2023-04-17

Skew Relative Hadamard Difference Set Groups

Andrew Haviland
Brigham Young University

Skew Relative Hadamard Difference Set Groups

Andrew Haviland

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Stephen Humphries, Chair
Michael Griffin
Paul Jenkins

Department of Mathematics

Brigham Young University

ABSTRACT

Skew Relative Hadamard Difference Set Groups

Andrew Haviland
Department of Mathematics, BYU
Master of Science

We study finite groups G having a nontrivial subgroup H and $D \subset G \setminus H$ such that (i) the multiset $\{xy^{-1} : x, y \in D\}$ has every element that is not in H occur the same number of times (such a D is called a *relative difference set*); (ii) $G = D \cup D^{(-1)} \cup H$; (iii) $D \cap D^{(-1)} = \emptyset$.

We show that $|H| = 2$, that H has to be normal, and that G is a group with a single involution. We also show that G cannot be abelian.

We give examples of such groups, including certain dicyclic groups, by using results of Schmidt and Ito.

We describe an infinite family of dicyclic groups with these relative difference sets, and classify which groups of order up to 72 contain them.

We also define a relative difference set in dicyclic groups having additional symmetries, and completely classify when these exist in generalized quaternion groups.

We make connections to Schur rings and prove additional results.

Keywords: difference set, subgroup, Hadamard difference set, Schur ring, dicyclic group.

Acknowledgements

All computations made in the preparation of this paper were accomplished using Magma [2]. Thanks to Brigham Young University Department of Mathematics for funding during the writing of this thesis.

Contents

Chapter 1. Introduction

A *difference set* D in a finite group G is a nonempty subset of G such that any non-identity element of G can be written in exactly λ ways as $d_1 d_2^{-1}$ where $d_1, d_2 \in D$. We say $D \subset G$ is a *(v,k,λ)-difference set* if $|G| = v$, $|D| = k$, and each non-identity element of G can be represented λ ways as a 'difference' of elements of D.

The study of difference sets is related to the study of designs. We describe the connection here.

An *incidence structure* is an ordered triple (P, B, I) consisting of a set of *points* P, a set of *blocks* B, and an *incidence relation* $I \subset P \times B$, where we say the point $p \in P$ and block $b \in B$ are *incident* if $(p, b) \in I$.

Given a difference set $D \subset G$, the *development* of D is the incidence structure whose points are the elements of G and whose blocks are the left translates of the difference set

$$\{aD \ ; \ a \in G\}.$$

A *symmetric* (v, k, λ) *design* is an incidence structure (P, B, I) in which $0 < k < v$ and the following hold:

(i) $|P| = |B| = v$.

(ii) Each point is incident with k blocks.

(iii) Each block is incident with k points.

(iv) Each pair of points is incident with λ blocks.

(v) Each pair of blocks is incident with λ points.

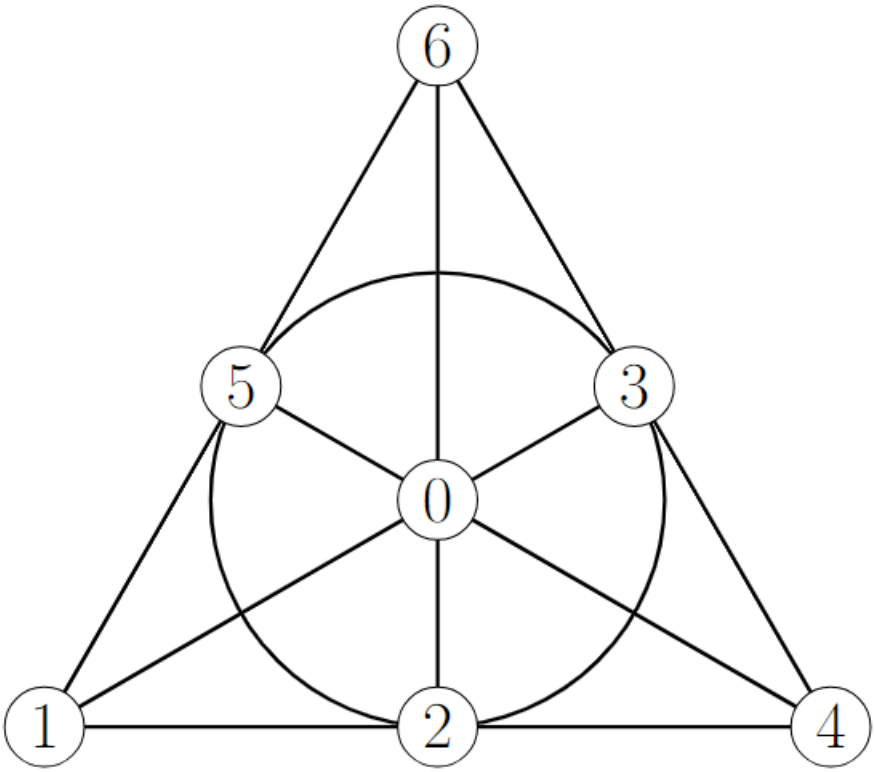
Theorem 1.0.1. *[19, Theorem 4.7, p. 54] Let $D \subset G$ be a (v, k, λ)-difference set. Then the development of D is a symmetric (v, k, λ) design.*

This connection between difference sets and designs allows many algebraic and geometric tools to be applied to difference set theory. A common example of a difference set is the

$(7,3,1)$-difference set $D = \{1,2,4\}$ of $G = \mathbb{Z}_7$. The corresponding design

$$\{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,0\},\{5,6,1\},\{6,0,2\},\{0,1,3\}\},$$

is known as the *Fano plane.*



We shall make use of the following technique commonly applied to difference sets: Let G be a group with a normal subgroup N. Let $\{g_1,\ldots,g_r\}$ be a complete set of coset representatives for N in G. If D is a difference set in G, then the numbers $n_i = |D \cap g_i N|$ are the *intersection numbers for D with respect to N.*

For a finite group G, we will identify $X \subseteq G$ with the element $\sum_{x\in X} x \in \mathbb{Z}G$ of the group algebra, and let $X^{(-1)} = \{x^{-1} : x \in X\}$. We write $\mathcal{C}_n$ for the cyclic group of order n.

Let $H \leq G$ and $h = |H| > 1$.

Then a (v,k,λ)-*relative difference set* (relative to H) is a subset $D \subset G \setminus H, |D| = k, v =$

$|G|$, such that

$$DD^{(-1)} = \lambda(G - H) + k,$$

so that every element $g \in G \setminus H$ occurs λ times in the multiset $\{xy^{-1} : x, y \in D\}$.

We now further assume

$$(1) \quad D \cap D^{(-1)} = \emptyset;$$

$$(2) \quad G = D \cup D^{(-1)} \cup H \quad \text{(disjoint union)}.$$

A group having a difference set of the above type will be called a (v, k, λ)-*skew relative Hadamard difference set group* (with difference set D and subgroup H); or a (v, k, λ)-*SRHDS group*. Categorizing which groups are SRHDS groups is the main motivation of this research.

Recall the following related concept: a group G is a *skew Hadamard difference set* if it has a difference set D where

$$G = D \cup D^{(-1)} \cup \{1\},$$

$$D \cap D^{(-1)} = \emptyset.$$

Such groups have been studied in [5, 6, 7, 10, 11, 12, 13, 20].

In this paper we find infinitely many examples of such SRHDS groups. We also find groups that cannot be SRHDS groups, but which satisfy certain properties of a SRHDS group, as given in:

Theorem 1.0.2. *For a (v, k, λ) SRHDS group G with difference set D and subgroup H we have:*

(i) $|H| = 2$;

(ii) $H \triangleleft G$;

(iii) G is a group having a single involution;

(iv) $v \equiv 0 \mod 8$;

(v) G is not abelian;

(vi) A Sylow 2-subgroup is a generalized quaternion group.

Parts $(i), (ii)$, and (iii) will follow from Proposition 3.1.1. Parts $(iv), (v)$ will follow from Corollaries 4.1.3 and 4.1.4. For part (vi), suppose that G is a finite group with a unique involution z. Let $Z = \langle z \rangle$ and let $Q = G/Z$. Since G has a unique involution, the same is true of any subgroup of G of even order, in particular, for any Sylow 2-subgroup of G. Now the 2-groups with unique involution were determined by Burnside (see [24, Theorems 6.11, 6.12] and [1, 4]); they must be cyclic or generalized quaternion groups. Corollary 4.1.5 will show that they cannot be cyclic. □

Groups with a single involution are studied in [21, 22, 14]. Dicyclic groups Dic_v are examples of such groups. However, we note that Dic_{72} has no SRHDS (Proposition 5.2.1).

We now establish a connection with Hadamard groups. Recall that a *Hadamard group* is a group G containing $H \leq Z(G)$ of order 2 such that there is an H-transversal $D, |D| = v/2$, that is a relative difference set relative to H, so that $DD^{(-1)} = \lambda(G - H) + |D|$.

We show that if $D \subset G$ is a SRHDS, then G is also a Hadamard group (where $E = D + 1$ is the relative difference set); see Proposition 3.1.5. Thus it is natural to try to obtain results for SRHDS groups that are similar to the results of Schmidt and Ito [29, 15] from the Hadamard group situation. For example Schmidt and Ito show that if $4p-1$ is a prime power or $2p - 1$ is a prime power, then the groups $\mathrm{Dic}_{8\mathrm{p}}$ and $\mathrm{Dic}_{4\mathrm{p}}$ (respectively) are Hadamard groups.

For dicyclic SRHDS groups we show:

Theorem 1.0.3. *If $p \in \mathbb{N}$ and $4p - 1$ is a prime power, then $\mathrm{Dic}_{8\mathrm{p}}$ is a SRHDS group.*

There is no analogous result when $2p - 1$ is prime.

Now Ito [15] determines a 'doubling process' that takes a Hadamard difference set for Dic_v and produces a Hadamard difference set for Dic_{2v}. We note that this doubling process does not work in general in the context of a SRHDS, however we will show that it does work under an additional 'symmetry' hypothesis (see Corollary 4.3.3) that is satisfied in the situation of Theorem 1.0.3. This allows us to prove:

Theorem 1.0.4. *If $p \in \mathbb{N}$ and $4p - 1$ is a prime power, then $\mathrm{Dic}_{16\mathrm{p}}$ is a SRHDS group.*

Theorems 1.0.3 and 1.0.4 will be a consequence of Theorems 4.2.1 and 4.3.3.

Theorem 1.0.5. *Let $G = C_p \times \mathrm{Dic}_{8n}$ with $p > 2$ prime and n odd. Then G is not a SRHDS group.*

This will be a consequence of Proposition 5.2.2.

We will also define *doubly symmetric SRHDS* groups that have even more 'symmetry' (see Definition 6.1.3). This will allow us to prove:

Theorem 1.0.6. *Let $G = \mathrm{Dic}_{8\cdot 2^u}$ be a generalized quaternion group for some $u \in \mathbb{Z}_{\geq 0}$. Then G contains a doubly symmetric SRHDS if and only if $2^{u+1} - 1$ is either prime or 1.*

This will be shown in Theorem 6.2.3.

We will also provide a detailed proof of a result known to Travis [31]:

Theorem 1.0.7. *Given a subgroup H of a finite group G, we have that (G, H) is a strong Gelfand pair if and only if $\mathbb{C}[G]^H$, the ring of H-classes in G, forms a commutative Schur ring.*

The definition of a strong Gelfand pair and the proof of this theorem can be found in Corollary 7.2.5.

