FINITE GROUPS HAVING EXACTLY ONE NON-LINEAR IRREDUCIBLE CHARACTER

KAORU MOTOSE

Recently, A.S. Muktibodh [12, 11, 10] considered a 2-Con-Cos group $G$ defined as follows: the commutator subgroup $G'$ of a finite group $G$ consist of two conjugate classes $C_a$ and $C_1 = \{1\}$, and cosets $G'x$ are conjugate classes $C_x$ of $x \in G \setminus G'$. In this paper, we replace ”2-Con-Cos” by ”concos”.

These groups are just groups having exactly one non-linear irreducible character because the number of irreducible characters is equal to the number of conjugate classes, $G' \neq \{1\}$ contains at least two conjugate classes and a coset $G'x$ of $G'$ contains at least one conjugate class $C_x$.

In §1, we shall prove these groups are isomorphic to affine groups over finite fields or central products of some dihedral groups $D$ of order 8 and quaternion groups $Q$, and conversely.

After my talk, Professor Y. Ninomiya informed me that this characterization was known in some papers [14, 13, 2]. Further the paper [2] stated that more general information was considered in [8]. However I have arranged this characterization for some reasons that our proof is slight different from others, rather self contained and necessary for §2 and §3.

In §2, we determine $\mathbb{C}$-irreducible $\mathbb{R}$-representations of concos groups.

In §3, we shall show concos groups appear in the proof of Hurwitz theorem concerning quadratic forms. We also determine $\mathbb{C}$-irreducible $\mathbb{R}$-representations of slight different groups in the proof of this theorem.

All representations and characters are considered over $\mathbb{C}$.

1. Characterization of concos groups

First we show elementary properties of concos groups from the definition.

**Lemma 1.** Let $G$ be concos. Then we have

1. If $N$ is a normal subgroup of $G$ then $N = \{1\}$ or $N \supset G'$.
2. $G'$ is an elementary abelian $p$-group.
3. Exactly one non-linear irreducible character $\eta$ of $G$ has the next values and we can see from these values that $\eta$ is faithful.

$$
\eta(1)^2 = \frac{|G|}{|G'|}(|G'| - 1), \quad \eta(x) = -\frac{|G'/G'|}{\eta(1)} \text{ for } x \in G' \setminus \{1\},
$$

and $\eta(x) = 0$ for $x \in G \setminus G'$.

---

The detailed version of this paper will be submitted for publication elsewhere.
Proof. (1) If $N$ contains $b \neq 1$, then $N$ contains $C_b$. In case $b \in G'$, $N \supset C_b = C_a$ and so $N \supset G'$. In case $b \not\in G'$, $N \supset C_b = G'\langle b \rangle$ and so $N = Nb^{-1} \supset G'$.

(2) $G'$ is a $p$-group because $G' = \{1\} \cup C_a$ and $G'$ contains an element of prime order $p$. Thus $G''$ is a normal subgroup of $G$ properly contained in a $p$-group $G'$ and so $G'' = 1$ from (1).

(3) Let $\rho_G$ and $\rho_{G/G'}$ are regular characters of $G$ and $G/G'$, respectively. Then we have

$$\rho_G = \rho_{G/G'} + \eta(1)\eta.$$

Using this we obtain our assertion.

The next theorem follows from Lemma 1 (1) and (2).

**Theorem 2** ([14, 13, 2, 12]). Let $G$ be concos. Then we have the next groups and conversely.

1. $G$ is the central product $QD^{-1}$ or $D^*$ where $D$ is the dihedral group of order 8 and $Q$ is the quaternion group of order 8.

