Lie derived length and involutions in group algebras

Zsolt Balogh

Institute of Mathematics and Computer Science, University College of Nyíregyháza, Nyíregyháza, Hungary

A R T I C L E   I N F O

Article history:
Received 13 May 2011
Received in revised form 23 November 2011
Available online 23 December 2011
Communicated by C. Kassel

MSC: 16W10; 16S34

A B S T R A C T

Let $G$ be a group such that the set of $p$-elements of $G$ forms a finite nonabelian subgroup, where $p$ is an odd prime, and let $F$ be a field of characteristic $p$. In this paper we prove that the lower bound of the Lie derived length of the group algebra $FG$ given by Shalev in [11] is also a lower bound for the Lie derived length of the set of symmetric elements of $FG$ for every involution which is linear extension of an involutive anti-automorphism of $G$. Furthermore, we provide counterexamples to the interesting cases which are not covered by the main theorem.

1. Introduction

Let $FG$ be a group algebra of a group $G$ over a field $F$. Then $FG$ may be considered as a Lie algebra with the Lie operation defined by $[x, y] = xy - yx$ for all $x, y \in FG$. For a subset $S \subseteq FG$ we define the Lie derived series by the following way. Let $\delta^{[0]}(S)$ be the vector space over $F$ spanned by $S$ and let $\delta^{[n+1]}(S)$ be the vector space spanned by all Lie commutators $[x, y]$ with $x, y \in \delta^{[n]}(S)$. The subset $S$ is said to be Lie solvable if there exists $n$ such that $\delta^{[n]}(S) = 0$, and the smallest such $n$ is called the Lie derived length of $S$ which will be denoted by $dl(S)$.

The study of Lie properties of $FG$ is very useful to get information about the whole group algebra and its group of units as well. Thus Lie methods play an important role in the theory of group algebras. More Lie properties such as Lie nilpotency, Lie $n$-Engel, Lie solvability, strong Lie solvability were considered in group algebras. The study of Lie solvability proves to be very difficult and we know very little about it in spite of the fact that it has been studied by many authors for group algebras as well as for their subsets. First Shalev [11] succeeded in giving a lower bound for the Lie derived length of group algebras of a nonabelian group $G$ and a field $F$ of positive characteristic $p$. This lower bound is $\lceil \log_p(p + 1) \rceil$, where $\lceil r \rceil$ is the upper integer part of $r$ and it turned out that is the correct one.

Let $\odot$ be an involution on $FG$. Denote by $FG^+_\odot$ and $FG^-_\odot$ the set of symmetric and skew-symmetric elements in $FG$ under involution $\odot$, respectively, that is $FG^+_\odot = \{x \in FG \mid x^\odot = x\}$ and $FG^-_\odot = \{x \in FG \mid x^\odot = -x\}$. Evidently, they are vector spaces over $F$. Amitsur's result (Theorem 6 in [1]) inspired the study of the properties of the set of symmetric and skew-symmetric elements in group algebras. It turned out that the symmetric or skew-symmetric elements determine the Lie derived length of the whole group algebra in some cases. The main result in [3] is that $dl(FG) = dl(FG^+_\odot) = dl(FG^-_\odot)$, where $\star$ is the canonical involution and $G$ is a nilpotent group with cyclic derived subgroup of order $p^n$ ( $p$ is an odd prime) and $F$ is a field of characteristic $p$. We refer the reader to the book [9] by Lee for further results on the Lie properties of the set of symmetric and skew-symmetric elements.

By group involution some authors mean an involutive group anti-automorphism. We say that an involution $\odot$ of $FG$ arises from the group $G$ if $\odot$ is $F$-linear extension of an involutive anti-automorphism of $G$. Jespers and Ruiz [5] gave the conditions for $G$ such that the elements of $RG^+_\odot$ ($R$ is a commutative ring) commute for all involutions $\odot$ which arise from $G$. In [6] they also studied the case when the Lie algebra of skew-symmetric elements $FG^-_\odot$ has Lie derived length 1 under an involution which is a linear extension of a group involution on $G$.

© 2011 Elsevier B.V. All rights reserved.

E-mail address: baloghzs@nyf.hu.

