Bull. Korean Math. Soc. **50** (2013), No. 2, pp. 697–704
http://dx.doi.org/10.4134/BKMS.2013.50.2.697

ON THE SOLUTIONS OF $x^k = g$ IN A FINITE GROUP

Sunil Kumar Prajapati and Ritumoni Sarma

Abstract. The function $g \mapsto \zeta_G^k(g)$ which counts the number of solutions of $x^k = g$ in a finite group G, is not necessarily a character of G. We study this function for the case of dihedral groups and generalized quaternion groups.

1. Introduction

Let $\mathfrak{F}_n$ be the free group on n generators $x_1, x_2, \ldots, x_n$. Suppose that $w(x_1, x_2, \ldots, x_n) \in \mathfrak{F}_n$. For a finite group G, define $\zeta_G^w : G \longrightarrow \mathbb{Z}$ by

$$\zeta_G^w(g) := |\{(g_1, g_2, \ldots, g_n) \in G^n : w(g_1, g_2, \ldots, g_n) = g\}|. \tag{1}$$

We prefer to write ζ_G^k instead of ζ_G^w if $n = 1$ and $w(x) = x^k$.

In [1], it was proved that ζ_G^k is a generalized character (i.e., a $\mathbb{Z}$-linear combination of irreducible characters). It is easy to prove that ζ_G^k is actually a character if G is an abelian group. In fact, for an abelian group G, the function ζ_G^w is always a character for any $w(x_1, x_2, \ldots, x_n) \in \mathfrak{F}_n$. In general, for a non-abelian group, this function need not be a character. For example, if Q_8 is the quaternion group, then $\zeta_{Q_8}^2$ is not a character. In this article, we prove that ζ_G^k is a character for finite dihedral groups and generalized quaternion groups except when $k \equiv 2 \pmod 4$ in the case of generalized quaternion groups.

In [4], it is shown that if $w(x_1, x_2, \ldots, x_n) = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, the function ζ_G^w is a generalized character for any finite group G. Here, Theorem 2.7 provides a sufficient condition for that ζ_G^w to be a character.

Throughout the article, G denotes a finite group and $\mathrm{Irr}(G)$, the set of its irreducible characters. For any class functions f and g, the expression $\langle f, g \rangle$ denotes their standard inner product. We record an elementary trigonometric

Received January 26, 2012; Revised March 30, 2012.
2010 *Mathematics Subject Classification.* 20C15.
Key words and phrases. finite groups, group characters.
The first author was supported by Council of Scientific and Industrial Research (CSIR), India.

identity for future use.

$$1+\sum_{1\le j\le n} 2\cos(jx) = \frac{\sin((n+\frac{1}{2})x)}{\sin(\frac{1}{2}x)}. \tag{2}$$

2. Main result

Let λ be a generalized character of G. For $k \in \mathbb{N}$, define functions $\lambda_{(k)}$ and $\lambda^{(k)}$ from G to $\mathbb{C}$ by

$$\lambda_{(k)}(g) := \sum_{z\in G,\ z^k=g} \lambda(z), \tag{3}$$

$$\lambda^{(k)}(g) := \lambda(g^k). \tag{4}$$

In [1], it is proved that both $\lambda_{(k)}$ and $\lambda^{(k)}$ are generalized characters of G. The following proposition gives a necessary and sufficient condition for ζ_G^k to be a character of G.

Proposition 2.1. *The function ζ_G^k is a character if and only if*

$$c_\chi^{(k)} := \frac{1}{|G|}\sum_{g\in G}\chi(g^k) \tag{5}$$

is a non-negative integer for every $\chi \in \mathrm{Irr}(G)$.

Proof. If 1 denotes the trivial irreducible character of a group G, then by definition

$$1_{(k)} = \zeta_G^k. \tag{6}$$

On the other hand, for any two generalized characters λ and χ of G, we have

$$\begin{aligned}\langle \lambda_{(k)}, \chi\rangle &= \frac{1}{|G|}\sum_{g\in G}\sum_{z\in G,\ z^k=g}\lambda(z)\ \chi(g^{-1})\\ &= \frac{1}{|G|}\sum_{z\in G}\lambda(z)\ \chi^{(k)}(z^{-1})\\ &= \langle \lambda, \chi^{(k)}\rangle.\end{aligned}$$

In particular, if $\lambda = 1$ and $\chi \in \mathrm{Irr}(G)$, we get by (6)

$$\langle \zeta_G^k, \chi\rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g^k).$$