Chapter 2. Definitions and Results from Representation Theory

One main tool for this research is representation theory, so we will list some well-established definitions and results from representation theory.

Let G be a finite group. A *representation* ρ of G is a group homomorphism

$$\rho : G \to \mathrm{GL}(V)$$

where V is a finite-dimensional vector space (which we will assume is over the complex numbers) and $\mathrm{GL}(V)$ is the general linear group of invertible linear transformations from V to itself. Given a basis for V, we can identify $\mathrm{GL}(V)$ with $\mathrm{GL}(\mathrm{n}, \mathbb{C})$, where n is the dimension of V, and think of a representation as mapping into a matrix group.

A representation of G in V is *irreducible* if its only G-invariant subspaces are V and $\{0\}$.

Theorem 2.0.1. *[19, Maschke's Theorem, p. 188] Every representation of a finite group G in a finite-dimensional vector space V over $\mathbb{C}$ can be written as a direct sum of irreducible representations.*

Given a finite group G and a commutative ring R, the *group algebra* RG is the set of formal linear combinations

$$\left\{ \sum_{g_i \in G} a_i g_i | a_i \in R \right\},$$

under the operations

$$\sum_{g_i \in G} a_i g_i + \sum_{g_i \in G} b_i g_i = \sum_{g_i \in G} (a_i + b_i) g_i,$$

$$\left(\sum_{g_i \in G} a_i g_i \right) \left(\sum_{g_i \in G} b_i g_i \right) = \sum_{h \in G} \left(\sum_{g_i g_j = h} a_i b_j \right) h.$$

The group algebra allows us to take advantage of the ring structure on matrices. We can extend a representation

$$\rho : G \to \mathrm{GL}(V),$$

to

$$\rho : \mathbb{C}G \to \mathrm{End}(V),$$

by extending linearly over $\mathbb{C}$. Here $\mathrm{End}(V)$ is the set of endomorphisms on V: that is, the set of linear transformations from V to itself. Thus V becomes a $\mathbb{C}G$-module under the action

$$u \cdot v = \rho(u)(v),$$

for all $u \in \mathbb{C}G$, and $v \in V$. A $\mathbb{C}G$-module V is *irreducible* if its only $\mathbb{C}G$-invariant subspaces are itself and $\{0\}$. A *$\mathbb{C}G$-module homomorphism* is a linear map between $\mathbb{C}G$-modules that commutes with the $\mathbb{C}G$ action: that is, a linear map $T : V_1 \to V_2$ such that

$$T(u \cdot v) = u \cdot T(v),$$

for all $u \in \mathbb{C}G$, $v \in V_1$.

Theorem 2.0.2. *[16, Schur's Lemma, p. 78] Let V and W be irreducible $\mathbb{C}G$-modules. If $T : V \to W$ is a $\mathbb{C}G$-module homomorphism, then T is either an isomorphism or the zero map. Additionally, if T is an isomorphism, then T is a scalar multiple of the identity endomorphism on V.*

A ring R is *semisimple* if any short exact sequence of left R-modules splits. The following is a portion of Wedderburn's Theorem that we will use later.

Theorem 2.0.3. *[9, Wedderburn's Theorem, p. 854] Every semisimple ring R considered as a left R-module is a direct sum*

$$R = L_1 \oplus L_2 \oplus \cdots \oplus L_n,$$

where each L_i is a simple module, and $L_i = Re_i$, where the $e_i \in R$ are primitive orthogonal idempotents.

The following two theorems are consequences of applying *Wedderburn's Theorem* to the group algebra $\mathbb{C}G$, which is semisimple [9, Corollary 5, p. 856].

Theorem 2.0.4. *[9, Theorem 10, p. 861] Let G be a finite group.*

(1) *There are $n_1, n_2, \ldots, n_r$ such that $\mathbb{C}G \equiv M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$;*

(2) *$\mathbb{C}G$ has exactly r distinct isomorphism types of irreducible modules and these have complex dimensions $n_1, n_2, \ldots, n_r$ (and so G has exactly r inequivalent irreducible complex representations of the corresponding degrees).*

(3) $\sum_{i=1}^{r} n_i^2 = |G|$.

(4) *r equals the number of conjugacy classes in G.*

Theorem 2.0.5. *[9, Corollary 11, p. 861] A finite group G is abelian if and only if every irreducible complex representation of G is 1-dimensional.*

Given a representation $\rho : G \to \mathrm{GL}(V)$, the *character* χ_ρ is the map $\chi_\rho : G \to \mathbb{C}$ given by

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g)).$$

Here Tr is the trace function. A character is *irreducible* if the associated representation is. The standard inner product on characters (or any class functions on G) is given by

$$(\chi, \sigma) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\sigma(g)}.$$

Theorem 2.0.6. *[9, The First Orthogonality Relation for Group Characters, p. 872] Let G be a finite group and let $\chi_1, \chi_2, \ldots, \chi_r$ be the irreducible characters of G over $\mathbb{C}$. Then with respect to the inner product $(\ ,\ )$ we have*

$$(\chi_i, \chi_j) = \delta_{ij},$$

and the irreducible characters are an orthonormal basis for the space of class functions on G.

Theorem 2.0.7. *[9, The Second Orthogonality Relation for Group Characters, p. 872] Let G be a finite group and let $\chi_1, \chi_2, \ldots, \chi_r$ be the irreducible characters of G over $\mathbb{C}$. Then for*

any $x, y \in G$,

$$\sum_{i=1}^{r} \chi_i(x)\overline{\chi_i(y)} = \begin{cases} |C_G(x)| & \textit{if } x \textit{ and } y \textit{ are conjugate in } G; \\ 0 & \textit{otherwise.} \end{cases}$$

Chapter 3. Difference sets and necessary conditions

3.1 $|H| = 2$ and normality of H

Recall that for $p \geq 1$ the *dicyclic group* is

$$\mathrm{Dic}_{8\mathrm{p}} = \langle \mathrm{x}, \mathrm{y} | \mathrm{x}^{2\mathrm{p}} = \mathrm{y}^2, \mathrm{x}^{4\mathrm{p}} = \mathrm{y}^4 = 1, \mathrm{x}^{\mathrm{y}} = \mathrm{x}^{-1} \rangle,$$

so that $|\mathrm{Dic}_{8\mathrm{p}}| = 8\mathrm{p}$. A *generalized quaternion group*, denoted Q_{2^a}, is just a dicyclic group $\mathrm{Dic}_{2^{\mathrm{a}}}$, $a \geq 3$.

Proposition 3.1.1. *Let G be a SRHDS group with subgroup H. Then G has a single involution t, and $H = \langle t \rangle$. In particular $h := |H| = 2, H \leq Z(G)$, and $H \triangleleft G$.*

Proof. Let D be a SRHDS for G. Since $D \cap D^{(-1)} = \emptyset$ we see that D does not contain an involution. Since $G - (D + D^{(-1)}) = H$ we see that all involutions are contained in H.

If we have $d_1, d_2 \in D$, with

$$h_1 d_1 = h_2 d_2 \in H d_1 \cap H d_2, \quad h_i \in H,$$

then

$$h_2^{-1} h_1 = d_2 d_1^{-1} \in H,$$

which implies that

$$h_2^{-1} h_1 = d_2 d_1^{-1} = 1,$$

(since $DD^{(-1)} = \lambda(G - H) + k$ implies that the only element of H of the form $d_2 d_1^{-1}$ is 1). Thus $d_1 = d_2$ and $h_1 = h_2$.

Thus the cosets $Hd, d \in D$, are disjoint, and so

$$| \cup_{d \in D} Hd| = |H| \cdot |D| = hk.$$

Since $Hd \subset G - H$ for $d \in D$, we see that

$$hk = | \cup_{d \in D} Hd| \leq |G - H| = |D + D^{(-1)}| = 2k.$$

Thus $h \leq 2$ and so $h = 2$ as $h > 1$. This implies that H consists of the identity and the unique involution $t \in G$. Since t is an involution, $(gtg^{-1})^2 = 1$ for all $g \in G$, so gtg^{-1} is in $\langle t \rangle$. It cannot be 1 since $t \neq 1$. Thus $gtg^{-1} = t$, so $t \in Z(G)$. This implies that $H = \{1, t\} \leq Z(G)$, and thus we have that H is normal in G. □

This proves (i), (ii) and (iii) of Theorem 1.0.2.

In what follows we will let $H = \langle t \rangle$, where $t \in Z(G)$ has order 2. Then:

$$G = D + D^{(-1)} + H, \qquad D \cdot D^{(-1)} = \lambda(G - H) + k \cdot 1. \tag{3.1}$$

These equations give

$$v = 2k + 2, \quad k^2 = k + \lambda(v - 2),$$

and solving gives (i) of

Lemma 3.1.2. *(i)* $v = 2k + 2, \quad \lambda = (k-1)/2 = (v-4)/4$ *and* $4|v$.
(ii) $DH = HD = D^{(-1)}H = HD^{(-1)} = G - H$.
(iii) $G, D, D^{(-1)}, H$ *all commute.*

Proof. From $D \subset G - H$ we have $DH \cap H = \emptyset$, and $DH \subset G - H$; but $|G - H| = 2k = |DH|$, so that

$$DH = HD = G - H = (G - H)^{(-1)} = D^{(-1)}H = HD^{(-1)},$$

giving (ii).

Since $D^{(-1)} = G - D - H$ and $H \leq Z(G)$ it now follows that D and $D^{(-1)}$ commute. This shows that $G, D, D^{(-1)}, H$ all commute. □

Lemma 3.1.3. *Let G be a SRHDS group with difference set D and subgroup $H = \langle t \rangle$. Then $D^{(-1)} = tD$.*

Proof. We have

$$\begin{aligned} D + Dt &= (1+t)D \\ &= HD \\ &= G - H \\ &= D + D^{(-1)}. \end{aligned}$$

□

We now define Schur rings [26, 30, 32, 33]. A subring $\mathfrak{S}$ of $\mathbb{Z}G$ is a *Schur ring* (or S-ring) if there is a partition $\mathcal{K} = \{C_i\}_{i=1}^{r}$ of G such that:

1. $\{1_G\} \in \mathcal{K}$;
2. for each $C \in \mathcal{K}$, $C^{(-1)} \in \mathcal{K}$;
3. $C_i \cdot C_j = \sum_k \lambda_{i,j,k} C_k$ for all $i, j \leq r$ where $\lambda_{i,j,k} \in \mathbb{Z}_{\geq 0}$.