2. $G$ is the next permutation group over a finite field $\mathbb{F}_q$ of order $q > 2$.

$$G = \{x \rightarrow ax + \beta \mid \alpha \in \mathbb{F}_q^* \text{ and } \beta \in \mathbb{F}_q\}.$$

2. **Real representations of concos groups**

Let $\Psi$ be a $C$-irreducible representation of a finite group $G$ and let $\chi$ be a character afforded by $\Psi$. We set

$$\nu(\chi) = \frac{1}{|G|} \sum_{x \in G} \chi(x^2).$$

If $\chi$ is linear, then $\nu(\chi) = (\chi, \bar{\chi})$, where $(\chi, \bar{\chi})$ is the inner product of $\chi$ and $\bar{\chi}$ is the complex conjugate of $\chi$. Thus it is easy to see that $\nu(\chi) = 1, 0$ and also that (1) $\nu(\chi) = 1$ if and only if $\chi = \bar{\chi}$ and (2) $\nu(\chi) = 0$ if and only if $\chi \neq \bar{\chi}$.

Frobenius and Schur proved in [4] (see [3]) that $\nu(\chi) = 1, 0, -1$ and

(1) $\nu(\chi) = 1$ if and only if $\Psi$ is equivalent to an $\mathbb{R}$-representation.

(2) $\nu(\chi) = 0$ if and only if $\chi \neq \bar{\chi}$.

(3) $\nu(\chi) = -1$ if and only if $\chi = \bar{\chi}$ but $\Psi$ is not equivalent to an $\mathbb{R}$-representation.

Let $d$ be a fixed element of a finite group $G$ and let $s_d$ be the number of elements $x \in G$ such that $x^2 = d$. There is the formula [3, p. 22 (3.6)] about $s_d$ as follows:

$$s_d = \sum_{\lambda \in \Lambda} \nu(\lambda)\lambda(d)$$

where $\Lambda$ is the set of irreducible characters of $G$.

The next lemma is useful on $C$-irreducible $\mathbb{R}$-representations of concos groups.

**Lemma 3.** Let $G$ be a concos group, $G' = \{1\} \cup C_a$ and let $\eta$ be exactly one non-linear irreducible character. Then we have

$$s_1 - s_{\eta} = \frac{|G|}{\eta(1)} \nu(\eta).$$
In the next proposition we can see \( \mathbb{C} \)-irreducible \( \mathbb{R} \)-representations of concs 2-groups. We also can see the numbers of elements of orders 4, 2 in these groups. Our counting method is different from [5, pp. 205-207]. Therefore this gives a different proof about that \( D^r \) and \( QD^{r-1} \) are not isomorphic (see Remark. (2)).

**Proposition 4.** Let \( G \) be an extra special 2-group \( D^r \) or \( QD^{r-1} \) of order \( 2^n \), where \( n = 2r + 1 \). Then elements in \( G \) are of order 1 or 2 or 4. Let \( R \) be the \( \mathbb{C} \)-irreducible representation of degree \( 2^r \) and \( \eta \) is a character afforded by \( R \). Let \( s \) be the number of elements of order 2 or 1 and let \( t \) be the number of elements of order 4. Then we have

1. In case \( G = D^r \), \( R \) is equivalent to an \( \mathbb{R} \)-representation, \( s = 2^{n-1} + 2^r \) and \( t = 2^{n-1} - 2^r \).
2. In case \( G = QD^{r-1} \), \( R \) is not equivalent to an \( \mathbb{R} \)-representation but \( \eta = \bar{\eta}, \ s = 2^{n-1} - 2^r \) and \( t = 2^{n-1} + 2^r \).

**Remark.**

1. The groups \( D \) and \( Q \) have the same character table. Hence group algebras \( \mathbb{CD} \) and \( \mathbb{CQ} \) over \( \mathbb{C} \) are isomorphic. But two group algebras over \( \mathbb{R} \) are not isomorphic. In fact,

\[
\mathbb{RD} \cong \mathbb{R}^{(4)} \oplus (\mathbb{R})_2 \text{ and } \mathbb{RQ} \cong \mathbb{R}^{(4)} \oplus H
\]

where \( H \) is the quaternion algebra over \( \mathbb{R} \).

2. \( D^r \) is not isomorphic to \( QD^{r-1} \) because \( \mathbb{C} \)-irreducible \( \mathbb{R} \)-representations of degree \( 2^r \) are different (see [5, pp. 205-206]).

Here we state about \( \mathbb{R} \)-representations of affine groups over finite fields.