Hence, the proposition follows. □

Now we study ζ_G^k when G is the dihedral group D_{2n} of order $2n$ with $n \ge 3$. We consider the following presentation: $D_{2n} = \langle a, b \mid a^n = 1, b^2 = 1, bab^{-1} = a^{-1}\rangle$. Then its character table is as follows:

Table(a): when $n = 2m + 1$

g	1	$a^r (1 \leq r \leq m)$	b
$\lvert C_G(g)\rvert$	$2n$	n	2
χ_1	1	1	1
χ_2	1	1	-1
ϕ_j $(1 \leq j \leq m)$	2	$2\cos(\frac{2\pi jr}{n})$	0

Table(b): when $n = 2m$

g	1	a^m	$a^r (1 \leq r \leq (m-1))$	b	ab
$\lvert C_G(g)\rvert$	$2n$	$2n$	n	4	4
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	$(-1)^m$	$(-1)^r$	1	-1
χ_4	1	$(-1)^m$	$(-1)^r$	-1	1
ϕ_j $(1 \leq j \leq (m-1))$	2	$2(-1)^j$	$2\cos(\frac{2\pi jr}{n})$	0	0

Lemma 2.2. *Let $n \geq 3$. Suppose that χ is a nonlinear irreducible character of D_{2n}. With the notation in the preceding paragraph, for every $k \in \mathbb{N}$, we have*

$$\sum_{1 \leq r \leq n} \chi(a^{rk}) = \begin{cases} 2n & \text{if } n \mid k, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $n \mid k$, then for any nonlinear irreducible character $\chi = \phi_j$ (see Table(a) and Table(b)) of D_{2n}, we have

$$\sum_{1 \leq r \leq n} \phi_j(a^{rk}) = \sum_{1 \leq r \leq n} \phi_j(1) = 2n.$$

Next assume that $n \nmid k$. Let $d := \gcd(n, k)$ and $\chi = \phi_j$. Then

$$\sum_{1 \leq r \leq n} \phi_j(a^{rk}) = \sum_{1 \leq r \leq \frac{n}{d}} d \cdot \phi_j(a^{rd}). \tag{7}$$

If $n = 2m + 1$, then (7) becomes

$$\begin{aligned} d \cdot \phi_j(1) + \sum_{1 \leq r \leq (\frac{n}{d}-1)/2} 2d \cdot \phi_j(a^{rd}) &= 2d + 2d \sum_{1 \leq r \leq (\frac{n}{d}-1)/2} 2\cos(r\frac{2\pi jd}{n}) \\ &= 2d + 2d \cdot (-1) \text{ (by using (2))} \\ &= 0. \end{aligned}$$

Next, suppose that $n = 2m$. If n/d is odd, then $rd \neq m$ for $1 \leq r \leq (\frac{n}{d} - 1)/2$. Thus, the computation of (7), is exactly like that of the case $n = 2m + 1$. Finally, if n/d is even, (7) reduces to

$$d \cdot \phi_j(1) + d \cdot \phi_j(a^m) + \sum_{1 \leq r \leq (\frac{n}{d}-2)/2} 2d \cdot \phi_j(a^{rd})$$

$$
\begin{aligned}
&= 2d + 2d\cdot(-1)^j + 2d \sum_{1\le r\le(\frac{n}{d}-1)/2} 2\cos(r\frac{2\pi jd}{n})\\
&= 2d + 2d\cdot(-1)^j + 2d\cdot\{(-1)^{j-1}-1\} \text{ (by using (2))}\\
&= 0.
\end{aligned}
$$

This completes the proof of the lemma. □

Theorem 2.3. *For every $k, n \in \mathbb{N}$, the function $\zeta^k_{D_{2n}}$ is a character.*

Proof. If $n \le 2$, D_{2n} is an abelian group and hence $\zeta^k_{D_{2n}}$ is a character for any $k \in \mathbb{N}$. Now for $n \ge 3$, by Proposition 2.1, it is sufficient to show that $c^{(k)}_\chi \ge 0$ for each $\chi \in \mathrm{Irr}(D_{2n})$.