The C_i are called the *principal sets* of $\mathfrak{S}$. Then we have:

Lemma 3.1.4. *$\{1\}, \{t\}, D, D^{(-1)}$ are the principal sets of a commutative Schur ring.*

Proof. The sets $\{1\}, \{t\}, D, D^{(-1)}$ partition G and we have each of the following:

$$\begin{aligned} &D^{(-1)} = tD, \\ &tD^{(-1)} = D, \\ &t^2 = 1, \\ &D^{(-1)}D = DD^{(-1)} = \lambda(G - H) + k = \lambda(D + D^{(-1)}) + k, \\ &D^2 = tDD^{(-1)} = t(\lambda(D + D^{(-1)}) + k). \end{aligned}$$

This concludes the proof. □

Proposition 3.1.5. *If $D \subset G$ is a SRHDS, then G is a Hadamard group.*

Proof. We have $DD^{(-1)} = \lambda(G - H) + k$. Let $E = D + 1$, so that

$$\begin{aligned} EE^{(-1)} &= DD^{(-1)} + D + D^{(-1)} + 1 \\ &= \lambda(G - H) + k + (G - H) + 1 \\ &= (\lambda + 1)(G - H) + k + 1, \end{aligned}$$

as required. □

3.2 Intersection numbers

Let $N \triangleleft G$ and let $g_1, g_2, \ldots, g_r$ be coset representatives for G/N. If G is a SRHDS group with difference set D, then the numbers $n_i = |D \cap Ng_i|$ are called the *intersection numbers*. Standard techniques give (see Section 7.1 of [19]):

Lemma 3.2.1. *Let $D \subset G$ be a SRHDS with subgroup $H = \langle t \rangle, t^2 = 1$. Let $N \triangleleft G$ have order s and index r in G. Let $g_1 = 1, g_2, \ldots, g_r$ be coset representatives for G/N and let $n_i = |D \cap Ng_i|, 1 \leq i \leq r$. Then*

$$\sum_{i=1}^{r} n_i = k, \qquad \sum_{i=1}^{r} n_i^2 = \lambda|N \setminus H| + k.$$

Proof. We have

$$G = \sum_{i=1}^{r} Ng_i,$$

and thus

$$\begin{aligned} k &= |D| \\ &= |D \cap G| \\ &= \sum_{i=1}^{r} |D \cap Ng_i| \\ &= \sum_{i=1}^{r} n_i. \end{aligned}$$

Since $DD^{(-1)} = \lambda(G - H) + k$, if we denote $D_i = |D \cap Ng_i|$, we get

$$\begin{aligned}\sum_{i=1}^{r} n_i^2 &= \sum_{i=1}^{r} |D_i|^2 \\ &= \sum_{i=1}^{r} |D_i D_i^{(-1)}| \\ &= |N \cap DD^{(-1)}| \\ &= |N \cap (\lambda(G \setminus H) + k)| \\ &= \lambda|N \setminus H| + k.\end{aligned}$$

□

Lemma 3.2.2. *Let G be a dicyclic group and let $N \triangleleft G$. Let $D \subset G$ be a SRHDS with subgroup H. Let $Ng_3, \cdots, Ng_r$ be the cosets that don't meet H, and let $n_i = |D \cap Ng_i|$. Suppose that we have distinct $i, i' > 2$ where $g_i g_{i'} \in N$. Then $n_i + n_{i'} = |N|$.*

Proof. Since $n_i = |D \cap Ng_i|$, we have $n_i = |D^{(-1)} \cap Ng_i^{-1}| = |D^{(-1)} \cap Ng_{i'}|$. But if $i \geq 3$, then we have $Ng_{i'} \subset G \setminus H = D + D^{(-1)}$, so that

$$\begin{aligned}|N| &= |(D + D^{(-1)}) \cap Ng_{i'}| \\ &= |D \cap Ng_{i'}| + |D^{(-1)} \cap Ng_{i'}| \\ &= n_{i'} + n_i.\end{aligned}$$

□

The next result concerns intersection numbers for subgroups that are not necessarily normal.

Proposition 3.2.3. *Let G be a SRHDS group with difference set D and subgroup H. Let $K \leq G$ be any subgroup where $t \in K$. Let $b = |G : K|$ and let $g_0 = 1, g_1, \cdots, g_{b-1}$ be coset representatives for $K \leq G$. Let $k_i = |D \cap Kg_i|, 0 \leq i < b$. Then*

$$k_0 = |K|/2 - 1 \text{ and } k_i = |K|/2, \;\; 0 < i < b.$$

Let $D_i = D \cap Kg_i, i = 0, \cdots, b-1$. Then

$$\sum_{i=0}^{b-1} D_i D_i^{(-1)} = \lambda(K - H) + k.$$

Proof. We have $D^{(-1)} = tD$. Let $D_i = D \cap Kg_i$; then

$$tD_i = t(D \cap Kg_i) = (tD) \cap tKg_i = D^{(-1)} \cap Kg_i,$$

so that $D \cap tD = \emptyset$ and $i > 0$ gives

$$\begin{aligned} D_i + tD_i &= (D \cap Kg_i) + (D^{(-1)} \cap Kg_i) \\ &= (D + D^{(-1)}) \cap Kg_i \\ &= (G - H) \cap Kg_i \\ &= G \cap Kg_i = Kg_i. \end{aligned}$$

Taking cardinalities, again using $D \cap tD = \emptyset$, gives $2k_i = |K|$ for $i > 0$.

Then $\sum_{i=0}^{b-1} k_i = k$ now gives

$$k_0 + (b-1)|K|/2 = k = v/2 - 1;$$

but $v = b \cdot |K|$, from which we obtain $k_0 = |K|/2 - 1$.

Now from $DD^{(-1)} = \lambda(G - H) + k$ and $D = \sum_{i=0}^{b-1} D_i g_i$ we get

$$\sum_{i=0}^{b-1} D_i D_i^{(-1)} + \cdots = \lambda(G - H) + k,$$

so that

$$\sum_{i=0}^{b-1} D_i D_i^{(-1)} \subseteq \lambda(K - H) + k.$$

The last part will follow if we can show that both sides of the set containment have the same size.

From $b = v/|K|$ and the first part, the number of elements of the left hand side is

$$\sum_{i=0}^{b-1} |D_i|^2 = (|K|/2 - 1)^2 + (b-1)|K|^2/4 = 2p|K| - |K| + 1,$$

and (since $H \subset K$) the number of elements of the right hand side is

$$\lambda(|K| - 2) + k = 2p|K| - |K| + 1,$$

and we are done. □

Chapter 4. The Schmidt process and the doubling process

4.1 Direct Products and G is not abelian

Let $\zeta_n = \exp 2\pi i/n, n \in \mathbb{N}$. We first show

Theorem 4.1.1. *Suppose that $N \trianglelefteq G$, $G/N \cong \mathcal{C}_{2^a}, a \geq 2$, and $t \notin N$. Assume that $k = |G|/2 - 1$ is not a perfect square. Then G is not a SRHDS group.*

Proof. Assume that G is a SRHDS group. Suppose that $N \trianglelefteq G$ with

$$G/N = \langle rN \rangle \cong \mathcal{C}_{2^a}$$

where $r \in G$. Then there is a linear character

$$\chi' : G/N \to \mathbb{C}^\times, \qquad \chi'(rN) = \zeta_{2^a}$$

that induces

$$\chi : G \to \mathbb{C}^\times, \qquad \chi(r) = \chi'(rN).$$

We note that $N = \ker \chi$. Further, any $g \in G$ can be written as

$$g = r^i b,\ 0 \leq i < 2^a,\ b \in N.$$

Then we can write

$$D = \sum_{j=0}^{2^a-1} r^j N_j, \text{ where } N_j \subseteq N.$$

Since $t \notin N$ we have $\chi(t) = -1$ and so $\chi(H) = 0$. We certainly have $\chi(G) = 0$.

From $G = D + D^{(-1)} + H$ we get

$$\chi(D) + \chi(D^{(-1)}) = 0,$$

and from $DD^{(-1)} = \lambda(G - H) + k$ we get $\chi(D)\chi(D^{(-1)}) = k$.

These then give

$$\chi(D)^2 = -k, \text{ and so } \chi(D) = \pm\sqrt{-k}.$$

But

$$\pm i\sqrt{k} = \chi(D) = \chi\left(\sum_{j=0}^{2^a-1} r^j N_j\right) = \sum_{j=0}^{2^a-1} (\zeta_{2^a})^j |N_j|, \tag{4.1}$$

which gives $\sqrt{k} \in \mathbb{Q}(i, \zeta_{2^a}) = \mathbb{Q}(\zeta_{2^a})$, since $a \geq 2$. But the Galois group of $\mathbb{Q}(\zeta_{2^a})/\mathbb{Q}$ is $\mathcal{C}_2 \times \mathcal{C}_{2^{a-2}}$. These groups have at most three subgroups of index 2. Thus the Galois correspondence [9, Theorem 14, p. 574] tells us that $\mathbb{Q}(\zeta_{2^a})$ contains at most three quadratic extensions, the only possibilities for which are $\mathbb{Q}(i)/\mathbb{Q}, \mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$. But the hypothesis says that k is not a perfect integer square, so that $\sqrt{k} \notin \mathbb{Z}$. But $k > 1$ is also odd, and so

$$\sqrt{k} \notin \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}).$$

This contradiction gives Theorem 4.1.1. □

Corollary 4.1.2. *Suppose that $N \trianglelefteq G$, $G/N \cong \mathcal{C}_{2^a}, a \geq 3$, and $t \notin N$. Then G is not a SRHDS group.*

Proof. Since $2^a \geq 8$ we see that $k = (|G| - 2)/2$ satisfies $k \equiv 3 \mod 4$, and so the result follows from Theorem 4.1.1. □

Corollary 4.1.3. *If G is an abelian group with $|G| \equiv 0 \mod 8$, then G is not a SRHDS group.*

Proof. Let G be an abelian SRHDS group, and write $G = A \times N$ where A is a Sylow 2-subgroup, and N is a subgroup of odd order. Since G has a single involution, we see that A is cyclic, say of order 2^a. The results now follow from Corollary 4.1.2 . □

Corollary 4.1.4. *If G is a SRHDS group, then $v = |G| \equiv 0 \mod 8$.*

Proof. Assume that G is a SRHDS group with subgroup $H = \langle t \rangle$ and difference set D. Then we know that $4|v$ by Lemma 3.1.2, so suppose that $|G| = 4n$ where n is odd. Then a Sylow 2-subgroup of G must be $\mathcal{C}_4 = \langle r \rangle$ and $t = r^2$. Burnside's theorem ([24, Theorem 5.13])

shows that $\langle r \rangle$ has a complement $N \lhd G, |N| = n, G = N \rtimes \langle r \rangle$. So we can write

$$D = D_0 + D_1 r + D_2 r^2 + D_3 r^3, D_i \subset N.$$

Now

$$D + D^{(-1)} = G - H = N + Nr + Nr^2 + Nr^3 - H$$

then gives

$$D_0 + D_0^{(-1)} = N - 1, \quad D_1 + (D_3^{(-1)})^{r^3} = N, \quad D_2 + (D_2^{(-1)})^{r^2} = N - 1$$
$$D_3 + (D_1^{(-1)})^r = N.$$

Next, $D^{(-1)} = tD$ gives

$$D_0^{(-1)} = tD_0, \ \ (D_1^{(-1)})^r = tD_3, \ \ (D_2^{(-1)})^{r^2} = tD_2, \ \ (D_3^{(-1)})^{r^3} = tD_1.$$

Using $D_1 + (D_3^{(-1)})^{r^3} = N$ and $(D_3^{(-1)})^{r^3} = tD_1$ we get $D_1(1+t) = N$. However $D_1(1+t)$ has an even number of elements (counting multiplicities), while $|N|$ is odd. This contradiction gives the result. □

Corollaries 4.1.3 and 4.1.4 now prove Theorem 1.0.2 (iv) and (v).

