Degrees of Irreducible Characters of the Suzuki 2-Groups

I. A. Sagirov

ABSTRACT. The degrees of the irreducible characters of the Suzuki 2-groups $A(m, \theta)$ are described. Assume that the order of an automorphism $\theta$ of the field $GF(2^m)$ is $k > 1$, $G = A(m, \theta)$, and $cd(G)$ is the set of degrees of the irreducible characters of $G$. If $k$ is odd, then $cd(G) = \{1, 2^{(m-n)/2}\}$, and if $k = 2$, then $cd(G) = \{1, 2^{m/2}\}$. If $k$ is even and $k \neq 2$, then $cd(G) = \{1, 2^{m/2}, 2^{m/2-n}k\}$, and the group $G$ has $(2^m - 1)2^{m/k}/(2^{m/k} + 1)$ characters of degree $2^{m/2}$ and $(2^m - 1)2^{m/k}/(2^{m/k} + 1)$ characters of degree $2^{m/2-n}$.

KEY WORDS: Suzuki 2-group, irreducible character, degree of a group character, nonprincipal character, Frattini subgroup, extraspecial group, semi-Abelian group.

§1. Introduction

Let $G$ be a group, let $Irr(G)$ be the set of all its irreducible characters, let $Irr_1(G)$ be the set of all its nonlinear irreducible characters, let $cd(G)$ be the set of degrees of the irreducible characters, let $Cl(G)$ be the set of conjugacy classes of $G$, and let $k(G) = |Cl(G)|$.

The Suzuki 2-groups were first introduced by Higman, and they are studied in detail in [1, Chap. VIII]. Let us recall their definition. Consider a finite field $GF(q)$, where $q = 2^m$ and $m > 1$, and an automorphism $\theta$ of this field of order $k$ for some divisor $k > 1$ of $m$. Write $n = m/k$. The Suzuki 2-group $A(m, \theta)$ is defined as the set of ordered pairs of elements of $GF(q)$ with the operation $(a, b)(c, d) = (a + c, b + d + c\theta(a))$ for any $a, b, c, d \in GF(q)$. In the present paper, the description of the degrees of the irreducible characters of the groups $A(m, \theta)$ is obtained. Namely, the following assertion holds.

Theorem. If $G = A(m, \theta)$ is the Suzuki 2-group of order $q^2$, where $m > 1$ is an integer, $q = 2^m$, and $\theta$ is an automorphism of the field $GF(q)$ of order $k > 1$ ($m/k = n$), then one of the following assertions holds:

1) if $k$ is odd, then $cd(G) = \{1, 2^{(m-n)/2}\}$,
2) if $k = 2$, then $cd(G) = \{1, 2^{m/2}\}$,
3) if $k$ is even and $k \neq 2$, then $cd(G) = \{1, 2^{m/2}, 2^{m/2-n}\}$, and $G$ has $(2^m - 1)2^n/(2^n + 1)$ characters of degree $2^{m/2}$ and $(2^m - 1)2^{m/2}/(2^n + 1)$ characters of degree $2^{m/2-n}$.

For the case in which the order of the automorphism $\theta$ is odd, the corresponding result is known [2]. However, for the completeness of our exposition, we include a proof of this fact.

§2. Auxiliary results

Everywhere below we assume that $G$ is the Suzuki 2-group $A(m, \theta)$, $\theta$ is an automorphism of order $k$ of the field $GF(q)$, $q = 2^m$, and $m/k = n$.

Lemma 2.1. $|G'| \geq 2^{m-n}$.

Proof. The commutator relation $[(a, b), (c, d)] = (0, a\theta(c) + c\theta(a))$ holds for arbitrary $a, b, c, d \in GF(q)$. If $c = 1$, then $[(a, b), (1, d)] = (0, a + \theta(a))$, and the number of distinct commutators of this form is $2^m/u$, where $u = |\{a \in GF(q) \mid a = \theta(a)\}|$. Therefore, $u$ is the number of fixed points of the automorphism $\theta$, and hence $u = 2^n$. Thus, $|G'| \geq 2^{m-n}$. □

Lemma 2.2. The number of conjugacy classes of the group $G$ is $2^{m+n} + 2^m - 2^n$. 
Proof. Obviously, \( Z(G) = \{(0, b) \mid b \in GF(q)\} \) and \( |Z(G)| = 2^m \). For an arbitrary element \((a, b) \in G, a \neq 0\), the relation \((c, d) \in C_G(a, b)\) holds if and only if \([[(a, b), (c, d)] = 1\), i.e., we have \(a \theta(c) + c \theta(a) = 0\). The latter means that \(ca^{-1} = \theta(ca^{-1})\). Since the set of fixed points of \( \theta \) is isomorphic to \( GF(2^n) \), it follows that \( |C_G(a, b)| = 2^{m+n} \), and hence the conjugacy class of an arbitrary element of \( G \setminus Z(G) \) contains \(2^{m-n}\) elements. Let \( r \) be the number of noncentral \( G \)-classes. Then \( r 2^{m-n} + 2^m = |G| \). This yields \( r = 2^{m+n} - 2^m \) and \( k(G) = 2^{m+n} + 2^m - 2^m \). □

Lemma 2.3. The mapping \( \varphi_\lambda(a, b) = (\lambda a, \lambda \theta(\lambda)b) \), where \( \lambda \in GF(q)^* \), is an automorphism of the group \( G \).