First we deal with the nonlinear characters ϕ_j (see Table(a) and Table(b)). Case ($n = 2m+1$): by Lemma 2.2,

$$
c^{(k)}_{\phi_j} = \frac{1}{|D_{2n}|}\sum_{g\in D_{2n}} \phi_j(g^k) = \begin{cases} 1+\alpha_j(a,k) & \text{if } n \mid k,\\ \alpha_j(a,k) & \text{otherwise,}\end{cases} \tag{8}
$$

where $\alpha_j(a,k) = \frac{1}{2n}\{|Cl_{D_{2n}}(b)|\cdot\phi_j(b^k)\}$. If k is even, $b^k = 1$. Then, we have

$$
\alpha_j(a,k) = \frac{1}{2n}\{n\cdot\phi_j(1)\} = 1.
$$

If k is odd, $b^k = b$. Then, $\alpha_j(a,k) = 0$. Hence in either cases, by (8), $c^{(k)}_{\phi_j}$ is a positive integer.

Case ($n = 2m$): by Lemma 2.2,

$$
c^{(k)}_{\phi_j} = \frac{1}{|D_{2n}|}\sum_{g\in D_{2n}} \phi_j(g^k) = \begin{cases} 1+\beta_j(b,k) & \text{if } n \mid k,\\ \beta_j(b,k) & \text{otherwise,}\end{cases} \tag{9}
$$

where $\beta_j(b,k) = \frac{1}{2n}\{|Cl_{D_{2n}}(b)|\cdot\phi_j(b^k) + |Cl_{D_{2n}}(ab)|\cdot\phi_j((ab)^k)\}$. If k is even, $b^k = (ab)^k = 1$. Therefore, we have

$$
\beta_j(b,k) = \frac{1}{2n}\{m\cdot\phi_j(1) + m\cdot\phi_j(1)\} = 1.
$$

If k is odd, $b^k = b$ and $(ab)^k = ab$. Then, $\beta_j(b,k) = 0$. Hence in both cases, by (9), $c^{(k)}_{\phi_j}$ is a positive integer.

Finally, for a linear character χ, it is not difficult to show that $c^{(k)}_\chi$ is either zero or one. Indeed, if $n = 2m+1$, $c^{(k)}_{\chi_1} = 1$ and $c^{(k)}_{\chi_2} = 1$ or 0 depending upon whether k is even or odd. Similarly, if $n = 2m$, then $c^{(k)}_{\chi_1} = 1$, $c^{(k)}_{\chi_i} = 1$ or 0 according as k is even or odd for each $i = 2, 3, 4$. This completes the proof. □

Next we study ζ^k_G when G is the generalized quaternion group Q_{2n} of order $4n$ with $n \ge 2$. We consider the following presentation: $Q_{2n} = \langle a, b : a^{2n} = 1, a^n = b^2, bab^{-1} = a^{-1}\rangle$. When n is odd, the character table of Q_{2n} is given by Table(c). When n is even, the character table of Q_{2n} is obtained from Table(c) by replacing i by 1.

Table(c)

g	1	a^n	$a^r (1 \le r \le (n-1))$	b	ab
$\lvert C_G(g)\rvert$	$4n$	$4n$	$2n$	4	4
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	$(-1)^n$	$(-1)^r$	i	$-i$
χ_4	1	$(-1)^n$	$(-1)^r$	$-i$	i
$\phi_j\ (1 \le j \le (n-1))$	2	$2(-1)^j$	$2\cos(\frac{\pi j r}{n})$	0	0

Lemma 2.4. *Let $n \ge 3$. Suppose that χ is a nonlinear irreducible character of Q_{2n}. With the notation in the preceding paragraph, for every $k \in \mathbb{N}$ we have*

$$\sum_{1 \le r \le 2n} \chi(a^{rk}) = \begin{cases} 4n & \text{if } 2n \mid k, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $2n \,|\, k$, then for any nonlinear irreducible character $\chi = \phi_j$ (see Table(c)) of Q_{2n}, we have

$$\sum_{1 \le r \le 2n} \phi_j(a^{rk}) = \sum_{1 \le r \le 2n} \phi_j(1) = 4n.$$

Next assume that $2n \nmid k$. Let $d := \gcd(2n, k)$ and $\chi = \phi_j$. If $2n/d$ is odd, then

$$\begin{aligned} \sum_{1 \le r \le 2n} \phi_j(a^{rk}) &= d \cdot \phi_j(1) + \sum_{1 \le r \le (\frac{2n}{d}-1)/2} 2d \cdot \phi_j(a^{rd}) \\ &= 2d + 2d \sum_{1 \le r \le (\frac{2n}{d}-1)/2} 2\cos(r\frac{dj\pi}{n}) \\ &= 2d + 2d(-1) \text{ (by using (2))} \\ &= 0. \end{aligned}$$