Corollary 4.1.5. *If G is a SRHDS group, then a Sylow 2-subgroup of G is not cyclic.*

Proof. Assume G is a SRHDS group with cyclic Sylow 2-subgroup $\langle r \rangle$. By Corollary 4.1.4, $|\langle r \rangle| \geq 8$. Again, Burnside's theorem ([24, Theorem 5.13]) shows that $\langle r \rangle$ has a complement $N \lhd G, G = N \rtimes \langle r \rangle$. This now contradicts Corollary 4.1.2.

This concludes the proof of Theorem 1.0.2. □

4.2 Construction of some SRHDS groups

Theorem 4.2.1. *Suppose that $4p - 1$ is a prime power. Then* $\mathrm{Dic}_{8\mathrm{p}}$ *contains a SRHDS.*

Proof. We follow [29, Theorem 3.3] where Schmidt proves a result of Ito about relative difference sets in Dicyclic groups. Let $q = 4p - 1$ and let $\mathbb{F}_{q^n}$ be the finite field of order q^n.

Let

$$tr : \mathbb{F}_{q^2} \to \mathbb{F}_q$$

denote the trace function [9, Exercise 18, p. 583]. Let $\alpha \in \mathbb{F}_{q^2}$ satisfy $tr(\alpha) = 0$. Let $z \in \mathbb{F}_{q^2}$ be a generator of the multiplicative group $\mathbb{F}_{q^2}^*$. Let Q denote the set of non-zero squares in $\mathbb{F}_q$. Note that $-1 \notin Q$ since $q \equiv 3 \mod 4$.

Since $\mathrm{Gal}(\mathbb{F}_{q^2}, \mathbb{F}_q)$ is generated by the Frobenius map we see that

$$tr(\alpha) = \alpha + \alpha^q,$$

so that $\alpha^q = -\alpha$. Now choose $D \in \mathbb{F}_q \setminus (Q \cup \{0\})$. Then any $\beta \in \mathbb{F}_{q^2}$ has the form $\beta = a + b\sqrt{D}$, for some $a, b \in \mathbb{F}_q$. Now the conjugate of $\alpha = a + b\sqrt{D}$ is $a - b\sqrt{D}$ and so

$$tr(\alpha) = 0$$

if and only if $a = 0$. Thus we can choose $\alpha = \sqrt{D}$. We note that the elements α' with $\mathrm{tr}(\alpha') = 0$ are just those in $\mathbb{F}_q\alpha$.

Let $U \leq \mathbb{F}_{q^2}^*$ be the subgroup of order $(q-1)/2$, and let

$$\pi : \mathbb{F}_{q^2}^* \to W := \mathbb{F}_{q^2}^*/U$$

be the natural map. Let $g := \pi(z)$ be a generator for W and note that $|W| = 2(q+1) = 8p$. Let

$$R = \{\pi(x) : x \in \mathbb{F}_{q^2}^*, tr(\alpha x) \in Q\}.$$

Then by [27, Thm 2.2.12], R is a relative $(q+1, 2, q, (q-1)/2)$ difference set in W relative to the subgroup $H := \langle g^{4p} \rangle$ of order 2. Define $R_1, R_2 \subset W_2 := \langle g^2 \rangle$ by

$$R = R_1 + R_2 g.$$

Since R is a relative $(q+1, 2, q, (q-1)/2)$ difference set,

$$RR^{(-1)} = \frac{q-1}{2}(W - H) + q$$

from which we get

$$R_1 R_1^{(-1)} + R_2 R_2^{(-1)} = q + \frac{q-1}{2}(W_2 - H).$$

If $d \in \mathbb{F}_{q^2}^*$ has order dividing $q+1$, then $d^q = d^{-1}$ and so

$$tr(\alpha d) = \alpha d + \alpha^q d^q = \alpha d - \alpha d^{-1} = -tr(\alpha d^{-1}).$$

Thus if $\mathrm{tr}(\alpha d) \in Q$, then $\mathrm{tr}(\alpha d^{-1}) \in -Q$. But $q \equiv 3 \mod 4$ tells us that $g^{4p} = -1 \notin Q$, so that

$$tr(\alpha g^{4p} d^{-1}) \in Q.$$

Thus $g^{4p}d^{-1} \in R_1$. Now the order of $g^{4p}d^{-1}$ is a divisor of $2(q+1) = |W|$. This gives a bijection,

$$Ud \leftrightarrow Ug^{4p}d^{-1},$$

between the elements of $R_1 \subset W_2$, which then gives $R_1^{(-1)} = g^{4p}R_1$. Now let

$$G = \mathrm{Dic}_{8\mathrm{p}} = \langle a, b | a^{2p} = b^2, b^4 = 1, a^b = a^{-1} \rangle$$

and identify $\langle a \rangle$ with W_2, so that $a \leftrightarrow g^2$. To construct the SRHDS in the dicyclic group, we first need to show the following:

Lemma 4.2.2. *(i) $R_1 + 1$ is a transversal for W_2/H.*
(ii) R_2 is a transversal for W_2/H.

Proof. From $R_1^{(-1)} = g^{4p}R_1$ we see that if $\gamma \in R_1 \cap R_1^{(-1)}$, then $g^{4p} \in R_1 R_1^{(-1)}$, a contradiction to R being a relative difference set relative to H. It follows that $R_1 \cap R_1^{(-1)} = \emptyset$. Now $1, -1 = g^{4p} \notin R_1$ as $\mathrm{tr}(\alpha 1) = 0 \notin Q$, and so

$$R_1 + R_1^{(-1)} = W_2 - H. \tag{4.2}$$

Then (4.2) and $R_1^{(-1)} = g^{4p}R_1$ gives

$$W_2 - H = R_1(1 + g^{4p}) = R_1 H,$$

This proves part (i).

For part (ii), We first show that R+1 is a transversal for W/H.

If $u \in W$, then $\mathrm{tr}(\alpha u) \in Q$, and it follows that

$$tr(\alpha g^{4p} u) = -tr(\alpha u) \notin Q.$$

This sets up a bijection $u \leftrightarrow g^{4p}u$ of $W - H$ where the orbits of this bijection are the non-trivial H-cosets and a transversal corresponds to the elements of Q.

Since R+1 is a transversal for W/H and $R_1 + 1$ is a transversal for W_2/H it follows that R_2 is a transversal for W_2/H. This concludes the proof. □

Now if $\alpha = \sqrt{D}, \beta = a + b\sqrt{D}$, then $\mathrm{tr}(\alpha\beta) = 2bD \in Q$ if and only if $2b \in \mathbb{F}_q^* \setminus Q$.

Define

$$S := a^{2p}R_1 + R_2 b.$$

First we show that $SS^{(-1)} = \lambda\,(G - H) + k$ where $k = (v-2)/2, \lambda = (k-1)/2$:

$$\begin{aligned}
SS^{(-1)} &= (a^{2p}R_1 + R_2 b)(a^{2p}R_1^{(-1)} + b^{-1}R_2^{(-1)}) \\
&= R_1R_1^{(-1)} + R_2R_2^{(-1)} + R_1R_2(1 + a^{2p})b \\
&= R_1R_1^{(-1)} + R_2R_2^{(-1)} + R_1R_2Hb \\
&= R_1R_1^{(-1)} + R_2R_2^{(-1)} + R_1W_2b \\
&= q + \frac{q-1}{2}\,(W_2 - H) + |R_1|W_2b \\
&= k + \lambda\,(W_2 - H) + \lambda W_2 b \\
&= k + \lambda\,(W_2 + W_2b - H) \qquad (4.3) \\
&= \lambda\,(G - H) + k, \qquad (4.4)
\end{aligned}$$

as desired. Next we need

Lemma 4.2.3. *For S as above we have $S \cap S^{(-1)} = \emptyset$.*

Proof. Assume that

$$r \in S \cap S^{(-1)},\ S = a^{2p}R_1 + R_2 b.$$

Then there are two cases.

(a) First assume that $r \in \langle a \rangle$. Then there are $x^i, x^j \in R_1$ where $r = a^{2p}a^i = a^{2p}a^{-j}$ so we have $i = -j$. Since a corresponds to g^2 the elements g^{2i}, g^{-2j} satisfy

$$tr(\alpha g^{2i}),\ tr(\alpha g^{-2j}) \in Q.$$

Let $g^i = c + b\sqrt{D}$. Then $\mathrm{tr}(\alpha g^{2i})$, $\mathrm{tr}(\alpha g^{-2j}) \in Q$ (respectively) gives $4bcD \in Q$,

$-\frac{4bcD}{(c^2-b^2D)^2} \in Q$ (respectively), which in turn gives $-1 \in Q$, a contradiction.

(b) Next assume that $r \in \langle a \rangle b$. Then there are i, j such that

$$r = a^i b = (a^j b)^{-1} = a^{j+2p} b,$$

where $a^i, a^j \in R_2$. Thus $i = j + 2p$. As in the first case this gives

$$tr(\alpha g^{2i+1}),\ tr(\alpha g^{2j+1}) = tr(\alpha g^{2i-4p+1}) \in Q.$$

Since $\mathrm{tr}(\alpha g^{2i-4p+1}) = -\mathrm{tr}(\alpha g^{2i+1})$, this gives $-1 \in Q$, a contradiction. □

From $S \cap S^{(-1)} = \emptyset = S \cap H$ we get

$$G = S + S^{(-1)} + H$$

and so Eq. (4.4) shows that S is a SRHDS, giving Theorem 4.2.1. □

We next wish to show that we can double this example (see the next section for the definition of this doubling process), and so we need the following 'symmetry' results:

Symmetry proof for R_1.

Now $S = a^{2p} R_1 + R_2 b$ and if $a^i \in a^{2p} R_1$, then $i = 2p + j$ where $tr(\alpha z^{2j}) \in Q$.

We note that z, the generator of $\mathbb{F}_{q^2}^*$, has order $q^2 - 1$, and so $(z^q)^q = z$, showing that the non-trivial Galois automorphism is determined by $z \mapsto z^q$.

So from $tr(\alpha z^{2j}) \in Q$ we get $tr(\alpha^q z^{2jq}) \in Q$. But $\alpha^q = -\alpha = \alpha z^{(q^2-1)/2}$. Thus

$$\begin{aligned} tr(\alpha^q z^{2jq}) &= tr(\alpha z^{2jq+(q^2-1)/2}) \\ &= tr(\alpha z^{2(jq+(q^2-1)/4)}) \in Q. \end{aligned}$$

This if $j' = (jq + (q^2 - 1)/4)$, then $a^{2p+j'} \in a^{2p} R_1$, and so $j \mapsto j'$ determines a function

$R_1 \to R_1$ that we show is an involution. If $j \mapsto j' \mapsto j''$, then

$$\begin{aligned} j'' &= j'q + (q^2-1)/4 \\ &= (jq + (q^2-1)/4)q + (q^2-1)/4 \\ &= jq^2 + (q^3-q)/4 + (q^2-1)/4 \\ &= j + (q^2-1)(j + (q+1)/4) \\ &= j + (q^2-1)(j+p). \end{aligned}$$

Thus $z^{j''} = z^j$ since $z^{q^2-1} = 1$.