0022-4049/$– see front matter © 2011 Elsevier B.V. All rights reserved.
Let \( p \) be an odd prime and \( FG \) the group algebra of a group \( G \) without 2-elements over a field \( F \) of characteristic \( p \). If the set of \( p \)-elements of \( G \) forms a finite normal subgroup, then \( FG^1_\circ \) (\( \circ \) is the canonical involution) is Lie solvable if and only if \( FG \) is Lie solvable by Theorem 1.1 in [8]. In general, we do not know any conditions on \( G \) such that \( FG^1_\circ \) or \( FG^2_\circ \) is Lie solvable with respect to an involution \( \circ \). The present paper is devoted to generalizing Shalev’s result in [11] by showing that the lower bound for the Lie derived length of \( FG^1_\circ \) coincides with the lower bound of the whole group algebra with respect to every involution \( \circ \) which arises from \( G \), when \( F \) is a field of odd characteristic \( p \) and the set of \( p \)-elements of \( G \) forms a finite nonabelian subgroup. Our main result is the following.

**Theorem 1.** Let \( p \) be an odd prime, \( G \) a group in which the set of \( p \)-elements forms a finite nonabelian subgroup and let \( FG \) be its group algebra over a field \( F \) of characteristic \( p \). Then

\[
dl(FG^1_\circ) \geq \lceil \log_p (p + 1) \rceil
\]

for every involution \( \circ \) which arises from \( G \).

Our main theorem and Proposition B in [11] give immediately the following corollary.

**Corollary 2.** Let \( F \) be a field of characteristic \( p > 2 \) and \( G \) a group in which the set of \( p \)-elements forms a finite nonabelian subgroup with central derived subgroup of order \( p \). Then \( dl(FG^1_\circ) = \lceil \log_p (p + 1) \rceil \) for every involution \( \circ \) which arises from \( G \).

Although, for an odd prime \( p \), the main result in [10] yields that \( FG \) is Lie solvable if and only if \( G \) is a \( p \)-abelian group (the derived subgroup of \( G \) is a finite \( p \)-group), in this case the lower bound of the Lie derived length of \( FG \) is not always attained by the Lie derived length of the set of symmetric elements. For example, for \( p > 2 \) the group algebra of \( G = \langle a, b \mid a^3 = b^3 = 1, ba = a^{-1}b \rangle \) has \( dl(FG^2_\circ) = 2 \) for any field \( F \) of characteristic \( p \), so for \( p > 3 \) \( dl(FG^1_\circ) < \lceil \log_p (p + 1) \rceil \).

It is worth noting that in our case the lower bound given by Shalev is not always attained by the Lie derived length of the Lie subalgebra of skew-symmetric elements. For example, let \( G = \langle a, b, c \mid a^3 = b^3 = c^3 = 1, (a, b) = c \rangle \). Then \( G \) has an involutive anti-automorphism \( \circ \) which acts on \( a \) and \( b \) by \( a^\circ = ac^{-1} \) and \( b^\circ = b \) and we can easily calculate that \( dl(FG^1_\circ) = 1 \), where \( F \) is a field of characteristic 3. Jespers and Ruiz [5] showed that the elements in \( FQ_8^1 \) commute with respect to the canonical involution \( \ast \), where \( Q_8 \) is the quaternion group of order eight and \( F \) is an arbitrary field. Thus the lower bound for the Lie derived length of symmetric elements can be one if either the group algebra is not modular or \( G \) is a 2-group and the characteristic of \( F \) is two.

### 2. Proof of the main theorem

Let \( FG \) be a group algebra of a finite nonabelian \( p \)-group \( G \) over a field \( F \) of characteristic \( p \). The following identities will be used freely throughout this paper

\[
xy - 1 = (x - 1)(y - 1) + (x - 1) + (y - 1);
\]

\[
[vw, z] = v[w, z] + [v, z]w \quad \text{and} \quad [v, wz] = w[v, z] + [v, w]z,
\]

where \( x, y, v, w, z \in FG \).

By the augmentation ideal of a group algebra \( FG \) we mean the ideal in \( FG \), generated by the set \( \{ g - 1 \mid g \in G \} \), and it will be denoted by \( \Delta(G) \). As it is well known, \( \Delta(G) \) is nilpotent if and only if \( G \) is a finite \( p \)-group and \( \text{char}(F) = p \) (see [4]). Using the first identity above, we can easily observe that

\[
g^m - 1 \equiv m(g - 1) \quad (\text{mod} \ \Delta(G)^2)
\]

for every \( g \in G \) and every integer \( m \). Let \( (a, b) \) denote the commutator \( a^{-1}b^{-1}ab \), where \( a, b \in G \). Then

\[
[a, b] = ab(1 - (b, a)), \quad [a, b] = ((a^{-1}, b^{-1}) - 1)ba \tag{2.2}
\]

and we can see that \( [a, b] \in FG \Delta(G') \), where \( G' \) is the derived subgroup of \( G \).

