Orbit Lengths and Character Degrees in $p$-Sylow Subgroups of Some Classical Lie Groups

Andrea Previtali*

Department of Mathematics, Mainz University, 55099 Mainz, Germany

Communicated by Gernot Stroth

Received March 6, 1994

1. INTRODUCTION

Let $G$ denote $SL(n, q)$ or $Sp(2n, q)$, the linear or symplectic group over $F_q$, $q$ a $p$-power. Let $\mathfrak{H}$ be a $p$-Sylow subgroup of $G$. We determine the set of conjugacy class lengths of suitable normal abelian subgroups $\mathfrak{H}$ of $\mathfrak{H}$ and use this information to get the character degrees of $\mathfrak{H}$. Given a group $G$ acting on a vector space $V$, it is known that $V$ and its dual $\hat{V}$ are not necessarily $G$-equivalent, if the action is not coprime. We introduce a weaker version of $G$-equivalence and show that this is enough to assure equality between the set of conjugacy class lengths and character degrees when $q = p$, $p$ odd. Some partial results are obtained when $q = p^m$, $m > 1$, using a linearization technique involving formal power series. Some results have been determined by Huppert (see [6]) for $SL(n, q)$. With a slightly different approach, we will obtain them ex novo and extend them to the symplectic case. The proof goes along the following lines:

(a) Determine a big abelian normal subgroup $\mathfrak{H}$ of $\mathfrak{H}$ such that

$$1 \rightarrow \mathfrak{H} \rightarrow \mathfrak{H} \xrightarrow{j} \mathfrak{H} \xrightarrow{\pi} \hat{\mathfrak{H}} \rightarrow 1$$

is a splitting exact sequence.

(b) Determine the orbit lengths of the action of $\hat{\mathfrak{H}}$ on $\mathfrak{H}$, where $\hat{\mathfrak{H}} = \hat{\mathfrak{H}}$ is the complement of $\mathfrak{H}$ in $\mathfrak{H}$.

(c) Prove that the same lengths appear in the dual action.

(d) Use some results of Clifford’s theory to get the desired character degrees when $q = p$.

* Research supported by Dottorato dell’Università di Pisa.
2. NOTATIONS AND PRELIMINARY RESULTS

Given a group \( G \), we denote with \( \text{Irr}(G) \) the set of its irreducible characters. As standard \( G_0 \) will denote a \( p \)-Sylow subgroup of \( G \). Suppose \( \chi \in \text{Irr}(N) \), where \( N \leq G \), then \( \text{Irr}(N) \) is a \( G \)-set via \( \chi^g(x^f) = \chi(x) \), \( g \in G, \ x \in N \). Call \( I_G(\chi) = C_G(\chi) \) the inertia subgroup of \( \chi \). Set \( cdG = \{ \chi^g \mid \chi \in \text{Irr}(G) \} \). Suppose \( \Omega \) is a \( G \)-set, then \( \omega^G = \{ \omega^g \mid g \in G \} \) is the \( G \)-orbit of \( \omega \in \Omega \) and \( \Theta(\omega^G) = \{ |\omega^g| \mid \omega \in \Omega \} \).

**Definition 2.1.** Given two \( G \)-sets \( \Omega_1, \Omega_2 \), we say they are \( G \)-equivalent if there exists a bijection \( \sigma \) from \( \Omega_1 \) onto \( \Omega_2 \) such that \( (\omega^g)^\sigma = (\omega^g)^\sigma \) for every \( g \in G \) and weak equivalent if \( \sigma(\Omega_1) = \sigma(\Omega_2) \).

Usually gothic letters will be used for groups of Lie type and capital ones for matrices. Given a matrix \( T, T^* = (T^{-1})^t \) will denote the adjoint matrix. We denote with \( E_{ij} \) the elementary matrix with entry 1 in the position \( (i, j) \) and zero elsewhere.

**Lemma 2.2.** Suppose \( G \) is a splitting extension of its normal subgroup \( N \), then any linear character \( \lambda \in \text{Irr}(N) \) can be extended to its inertia subgroup \( I_G(\lambda) \).

**Proof.** Suppose \( K \) is a complement of \( N \) in \( G \), then, by Dedekind’s identity, is \( I = I_G(\lambda) = N(I_G(\lambda) \cap K) = NK \). Define \( \lambda_0(ax) := \lambda(a) \), where \( a \in N, x \in K \). Let \( ab = a'b' \), then \( a^{-1}a' = b^{-1}b' \in N \cap K = 1 \), so \( a = a', b = b' \), and \( \lambda_0 \) is well defined.

\[
\lambda_0(abxy) = \lambda_0(ab^{-1}xy) = \lambda(ab) = \lambda(a)\lambda(b) = \lambda_0(ax)\lambda_0(by) \quad (2)
\]

proves that also \( \lambda_0 \) is a character of \( I_G(\lambda) \) extending \( \lambda \) (compare also [9, Ex. 6.18] for a more general assertion).

**Lemma 2.3.** Suppose \( G = A \rtimes T \), where \( A \leq G \) abelian, then \( cdG = \{ \beta(1)|G : I_G(\lambda) \lambda \in \text{Irr}(A) \text{ and } \beta \in \text{Irr}(I_G(\lambda)/A) \} \).

**Proof.** Let \( \psi \in \text{Irr}(G) \), then \( \psi_\lambda = e(\psi) \sum \lambda_i \), hence, by Frobenius’ reciprocity law, \( e(\psi) = (\psi, \lambda) = (\psi, \lambda G) \). But, by Gallagher’s theorem (see [9, p. 85]), \( \lambda G = \sum (\lambda_0, \beta)^G, \) where \( \lambda_0 \in \text{Irr}(I_G(\lambda)) \) is a linear character extending \( \lambda \) and \( \beta \) varies in \( \text{Irr}(I_G(\lambda)/A) \). By Clifford’s theory \( (\lambda_0, \beta)^G \in \text{Irr}(G) \), then \( \psi = (\lambda_0, \beta)^G \) for a suitable index \( i \). But, as easy consequence of the definition of induced character,