One can then check that $j = p + r$ is sent to $j' = p - r$ (recalling that j is defined mod $4p$). This gives a 'reflective' symmetry for R_1. We note this result for later.

$$a^j = a^{p+r} \in R_1 \implies a^{j'} = a^{p-r} \in R_1. \tag{4.5}$$

Symmetry proof for R_2. We now do a similar thing for R_2. Let $a^i b \in R_2 b$, so that $tr(\alpha z^{2i+1}) \in Q$. Then acting by the Galois automorphism we get

$$\begin{aligned} tr(\alpha^q z^{(2i+1)q}) &= tr(\alpha z^{(2i+1)q + (q^2-1)/2}) \\ &= tr(\alpha z^{2(iq + (q^2-1)/4 + (2p-1)) + 1}) \in Q. \end{aligned}$$

This similarly gives the involutive map

$$i \mapsto iq + (q^2-1)/4 + (2p-1) \equiv -i - 1 \mod 4p. \quad \square$$

So we have

$$a^i \in R_2 \implies a^{-i-1} \in R_2. \tag{4.6}$$

Using the results of the next section, these symmetry results will show that we can apply the doubling process to the Schmidt construction given in Theorem 4.2.1.

4.3 The Doubling Process

Let $G = \mathrm{Dic}_v = \langle x, y \rangle$, $v = 4n$, so that $k = 2n-1, \lambda = n-1$.

We denote $K = \langle x \rangle$ and put

$$D = D_1 + D_2 y, D_i \subset K, k_i = |D_i|.$$

Then $k_1 = n - 1, k_2 = n$ and $D_1 \cup \{1\}$ and D_2 are transversal for K/H (this comes from looking at $G - H = D + D^{(-1)} = D_1 + D_2 y + (D_1^{(-1)} + (D_2 y)^{(-1)})$).

We also have (from $DD^{(-1)} = \lambda(G - H) + k$)

$$(i)\ \ \lambda D_1 H + k = D_1 D_1^{(-1)} + D_2 D_2^{(-1)},$$

$$(ii)\ \ \lambda K y = D_2 D_1 y + D_1 D_2 y^{-1}.$$

Also $D_1^{(-1)} = tD_1$ and $D_i^y = D_i^{(-1)}$.

Now (ii) is equivalent to $D_1 D_2(1 + t) = \lambda K$ or $D_1 K = \lambda K$. But $D_1 K = \lambda K$ follows directly from $D_i \subset K$, and $|D_1| = \lambda$.

Thus (i) and (ii) are equivalent to

$$\lambda D_1 H + k = D_1 D_1^{(-1)} + D_2 D_2^{(-1)}.$$

So we have

Lemma 4.3.1. *The requirement that $D = D_1 + D_2 y$ is a SRHDS is equivalent to*

$$(a)\ \ D_1 H = K - H,$$

$$(b)\ \ D_1^{(-1)} = tD_1,$$

$$(c)\ \ D_2 H = K,$$

$$(d)\ \ \lambda(K - H) + k = D_1 D_1^{(-1)} + D_2 D_2^{(-1)}.$$ □

Now

$$\mathrm{Dic}_{16\mathrm{p}} = \langle x, y \mid x^{8p} = y^4 = 1, x^y = x^{-1} \rangle,\ t = y^2.$$

We let

$$\mathrm{Dic}_{8\mathrm{p}} = \langle x^2, y \rangle \leq \mathrm{Dic}_{16\mathrm{p}}.$$

Let D be a (v_1, k_1, λ_1)-SRHDS in $\mathrm{Dic}_{8\mathrm{p}}$, so $v_1 = 8p$, $k_1 = 4p - 1$, and $\lambda_1 = 2p - 1$. We note that the t in $\mathrm{Dic}_{16\mathrm{p}}$ is the same as the t in $\mathrm{Dic}_{8\mathrm{p}}$. Write $D = D_0 + D_1 y$. We construct the

set $E \subseteq \mathrm{Dic}_{16\mathrm{p}}$ as

$$E := E_0 + E_1 y$$

with

$$E_0 := D_0 + D_1 x \quad \text{and} \quad E_1 := D_1^{(-1)} x^{-1} t + D_0^{(-1)} + 1.$$

We show that if D_1 satisfies the symmetry: $x^{2i} \in D_1$ implies $x^{4p-2i-2} \in D_1$, then E is a (v_2, k_2, λ_2)-SRHDS with

$$v_2 = 16p,\ k_2 = 8p - 1,\ \lambda_2 = 4p - 1.$$

Theorem 4.3.2. *The set E as defined above is an SRHDS if $D = D_0 + D_1 y$ is an SRHDS in $\mathrm{Dic}_{8\mathrm{p}}$ and $x^{2i} \in D_1$ implies $x^{4p-2i-2} \in D_1$.*

Proof. We note that $D^{(-1)} = tD$ implies that $E^{(-1)} = tE$. We also observe that the map $x^{2i} \to x^{4p-2i-2}$ is an involution. Using Lemma 4.3.1, to show E is a SRHDS it suffices to show that E satisfies

(1) $E \cup E^{(-1)} = \mathrm{Dic}_{16\mathrm{p}} - \langle \mathrm{t} \rangle$;

(2) $E \cap E^{(-1)} = \emptyset$;

(3) $E_0 E_0^{(-1)} + E_1 E_1^{(-1)} = \lambda_2(\langle x \rangle - \langle t \rangle) + k_2$.

They are sufficient because conditions (1) and (2) along with $E^{(-1)} = tE$ imply conditions (a) and (c) of Lemma 4.3.1.

First we note that E does not contain t or the identity, as this would imply D_0 contains these. We now show (2), which will imply (1). We split condition (2) by considering the intersection of E with each of the cosets of $\langle x^2 \rangle$, all of which cosets are their own inverses. There are four such cosets: $\langle x^2 \rangle, \langle x^2 \rangle x, \langle x^2 \rangle y$, and $\langle x^2 \rangle xy$.

$\langle x^2 \rangle$: For $E \cap \langle x^2 \rangle = D_0$, we know that $x^{2i} \in D_0$ implies $x^{-2i} \notin D_0$ since $D_0 \cap D_0^{(-1)} = \emptyset$.

$\langle x^2\rangle x$: We have $E \cap \langle x^2\rangle x = D_1 x$. We show $D_1 x \cap (D_1 x)^{(-1)} = \emptyset$.

$$\begin{aligned} x^{2i+1} \in D_1 x &\iff x^{2i} \in D_1 \\ &\iff x^{4p-2i-2} \in D_1 \\ &\iff x^{4p-2i-2} y \in D_1 y \\ &\iff t x^{4p-2i-2} y \notin D_1 y \qquad (4.7) \\ &\iff x^{-2i-2} \notin D_1 \qquad (4.8) \\ &\iff x^{-2i-1} \notin D_1 x. \qquad (4.9) \end{aligned}$$

Here we used the symmetry and the fact that $(D_1 y) \cap (D_1 y)^{(-1)} = \emptyset$ where $(D_1 y)^{(-1)} = t D_1 y$.

$\langle x^2\rangle y$: Here we have $E \cap \langle x^2\rangle y = D_0^{(-1)} y + y$. First we check that $D_0^{(-1)} y$ doesn't contain any of its inverses:

$$x^{-2i} y \in D_0^{(-1)} y \iff (x^{-2i} y)^{-1} = t x^{-2i} y \notin D_0^{(-1)} y.$$

We also check the additional y doesn't have an inverse in $D_0^{(-1)} y$:

$$t \notin D_0^{(-1)} \iff y^{-1} = ty \notin D_0^{(-1)} y.$$

$\langle x^2\rangle xy$: Here we have $E \cap \langle x^2\rangle xy = D_1^{(-1)} x^{-1} ty$, and

$$\begin{aligned} x^{-2i-1} ty \in D_1^{(-1)} x^{-1} ty &\iff x^{2i} \in D_1 \\ &\iff t x^{2i} \notin D_1 \\ &\iff t x^{-2i} \notin D_1^{(-1)} \\ &\iff x^{-2i-1} y = t x^{-2i} x^{-1} ty \notin D_1^{(-1)} x^{-1} ty. \end{aligned}$$

Thus $E \cap E^{(-1)} = \emptyset$. This concludes (2) and implies (1), since both E and $E^{(-1)}$ don't intersect $\langle t\rangle$ and $|E| = k_2 = 8p - 1$.

Now we prove (3): we have

$$\begin{aligned} E_0E_0^{(-1)} + E_1E_1^{(-1)} &= (D_0 + D_1x)\left(D_0^{(-1)} + D_1^{(-1)}x^{-1}\right) \\ &\quad + \left(D_1^{(-1)}x^{-1}t + D_0^{(-1)} + 1\right)(D_1xt + D_0 + 1) \\ &= 2D_0D_0^{(-1)} + 2D_1D_1^{(-1)} \\ &\quad + (1+t)D_0D_1^{(-1)}x^{-1} + (1+t)D_1D_0^{(-1)}x \\ &\quad + D_1xt + D_0 + D_1^{(-1)}x^{-1}t + D_0^{(-1)} + 1. \end{aligned} \tag{4.10}$$

For E to be a SRHDS we need (4.10) to be equal to $\lambda_2(\langle x\rangle - \langle t\rangle) + k_2$. Looking at just the even powers of x, we need

$$2D_0D_0^{(-1)} + 2D_1D_1^{(-1)} + D_0 + D_0^{(-1)} + 1$$

to be equal to $\lambda_2(\langle x^2\rangle - \langle t\rangle) + k_2$. We note that

$$D_0 + D_0^{(-1)} = \langle x^2\rangle - \langle t\rangle,$$

and

$$D_0D_0^{(-1)} + D_1D_1^{(-1)} = \lambda_1(\langle x^2\rangle - \langle t\rangle) + k_1$$

since D is a SRHDS for $\langle x^2, y\rangle$. Since $\frac{k_2-1}{2} = \lambda_2$, we have

$$\begin{aligned} &2(D_0D_0^{(-1)} + D_1D_1^{(-1)}) + (D_0 + D_0^{(-1)}) + 1 \\ &\quad = 2(\lambda_1(\langle x^2\rangle - \langle t\rangle) + k_1) + (\langle x^2\rangle - \langle t\rangle) + 1 \\ &\quad = (2\lambda_1 + 1)(\langle x^2\rangle - \langle t\rangle) + (2k_1 + 1) \\ &\quad = \lambda_2(\langle x^2\rangle - \langle t\rangle) + k_2, \end{aligned}$$

as desired. We now look at the odd powers of x in (4.10), which must equal $\lambda_2\langle x^2\rangle x$. We see that

$$\begin{aligned} &(1+t)D_0D_1^{(-1)}x^{-1} + (1+t)D_1D_0^{(-1)}x + D_1xt + D_1^{(-1)}x^{-1}t \\ &\quad = (1+t)\,(D_0+1)\,D_1^{(-1)}x^{-1} + (1+t)\,(D_0+1)^{(-1)}\,D_1x \\ &\qquad - (D_1x)^{(-1)} + D_1x. \end{aligned} \tag{4.11}$$

Looking at the first two terms of (4.11), $D_0 + 1$ is a transversal of $\langle t \rangle$ in $\langle x^2 \rangle$, so

$$(1 + t)(D_0 + 1) = \langle x^2 \rangle$$

and

$$(1 + t)(D_0 + 1)^{(-1)} = \langle x^2 \rangle.$$

So we can reduce (4.11) to

$$\langle x^2 \rangle D_1^{(-1)} x^{-1} + \langle x^2 \rangle D_1 x - (D_1 x)^{(-1)} + D_1 x.$$

