebra*, 2-nd Edition, John Willey and Sons Inc., New York (1975).

[5] B. Huppert, *Endliche Grupper I, Die Grundlelren der Mathematischen*, Springer, Berlin (1967).

[6] S. Lipschutz, *Schaums outline Series, Linear Algebra*, McGraw Hill, New York (1991).

[7] P.M. Maurer, *The $GF(2)$ General Linear Groups for Dimensions 2, 3, 4 and 5*, Master Thesis, Baylor University, Waco, Texas (2000), 1-36.

[8] J. Moori, A.M. Basheer, On the regular semi-simple elements and primary classes of $GL(n, q)$, *Journal of Finite Fields and Their Applications,* **17** (2011), 275-285.