If $2n/d$ is even, then

$$\begin{aligned} \sum_{1 \le r \le 2n} \phi_j(a^{rk}) &= d \cdot \phi_j(1) + \sum_{1 \le r \le (\frac{2n}{d}-2)/2} 2d \cdot \phi_j(a^{rd}) + d\phi_j(a^n) \\ &= 2d + 2d \sum_{1 \le r \le (\frac{2n}{d}-2)/2} 2\cos(r\frac{dj\pi}{n}) + 2d(-1)^j \\ &= 2d + 2d\{(-1)^{j-1} - 1\} + 2d(-1)^j \text{ (by using (2))} \\ &= 0. \end{aligned}$$

This completes the proof of the lemma. □

Theorem 2.5. *For every $n \in \mathbb{N}$, the function $\zeta^k_{Q_{2n}}$ is a character for $k \equiv 0, 1$ or 3 (mod 4). When $k \equiv 2 \pmod 4$, $\zeta^k_{Q_{2n}}$ is a character if and only if $2n \mid k$.*

Proof. We compute $c_\chi^{(k)}$ for each $\chi \in \mathrm{Irr}(Q_{2n})$. First consider the nonlinear irreducible characters ϕ_j $(1 \le j < n)$ (see Table(c)). By Lemma 2.4, we have

$$c_{\phi_j}^{(k)} = \begin{cases} 1 + \alpha_j(b,k) & \text{if } 2n \mid k, \\ \alpha_j(b,k) & \text{otherwise,} \end{cases} \tag{10}$$

where $\alpha_j(b,k) = \frac{1}{4n}\{|Cl_{Q_{2n}}(b)| \cdot \phi_j(b^k) + |Cl_{Q_{2n}}(ab)| \cdot \phi_j((ab)^k)\}$. We perform the computation in four exhaustive cases.

Case $k \equiv 2 \pmod 4$: Then $b^k = (ab)^k = a^n$. Therefore,

$$\begin{aligned} \alpha_j(b,k) &= \frac{1}{4n}\{n \cdot \phi_j(a^n) + n \cdot \phi_j(a^n)\} \\ &= (-1)^j. \end{aligned}$$

Hence $c_{\phi_1}^{(k)} = -1$, under the condition $k \equiv 2 \pmod 4$ and $2n \nmid k$.

Case $k \equiv 0 \pmod 4$: Then $b^k = (ab)^k = 1$. Therefore,

$$\begin{aligned} \alpha_j(b,k) &= \frac{1}{4n}\{n \cdot \phi_j(1) + n \cdot \phi_j(1))\} \\ &= 1. \end{aligned}$$

Case $k \equiv 1 \pmod 4$: Then $b^k = b$, $(ab)^k = ab$. Therefore, we have

$$\begin{aligned} \alpha_j(b,k) &= \frac{1}{4n}\{n \cdot \phi_j(b) + n \cdot \phi_j(ab)\} \\ &= 0. \end{aligned}$$

Case $k \equiv 3 \pmod 4$: Then $b^k = a^n b$ and $(ab)^k = a^{n+1}b$. Therefore they are conjugate to either b or ab. Hence $\alpha_j(b,k) = 0$.

Hence by (10), $c_{\phi_j}^{(k)} \ge 0$ for all nonlinear irreducible character of Q_{2n} except the case when $k \equiv 2 \pmod 4$ and $2n \nmid k$.

Finally, for the linear characters of Q_{2n} we have $c_{\chi_1}^{(k)} = 1$; $c_{\chi_2}^{(k)} = 1$ or 0 according as k is even or odd and $c_{\chi_3}^{(k)} = c_{\chi_4}^{(k)} = 0$ or 1 according as $(k-1)(n-1)$ is even or odd.

Thus, when $k \not\equiv 2 \pmod 4$ or $2n \mid k$, $c_\chi^{(k)} \ge 0$ for each $\chi \in \mathrm{Irr}(Q_{2n})$. Hence, the theorem follows from Proposition 2.1. □

We have the following theorem for the symmetric group S_n of degree n.