Let \( I_n \) denote the ideal \( \langle (\Delta(G)^2)^{n-1}, I_n \rangle \subseteq I_{n+1} \) and \( \{ I_n, I_n \} \subseteq I_{n+1} \).

**Proof.** For \( G \) the conditions of Lemma 3 in [2] are satisfied, so

\[
[\Delta(G)^k \Delta(G'), \Delta(G)^i \Delta(G')] \subseteq \Delta(G)^{k+i-2} \Delta(G')^{i+j+1},
\]

where \( k, l, i, j \geq 1 \) and by definition, \( \Delta(G)^0 = FG \).

Using (2.3), the identity

\[
FG \Delta(G')^i = \Delta(G)\Delta(G')^i + \Delta(G)^i
\]
and the fact that \( \Delta(H) \) is a subalgebras of the center of \( FG \) we get that

\[
\begin{align*}
[\Delta(G)\Delta(G')^2]^n \subseteq & \ [\Delta(G)^2\Delta(G')^2]^n, \\
& \Delta(G)^3\Delta(G')^3 + [\Delta(G)^2\Delta(G')^2, \Delta(G)\Delta(G')^3]
\end{align*}
\]

Applying the same identities and facts as before we have

\[
[I_n, I_n] \subseteq [\Delta(G)^3\Delta(G')^3, \Delta(G)^4\Delta(G')^4] + [\Delta(G)^2\Delta(G')^2, \Delta(G)\Delta(G')^3]
\]

as required. \( \square \)

Let \( G \) be a finite \( p \)-group with derived subgroup \( G' \) of order \( p \) and \( a, b, c \) elements of \( G \) such that \( (a, b) = c \). It is easy to check (see e.g. [7] p. 252) that

\[
[b^i a^m, b^j a^l] \equiv (ms - lt)b^{i+j}a^{m+l+c} (\text{mod } FG\Delta(G')^2).
\]

We will use freely the easily verifiable fact that the value of the product

\[(g - 1)(h - 1)(c - 1)\]

is independent of the order of its factors modulo \( I_1 \) for all \( g, h \in G \) and \( c \in G' \).

Throughout the following lemmata by \( p \) we mean an odd prime and let \( F \) denote a field of characteristic \( p \). We write \( C_p \) for the cyclic group of order \( p \) and \( G_\infty \) for the set \( \{g \in G \mid g^p \in C_p(g)\} \) of \( G \), where \( C_p(g) \) is the centralizer of \( g \) in \( G \).

**Lemma 4.** Let \( G \) be a finite \( p \)-group with derived subgroup of order \( p \), such that \( G/\zeta(G) \cong C_p \times C_p \), \( FG \) its group algebra over \( F \) and let \( \zeta \) be an involution on \( FG \) which arises from \( G \). If \( G_\infty = G \), then

\[
dl(FG_\infty^+) \geq \lfloor \log_2(p + 1) \rfloor.
\]

**Proof.** Let \( a, b \in G \) such that \( (a, b) = c \neq 1 \) for some \( c \in G' \). Evidently, \( \zeta(G) \supseteq \Phi(G) = G'G^p \), where \( G^p = \{g^p \mid g \in G \} \) and \( \Phi(G) \) is the Frattini subgroup of \( G \). Then \( a^e = b^a y_1 \) and \( b^e = b^a y_2 \), where \( y_1, y_2 \in \zeta(G) \) and \( 0 \leq l, m, s, t < p \). Since \( a, b, ab \in G_\infty \), we conclude that \( l = t = 0 \) and \( m = s \). Therefore \( a^e = a^m y_1 \) and \( b^e = b^m y_2 \) for \( y_1, y_2 \in \zeta(G) \), where \( m \) is either \( 1 \) or \( p - 1 \).