To evaluate the last two terms of (4.11), we note that (4.7) gives us: if $x^{2i} \in D_1$, then $x^{-2i-2} \notin D_1$. Thus D_1 and $(D_1 x^2)^{(-1)}$ are disjoint, so their sum is $\langle x^2 \rangle$ since $|D_1| = 4p$. Thus

$$(D_1 x)^{(-1)} + D_1 x = \left(\left(D_1 x^{-2} \right)^{(-1)} + D_1 \right) x = \langle x^2 \rangle x.$$

So the sum of the odd powered terms is

$$\begin{aligned} \langle x^2 \rangle (D_1)^{(-1)} x^{-1} + \langle x^2 \rangle D_1 x - \langle x^2 \rangle x &= D_1^{(-1)} \langle x^2 \rangle x^{-1} + (D_1 - 1) \langle x^2 \rangle x \\ &= |D_1| \langle x^2 \rangle x + (|D_1| - 1) \langle x^2 \rangle x \\ &= \lambda_2 \langle x^2 \rangle x \end{aligned}$$

as desired. Therefore we have shown (3), and E is a SRHDS. □

Corollary 4.3.3. *The set $E = E_0 + E_1 y$ as defined above is an SRHDS in* $\mathrm{Dic}_{16\mathrm{p}}$ *if $D = D_0 + D_1 y$ is an SRHDS in* $\mathrm{Dic}_{8\mathrm{p}}$ *and $x^{2i} \in D_1$ implies $x^{-2i-2} \in D_1$.*

Proof. This follows by applying the automorphism $\varphi(x) = x, \varphi(y) = x^{2p} y$ to $\mathrm{Dic}_{16\mathrm{p}}$ in the preceding theorem. We have that D is a SRHDS for $\mathrm{Dic}_{8\mathrm{p}}$ if and only if $\varphi(D)$ is, and similarly E is a SRHDS for $\mathrm{Dic}_{16\mathrm{p}}$ if and only if $\varphi(E)$ is. The condition $x^{2i} \in \varphi(D_1)$ implies $x^{-2i-2} \in \varphi(D_1)$ is equivalent to the condition $x^{2i} \in D_1$ implies $x^{4p-2i-2} \in D_1$. □

Many other equivalent symmetries can be obtained by using a different automorphism that fixes $\langle x \rangle$. The one we have used is that obtained at the end of Theorem 4.2.1). In the SRHDS $S = a^{2p} R_1 + R_2 b$ of $\mathrm{Dic}_{8\mathrm{p}}$ from Theorem 4.2.1, we showed that $a^i \in R_2$ implies $a^{-i-1} \in R_2$ (See (4.6)). As a subgroup of $\mathrm{Dic}_{16\mathrm{p}}$, this is the necessary symmetry condition

for Corollary 4.3.3 to apply. Thus $\mathrm{Dic}_{16\mathrm{p}}$ is a SRHDS group when $4p-1$ is a prime power. This proves Theorem 1.0.4. □

Chapter 5. Identifying SRHDS and non-SRHDS groups

5.1 D and cosets of Q_8

Let G be a SRHDS group with subgroup H and difference set D. Suppose that $Q \leq G$ has even order and that $g_0 = 1, \cdots, g_{p-1}$ is a transversal for $Q \leq G$. Then we can write

$$D = F_0 g_0 + F_1 g_1 + \cdots + F_{p-1} g_{p-1}, \quad F_i \subset Q. \tag{5.1}$$

Lemma 5.1.1. *Let $Q \leq G$ be as above. For all subsets $F \subseteq Q$ of size greater than $|Q|/2$, the multiplicity of t in $FF^{(-1)}$ is greater than zero.*

Proof. We have $t \in Q$, so $H \leq Q$ and if $|F| > |Q|/2$, then some coset of $H \leq Q$ meets F in two elements and so $t \in FF^{(-1)}$. □

Now $DD^{(-1)} = \lambda(G - H) + k$ and a part of the left hand side is $\sum_{i=0}^{p-1} F_i F_i^{(-1)}$. Thus $|F_i| \leq |Q|/2$ when D is written as in Eq. (5.1).

Now let $f_i = |F_i|, 0 \leq i < p - 1$, so that

$$\begin{aligned} \sum_{i=0}^{p-1} f_i = |D| = k &= \frac{(|G| - 2)}{2} \\ &= \frac{(|Q|p - 2)}{2} = \frac{|Q|}{2} p - 1. \end{aligned}$$

Since $f_i \leq |Q|/2$ we must have $f_i = |Q|/2$ for all $0 \leq i \leq p - 1$ except one. To see that $f_0 = |Q|/2 - 1$ we just note that $Q - H$ has $|Q| - 2$ elements that come in inverse pairs. Thus $f_0 = |Q|/2 - 1$.

Next note that $DD^{(-1)} = \lambda(G - H) + k$ and $F_i F_i^{(-1)} \subseteq Q$. We want to show

$$\sum_{i=0}^{p-1} F_i F_i^{(-1)} = \lambda(Q - H) + k. \tag{5.2}$$

Now, $v = 8p, k = \frac{|Q|}{2} p - 1, \lambda = \frac{|Q|}{4} p - 1$ and so $\lambda(Q - H) + k$ has

$$\left(\frac{|Q|}{4} p - 1 \right) (|Q| - 2) + \left(\frac{|Q|}{2} p - 1 \right) = \frac{|Q|^2}{4} p - |Q| + 1$$

elements, while $\sum_{i=0}^{p-1} F_i F_i^{(-1)}$ has

$$\left(\frac{|Q|}{2}-1\right)^2+(p-1)\left(\frac{|Q|}{2}\right)^2=\frac{|Q|^2}{4}p-|Q|+1$$

elements, so we must have Eq. (5.2).

For $Q=Q_8$, considering those F_i of size $|Q|/2=4$ a Magma [21] calculation gives the following result by finding all those subsets $F\subset Q_8$ such that $FF^{(-1)}$ does not contain t:

Lemma 5.1.2. *Suppose that $Q=Q_8\leq G$. Then each F_i of size 4 is one of the following 16 sets:*

$$\{1,x,y,xy\};\quad \{1,x,y,x^3y\};\quad \{x,x^2,x^2y,x^3y\};\quad \{1,x,x^2y,x^3y\};$$
$$\{1,x^3,x^2y,x^3y\};\quad \{1,x^3,y,xy\};\quad \{x,x^2,y,x^3y\};\quad \{x^2,x^3,y,x^3y\};$$
$$\{x,x^2,xy,x^2y\};\quad \{x^2,x^3,xy,x^2y\};\quad \{x^2,x^3,y,xy\};\quad \{1,x,xy,x^2y\};$$
$$\{x,x^2,y,x^2y\};\quad \{x^2,x^3,x^2y,x^3y\};\quad \{1,x,xy,x^2y\};\quad \{1,x^3,y,x^3y\}.$$

□

Each of these is a relative difference set for Q_8. Thus each $F_i, i>0$, is a relative difference set for Q_8. It follows then from Eq. (5.2) that F_0 is a SRHDS for Q_8. Thus F_0 is determined by

Lemma 5.1.3. *The following sets are equal:*

(i) The set of all SRHDS for $Q_8=\langle i,j,k\rangle$.

(ii) The set of all conjugate (by elements of Q_8)-translates (by elements of H) of $\{i,j,k\}$.

(iii) The set of all $\{a,b,c\}\subset Q_8\setminus H$ where $|\{a,b,c\}|=3$ and $t\notin\{uv^{-1}:u,v\in\{a,b,c\}\}$.

□

Call this common set $\mathcal{S}$ and note that $|\mathcal{S}|=8$.

Now any F_0 must satisfy (iii), so $F_0\in\mathcal{S}$. Further, we can choose F_0 to be any element of $\mathcal{S}$ by applying the operations in (ii) to D, which still result in a SRHDS.

Assume that $G=\mathrm{Dic}_{8\mathrm{p}}$ so that a transversal of $Q_8\leq G$ is $1,x,\cdots,x^{p-1}$. Now we can write

$$D=F_0+F_1x+F_2x^2+\cdots+F_{p-1}x^{p-1}$$

where $F_i \subset Q_8$ and $F_0 \in \mathcal{S}$.

Here each $F_i, i > 0$, is one of the 16 subsets of Q_8 in Lemma 5.1.2 and

$$F_i = (1 + x^p)(a + by) = a + by + x^p a + x^p by, \text{ where } a, b \in \langle x^p \rangle.$$

Now $D^{(-1)}t = D$ and so if $F_i x^i \subset D$, then $t(F_i x^i)^{(-1)} = tx^{-i} F_i^{(-1)} \subset D$. Here

$$F_i^{(-1)} = a^{-1} + bty + x^{-p}a^{-1} + x^p bty,$$

and so

$$\begin{aligned} t(F_i x^i)^{(-1)} &= tx^{-1} F_i^{(-1)} \\ &= tx^{-i}(a^{-1} + bty + x^{-p}a^{-1} + x^p bty) \\ &= ta^{-1}x^{-i} + tx^{-p}a^{-1}x^{-i} + byx^i + x^p byx^i. \end{aligned}$$

Thus F_i and $t(F_i x^i)^{(-1)}$ have $byx^i + x^p byx^i$ in common and so

$$F_i x^i \cup t(F_i x^i)^{(-1)} = ax^i + byx^i + x^p ax^i + x^p byx^i + ta^{-1}x^{-i} + tx^{-p}a^{-1}x^{-i}.$$

We denote this by $J_i(a, b)$, so that D is a union of D_0 and some of the $J_i(a, b)$.

Now $J_i(a, b)$ has four elements in $Q_8 x^i$ and has two elements in $Q_8 x^{-i}$. Since we know that each non-trivial coset of Q_8 has to contain four elements of D we know that D has to contain some $J_{-i}(c, d)$ so that

$$(a + x^p a)x^i + (a^{-1} + x^{-p}a^{-1})tx^{-i} = (c + x^p c)x^{-i} + (b^{-1} + x^{-p}b^{-1})tx^i.$$

This is true if and only if we have

$$a + x^p a = b^{-1}t + x^{-p}b^{-1}t \text{ and } (a^{-1} + x^{-p}a^{-1})t = b + x^p b.$$

However these equations are equivalent and we note that for any choice of $a \in \langle x^p \rangle$ there is a $b \in \langle x^p \rangle$ that solves the first equation.

Thus we now obtain eight element sets by taking the union of these two $J's$. We denote these by $L_i(a, b, c)$:

$$\begin{aligned} &(a + x^p a)x^i + (a^{-1} + x^{-p}a^{-1})tx^{-i} + (by + x^p by)x^i + (cy + x^p cy)x^{-i} \\ &= (1 + x^p)(a + by)x^i + (1 + x^p)(x^p a^{-1} + cy)x^{-i}. \end{aligned}$$

We note that $L_i(a,b,c) = L_j(a',b',c')$ if and only if $i = j, a = a', b = b', c = c'$. For $1 \leq i \leq p-1$ let

$$\mathcal{L}_i = \{L_i(a,b,c) : a,b,c \in \langle x^p \rangle\}.$$

Then $|\mathcal{L}_i| = 64$.