**Proposition 5.** Let \( G \) be a permutation group on finite field \( \mathbb{F}_q \), where \( q \) is a power of a prime \( p \), defined by

\[
G = \{ x \to ax + b \mid a \in \mathbb{F}_q^*, \ b \in \mathbb{F}_q \}.
\]

Let \( s \) be the number of elements \( x \) with \( x^2 = 1 \) and let \( t \) be the number of elements \( x \in G \) such that \( x^2 = u_1 \) where \( u_1 : x \to x + 1 \). Then in case \( p \neq 2 \), \( s = |G^*| + 1 \) and \( t = 1 \) and in case \( p = 2 \), \( s = |G^*| \) and \( t = 0 \). The \( \mathbb{C} \)-irreducible representation of degree \( |G^*| - 1 \) is equivalent to an \( \mathbb{R} \)-representation.

**3. Theorem of Hurwitz**

The converse of the next theorem is well known. In case \( n = 1 \), it is trivial. In case \( n = 2, 4 \), we have

1. \( (x_1^2 + x_3^2)(y_1^2 + y_3^2) = (x_1y_1 + x_3y_3)^2 + (x_1y_2 - x_2y_1)^2 \).
2. \( (x_1^2 + x_3^2 + x_4^2)(y_1^2 + y_3^2 + y_4^2) = (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2 \).

In case \( n = 8 \), it is also known. The next theorem is very interested to suggest that algebras over the real number field can be constructed.

**Theorem 6 (Hurwitz [7,1,6]).** In polynomial ring \( \mathbb{C}[x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n] \),
if the next equation is satisfied for \( z_s = \sum_{k} x_k y_k \), then \( n = 1, 2, 4, 8 \)

\[
(x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2) = z_1^2 + z_2^2 + \cdots + z_n^2.
\]

A key point in the above theorem is to prove \( n = 1, 2, 4, 8 \) if the next group \( H_n \) has a faithful representation of degree \( n \), namely, there is such a group \( H_n \) in \( GL(n, \mathbb{C}) \).

\[
H_n = \{ (-I)^{s_0} B_1^{s_1} B_2^{s_2} \cdots B_{n-1}^{s_{n-1}} \mid s_k = 0, 1 \}
\]

where \( B_k^2 = -I \), \( B_k B_\ell = -B_\ell B_k \) for \( k \neq \ell \).

However we can show that 2-groups \( H_n \) are realized in \( GL(m, \mathbb{C}) \) for some \( m \). Therefore we shall state about \( \mathbb{C} \)-irreducible \( \mathbb{R} \)-representations of 2-groups \( H_n \).

**Lemma 7.** The group \( H_n \) has two irreducible characters \( \eta_1 \) and \( \eta_2 \) for an even integer \( n \). Let \( s \) be the number of elements \( x \in H_n \) with \( x^2 = 1 \) and let \( t \) be the number of elements \( x \in H_n \) of order 4. Then we obtain.

1. \( s + t = 2^n \).
2. \( \nu(\eta_1) = \nu(\eta_2) = 2^{-\frac{n+2}{2}}(s - t) \).
3. \( \nu(\eta_1) = \begin{cases} 1 & \text{for } s > 2^{n-1}, \\ -1 & \text{for } s < 2^{n-1}, \\ 0 & \text{for } s = 2^{n-1}. \end{cases} \)
4. \( s = 2^{n-1} + 2^n \nu(\eta_1) \) and \( t = 2^{n-1} - 2^n \nu(\eta_1) \).
5. \( \frac{s}{2} = \sum_{k \equiv 0, 3 \text{ mod } 4} (n - 1) \) and \( \frac{t}{2} = \sum_{k \equiv 1, 2 \text{ mod } 4} (n - 1) \).

**Proof.** (1) is clear since every element of \( H_n \) is of order 1, 2, 4.

(2) follows from \( \eta_1(1) = \eta_2(1) = 2^{\frac{n+2}{2}} \), \( \eta_1(-1) = \eta_2(-1) = -2^{\frac{n-2}{2}} \) and the next equations

\[
\nu(\eta_1) = \frac{1}{|H_n|} (s \eta_1(1) + t \eta_1(-1)) = \frac{\eta_1(1)}{|H_n|} (s - t) = \nu(\eta_2).
\]

(3) and (4) follow easily from (1) and (2).