\[
(\lambda_0, \beta)^G(1) = \lambda_0(1)\beta_i(1)|G : I_G(\lambda)| = \beta_i(1)|G : I_G(\lambda)|, \quad (3)
\]
as asserted.
In particular, for $\beta$, the trivial character in $\text{Irr}(I_G(\lambda)/A)$, $\lambda^G_0 \in \text{Irr}(G)$, so $\lambda^G_0(1) = |G : I_G(\lambda)| \in cdG$. Our problem reduces to the search of suitable linear characters of a normal subgroup, in such a way that any character degree could be obtained as above described. It has been conjectured that for $\mathfrak{B} \in \text{Syl}_p(\mathcal{L}_q^*(\mathbb{F}_q))$, $\mathcal{L}_q^*(\mathbb{F}_q)$ a classical Lie group, $cd\mathfrak{B}$ is a set of $q$-powers. By the preceding lemma this would imply that $|G : I_G(\lambda)|$ is a $q$-power. We will prove that this holds in our setting, providing some weak evidence for this conjecture. Remark that the conjecture on character degrees is equivalent to state that $\forall A \leq G, \forall \lambda \in \text{Irr}(A)$ and $\mathfrak{B} \beta \in \text{Irr}(I_G(\lambda)/A)$, $\beta(1)$ is a $q$-power. Observe that in the symplectic situation $I_G(\lambda)/A \leq \mathfrak{T}_1 \times \mathfrak{T}_2$, where $\mathfrak{T}_i \in \text{Syl}_p(\text{SL}(m_i, q))$ for suitable $m_i$. Since any finite $p$-group can be embedded in such groups, the truth of the character degree conjecture would imply a strong restriction on the structure of the inertia subgroups $I_{\mathfrak{B}}(\lambda)$. We now carry over the proof distinguishing the two possible cases.

3. ORBIT LENGTHS

In [6], Huppert defined the following function:

$$ f(n) = \begin{cases} 
\frac{(n - 1)^2}{4}, & n \text{ odd}, \\
\frac{n(n - 2)}{4}, & n \text{ even}.
\end{cases} \quad (4) $$

The main result of this and the next section is:

**Theorem 3.4 (Orbit Lengths).** Suppose $\mathfrak{B} \in \text{Syl}_p(\mathcal{L}_q^*(\mathbb{F}_q))$, where $\mathcal{L}_q^*(\mathbb{F}_q)$ is $\text{SL}(n, q)$ or $\text{Sp}(n, q)$, $q$ odd in the symplectic case. Set

$$ g(n) = \begin{cases} 
\frac{f(n)}{2}, & \mathcal{L}_q^*(\mathbb{F}_q) \text{ linear,} \\
\frac{n}{2}, & \mathcal{L}_q^*(\mathbb{F}_q) \text{ symplectic},
\end{cases} \quad (5) $$

then $\mathfrak{C}(1) = \{q^j : 0 \leq j \leq g(n)\}$.

We will need this well known lemma:

**Lemma 3.5.** $A$ is a maximal abelian subgroup of $G$ iff $A$ is self-centralizing.

**Proof.** Compare [5].


3.1. The Linear Case

**Theorem 3.6.** \( \mathcal{V} \in \text{Syl}_p(SL(n, q)) \) is a splitting extension of a maximal abelian normal subgroup \( \mathcal{V} \).

**Proof.** Set \( k = n - r \) and consider

\[
\mathcal{V} = \left\{ \begin{pmatrix} I & 0 \\ A & I_k \end{pmatrix} : A \in (\mathbb{F}_q)_{k \times r} \right\}
\]

(6)

and

\[
\mathcal{X}_k = \mathcal{X} = \left\{ \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} : X \in SL(r, \mathbb{F}_q)_p, Y \in SL(k, \mathbb{F}_q)_p \right\};
\]

(7)

then \( \mathcal{V} = \mathcal{V} \mathcal{X}, \mathcal{V} \cap \mathcal{X} = 1 \), and \( \mathcal{V} \) is an elementary abelian normal subgroup (it is \( \mathcal{X} \)-invariant).

We now show that \( \mathcal{V} \) is maximal in \( \mathcal{A} = \{ \mathcal{C} \leq \mathcal{V} : \mathcal{C} \cap \mathcal{V} = 1 \} \). It’s enough to prove that \( \mathcal{V} \) self-centralizes. If not, by Dedekind’s identity, there is an element of \( \mathcal{X} \) commuting with every element of \( \mathcal{V} \):

\[
\begin{pmatrix} X^{-1} & 0 \\ 0 & Y^{-1} \end{pmatrix} \begin{pmatrix} I & 0 \\ A & I \end{pmatrix} \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} = \begin{pmatrix} I & 0 \\ Y^{-1}AX & I \end{pmatrix}.
\]

(8)

Hence \( Y^{-1}AX = A, \forall A \in (\mathbb{F}_q)_{k \times r} \). Bordering \( A \) and \( X \) as \( A = (A_1, a'_1), X = (x_1, \theta) \), we get

\[
(Y^{-1}A_1X_1 + Y^{-1}a'_1x_2, Y^{-1}a'_1) = (A_1, a'_1).
\]

(9)

Since \( a'_1 \) is arbitrary, this implies that \( Y = I \). Setting \( A_1 = I, a_1 \neq 0 \), we get \( X_1 = I \). Finally, for \( A_1 = 0, \) we get \( x_2 = 0 \). \( \square \)

We are in particular interested in those normal abelian subgroups of minimal index. This corresponds to the following choice for \( r \).

Set \( r = n \pmod{2} \), where \( r \in \{0, 1\} \) and \( r = (n + e)/2 \). The importance of establishing that \( \mathcal{V} \in \mathcal{A} \), is explained by a theorem of Itô stating that the degree of irreducible characters of a group has to divide the index of subnormal abelian subgroups. We now carry out the second step, i.e., determine the orbit lengths of \( \mathcal{V} \) considered as a \( \mathcal{X} \)-set. As will be clear at the end of the proof, we could at once attack the problem in the dual space \( \hat{\mathcal{V}} \), but our approach reflects the general philosophy of considering first the direct action (this being generally easier) and from this retrieving information on the dual action. Much is known (see [1, 4, 8]) when the
action is coprime, that is, when $T$ is a group acting on a group $A$, and $(|A|, |T|) = 1$. The purpose of this approach is also to find a way to generalize such results when the action is no more coprime. The problem is that $A$ and $\text{Irr}(A)$ need not be equivalent $T$-sets when coprimality drops down (see [7, Vol. II, p. 121]). It would be interesting to understand whether a weaker condition still holds:

**Question.** Is it true that $A$ and $\text{Irr}(A)$, considered as $T$-sets are weakly equivalent?

We shift back to gothic notations. As we will see, the proof in the linear case is by far the most complex.