It is easy to see that \( (g - 1)(g\zeta - 1) \in FG_\infty^+ \) for all \( g \in G \). Let \( u_0 = (a - 1)(a\zeta - 1) \), \( v_0 = (b - 1)(b\zeta - 1) \) and \( w_0 = (ab - 1)(ab\zeta - 1) \). Let \( H \) be the center \( \zeta(G) \) of \( G \) and let \( I_1 \) be the ideal of \( FG \) as defined before. Let us calculate the Lie commutator of the symmetric elements \( u_0, v_0 \)

\[
[u_0, v_0] = (a - 1)(b - 1)[a^e, b^e] + (a - 1)[a^e, b](b^e - 1) + (b - 1)[a, b^e](a^e - 1) + [a, b][b^e - 1](a^e - 1)
\]

\[
= (a - 1)(b - 1)[a^m y_1, b^m y_2] + (a - 1)[a^m y_1, b](b^m y_2 - 1)
\]

\[
+ (b - 1)[a, b^m y_2](a^m y_1 - 1) + [a, b][b^m y_2 - 1](a^m y_1 - 1).
\]

Using (2.1) and (2.4) we have that

\[
[u_0, v_0] \equiv 4m^2(a - 1)(b - 1)(c - 1) + 4m^2(a - 1)^2(c - 1) (\text{mod } I_1).
\]

Similar computations show that

\[
[w_0, v_0] \equiv 4m^2(a - 1)(b - 1)(c - 1) + 4m^2(b - 1)^2(c - 1) (\text{mod } I_1).
\]

The fact that \( \delta^{[1]}(FG_\infty^+) \) is a linear space over \( F \) guarantees that there exist elements \( u_1, v_1, w_1 \in \delta^{[1]}(FG_\infty^+) \) such that

\[
u_1 \equiv (a - 1)(b - 1)(c - 1) (\text{mod } I_1);
\]

\[
v_1 \equiv (a - 1)^2(c - 1) (\text{mod } I_1);
\]

\[
w_1 \equiv (b - 1)^2(c - 1) (\text{mod } I_1).
\]

Assume that for some \( n > 1 \), we have \( u_n, v_n, w_n \in \delta^{[n]}(FG_\infty^+) \) with properties

\[
u_n \equiv (a - 1)(b - 1)(c - 1)^{2n-1} (\text{mod } I_n);
\]

\[
v_n \equiv (a - 1)^2(c - 1)^{2n-1} (\text{mod } I_n);
\]

\[
w_n \equiv (b - 1)^2(c - 1)^{2n-1} (\text{mod } I_n).
\]
Using Lemma 3 we get

\[(v_0, w_0) \equiv [(a-1)^2(c-1)^{2n-1}, (b-1)^2(c-1)^{2n-1}]\]

\[\equiv [(a-1)^2, (b-1)^2](c-1)^{2n+1-2} \quad (\text{mod } I_{n+1}),\]

furthermore, by (2.2)

\[[(a-1)^2, (b-1)^2] \equiv (a-1)(b-1)(a, b) + (a-1)(a, b)(b-1) + (b-1)(a, b)(a-1) + [a, b](b-1)(a-1)\]

\[\equiv 4(a-1)(b-1)(c-1) \quad (\text{mod } I_1),\]

so \(4^{-1}v_0, w_0] \equiv (a-1)(b-1)(c-1)^{2n+1-1} \quad (\text{mod } I_{n+1})\) and \(u_{n+1} = 4^{-1}[v_0, w_0]\) is contained in \(\delta^{[n+1]}(FG^+).\) Using Lemma 3 again, we have

\[[(a-1)^2, (a-1)(b-1)] \equiv [(a-1)^2, a, b](a-1)\]

\[\equiv 2(a-1)^2(c-1) \quad (\text{mod } I_1),\]

so \(v_{n+1} = 2^{-1}[v_0, u_0] \equiv (a-1)^2(c-1)^{2n+1-1} \quad (\text{mod } I_{n+1}).\)

Finally,

\[[(b-1)^2, (a-1)(b-1)] \equiv [(b-1)^2, (b-1)(a-1)]\]

\[\equiv [(b-1)^2, (a-1)(b-1)](c-1)^{2n+1-2} \quad (\text{mod } I_{n+1}),\]

and

\[[(b-1)^2, (a-1)(b-1)] \equiv [b, a)(b-1)^2 + (b-1)[b, a](b-1)\]

\[\equiv -2(b-1)^2(c-1) \quad (\text{mod } I_1),\]

so \(u_{n+1} = -2^{-1}[v_0, u_0] \equiv (b-1)^2(c-1)^{2n+1-1} \quad (\text{mod } I_{n+1}).\)