Proof. We write \( \mu = \lambda \theta(\lambda) \). Then

\[
\varphi_\lambda(a, b) = (\lambda a, \mu b), \quad \varphi_\lambda(c, d) = (\lambda c, \mu d), \quad \varphi_\lambda((a, b)(c, d)) = \varphi_\lambda(a + c, b + d + \mu c \theta(\lambda)a) = (\lambda(a + c), \mu(b + d + \mu c \theta(\lambda)a)).
\]

On the other hand,

\[
\varphi_\lambda(a, b)\varphi_\lambda(c, d) = (\lambda a, \mu b)(\lambda c, \mu d) = (\lambda a + \lambda c, \mu b + \mu d + \mu c \theta(\lambda)a) = (\lambda(a + c), \mu(b + d + \mu c \theta(\lambda)a)) = \varphi_\lambda((a, b)(c, d)).
\]

Therefore, \( \varphi_\lambda \) is an endomorphism of the group \( G \), and \( \varphi_\lambda(a, b) = (0, 0) \) only if \((a, b) = (0, 0)\), which means that \( \varphi_\lambda \) is an automorphism. □

Since \( \theta \) is an automorphism of the field \( GF(q) \) of order \( k \), it follows that for any \( x \in GF(q) \) we have \( \theta(x) = x^{2^nt} \) for some \( t \), \((t, k) = 1\). Let us fix this number \( t \).

Lemma 2.4. If \( m = nk \) is a product of two positive integers and if \((t, k) = 1\) for the above number \( t \), then

\[
(2^m - 1, 2^nt + 1) = \begin{cases} 1 & \text{for odd } k, \\ 2^n + 1 & \text{for even } k. \end{cases}
\]

Proof. As is known, \((p^m - 1, p^n - 1) = p^{(m, n)} - 1\) for any \(m, n \in \mathbb{N}\) and any prime \(p\). Therefore,

\[
(2^m - 1, 2^nt - 1) = \begin{cases} 2^n - 1 & \text{for odd } k, \\ 2^n - 1 & \text{for even } k. \end{cases}
\]

Obviously, \((2^m - 1, 2^nt + 1) | (2^m - 1, 2^nt - 1)\).

Note that \((2^nt + 1, 2^m - 1) = 1\). Indeed, if \(p | (2^nt + 1, 2^m - 1)\) and \(p\) is a prime, then \(2^m \equiv 1 \pmod{p}\), and thus \(2^nt \equiv 1^t \pmod{p}\). We have arrived at a contradiction because \(2^nt \equiv 1 \pmod{p}\). Therefore, \((2^m - 1, 2^nt + 1) = 1\) for odd \(k\). Since \(2^m - 1 = (2^m - 1)(2^nt + 1), (2^nt + 1, 2^m - 1) = 1,\) and \(2^m + 1 | 2^nt + 1\), it follows that \((2^m - 1, 2^nt + 1) = 2^n + 1\) for even \(k\). □

Lemma 2.5. Let \( \lambda \) be a primitive element of the field \( GF(q) \). The length of the orbit of \( \varphi_\lambda \) on \( G \setminus Z(G) \) is equal to \( 2^m - 1 \). The length of the orbit of \( \varphi_\lambda \) on \( Z(G)^\# \) is equal to \( 2^m - 1 \) for odd \( k \) and to \((2^m - 1)/(2^nt + 1)\) for even \( k \).

Proof. For any \((a, b) \in G \) we have \( \varphi^i_\lambda(a, b) = (\lambda^i, (\lambda \theta(\lambda))^ib) \). Let \( a \neq 0 \). In this case, \( \varphi^i_\lambda(a, b) = (a, b) \) if and only if \((\lambda^i - 1)a = 0\), which is impossible for \(0 < i < 2^m - 1\).

Let \( a = 0 \). In this case, \( \varphi^i_\lambda(0, b) = (0, (\lambda \theta(\lambda))^ib) = (0, b) \) only if \((\lambda \theta(\lambda))^i = 1\). This holds for \(\lambda(2^m + 1)i = 1\) because \(\theta(\lambda) = \lambda 2^nt\). By Lemma 2.4, for odd \(k\) this yields \(2^m - 1 | i\), and all elements of \(Z(G)^\#\) are conjugate under the action of \(\varphi_\lambda\). We have \((2^m - 1)/(2^nt + 1) | i\) for even \(k\), and the length of the \(\varphi_\lambda\)-orbit of the element \((0, b)\) is equal to \((2^m - 1)/(2^nt + 1)\). □

Corollary. If \(k > 1\) is odd, then \(G' = Z(G)\).