**Theorem 3.7.** $\mathcal{E}(\Pi) \supseteq \{q^j : 0 \leq j \leq f(n)\}$ where $q^{f(n)} = |\Psi : \Pi|$.

**Proof.** The second part of the statement is straightforward. The action on $\Pi$ is described by $Y^{-1}AX$ as above seen. Since the inversion is an anti-isomorphism of $\text{SL}(k, \mathbb{F}_q)$, we may substitute $Y^{-1}$ with $Y$. We distinguish the cases $n = 2k$ and $n = 2k + 1$. We will now proceed by induction on $k$, showing how the inductive hypothesis at the $k$th level implies the truth of the assertion for $n = 2k + 1, 2k + 2 = 2(k + 1)$. If $k = 1$, then $n = 1, 2$ and $\Psi$ is abelian. By induction, $3B \in (\mathbb{F}_q)_{2k}$ which are representatives of the orbit lengths from 1 up to $q^{(k-1)}$. We refine the induction hypothesis claiming the existence of $B_0, \ldots, B_{k-1} \in (\mathbb{F}_q)_{2k}$ such that:

(a) $B_i$ is non-singular.

(b) $|B_i| = q^{(k-1)-i}$.

We will call such matrices the carriers of long orbits.

**Step 1.** We first search representatives for short orbits. Just consider this partition:

$$
Y(B, b') \begin{pmatrix} T & 0 \\ t & 1 \end{pmatrix} = (YBT + Yb', Yb')
$$

and set $b = 0$. By induction, there are matrices $B \in (\mathbb{F}_q)_k$, with orbit lengths from 1 up to $q^{(k-1)}$; then $(B, 0)$ provide the same lengths.

**Step 2.** Consider the following situation:

$$
Y(b', B) \begin{pmatrix} 1 & 0 \\ t' & T \end{pmatrix} = (Y(b' + Bt'), YBT).
$$

Here $Y, T \in (\mathbb{F}_q)_k$ are lower triangular unipotent matrices. The idea is to get elements representing long orbits saturating the first column of the
above matrix for any choice of \( Y \). Since \( Y \) is invertible, this request does not really depend on \( Y \). In fact,

\[
\{ Y(b' + Bt') : t \in \mathbb{F}_q^k \} = \{ b' + Bt' : t \in \mathbb{F}_q^k \} = \{ Bt' : t \in \mathbb{F}_q^k \} = \mathbb{F}_q^k
\]

if and only if \( B \) represents a surjective linear operator in \( \text{End}(\mathbb{F}_q^k) \), that is, if and only if \( B \) is non-singular. But, by induction, there exist \( k \) elements \( B \), which are the carriers of long orbits at the \( k \)th level. Set, for example, \( b = 0 \), then \( (0, B) \) will have orbit length \( q^{k+i-1} \), \( i = 0, \ldots, k - 1 \).

Observe that those steps provide every orbit length when \( n = 2k + 1 \).

Step 3. To get short orbit representatives, just consider

\[
\begin{pmatrix}
1 & 0 \\
t' & t
\end{pmatrix}
\begin{pmatrix}
b \\
\tilde{b}
\end{pmatrix} X =
\begin{pmatrix}
\tilde{b} X \\
t' \tilde{b} X + T \tilde{b} X
\end{pmatrix}
\] (12)

and set \( \tilde{b} = 0 \). By the comment at the end of Step 2, we get all lengths from 1 up to \( q^{k+i} \).

Step 4. Now we partition the matrix \( Y \in (\mathbb{F}_q)_k \), hence

\[
\begin{pmatrix}
T & 0 \\
t & 1
\end{pmatrix}
\begin{pmatrix}
\tilde{B} \\
\tilde{b}
\end{pmatrix} X =
\begin{pmatrix}
T \tilde{B} X \\
(t \tilde{B} + \tilde{b}) X
\end{pmatrix}.
\] (13)

Again, saturation of the last row, for any \( X \), is implied as soon as \( \tilde{B} \) is of maximal rank, that is, \( rk \tilde{B} = k \). That surely happens if we set \( \tilde{B} = (0 \ B) \), where \( B \) is a long orbit carrier in step 1. So the elements \( (\tilde{b}) \) are long orbit representatives for any choice of \( b \). If we set \( \tilde{b} = e_1 \), then these are also non-singular, hence long orbit carriers. Observe that there are \( k \), with orbit length \( q^{k+i+1-i} \), \( i = 0, \ldots, k - 1 \).

Step 5. Unfortunately Step 3 provides a singular element with orbit length \( q^{k} \). To get a non-singular one, take the long orbit carrier \( B_0 \) and embed it in the non-singular matrix \( (\overset{\text{B}_0}{\vphantom{\emptyset}} \overset{s}{\text{\emptyset}}) \). Then

\[
\begin{pmatrix}
T & 0 \\
t & 1
\end{pmatrix}
\begin{pmatrix}
B_0 & 0 \\
0 & 1
\end{pmatrix}
\begin{pmatrix}
S & 0 \\
s & 1
\end{pmatrix} =
\begin{pmatrix}
TB_0 S \\
tB_0 s + s & 1
\end{pmatrix}.
\] (14)

Since \( s \) varies arbitrarily in \( \mathbb{F}_q^k \), this matrix has orbit length \( q^{k+1-i} \).

Remark 3.1. The precedent proof also shows how to construct elements with a prescribed orbit length. Let us just work out the calculation when
Take the matrix (1). Bordering it as in Steps 1 and 3, we have \((\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix})\), which is central. Bordering it as in Steps 2 and 4, we get \((\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix})\) with orbit length \(q^2\). Using Step 5, we get \((\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix})\) with orbit length \(q\).

Remark 3.2. It is proved once more than \(\mathfrak{I}\) is a maximal abelian subgroup. In fact there are elements of maximal possible orbit length \(|A^\mathfrak{I}| = |\mathfrak{I}|\), which is equivalent to \(C_2(A) = 1\) and, by Dedekind's identity, one may conclude that \(\mathfrak{I} = C_\mathfrak{I}(\mathfrak{I})\).