Assume that \(u_k, v_k, w_k\) are in \(I_k\) if \(2^k - 1 < p.\) Since \(c\) is a commutator the element \(-c - 1\) is of weight \(t \geq 2\) by Jenning’s theory [4]. Evidently, the common weight of \(u_k, v_k, w_k\) is \(2 + t(2^k - 1)\) which means that \(u_k, v_k, w_k\) are in \(\Delta(G)^{2^k+1}(t^2-1) \setminus \Delta(G)^{3^k+1}(2^k-1).\) According to the Jenning’s theory \(\Delta(G)^t\) has an \(F\)-basis consisting of regular elements of weight not less than \(s.\) Thus \(\Delta(G)^3 \Delta(G)^{t^2-1} \leq \Delta(G)^{3^k+1}(2^k-1)\) and the non-zero elements

\[(a-1)(b-1)(c-1)^{2^k-1}, (a-1)^2(c-1)^{2^k-1}\]

are in \(FG\Delta(\xi(G))(c-1)^{2^k-1}\) which is impossible.

Since \(u_k, v_k, w_k\) are nonzero elements of \(\delta^{[k]}(FG^+),\) if \(2^k - 1 < p\) so \(d_l(FG^+) \geq \lceil \log_2(p + 1) \rceil,\) as required. \(\square\)

**Lemma 5.** Let \(G\) be a finite p-group of nilpotency class two such that \(G\) is an elementary abelian subgroup. Let \(FG\) be the group algebra of \(G\) over \(F\) and let \(\circ\) be an involution on \(FG\) which arises from \(G.\) If \(G\) is of weight \(G,\) then

\[d_l(FG^+) \geq \lceil \log_2(p + 1) \rceil.\]

**Proof.** First we state some simple facts which will be used freely in this proof. Since \(G\) is a group of nilpotency class two we have that \((a, b)^2 = (a^2, b^2)^{-1}\) for all \(a, b \in G.\) We conclude from \((ab)(ab)^{-1} = 1\) that \((a, b) = (a^2, b^2)\) for all \(a, b \in G.\)

Assume that there exists a two generated \(\circ\)-invariant nonabelian subgroup \(H\) of \(G.\) Then \(H^p \subseteq \xi(H)\) and Lemma 4 says that

\[d_l(FG^+) \geq \lceil \log_2(p + 1) \rceil.\]

Otherwise, let \(a, b \in G\) such that \((a, b)^{c} \neq 1\) for some \(c \in \langle G \rangle\) and \(H = \{a, b, a^c, b^c\}.\) Clearly, \(aa^c\) and \(bb^c\) are symmetric elements of \(H.\) It is easy to see from \((ab)^c = (ab)^c\) that \(c^c = c^{-1}.\) If \(aa^c\) and \(bb^c\) did not commute, then \((aa^c, bb^c)\) would be a two generated \(\circ\)-invariant nonabelian subgroup which is impossible. Thus we can assume that \((aa^c, bb^c) = 1.\) We can easily calculate that \((aa^c, bb^c) = (aa^c, bb^c) = 1)\) which shows that \((a^c, b) = (a, b^c) = c^{-1}.\) Therefore \((a, b^c) = (a^c, b) = 1\) and \((b, a^c) = (b^c, aa^c) = 1.\) Since \(H = \{a, b, a^c, bb^c\}\) and \(aa^c, bb^c\) are in \(\xi(H)\) we have proved that \(H/\xi(H) \cong C_p \times C_p.\) Applying Lemma 4 the inequalities \(d_l(FG^+) \geq d_l(FG^+) \geq \lceil \log_2(p + 1) \rceil\) complete the proof. \(\square\)

**Lemma 6.** Let \(G\) be a finite \(p\)-group with derived subgroup of order \(p\) and \(\circ\) an involution on \(FG\) which arises from \(G.\) If \(G\) is not of weight \(G,\) then

\[d_l(FG^+) \geq \lceil \log_2(p + 1) \rceil.\]
Proof. Let $g$ be a fixed element of $G \setminus G_s$ and $(g, g^s) = c$ for some $c \in G'$. Clearly $G' = \langle c \rangle$ and $h + h^s \in FG^+_s$ for any $h \in G$. Using (2.2) we can calculate that

$$[g^i + (g^i)^s, g^j + (g^j)^s] = -g^i(g^j)^s(c^{-1} - 1) + g^i(g^j)^s(c^{-1} - 1)$$

for any $0 < i, j < p$, where $i \neq j$. We get that

$$[g^i + (g^i)^s, g^j + (g^j)^s] = ij(g^i(g^j)^s - g^i(g^j)^s)(c - 1) \pmod{FG\Delta(G')^2}$$

by (2.1). It is easy to check that $h - h^s \notin FG\Delta(G')$ when $h \in G \setminus G_s$, so we have proved that $\delta^{[1]}(FG^+_s) \neq 0$. Since $\lceil \log_2(3 + 1) \rceil = 2$ the lemma is true for $p = 3$.