Theorem 2.6. *For every $n \ge 1$, the function $\zeta_{S_n}^2$ is a character.*

Proof. By Proposition 2.1, it is sufficient to show that $c_\chi^{(2)}$ is a non-negative integer. Since every irreducible character of S_n is defined over the real field [2, theorem 75.19], the theorem follows from [3, Corollary 4.15]. □

Theorem 2.7. *Let S be a nonempty subset of $\mathbb{Z}$. Suppose that ζ_G^k is a character of G for every $k \in S$. If $k_1, k_2, \ldots, k_n \in S$, then ζ_G^w is a character of G for $w(x_1, x_2, \ldots, x_n) = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$.*

Table(d)

g	1	(12)	(12)(34)	(123)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	3	1	-1	0	-1
χ_4	3	-1	-1	0	1
χ_5	2	0	2	-1	0

Proof. The proof is by induction on n. By assumption, the statement holds for $n = 1$. Suppose that $n \geq 2$. Let $u(x_1, x_2, \dots, x_{n-1}) = x_1^{k_1} x_2^{k_2} \cdots x_{n-1}^{k_{n-1}}$. Then $w = u \cdot x_n^{k_n}$. By assumption, $\zeta_G^{k_n}$ is a character and by the induction hypothesis, ζ_G^u is a character. Therefore, we may assume that for some $\alpha_\chi, \beta_\chi \in \mathbb{N} \cup \{0\}$,

$$\zeta_G^{k_n} = \sum_{\chi \in \mathrm{Irr}(G)} \alpha_\chi \chi, \ \zeta_G^u = \sum_{\chi \in \mathrm{Irr}(G)} \beta_\chi \chi. \tag{11}$$

Then we have,

$$\begin{aligned}
\zeta_G^w(g) &= \sum_{x_1, x_2, \dots, x_{n-1} \in G} \zeta_G^{k_n}((x_1^{k_1} \cdots x_{n-2}^{k_{n-2}} x_{n-1}^{k_{n-1}})^{-1} g) \\
&= \sum_{t \in G} \zeta_G^{k_n}(t^{-1}g) \zeta_G^u(t) \\
&= \sum_{\chi, \psi \in \mathrm{Irr}(G)} \alpha_\chi \beta_\psi \sum_{t \in G} \chi(t^{-1}g)\psi(t) \ \text{(using (11))} \\
&= \sum_{\chi \in \mathrm{Irr}(G)} \alpha_\chi \beta_\chi \frac{|G|}{\chi(1)} \chi(g) \ \text{(by orthogonality relation [3, Theorem 2.13]).}
\end{aligned}$$

Since the coefficient of χ in ζ_G^w is non-negative for each $\chi \in \mathrm{Irr}(G)$, the function ζ_G^w is a character. □

Corollary 2.8. *Suppose that $w(x_1, x_2, \dots, x_n) = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$. Then*

(1) *The function $\zeta_{D_{2n}}^w$ is a character.*
(2) *The function $\zeta_{Q_{2n}}^w$ is a character if $k_i \equiv 0, 1$ or $3 \pmod 4$ for each i.*

Remark 2.9. If the hypothesis of Theorem 2.7 is weakened by allowing repetition of letters in w, then the conclusion is no more valid. For example, if $S = \{\pm 1, \pm 2\}$ and $w(x, y, z) = x^2 y z x^{-1} z^{-1} y^{-1}$, the function $\zeta_{S_4}^w$ is not a character (although $\zeta_{S_4}^{\pm 1}, \zeta_{S_4}^{\pm 2}$ are characters). In fact,

$$\zeta_{S_4}^w = 1152\,\chi_1 + 0\,\chi_2 + 192\,\chi_3 - 192\,\chi_4 + 288\,\chi_5,$$

where $\chi_1, \chi_2, \chi_3, \chi_4$ and χ_5 are the irreducible characters of S_4 defined in Table(d).

References

[1] R. M. Bryant and L. G. Kovács, *A note on generalized characters*, Bull. Aust. Math. Soc. **5** (1971), no. 2, 265–269.

[2] C. W. Charles and I. Reiner, *Methods of Representation Theory. Vol. II*, With applications to finite groups and orders, John Wiley & Sons Inc., New York, 1987.

[3] I. M. Isaacs, *Character Theory of Finite Groups*, AMS Chelsea Publishing, Academic Press, New York, 2000.

[4] A. Kerber and B. Wagner, *Gleichungen in endlichen Gruppen*, Arch. Math. (Basel) **35** (1980), no. 3, 252–262.

Sunil Kumar Prajapati
Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas, New Delhi-110016, India
E-mail address: skprajapati.iitd@gmail.com

Ritumoni Sarma
Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas, New Delhi-110016, India
E-mail address: ritumoni@maths.iitd.ac.in