3.2. The Symplectic Case

Once the theme has been settled, let us just play the variations.

Theorem 3.8. \(\mathfrak{V} \in \text{Syl}_p(\text{Sp}(2n, q))\) is a splitting extension of a maximal abelian normal subgroup \(\mathfrak{I}\).

Proof. We first investigate the structure of \(\mathfrak{V}\). As is well known, there exists, up to equivalence, just one symplectic form which can be described by the matrix

\[
E = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.
\]  

Consider now the equation

\[
\begin{pmatrix} T' & B' \\ 0 & C' \end{pmatrix} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \begin{pmatrix} T & 0 \\ B & C \end{pmatrix} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix},
\]  

that is, \(C = T^{-t}\) and \(B = AT\), where \(A' = A\). Consider now the decomposition

\[
\begin{pmatrix} T & 0 \\ AT & T^{-t} \end{pmatrix} = \begin{pmatrix} I & 0 \\ A & I \end{pmatrix} \begin{pmatrix} T & 0 \\ 0 & T^{-t} \end{pmatrix}.
\]  

\(\mathfrak{I}\) acts on \(\mathfrak{I}\) via \(A \to T'AT\); in fact,

\[
\begin{pmatrix} T^{-1} & 0 \\ 0 & T' \end{pmatrix} \begin{pmatrix} I & 0 \\ A & I \end{pmatrix} \begin{pmatrix} T & 0 \\ 0 & T^{-t} \end{pmatrix} = \begin{pmatrix} I & 0 \\ T'AT & I \end{pmatrix}.
\]

This proves that \(\mathfrak{V} = \mathfrak{I} \ltimes \mathfrak{I}\), where \(\mathfrak{I}\), \(\mathfrak{I}\) are the groups constituted by the matrices which appear as the first and the second factor, respectively, in (17). To prove that \(\mathfrak{V}\) is a \(p\)-Sylow subgroup, just consider that its order is \(q^{2(n+1)}\), but that is exactly the maximal \(p\)-power dividing the group order (see [2, Chap. I] or [3]). As in the linear case, to prove the maximality of \(\mathfrak{I}\), it is enough to show that \(T = I\), whenever \(T \in C_\mathfrak{I}(\mathfrak{I})\). Set \(A = I\),
then \( T'T = I \). So \( T = (T')^{-1} = T^* \). But \( T \) is lower triangular with 1 along the diagonal; hence, \( T = I \). □

**Theorem 3.9.** \( \mathcal{O}(1) \supseteq \{ q^j : 0 \leq j \leq (\xi) \} \).

**Proof.** Observe that \( q^j = |B^j : 1| \). Now proceed by induction on \( n \). If \( n = 1 \) there is nothing to show. Let \( n > 1 \) and partition \( A \) and \( T \) in four submatrices. Then we have

\[
\begin{pmatrix}
T' & t' \\
0 & 1
\end{pmatrix}
\begin{pmatrix}
B & b' \\
b & \beta
\end{pmatrix}
\begin{pmatrix}
T & 0 \\
t & 1
\end{pmatrix}
= \begin{pmatrix}
T'BT + t'bT + T'b't + t't\beta & T'b' + \beta t' \\
bT + \beta t & \beta
\end{pmatrix}.
\]  

(19)

*Step 1.* By induction there are matrices \( B_i \in \Pi_{n-1} : q^i = |B_i^{2^{i-1}}| = |B_i^{2^i+1}| \), where \( B_i \) can be thought of as embedded in \( \Pi_n \) setting \( b = 0 \), \( \beta = 0 \).

*Step 2.* Set \( B = 0 \), \( b = 0 \), \( \beta = 1 \); then \((i_1', i_2')\) generates an orbit of length \( q^{n-1} \).

By Step 1, \( \{q^j : 0 \leq j \leq (\xi)\} \subseteq \mathcal{O}(1) \).

By Step 2, \( \{q^j : n - 1 \leq j \leq (\xi)\} \subseteq \mathcal{O}(1) \), since \((i_1', i_2')\) and \((i_1', i_2')\) vary independently. By the first observation, \( \mathcal{O}(X) \) cannot contain a greater \( q \)-power. □

**Remark 3.3.** We may here provide exactly a set of elements each for any orbit length. A careful analysis of the proof shows that only diagonal elements are needed. In fact, \( b = 0 \) in both cases. Consider now

\[
A(i, r) = \begin{pmatrix}
I_i & 0 & & \\
& I_{r-i-1} & & \\
& 0 & \ddots & \\
& & & 0
\end{pmatrix};
\]  

(20)

that is,

\[
A(i, r) = \text{diag}\left(1, \ldots, 1, 0, 1, \ldots, 1, 0, \ldots, 0\right).
\]
Then, an easy induction argument and the proof of the precedent theorem show that \( A(i, r) \) has an orbit of length \( q^{i-1} \). Since \( A(r - 1, r) = A(0, r - 1) \), set, for uniqueness, the restriction \( 0 \leq i \leq r - 2 \), where \( 1 \leq r \leq n \).

4. LIE METHODS

In this section, we will prove the reverse inclusion, that is, any orbit length is a \( q \)-power, unless \( \mathfrak{g} \) symplectic and \( p = 2 \). The idea is to extend some of the methods used by Chevalley to define the finite correspondent of automorphism groups of simple Lie algebras. In his considerations a central role is played by the exponential function defined over a nilpotent \( \mathfrak{g} \)-algebra of operators. The principal obstruction in this approach is that this map cannot be defined for \( \mathbb{F}_q \)-algebras when the index of nilpotency overcomes \( p \), the characteristic of the finite field. We will prove there exists a family of maps providing bijections between particular nilpotent \( \mathbb{F}_q \)-algebras and linear groups. We will find a particularly simple map for \( \mathfrak{g} = SL(n, q) \), which will allow us to prove that every conjugacy class in \( \mathfrak{g} \) has \( q \)-power order.

**Definition 4.10.** Denote with \( K[[x]] \) the \( K \)-algebra of formal power series over the field \( K \).

**Definition 4.11.** Denote with \( \mathcal{N}_n \) the nilpotent \( K \)-algebra of strictly lower triangular matrices of \( (K)_n \).