Assume that $p > 3$. We will prove by induction on $n$ that if $n$ is odd, then there exist elements $x_{i,j}^n \in \delta^n(FG^+_s)$ such that

$$x_{i,j}^n \equiv (g^i(g^j)^s - g^i(g^j)^s)(c - 1)^{2^{n-1}} \pmod{FG\Delta(G')^{2^n}},$$

where $0 < i, j < p, i \neq j$, and for even $n$ that there exist elements $x_{i}^n \in \delta^n(FG^+_s)$ with property

$$x_{i}^n \equiv (g^i - (g^i)^s)(c - 1)^{2^{n-1}} \pmod{FG\Delta(G')^{2^n}},$$

where $0 < s < p$.

As we have seen before, we have $x_{i,j}^1 \in \delta^{[1]}(FG^+_s)$ with the required properties. Assume that $n$ is even. Since $p \geq 5$ there exist $0 < j, k < p$ such that $jk \equiv -1 \pmod{p}$ and $j + k \equiv 0 \pmod{p}$. Evidently, $g^{jk}(g^r)^s \in C_c(g^{r-(r^s)^s})$ for any $r \not\equiv 0 \pmod{p}$, so

$$[(g^i)^s - (g^j)^s)](c - 1)^{2^{n-1} - 1}, (g^{jk}(g^r)^s - g^j(g^j)^s)(c - 1)^{2^{n-1} - 1}$$

$$\equiv -[g^{i,j}(g^j)^s - g^j(g^j)^s](c - 1)^{2^{n-2}} - [g^{i,j}(g^j)^s - g^{i}(g^j)^s](c - 1)^{2^{n-2}}$$

$$\equiv -r^2(i + k)(g^{r(j + k)} - (g^{r(j+k)})^s)(c - 1)^{2^{n-1} - 1} \pmod{FG\Delta(G')^{2^n}}$$

by (2.1) and (2.2). Let $0 < s < p$. Since $j + k \not\equiv 0 \pmod{p}$ we can choose an $r \not\equiv 0 \pmod{p}$ such that $r(j + k) \equiv s \pmod{p}$. The fact that $\delta^n(FG^+_s)$ is a linear space over $F$ ensures the existence of $x_{i}^n \in \delta^n(FG^+_s)$ such that

$$x_{i}^n \equiv (g^i - (g^i)^s)(c - 1)^{2^{n-1}} \pmod{FG\Delta(G')^{2^n}}.$$

Suppose that $n > 1$ is odd. According to the inductive hypothesis, there exist $x_{i,j}^{n-1}, x_{j,i}^{n-1} \in \delta^{[n-1]}(FG^+_s)$ with properties

$$x_{i,j}^{n-1} \equiv (g^i - (g^i)^s)(c - 1)^{2^{n-1} - 1} \pmod{FG\Delta(G')^{2^{n-1}}},$$

and

$$x_{j,i}^{n-1} \equiv (g^i - (g^i)^s)(c - 1)^{2^{n-1} - 1} \pmod{FG\Delta(G')^{2^{n-1}}}$$

for any $0 < i, j < p$, where $i \neq j$. We can calculate as before that

$$[(g^i)^s - (g^j)^s](c - 1)^{2^{n-1} - 1}, (g^i - (g^j)^s)(c - 1)^{2^{n-1} - 1}$$

$$\equiv -[g^{i,j}(g^j)^s - g^j(g^j)^s](c - 1)^{2^{n-2}} - [g^{i,j}(g^j)^s - g^j(g^j)^s](c - 1)^{2^{n-2}}$$