5.2 Groups that are not SRHDS groups

Proposition 5.2.1. *The dicyclic group* Dic_{72} *is not a SRHDS group.*

Proof. Suppose it is and that D is the SRHDS. Let

$$G = \mathrm{Dic}_{72} = \langle x, y | x^{36} = y^4 = 1, y^2 = x^{18}, x^y = x^{-1} \rangle.$$

Then by the above section there are $D_i \in \mathcal{L}_i, 1 \leq i \leq 4$, such that

$$D = D_0 + \sum_{i=1}^{4} D_i.$$

There are $64 = |L_i|$ choices for each $D_i, 1 \leq i \leq 4$. Using the standard irreducible representation $\rho : \mathrm{Dic}_{72} \to \mathrm{GL}(2,\mathbb{C})$ given by

$$\rho(x) = \begin{bmatrix} \zeta_{36} & 0 \\ 0 & \zeta_{36}^{-1} \end{bmatrix}, \rho(y) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \zeta_{36} = e^{2\pi i/36},$$

we have $\rho(G) = \rho(H) = 0$. From $D + D^{(-1)} = G - H$ we then have $\rho(D) + \rho(D^{(-1)}) = 0$. By $DD^{(-1)} = \lambda(G - H) + k$ we have $\rho(D)\rho(D^{(-1)}) = kI_2 = 35I_2$. Therefore,

$$35I_2 = \rho(D)\rho(D^{(-1)}) = -\rho(D)^2.$$

A Magma calculation determines that of the 64^4 possibilites for D, only 648 have $\rho(D)^2 = -35I_2$. Another Magma [2] calculation verifies that none of these 648 give a SRHDS, completing the proof. □

Proposition 5.2.2. *Let* G *be a group where* $Q_8 \leq G$. *Suppose that there is an epimorphism* $\pi : G \to \mathcal{C}_p \times Q_8$ *for* p *prime where* $\pi(Q_8) = \{1\} \times Q_8$ *and* $|\ker \pi|$ *is odd. Then* G *is not a SRHDS group.*

Proof. Suppose that G is a SRHDS group with difference set D and subgroup $H = \langle t \rangle$. Let

$$Q_8 = \langle x, y | x^4, x^2 = y^2, x^y = x^{-1} \rangle \leq G,$$

so that

$$t = x^2, \pi(x) = x, \pi(y) = y.$$

First note that p must be odd since G has a unique involution. Let $N = \ker \pi$. Put $\mathcal{C}_p = \langle \pi(r) \rangle, r \in G$, so that we can write

$$D = \sum_{i=0}^{p-1} \sum_{j=0}^{3} r^i x^j D_{0,i,j} + \sum_{i=0}^{p-1} \sum_{j=0}^{3} r^i x^j y D_{1,i,j}, \quad D_{k,i,j} \subset N.$$

We note that $|D_{i,j,k}| \leq |N|$.

Let $p_2 = (p-1)/2$. We can also write $D = \sum_{i=0}^{p-1} r^i D_i, D_i \subset \langle x, y, N \rangle$ so that

$$D_i = \sum_{j=0}^{3} x^j D_{0,i,j} + \sum_{j=0}^{3} x^j y D_{1,i,j}.$$

From $D^{(-1)} = tD$ we get

$$D_i^{(-1)} r^{-i} = t r^{p-i} D_{p-i}, \ 0 \leq i < p,$$

so that $D_{p-i} = t r^{-p} (D_i^{(-1)})^{r^{-i}}$. Thus

$$D = D_0 + \sum_{i=1}^{p_2} r^i D_i + r^{-i} t (D_i^{(-1)})^{r^{-i}}.$$

Now let $\rho : Q_8 \to \mathrm{GL}(2, \mathbb{Q}(i))$, $i = \sqrt{-1}$, be an irreducible faithful unitary representation of Q_8 where

$$\rho(x) = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \ \rho(y) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Then the $\mathbb{Q}$-span of the image of ρ has basis

$$B_1 = I_2, \ B_2 = \rho(x) = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \ B_3 = \rho(y) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \ B_4 = \rho(xy) = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

since $\rho(x^2) = -B_1$. We note from Lemma 5.1.3 that we may assume $D_0 = \{x, y, xy\}$, so

$$\rho(D_0) = \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} = B_2 + B_3 + B_4.$$

Let $\omega = \exp 2\pi i/p$. Then π, ρ and $r \mapsto \omega I_2$ determine an irreducible unitary representation of G that we also call ρ. Then

$$\rho(r^i D_i) = \omega^i \sum_{j=1}^{4} a_{ij} B_j,$$

where $a_{ij} \in \mathbb{Z}$, so that

$$\begin{aligned} \rho(r^{-i} t (D_i^{(-1)})^{r^{-i}}) &= -\omega^{-i} \rho(D_i^{(-1)})^{r^{-i}}) \\ &= -\omega^{-i} \rho(D_i^{(-1)}) \\ &= -\omega^{-i} \sum_{j=1}^{4} a_{ij} B_j^*. \end{aligned}$$

Here

$$B_1^* = B_1, B_2^* = -B_2, B_3^* = -B_3, B_4^* = -B_4.$$

This gives

$$\begin{aligned} \rho(D) &= \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} + \sum_{i=1}^{p_2} \rho(D_i r^i + r^{-i} t (D_i^{(-1)})^{r^{-i}}) \\ &= \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} + \sum_{i=1}^{p_2} \sum_{j=1}^{4} (a_{ij} B_j \omega^i - a_{ij} B_j^* \omega^{-i}). \end{aligned} \tag{5.3}$$

We can write this matrix as

$$\rho(D) = \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} + \sum_{u=1}^{4} a_u B_u, \text{ where } a_u \in \mathbb{Z}[\omega]. \tag{5.4}$$

From $DD^{(-1)} = \lambda(G - H) + k$ and $D^{(-1)} = tD$ we get $D^2 = \lambda(G - H) + kt$. Now if $\rho(D)^2 = (e_{ij})$, then from

$$(e_{ij}) = \rho(D^2) = \rho(\lambda(G - H) + tk) = -kI_2$$

and Eq. (5.4) we get

$$0 = e_{11} - e_{22} = 4ia_1(1 + a_2), \;\; 0 = e_{12} = 2a_1(i + 1 + a_3 + ia_4),$$

$$0 = e_{21} = 2a_1(-1 + i - a_3 + ia_4).$$

Solving, we must have either

$$(i) \;\; a_1 = 0; \text{ or}$$

$$(ii) \;\; a_2 = -1, \;\; a_3 = -1, \;\; a_4 = -1.$$

Now we find $a_1, \cdots, a_4$ in terms of the a_{ij}. From (5.3) and (5.4) we have

$$\begin{aligned}\sum_{u=1}^{4} a_u B_u &= \sum_{i=1}^{p_2}\sum_{j=1}^{4} a_{ij}B_j\omega^i - a_{ij}B_j^*\omega^{-i} \\ &= \sum_{i=1}^{p_2} a_{i1}B_1\omega^i - a_{i1}B_1\omega^{-i} + a_{i2}B_2\omega^i + a_{i2}B_2\omega^{-i} \\ &\quad + a_{i3}B_3\omega^i + a_{i3}B_3\omega^{-i} + a_{i4}B_4\omega^i + a_{i4}B_4\omega^{-i}.\end{aligned}$$

From this we get

$$\begin{aligned} a_1 &= \sum_{i=1}^{p_2} a_{i1}(\omega^i - \omega^{-i}); \quad a_2 = \sum_{i=1}^{p_2} a_{i2}(\omega^i + \omega^{-i}); \\ a_3 &= \sum_{i=1}^{p_2} a_{i3}(\omega^i + \omega^{-i}); \quad a_4 = \sum_{i=1}^{p_2} a_{i4}(\omega^i + \omega^{-i}).\end{aligned}$$

Now if we have (i) $a_1 = 0$, then the fact that $p > 2$ is a prime means that the $\omega^i - \omega^{-i}, i = 1, 2, \cdots, p_2$ are linearly independent over $\mathbb{Q}$, so that we must than have $a_{i1} = 0$ for all i.

Observe from previous definitions that $a_{i1} = |D_{0,i,0}| - |D_{0,i,2}|$. From $D^{(-1)} = tD$ and $D \cup D^{(-1)} = G - \langle t \rangle$ we have

$$|D_{0,i,0}| + |D_{0,i,2}| = |N|.$$

So

$$|D_{0,i,0}| = |D_{0,i,2}| = |N|/2.$$

Thus $|N|$ is even, which contradicts our assumption on $\ker \pi$.

So now assume (ii), so that

$$\begin{aligned}\rho(D) &= \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} + \sum_{i=1}^{4} a_i B_i \\ &= \begin{bmatrix} i & -i-1 \\ 1-1 & -i \end{bmatrix} + a_1 B_1 - B_2 - B_3 - B_4 \\ &= a_1 I_2.\end{aligned}$$

But

$$-\rho(D^2) = \rho(DD^{(-1)}) = kI_2$$

then gives $a_1^2 = -k$. Here $a_1 \in \mathbb{Q}[\omega]$. Recall that $\omega = e^{\frac{2\pi i}{p}}$, so the Galois group of $[\mathbb{Q}(\omega) : \mathbb{Q}]$ is cyclic of even order $p-1$. By the Galois correspondence, $\mathbb{Q}(\omega)$ has a unique quadratic subfield. In particular, we can verify that the subfield is exactly $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod 4$, and $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod 4$. This follows from the Gauss sum:

$$\left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \omega^n\right)^2 = (-1)^{\frac{p-1}{2}} p$$

Note that $k \equiv 3 \pmod 4$ so k is not an integer square. Therefore $a_1^2 = -k$ implies $k = px^2$ for some $x \in \mathbb{Z}$. However, $k = 4p|N| - 1$ so we have a contradiction, as k must be congruent to both 0 and $-1 \pmod p$. □

5.3 Groups of order less than or equal to 72

Here is the list of non-dicyclic groups (using the magma notation) of order less than or equal to 72 that meet the following requirements:

(i) they are not abelian;

(ii) the Sylow 2-subgroups are generalized quaternion groups;

(iii) they have a single involution.

$$G_{24,3}, \quad G_{24,11}, \quad G_{40,11}, \quad G_{48,18}, \quad G_{48,27}, \quad G_{48,28}, \quad G_{72,3},$$
$$G_{72,11}, \quad G_{72,24}, \quad G_{72,25}, \quad G_{72,26}, \quad G_{72,31}, \quad G_{72,38}.$$

We note that all of the dicyclic groups of order less than 72 and divisible by 8 are SRHDS groups by Theorems 1.0.3 and 1.0.4, while Dic_{72} is not by Proposition 5.2.1.

We will determine whether the remaining groups have a SRHDS. If they have a SRHDS then we give a SRHDS explicitly. If not, then we give a proof that the group is not a SRHDS group.

Remark 5.3.1. *In the cases of $G_{72,3}$, $G_{72,11}$, $G_{72,24}$, $G_{72,25}$, and $G_{72,31}$, we use the following process to show they are not SRHDS groups: Given one of the five groups G, we take a right transversal $g_0 = 1, \ldots, g_8$ for $Q_8 \leq G$. Assuming there is an SRHDS D, we write D as in (5.1). We can assume $F_0 = \{x, y, xy\}$ by Lemma 5.1.3. By Lemma 5.1.2, there are 16 possibilities for each F_i, and a Magma [2] calculation verifies that none of these combinations give a SRHDS.*

(1) $G_{24,3} = \mathrm{SL}(2,3) = \langle a, b, c, d | a^3 = 1, b^2 = d, c^2 = d, d^2, b^a = c, c^a = bc, c^b = cd \rangle$. Here $D = \{a^2cd, abcd, acd, cd, a^2bd, a^2d, a^2bc, a, bc, ab, b\}$.