**Definition 4.12.** Suppose \( \mathcal{N} \) is a nilpotent algebra, denote with \( \nu(\mathcal{N}) \) the index of nilpotency of \( \mathcal{N} \), that is, the minimal integer such that \( N^r = 0 \), \( \forall N \in \mathcal{N} \).

In particular, we have \( \nu(\mathcal{N}_n) = n \).

**Lemma 4.13.** Suppose \( M_1, M_2 \) are elements of \( \mathcal{N}_n \), \( \mathcal{N}_r \), respectively. Let \( f = \sum_i f_i x^i \in K[[x]] \) and \( A \in (K)_n \). Set \( Y = M_1 A - A M_2 \); then

\[
f(M_1)A = Af(M_2) + \sum_{i=1}^{\infty} \left( \sum_{j=0}^{i-1} f_j M_1 Y M_2^{i-1-j} \right).
\]

**Proof.** We first prove by induction on \( i \) that

\[
M_1^i A = A M_2^i + \sum_{j=0}^{i-1} M_1^j Y M_2^{i-1-j}.
\]  \hspace{1cm} (21)
For $i = 1$, we have $\Sigma_{j=0}^{i-1} M_i^j Y M_2^{i-j} = Y$, which is just the definition of $Y$.

Now

$$M_i^{i+1} A = M_i \left( AM_i^{i+1} + \sum_{j=0}^{i-1} M_i^j Y M_2^{i-j} \right)$$

$$= AM_i^{i+1} + Y M_2^{i} + \sum_{j=0}^{i-1} M_i^j M_2^{i-j}$$

$$= AM_i^{i+1} + \sum_{j=0}^{i} M_i^j Y M_2^{i-j}, \hspace{1cm} (22)$$

completing the induction step. Multiply now by $f_i$ and sum up. Observe that the number of summands is actually finite by the nilpotency of $M_i$.

We now need to establish some facts about nilpotent commutative algebras.

**Lemma 4.14.** Suppose $x$, $y$ are nilpotent operators and $xy = yx$. Set $\nu(x) = i$ and $\nu(y) = j$, then $(x + y)^{i+j-1} = 0$; in particular, $x + y$ is nilpotent.

**Proof.** Use the binomial theorem and observe that $x^n y^m = 0$ whenever $n + m \geq i + j - 1$.

**Definition 4.15.** Set $\Phi_{M_1, M_2} (Y) = \Sigma_{i=0}^{i} \Sigma_{j=0}^{i-1} f_i M_i^j Y M_2^{i-j-1}$, where $Y \in (K)_{K \times r}$ and $M_1 \in \mathcal{A}_i$, $M_2 \in \mathcal{A}_j$.

**Lemma 4.16.** If $Y \in (K)_{K \times r}$ and $M_1 \in \mathcal{A}_i$, $M_2 \in \mathcal{A}_j$, then $\Phi_{M_1, M_2} (Y)$ is a linear operator in $Y$ and is invertible if and only if $f_1 \neq 0$.

**Proof.** The linearity is obvious. Denote now with $\lambda = \lambda M_i$ the operator $Y \lambda \rightarrow M_i Y$ and with $\rho = \rho_{M_2}$ the operator $Y \rho \rightarrow Y M_2$. Clearly $\lambda$ and $\rho$ are commuting nilpotent operators. Now

$$\Phi_{M_1, M_2} = \sum_{i \geq 0} f_{i+1} \sum_{j} M_i^{j} Y M_2^{i-j} = f_1 I + \sigma. \hspace{1cm} (23)$$

Applying the preceding lemma repeatedly, we see that $\sigma$ is a nilpotent operator. Hence $\Phi_{M_1, M_2}$ is invertible iff $f_1 \neq 0$.

Suppose now that $\text{char} K = 0$ or $n \leq \text{char} K$, then $\exp(M) = \Sigma_{i=0}^{\infty} M^i/i!$ is well defined for every element in $\mathcal{A}_n$. Suppose $Y = 0$, then we have the following result:

**Corollary 4.17.** Suppose $M_1 A + AM_2 = 0$, $M_i \in \mathcal{A}_n$ and $A \in (K)_{n}$, then $\exp(M_1) A \exp(M_2) = A$. 
Proof. Simply observe that \( \exp(-M_2) = \exp(M_2)^{-1} \) and apply Lemma 4.13. 

We point out two facts:

(a) We have used the well known property of the classical exponential map \( \exp(-x) = \exp(x)^{-1} \) over \( \mathbb{C} \). This property carries over even when \( \exp \) is defined as a formal power series repeating exactly the proof for the complex case.

(b) The last result provides a correspondence between nilpotent operators and elements that, roughly speaking, centralize the matrix \( A \).

The aim is to construct a bijection from \( \mathcal{N}_n \) onto \( \mathfrak{g}_n \), where \( \mathfrak{g}_n \) denotes the unipotent lower triangular matrices in \( (K)_n \), through a suitable power series \( f \) sharing some of the properties of the exponential map. To attain a simpler notation, we will not distinguish between the power series \( f \) and the operator induced by it on \( \mathcal{N}_n \).

**Theorem 4.18.** There exists \( f = 1 + x + \sum_{i \geq 2} f_i x^i \in \mathbb{F}_q[[x]] \), \( p > 2 \), with the following properties:

(a) \( f(N) = f(N)^{-1} \) \( \forall N \in \mathcal{N}_n \).

(b) \( f(M_1)A f(-M_2) = A \leftrightarrow M_1A = AM_2 \).

(c) \( f \) induces a bijection from \( \mathcal{N}_n \) onto \( \mathfrak{g}_n \).

Observe that we do not require \( \dim M_1 = \dim M_2 \).

**Proof.** Set \( f(x) := \sum_{i \geq 0} f_i x^i \). We will show that for \( p > 2 \) it is possible to determine the coefficients \( f_i \in \mathbb{F}_q \) in such a way that the above conditions are satisfied.

**Step 1.** Given \( N \in \mathcal{N} \), clearly \( f(N) \) is lower triangular and unipotency is equivalent to \( f_0 = 1 \).