$$\equiv -ij(g^i(g^j)^s - g^i(g^j)^s)(c - 1)^{2^{n-1} - 1} \pmod{FG\Delta(G')^{2^n}}.$$
Let $G$ be a group with an involutive anti-automorphism $\circlearrowright$ and let $H$ be a characteristic subgroup of $G$. The previous lemma says that $H$ is $\circlearrowright$-invariant, so for every $g \in G$ and $h \in H$ we have that $(gh)^* = g^* h$ for some $h \in H$. This shows that $\circlearrowright$ induces a mapping on $G = G/H$ (we will also denote this induced mapping by $\circlearrowright$) and $\circlearrowright$ is either the identity map on $G$ or an involutive anti-automorphism of $G$. Evidently, if $G$ is nonabelian, then $\circlearrowright$ cannot be the identity map. Indeed, if $\circlearrowright$ is the identity map on $G$, then $\overline{gh} = (gh)^* = (gh)^* = h^* \overline{g}$ for every $g, h \in G$ which shows that $G$ must be an abelian group. It is well-known that $\overline{FG} \cong FG/FG\Delta(H)$, where $F$ is a field and if $\circlearrowright$ is an involutive anti-automorphism of the nonabelian group $G$, then the linear extension of $\circlearrowright$ from $G$ is an involution on $\overline{FG}$. This involution of $\overline{FG}$ coincides with the involution induced by the linear extension of $\circlearrowright$ from $G$ into $FG$.

**Proof of the main Theorem.** Let $G$ be a finite nonabelian $p$-group, where $p$ is an odd prime and $F$ a field of characteristic $p$ and let $\circlearrowright$ be an involution of $FG$ which arises from $G$. According to Lemma 7, the third term $\gamma_3(G)$ of the lower central series of $G$ is $\circlearrowright$-invariant, so $\circlearrowright$ induces a mapping on $G_1 = G/\gamma_3(G)$ which is also denoted by $\circlearrowright$. As we mentioned before, $\circlearrowright$ is an involutive anti-automorphism on $G_1$. The Frattini subgroup $\Psi(G_1)$ of the derived subgroup of $G_1$ is also $\circlearrowright$-invariant in $G_1$ and $G_1 = G_1/\Phi(G_1')$ has an involutive anti-automorphism induced by $\circlearrowright$. Then $G_1$ is a group of nilpotency class two and $\overline{G_1}$ is an elementary abelian $p$-group. Let $\circlearrowright$ denote the induced anti-automorphism on $\overline{G}$. If $\overline{G}_S \neq \overline{G}$, then there exists a $g \in \overline{G}$ such that $(g, g^*) \neq 1$. Then $H = \langle g, g^* \rangle$ is a $\circlearrowright$-invariant subgroup and $|H'| = p$. According to Lemma 6,

$$\text{dl}(\overline{FG}_S) \geq \text{dl}(\overline{FH}^+_* \rangle \geq \lceil \log_2 (p + 1) \rceil.$$  

Suppose that $\overline{G}_S = \overline{G}$. Then Lemma 5 asserts that

$$\text{dl}(\overline{FG}_S^+) \geq \lceil \log_2 (p + 1) \rceil.$$  

Let $\psi$ be the natural homomorphism of $G$ onto $\overline{G}$. Then the mapping $\psi : FG \rightarrow \overline{FG}$ given by

$$\psi \left( \sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} \alpha_g \psi(g),$$  

where $\alpha_g \in F$ is a homomorphism.

Clearly, elements of $FG^+_S$ can be written in the form $\sum_{g \in G} \alpha_g(g + g^*)$, where $\alpha_g \in F$. Since $\psi(g + g^*) = \overline{g} + \overline{g}$ for all $g \in G$ and the Lie operator is $F$-linear we get that $\text{dl}(FG^+_S) \geq \text{dl}(FG^+_S\overline{\psi})$.

Finally, assume that the set of $p$-elements forms a finite non-abelian $P$ subgroup in $G$. Then $P$ is a characteristic subgroup and the inequality $\text{dl}(FG^+_S) \geq \text{dl}(FP^+_S) \geq \lceil \log_2 (p + 1) \rceil$ completes the proof. \hfill $\square$

**Acknowledgements**

The author would like to thank the referee for the valuable comments and suggestions for clarifying the exposition.

This research was supported by REA-NIH-OTKA-EU FP7 (Marie Curie action) co-funded grant No. MB08A-82343. This paper was written while the author was visiting the University College Dublin. He would like to gratefully acknowledge the kind hospitality from the host institution. The author thanks Thomas Unger for a careful reading of an earlier draft.

**References**