(5) follows from the equations

\[
(B_{i_1} B_{i_2} \cdots B_{i_k})^2 = \begin{cases} I & \text{for } k \equiv 0, 3 \text{ mod } 4, \\ -I & \text{for } k \equiv 1, 2 \text{ mod } 4. \end{cases}
\]

We proved our assertion.

Using (5) in the above lemma, we can find value of \( \nu(\eta_1) \). For this purpose, we consider the next equation

\[
(1 + i)^m = \sqrt{2}(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})^m = 2^\frac{m}{2} (\cos \frac{m\pi}{4} + i \sin \frac{m\pi}{4})
\]

where \( i = \sqrt{-1} \). Comparing imaginary parts between left and right sides in the above equation, we have the next formula

\[
\sum_{r=0}^{[\frac{m-1}{2}]} (-1)^r \binom{m}{2r + 1} = 2^\frac{m}{2} \sin \frac{m\pi}{4}
\]
where \([\ ]\) is the Gauss symbol. In particular, we have for \(m = 4k + 2\).

\[
\sum_{r=0}^{\frac{m-1}{2}} (-1)^r \binom{m}{2r + 1} = (-1)^{\frac{m-2}{2}} 2^m \quad (\text{see [9, p.11]}).
\]  

The next proposition states about \(\mathbb{C}\)-irreducible \(\mathbb{R}\)-representations of groups \(H_n\).

**Proposition 8.** Let \(\eta\) be a non-linear irreducible character of \(H_n\). Then in case \(n\) is odd, \(H_n\) is concos and so we already know about \(\mathbb{C}\)-irreducible \(\mathbb{R}\)-representations of groups \(H_n\). In case \(n\) is even, we have

\[
\nu(\eta) = \begin{cases} 0 & \text{for } n \equiv 2 \mod 4, \\ -1 & \text{for } n \equiv 4 \mod 8, \\ 1 & \text{for } n \equiv 0 \mod 8. \end{cases}
\]

**Proof.** In case \(n \equiv 2 \mod 4\), noting that \(k \equiv 0, 3 \mod 4\) is equivalent to \(n - 1 - k \equiv 1, 2 \mod 4\) for \(0 \leq k \leq n - 1\), we obtain easily

\[
\frac{s}{2} = \sum_{k \equiv 0, 3 \mod 4} \binom{n - 1}{k} = \sum_{k \equiv 0, 3 \mod 4} \binom{n - 1}{n - 1 - k} = \sum_{\ell = 1, 2 \mod 4} \binom{n - 1}{\ell} = \frac{t}{2}.
\]

In the other cases, using the above formula (\(\#\)), we have the following assertions.

\[
\frac{s}{2} = \sum_{k \equiv 0, 3 \mod 4} \binom{n - 1}{k} = \sum_{k \equiv 0, 3 \mod 4} \left\{ \binom{n - 2}{k - 1} + \binom{n - 2}{k} \right\}
\]

\[
= 2^{n-2} - \sum_{\ell = 0}^{\frac{[n-1]}{2}} (-1)^{\ell} \binom{n - 2}{2\ell + 1} = \begin{cases} 2^{n-2} + 2^{\frac{n-2}{2}} & \text{for } n \equiv 0 \mod 8, \\ 2^{n-2} - 2^{\frac{n-2}{2}} & \text{for } n \equiv 4 \mod 8. \end{cases}
\]

where \(0 \leq k \leq n - 1\) and \(\binom{n-2}{-1} = \binom{n-2}{n-1} = 0\).

**References**


K. MOTOSE
DEPARTMENT OF MATHEMATICAL SCIENCES
FACULTY OF SCIENCE AND TECHNOLOGY
HIROSAKI UNIVERSITY
HIROSAKI 036-8561, JAPAN
E-mail address: skm@cc.hirosaki-u.ac.jp