**Step 2.** Set \( g(x) = f(x) f(-x) = \sum_{i \geq 0} c_i x^i \). Clearly \( g(x) = g(-x) \), hence \( c_{2i+1} = 0 \). We have only to consider the conditions

\[
\begin{align*}
  c_0 &= 1 \\
  c_i &= 0 \quad 0 < i < n.
\end{align*}
\]

(24)

Now \( c_0 = f_0^2 = 1 \). Suppose we determined \( f_i \) for \( i < 2k \). The condition \( c_{2k} = 0 \) is satisfied as soon as

\[
2 f_{2k} = 2 f_{2k-1} f_1 - 2 f_{2k-2} f_2 + \cdots + 2(-1)^{k+1} f_{k+1} f_{k-1} + (-1)^{k+1} f_k^2,
\]

(25)
which is solvable in $f_{2k}^1$ since $p > 2$. Observe that no condition is given on the odd indexed coefficients.

Step 3. By Lemma 4.13, with $Y = 0$, we already still know that
\[ M_1 A = A M_2 \Rightarrow f(M_1) A = A f(M_2) = A f(-M_2)^{-1}. \]
Conversely, let $T$ be a unipotent matrix. As we will prove in the next step, there exists $N \in \mathcal{X}$ such that $T = f(N)$. Define $Y$ so that $M_1 A = A M_2 + Y$. Then $\Phi_{M_1, M_2}(Y) = 0$. By Lemma 4.16, $f_1 = 1$ implies $Y = 0$.

Step 4. We must now prove that $f$ actually induces a bijection from $\mathcal{X}$ onto $\mathcal{X}_n$. It is clearly enough to determine a power series $h$ centered in the identity such that $h(f(N)) = N$. In such a case $h$ would be defined on all of $\mathcal{X}$ since $T - I$ is nilpotent whenever $T \in \mathcal{X}$. This implies immediately that $f$ induces an injective map from $\mathcal{X}$ into $\mathcal{X}_n$. Since $|\mathcal{X}_n| = q^{\frac{n}{2} + 1} = |\mathcal{X}|$, clearly $f$ induces also a bijection. Set now $h(y) = \sum_{j \geq 0} h_j (y - 1)^j$. Since $f(0) = I$, then $h_0 = 0$. Substituting formally $y$ with $\sum_{j \geq 0} f_j x^j$, we get

\[ \sum_{i \geq 1} h_i \left( \sum_{j \geq 1} f_j x^j \right)^i = x. \]  

(26)

Collecting $x^j$ in each summand we see that this system is equivalent to a set of equations involving just a finite number of coefficients $h_i$ each time. More precisely, $h_i = f_i = 1$. Again by induction, suppose we have determined every coefficient $h_i$ with $i < k$, then $h_k = s(h_1, \ldots, h_{k-1}, f_k)$, where $0 \leq j < n$, for some term $s$ depending on the coefficients enclosed by the parentheses.

Observe that $M_1 A = A M_2$ is a linear condition in the entries of $M_1$, hence the number of solutions of this equation over $\mathbb{F}_q$ is actually a $q$-power and clearly this holds for the corresponding image via $f$. Specializing $M_1, M_2, A, n$, we are in the position to prove that the orbit lengths are only $q$-powers. We start with the linear case, where a slightly more general result holds.

Theorem 4.19. Let $\mathfrak{B}$ be the $p$-Sylow subgroup of $GL(n, q)$, then $\forall g \in \mathfrak{B}, |g^{\mathfrak{B}}|$ is a $q$-power.

Proof. It is enough to show that $|C_{\mathfrak{B}}(g)|$ is a $q$-power. Suppose $g = I + N$, where $N$ is a strictly lower triangular matrix, then

\[ (I + N)(I + M) = (I + M)(I + N) \Leftrightarrow I + M \in C_{\mathfrak{B}}(g). \]  

(27)

But this is equivalent to $NM = MN$, which is a linear condition in the entries of $M$.  

Observe that no restriction on \( p \) is needed for the preceding result.

We can now prove that the \( \Xi \)-orbit in \( \mathfrak{H} \) have only \( q \)-power order, completing the proof of Theorem 3.4.

**Theorem 4.20.** \( \mathfrak{S}(\mathfrak{H}) \subseteq \{ q^j \mid 0 \leq j \leq g(n) \} \) unless \( \mathfrak{H} \) is symplectic and \( p = 2 \).

**Proof.** It is enough to declare which matrices play the role of \( M_1, M_2, A \) and observe that \( f(N') = f(N) \).

(a) In the symplectic case let \( M_1 = N' \), \( M_2 = -N \), \( A \) symmetric, where all matrices have dimension \( n \).

(b) In the linear case, just apply Theorem 4.19.

**Remark 4.1.** To show the elegance of this approach, we will prove once again that the matrices described in the symplectic case have the required orbit lengths. Consider first \( A = A(I, r) = \left( \begin{smallmatrix} I & b \\ 0 & 0 \end{smallmatrix} \right) \). Then \( N'A + AN = 0 \) is equivalent to

\[
\begin{pmatrix}
N' & M' \\
0 & L'
\end{pmatrix}
\begin{pmatrix}
I & 0 \\
0 & 0
\end{pmatrix}
+
\begin{pmatrix}
I & 0 \\
0 & 0
\end{pmatrix}
\begin{pmatrix}
N & 0 \\
M & L
\end{pmatrix}
= 0;
\]

that is, \( N = 0 \). Hence this equation has \( q^{(n-r)+r+1} \) solutions. But this is also the order of the centralizer of \( A \). It follows that the orbit length is \( q^{(r^2-r)-r(n-r)} = q^{r^2} \). Let now \( A = A(I, r) \). Without restriction we may think that \( r = n \). Set \( s = n - l - 1 \), then

\[
\begin{pmatrix}
N' & a & M' \\
0 & 0 & b \\
0 & 0 & L'
\end{pmatrix}
\begin{pmatrix}
I & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & I_r
\end{pmatrix}
+
\begin{pmatrix}
I & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & I_r
\end{pmatrix}
\begin{pmatrix}
N & 0 & 0 \\
M & b' & L
\end{pmatrix}
\]

is the zero matrix and this implies \( N, M, L, b \) must annihilate. The only term surviving is the vector \( a \) which can be chosen in \( q^l \) ways, so the corresponding orbit length for the element \( A \) is \( q^{r^2-l} \).

An interesting question is whether every conjugacy class in these groups has \( q \)-power order.

5. CHARACTER DEGREES

We will finally prove that the restriction \( q = p \) forces \( cdA = \mathfrak{S}(\mathfrak{H}) \).

