Note on Hadamard groups and difference sets

Noboru Ito

Department of Mathematics, Meijo University
Nagoya, Tenpaku, 468 Japan

In honour of Albert Leon Whiteman's eightieth birthday

Abstract. A representation theoretical characterization of an Hadamard subset is given.

§1. Introduction. A finite group $G$ of order $2n$ is called an Hadamard group if $G$ contains an $n$-subset $D$ and an element $e^*$ such that

1. $D$ and $De^*$ are disjoint,
2. $D$ and $Da$ intersect exactly in $n/2$ elements for any element $a$ of $G$ distinct from $e^*$ and the identity element $e$ of $G$, and
3. $Da$ and $\{b, be^*\}$ intersect exactly in one element for any elements $a$ and $b$ of $G$.

The subset $D$ will be called an Hadamard subset corresponding to $e^*$.

We consider the group ring of $G$ over the field of complex numbers. If $S$ is a subset of $G$, then $S$ also denotes the sum of elements of $S$. Now (1) and (2) together will be expressed as

4. \[ D^{-1}D = ne + (n/2)(G - e - e^*) \]

We have shown in (2, Proposition 1) that $e^*$ is a central involution. For the basic facts on the representations of finite groups the reader is referred to our reference (1). Then we have
that $R(e^*) = I$ or $-I$ for any irreducible representation $R$ of $G$ over the field of complex numbers, where $I$ denotes the identity matrix of order equal to the degree of $R$. Now from (4) we obtain that

(I) \[ R(D^{-1}D) = nI \text{ if } R(e^*) = -I, \text{ and } R(D^{-1}D) = 0 \text{ if } R(e^*) = I, \]

and if $R$ is distinct from the identity representation $1_G$ of $G$. For a justification of this statement the reader should see (2, Proposition 4). Now the purpose of this note is to prove the following proposition.

Proposition 1. (I) is sufficient for an $n$-subset $D$ of $G$ satisfying (1) and (3) to be an Hadamard subset corresponding to $e^*$.

Incidentally we have noticed that the similar fact holds for difference sets. Let $E$ be a $(v, k, \lambda)$-difference set in a group $H$ of order $v$. Then we have that

(5) \[ E^{-1}E = ke + \lambda(H - e), \text{ where } e \text{ also denotes the identity element of } H. \]

So from (5) we obtain that

(II) \[ R(E^{-1}E) = (k - \lambda)I \text{ for any irreducible non-identity representation } R \text{ of } H. \]

Then the following proposition holds.

Proposition 2. (II) is sufficient for a $k$-subset $E$ of $H$ to be a difference set.

The proof of Proposition 2 is similar to that of Proposition 1. Actually it is simpler and it will be omitted.

§2. Proof of Proposition 1. Let $D$ be an $n$-subset of $G$ satisfying (1), (3) and (I). In this section the summation except the
last one always runs over $G - \{e, e^*\}$. Put
\[ D^{-1}D = ne + \sum m(g)g, \] where $m(g)$ denotes the multiplicity of an element $g$ of $G$ in $D^{-1}D$.

Then by (I) we have that
\[ n^2 - n = \sum m(g)1_G(g), \quad 0 = \sum m(g)R(g), \] where $R$ is any irreducible representation of $G$ such that $R(e^*) = -I$, and $-nI = \sum m(g)R(g)$, where $R$ is any non-identity irreducible representation of $G$ such that $R(e^*) = I$.

Let $h$ be any fixed element of $G$ distinct from $e$ and $e^*$. Then from (6) we get that
\[ n^2 - n = \sum m(g)1_G(gh^{-1}), \quad 0 = \sum m(g)R(gh^{-1}), \] where $R$ is any irreducible representation of $G$ such that $R(e^*) = -I$, and $-nR(h^{-1}) = \sum m(g)R(gh^{-1})$, where $R$ is any non-identity irreducible representation of $G$ such that $R(e^*) = I$.

Let $\chi$ denote the character of $G$ corresponding to $R$. Then from (7) we get that
\[ n^2 - n = \sum m(g)1_G(gh^{-1}), \quad 0 = \sum m(g)\chi(gh^{-1}), \] where $\chi$ corresponds to $R$ such that $R(e^*) = -I$, and $-n\chi(h^{-1}) = \sum m(g)\chi(gh^{-1})$, where $\chi$ corresponds to $R$ such that $R(e^*) = 1$ and $R \neq 1_G$.

Now from (8) we obtain that
\[ n^2 - n = \sum m(g)1_G(gh^{-1})1_G(e), \quad 0 = \sum m(g)\chi(gh^{-1})\chi(e), \] where $\chi$ corresponds to $R$ such that $R(e^*) = -I$, and $-n\chi(h^{-1})\chi(e) = \sum m(g)\chi(gh^{-1})\chi(e)$, where $\chi$ corresponds to $R$ such that $R(e^*) = 1$ and $R \neq 1_G$.

Adding up in (9) all irreducible characters and using orthogonality relations for irreducible characters, we get that
\[ n^2 - n - \sum_{(h^{-1}) \in \chi(e^*) \neq \chi(e)} \chi(h^{-1}) \chi(e) = n^2 = m(h)2n, \]

namely \( m(h) = n/2 \), as desired.

We add the following remark: \( R \) always can be assumed to be unitary. Then we have that \( R(D^{-1}) = R(D)^* \), where \( * \) denotes the composition of complex conjugation and transposition. If \( R(D^{-1}D) = nI \), then \( R(D)^*R(D) = nI \), and hence \( n^{-1/2}R(D) \) is a unitary matrix.

The propositions above imply the following propositions immediately.

(i) If \( G \) is an Hadamard group with prescribed subset \( D \) and element \( e^* \), then \( DD^{-1} = D^{-1}D \), and \( G \) is an Hadamard group with prescribed subset \( D^{-1} \) and element \( e^* \).

(ii) If \( E \) is an Hadamard difference set in a group \( H \), then \( EE^{-1} = E^{-1}E \), and \( E^{-1} \) is also an Hadamard difference set in \( H \).

References

(Received 9/3/94)