We provide a correspondence between \( \mathfrak{H} \) and \( \mathfrak{H} \), considered as sets of matrices, which induces a weak \( \Xi \)-equivalence; that is, \( \mathfrak{S}(\mathfrak{H}) = \mathfrak{S}(\mathfrak{H}) \).
**Definition 5.21.** Consider
\[ A = \sum_{1 \leq i \leq k} \sum_{1 \leq j \leq r} a_{ij} E_{ij} \in (K)_{k \times r} \]
and define
\[ A^t := \sum_{1 \leq i \leq k} \sum_{1 \leq j \leq r} a_{k-i, j-i} E_{ij} \in (K)_{r \times k}. \]

We will call $s$ the reflection or specular operator (Spiegelung operator).

Observe that $s$ corresponds to the reflection along the diagonal starting from the bottom left corner. We provide a more manageable description of the reflection operator.

**Lemma 5.22.** Let $J_i = \sum_{j=1}^i E_{ij} \cdots$ and $A$ as above, then $A^t = J_i A^t J_i$.

**Proof.** Set $A = \sum_{i=m}^r a_{im} E_{im}$, then
\[ \sum_{i=1}^r E_{i, r+1-i} \sum_{1 \leq m \leq r} \sum_{1 \leq l \leq k} a_{im} E_{mi} \sum_{j=1}^k E_{k+1-j, l} = \sum_{1 \leq l \leq k} a_{k+1-j, r+1-i} E_{ij}, \] as asserted.  □

Observe that $J_i = J_i^t = J_i^{-1} = J_i^t$.

**Corollary 5.23.** Suppose dimension matches. Then $(AB)^t = B^t A^t$.

**Proof.** Let $A \in (K)_{k \times r}$, $B \in (K)_{r \times m}$. Then $(AB)^t = J_m (AB) J_k = J_m B^t J_i A^t J_k = B^t A^t$.  □

Hence, for $k = r = m$, $s$ is an involutory ring anti-automorphism of $(K)_k$.

**Corollary 5.24.** Denoting with $s$ and $t$ the reflection and transposition operator, we have $st = ts$.

**Proof.** $A^{st} = \sum_{i=m}^r a_{im} E_{mi} = J_k A J_i = A^t$.  □

For $r = k$, it turns out that $st$ is an automorphism of the central simple algebra $(K)$, and, by a theorem of Noether and Skolem, it would be an inner one, precisely that induced by conjugation by $J$.

The second ingredient of the proof is a lemma establishing how the dual action can be expressed in terms of matrices.

**Definition 5.25.** Given a matrix $A \in (F_q)_r$, let $\tau(A) = Tr_{F_q \rightarrow F_p}(Tr(A))$.

**Lemma 5.26.** Let $V = (F_q)_{k \times r}$ and define $\hat{\tau} : V \rightarrow Hom(V, F_p)$ by $\hat{\tau}(B) = \tau(A^t B)$. Then $\hat{\tau}$ is an $F_p$-isomorphism.
Proof. $F_p$-linearity is clear. By finite dimensionality, it is enough to show that $\tau$ is injective. In fact, let $A = \sum_{m,j} a_{m,j} E_{lm}$ and $B = bE_{ij}$ then

$$0 = \tau \left( \sum_{m,j} a_{m,j} E_{lm} b E_{ij} \right) = \text{Tr}_{F_p^*} (ba).$$

(31)

Since $\text{Tr}(F_p) = F_p$ and $b$ is arbitrary, this forces $a_{m,j} = 0$, $j = 1, \ldots, k$, $i = 1, \ldots, r$. $\blacksquare$

Lemma 5.27. Let $\tilde{\mathcal{X}} = \left( (T_1, 0, T_2) \right)$, where $T_1, T_2$ are unipotent lower triangular matrices of dimension $r, k$. Let $V = (F_p^k)_{k-r}$ be endowed with a $\tilde{\mathcal{X}}$-set structure via $A^T = T_1 A T_2$, where $T = \left( \begin{smallmatrix} T_1 & 0 \\ 0 & T_2 \end{smallmatrix} \right) \in \tilde{\mathcal{X}}$. Then the induced $\tilde{\mathcal{X}}$-action on $\text{Hom}(V, F_p)$ is described by $A^T = T_2 A T_1^*$. In particular, $C_{\tau}(A) = \{ T \in \tilde{\mathcal{X}} : A = T_2 A T_1^* \}$.

Proof. We remark that for an arbitrary $G$-module $M$, the induced action on the dual space $\overset{\sim}{M}$ is given by $\mu'(m) = \mu(m^*)$. Now

$$(\overset{\sim}{A})^T(B) = \overset{\sim}{A}(B^T) = \tau(A^T T_2^{-1} B T_1^{-1})$$

$$= \tau(T_1^{-1} A^T T_2^{-1} B) = \tau((T_2^* A T_1^*)^T B)$$

$$= T_2^* A T_1^*(B).$$

(32)

It follows that $\overset{\sim}{A} = \overset{\sim}{A}$ if and only if $\overset{\sim}{A} = T_2^* A T_1^*$. The second part of the lemma is a simple consequence of the injectivity of $\tau$. $\blacksquare$

Theorem 5.28 (Weak Equivalence). Let $\tilde{\mathcal{X}}$ be as in Lemma 5.27 and $\mathfrak{l} = \left( \begin{smallmatrix} T_1 & 0 \\ 0 & T_2 \end{smallmatrix} \right) : A \in (F_p^k)_{k-r}$. Then $\mathfrak{l}$ and $\overset{\sim}{\mathfrak{l}}$ are weakly equivalent $\tilde{\mathcal{X}}$-sets.

Proof. $B^\mathfrak{l} = (T_2 B T_1)$ where $T_i$ varies in the set of unitriangular lower matrices of suitable dimension. Now the $\tilde{\mathcal{X}}$-orbit of $B^\mathfrak{m} \in \overset{\sim}{V}$ is

$$\left\{ T_2^* B^\mathfrak{m} T_1^* \right\} = \left\{ (T_2^* B T_1^{-1})^T \right\}.$$

Since the map $T \rightarrow T^{-1}$ is an automorphism of the group of unitriangular lower matrices and $^*$ is one-to-one, this set has the same order as the $\tilde{\mathcal{X}}$-orbit of $B \in V$. Hence $\sigma(\mathfrak{m}) \subseteq \sigma(\overset{\sim}{\mathfrak{m}})$. The converse inclusion follows analogously. $\blacksquare$

We now consider the symplectic case.

Lemma 5.29. Let $\mathfrak{h} = \left( \begin{smallmatrix} 0 & F_q^r \\ F_q^r & 0 \end{smallmatrix} \right)$, where $T$ is a unipotent lower triangular matrix of dimension $n$. Let $V$, the set of symmetric matrices in $(F_q)^n$, $q$ odd.
be endowed with the structure of a \( \mathcal{X} \)-set via \( A^3 = T'AT \), where \( S = (t_{i,j}) \in \mathcal{X} \). Define \( \lambda : V \to \text{Hom}(V, F_\mathbb{P}) \) via \( \lambda(A) = \tau(A'B) \), then:

(a) For any \( \lambda \in \text{Hom}(V, F_\mathbb{P}) \) and \( B \in V, \exists! A \in V \) such that \( \lambda(B) = \hat{A}(B) \),

(b) \( \hat{V} = \text{Hom}(V, F_\mathbb{P}) \),

(c) \( \hat{A} = T'^{-1}AT^* \),

(d) \( C(A) = \{ S \in \mathcal{X} : A = T^{-1}AT^* \} \).

Proof. The part relative to the structure of \( \text{Hom}(V, F_\mathbb{P}) \) as a \( \mathcal{X} \)-set is a particular case of Lemma 5.27 when \( k = r = n \) and \( T = T' \). We need to assure the regularity of the bilinear form \( \langle , \rangle : V \times V \to F_\mathbb{P} \), defined by \( (A, B) = \tau(A'B) \). It is enough to show that \( \hat{V} \to \text{Hom}(V, F_\mathbb{P}) \) is surjective. By Lemma 5.26, any \( \mu \in \text{Hom}(F_q, F_\mathbb{P}) \) is of the form \( \hat{C} \), where \( C \in (F_q)^n \).

We prove that \( \lambda = \mu_\mathcal{A} \), the restriction of \( \mu \) to symmetric matrices, is of the form \( \hat{A} \) for some symmetric matrix \( A \). Let \( B \) be symmetric, then

\[
(C, B) = \tau(C'B) = \tau(B'C) = \tau(CB) = (C', B).
\]

Since \( q \) is odd, \( (C, B) = \frac{1}{2}(C' + C), B = (A, B), \) where \( A = \frac{1}{2}(C' + C) \) is the symmetric matrix for which we were looking.

Theorem 5.30 (Weak Equivalence). Let \( \mathcal{X} \) be as in Lemma 5.29 and \( \mathcal{I} = \{(t_{i,j}) : A \in (F_q)^n, A' = A \} \). Then \( \mathcal{I} \) and \( \hat{\mathcal{I}} \) are weakly equivalent \( \mathcal{X} \)-sets.

Proof. We will show that the reflection operator induces a weak equivalence between \( \mathcal{I} \) and its dual. Observe that the operator group is closed under \( s \). The \( \mathcal{X} \)-action is given by \( T'BT \), where \( B \) is symmetric. By Corollary 5.23, we have

\[
(T'BT)^s = T'B'(T')^s.
\]

Set \( S^{-1} = T' \), then, by Corollary 5.24, \( S^* = (T')^s \). Hence the reflected image is \( S^{-1}B'S^* \). But, by Lemma 5.29, this term describes the dual action. Since \( s \) is a bijection onto \( \mathcal{X} \), this implies that

\[
|B^s| = |(B')^s|,
\]

where \( ^s \) suggests that \( \mathcal{X} \) is acting on the dual space. Hence \( \mathcal{E}(\mathcal{I}) \subseteq \mathcal{E}(\hat{\mathcal{I}}) \).

By Lemma 5.29, we obtain analogously the converse inclusion.
With the usual restriction $p \neq 2$ when $\Psi$ is symplectic, the following statement holds:

**Corollary 5.31.** Let $\lambda \in Irr(\Pi)$, then $|I_{q}(\lambda) : \Pi|$ is a $q$-power.

**Proof.** This follows by weak equivalence and Theorem 4.20.

The necessity of the condition $p \neq 2$ in the symplectic case was pointed out to me by Isaacs. One can show that for the $\Xi$-set $V$ of symmetric matrices in $(\mathbb{F}_{q})_{2}$, $q$ even, $\sigma(V) = \{1, q\}$, but $\sigma(V) = cd\Psi = \{1, q/2, q\}$. Hence $\Pi$, $\hat{\Pi}$ are not weakly $\Xi$-equivalent and the character degrees conjecture is false in even characteristic. We now show that the restriction $q = p$ implies:

**Theorem 5.32 (Character Degrees).** Suppose $\Psi \in Syl_{p}(\mathcal{S}_{n}(\mathbb{F}_{p}))$, where $\mathcal{S}_{n}(\mathbb{F}_{p})$ is $SL(n, p)$ or $Sp(n, p)$. Set

$$g(n) = \begin{cases} 
 f(n), & \mathcal{S}_{n}(\mathbb{F}_{p}) \text{ linear,} \\
 n/2, & \mathcal{S}_{n}(\mathbb{F}_{p}) \text{ symplectic,}
\end{cases}$$

then $cd\Psi = \{p^j : 0 \leq j \leq g(n)\}$.

**Proof.** Unless the symplectic case in even characteristic, $\sigma(\Pi) = \sigma(\hat{\Pi})$ by Theorems 5.28 and 5.30. By Lemma 2.3, $\sigma(\hat{\Pi}) \subseteq cd\Psi$. By Itô's theorem equality holds. In the remaining case, Lemma 5.29 assures only that $\sigma(\Pi) \subseteq \sigma(\hat{\Pi})$, but the restriction $q = 2$ forces again equality.

Isaacs has recently established that the character degrees of the $p$-Sylow subgroup of $SL(n, q)$ are only $q$-powers. The author, using a similar procedure, extended this result to the symplectic case in odd characteristic. This shows that the restriction $q = p$ is not necessary in Theorem 5.32.

**Acknowledgment**

This paper is part of the author's dissertation written under the direction of Professor B. Huppert. The author thanks Professor Huppert for his helpful suggestions.

**References**

1. R. Brauer, On groups whose order contains a prime number to the first power I. *Amer. J. Math.*, 64 (1942), 401–420.