(2) $G_{24,11} = \mathcal{C}_3 \times Q_8$. This is not a SRHDS group by Proposition 5.2.2.

(3) $G_{40,11} = \mathcal{C}_5 \times Q_8$. This is not a SRHDS group by Proposition 5.2.2.

(4) $G_{48,18} = \mathcal{C}_3 \rtimes \mathrm{Dic}_{16} = \langle a, b, c, d, e | d^2 = e^3 = 1, a^2 = b^2 = c^2 = d, b^a = bc, c^a = c^b = cd, d^a = d^b = d^c = d, e^a = e^2, e^b = e^c = e^d = e \rangle$ and let D be

$$\{ade^2, de^2, ae, e, abce^2, abc, bce^2, abde^2, bde^2, bce, acd, acde^2, abd,$$
$$cde^2, cd, acde, cde, bde, bcd, a, abcde, b, abe\}.$$

(5) $G_{48,27} = \mathcal{C}_3 \times \mathrm{Dic}_{16}$. We show $G_{48,27}$ is not a SRHDS group. Let $\mathcal{C}_3 = \langle r \rangle$. Then $D = D_0 + D_1 r + D_2 r^2, D_i \subset \mathrm{Dic}_{16}$. Now $D^{(-1)} = tD$ gives $D_0^{(-1)} = tD_0$ and $D_2 = tD_1^{(-1)}$. Also Lemma 3.2.1 shows that the sizes of D_0, D_1, D_2 are $7, 8, 8$ (in some order). By replacing

D by r^iD if necessary we may assume that $|D_0| = 7$ and that $D_0 + 1, D_1, D_2$ are transversals for G/H. Using $D_0^{(-1)} = tD_0$ one sees that there are 64 possible D_0s and 256 possible D_1s. Further, D_2 is determined by $D_2 = tD_1^{(-1)}$. There are thus $64 \cdot 256$ possibilities for D and one checks that none of these give a SRHDS.

(6) Let $G_{48,28} = \langle a, b, c, d, e | b^3 = e^2 = 1, a^2 = c^2 = d^2 = e, b^a = b^2, c^a = d, c^b = de, d^a = c, d^b = cd, d^c = de, e^a = e^b = e^c = e^d = e \rangle$. Here one D is

$$\{ab^2de, ab^2cde, b^2cde, ce, abc, b^2c, bc, d, ade, ab^2ce, ac, ab^2, acd, cd,$$
$$b^2d, b^2e, abde, bde, bcd, a, ab, abcde, b\}.$$

(7) $G_{72,3} = Q_8 \rtimes \mathcal{C}_9 = \langle i, j, b | i^4 = j^4 = b^9 = 1, i^j = i^{-1}, i^2 = j^2, i^b = j, j^b = ij \rangle$. Remark 5.3.1 shows this is not an SRHDS group.

(8) $G_{72,11} = \mathcal{C}_9 \times Q_8$. Remark 5.3.1 shows this is not an SRHDS group.

(9) $G_{72,24} = \mathcal{C}_3^2 \rtimes Q_8 = \langle a, b, i, j | a^3 = b^3 = i^4 = j^4 = 1, ab = ba, i^j = i^{-1}, i^2 = j^2, a^i = a, b^i = b^2, a^j = a^2, b^j = b \rangle$. Remark 5.3.1 shows this is not an SRHDS group.

(10) $G_{72,25} = \mathcal{C}_3 \times SL(2,3)$. Remark 5.3.1 shows this is not an SRHDS group.

(11) $G_{72,26} = \mathcal{C}_3 \times Dic_{24}$. This is not an SRHDS group by Proposition 5.2.2.

(12) $G_{72,31} = \mathcal{C}_3^2 \rtimes Q_8 = \langle a, b, i, j | a^3 = b^3 = i^4 = j^4 = 1, ab = ba, i^j = i^{-1}, i^2 = j^2, a^i = a^2, b^i = b^2, a^j = a, b^j = b \rangle$. Remark 5.3.1 shows this is not an SRHDS group.

(13) $G_{72,38} = \mathcal{C}_3^2 \times Q_8$. This is not an SRHDS group by Proposition 5.2.2.

Chapter 6. Symmetry in doubled SRHDS dicyclic groups

6.1 Defining doubly symmetric SRDRS groups

Recall that a SRHDS is a relative difference set with additional conditions imposed. The results of this paper up to this point have looked at categorizing when these exist in a particular finite group. We will now add an additional symmetry condition present in a SRHDS constructed by the doubling process, which will allow us to completely determine which generalized quaternion groups have this type of SRHDS. Recall that $\mathrm{Dic}_{8\mathrm{p}} = \langle \mathrm{x}, \mathrm{y} \mid \mathrm{x}^{4\mathrm{p}} = \mathrm{y}^4 = 1, \mathrm{x}^{2\mathrm{p}} = \mathrm{y}^2, \mathrm{x}^{\mathrm{y}} = \mathrm{x}^{-1} \rangle$, where we denote $t = x^{2p} = y^2$.

Proposition 6.1.1. *Let D be a SRHDS in $\mathrm{Dic}_{8\mathrm{p}}$. Write $D = D_0 + D_1 y$ with $D_0, D_1 \subset \langle x \rangle \subset \mathrm{Dic}_{8\mathrm{p}}$. Then $x^i \in D_0$ if and only if $tx^{-i} \in D_0$.*

Proof. Applying Lemma 3.1.3, and knowing $D \cap D^{(-1)} = \emptyset$, we have

$$\begin{aligned} x^i \in D_0 &\iff x^{-i} \in D_0^{(-1)} \\ &\iff tx^{-i} \in tD_0^{(-1)} \\ &\iff tx^{-i} \in t^2 D_0 = D_0. \end{aligned}$$

□

This symmetry is present in all dicyclic group SRHDS. Additionally, for SRHDS constructed by the doubling process (Corollary 4.3.2), there is nearly the same symmetry in D_1.

Proposition 6.1.2. *Let E be a SRHDS in $\mathrm{Dic}_{16\mathrm{p}}$ that was constructed by the doubling process (Corollary 4.3.2). Write $E = E_0 + E_1 y$ with $E_0, E_1 \subset \langle x \rangle \leq \mathrm{Dic}_{16\mathrm{p}}$. Then $x^i \in E_1 - \{1\}$ implies $tx^{-i} \in E_1 - \{1\}$.*

Proof. Let $D = D_0 + D_1 y \subset \langle x^2, y \rangle$ be the SRHDS that was doubled to obtain E. Then by the hypothesis of the doubling process, we assume that $x^{2j} \in D_1$ implies $x^{4p-2j-2} \in D_1$, and

$$E_1 - \{1\} = D_1^{(-1)} x^{-1} t + D_0^{(-1)}.$$

Let $x^i \in E_1 - \{1\}$. Then there are two cases, depending on whether i is even or odd:

$$\begin{aligned} i = 2j &\implies x^{2j} \in D_0^{(-1)} \\ &\implies x^{-2j} \in D_0 \\ &\implies tx^{-2j} \in tD_0 = D_0^{(-1)} \\ &\implies tx^{-i} \in D_0^{(-1)}, \end{aligned}$$

and

$$\begin{aligned} i = 2j-1 &\implies x^{2j-1} \in D_1^{(-1)} x^{-1} t \\ &\implies tx^{2j} \in D_1^{(-1)} \\ &\implies x^{4p+2j} \in D_1^{(-1)} \\ &\implies x^{-4p-2j} = x^{2(-j-2p)} \in D_1 \\ &\implies x^{4p-2(-j-2p)-2} \in D_1 \\ &\implies x^{8p+2j-2} = x^{2j-2} \in D_1 \\ &\implies x^{-2j+2} \in D_1^{(-1)} \\ &\implies tx^{-2j+1} = tx^{-i} \in D_1^{(-1)} x^{-1} t. \end{aligned}$$

This concludes the proof. □

Definition 6.1.3. *We say a SRHDS $D = D_0 + D_1 y$ in* $\mathrm{Dic}_{8\mathrm{p}}$ *is* doubly symmetric *if $x^i \in D_1 - \langle t \rangle$ implies $tx^{-i} \in D_1 - \langle t \rangle$.*

Note that D_1 will contain exactly one of $\{1, t\}$.

Corollary 6.1.4. *Let $4p-1$ be a prime power. Then* $\mathrm{Dic}_{16\mathrm{p}}$ *contains a doubly symmetric SRHDS.*

Proof. We constructed an SHRDS for $\mathrm{Dic}_{16\mathrm{p}}$ using the doubling process. See Corollary 4.3.3 and the paragraph following it. By Proposition 6.1.2, this SHRDS is doubly symmetric. □

Let $\rho : \mathrm{Dic}_{8\mathrm{p}} \to \mathrm{M}_2(\mathbb{C})$ be the representation determined by

$$\rho(x) = \begin{bmatrix} \zeta_{4p} & 0 \\ 0 & \zeta_{4p}^{-1} \end{bmatrix}, \quad \rho(y) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

where $\zeta_{4p} = e^{2\pi i/4p}$. We observe that

$$\rho(x^i) = \begin{bmatrix} \zeta_{4p}^{i} & 0 \\ 0 & \zeta_{4p}^{-i} \end{bmatrix}, \quad \rho(x^i y) = \begin{bmatrix} 0 & -\zeta_{4p}^{i} \\ \zeta_{4p}^{-i} & 0 \end{bmatrix}, \quad \rho(t) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Since $\zeta^{-1} = \bar{\zeta}$ for any root of unity ζ, any sum of matrices in this representation will be of the form

$$\begin{bmatrix} d + ai & -c - bi \\ c - bi & d - ai \end{bmatrix},$$

for some $a, b, c, d \in \mathbb{R}$.

Let $D = D_0 + D_1 y$ be a SRHDS in $\mathrm{Dic}_{8\mathrm{p}}$. Then

$$\rho(D) = \begin{bmatrix} d + ai & -c - bi \\ c - bi & d - ai \end{bmatrix},$$

where $d + ai = \sum\{\zeta_{4p}^{i} \mid x^i \in D_0\}$ and $c + bi = \sum\{\zeta_{4p}^{i} \mid x^i \in D_1\}$.

Lemma 6.1.5. *With a, b, c, d as defined above, we have $d = 0$, and $a^2 + b^2 + c^2 = 4p - 1$. Additionally, if D is doubly symmetric, then $c^2 = 1$, so $a^2 + b^2 = 4p - 2$.*

Proof. By Proposition 6.1.1, we have $x^i \in D_0$ implies $tx^{-i} = x^{2p-i} \in D_0$, so the sum $d + ai = \sum\{\zeta_{4p}^{i} \mid x^i \in D_0\}$ can be written as a sum of elements of the form

$$\begin{aligned} \zeta_{4p}^{i} + \zeta_{4p}^{2p-i} &= \zeta_{4p}^{i} - \zeta_{4p}^{-i} \\ &= \zeta_{4p}^{i} - \overline{\zeta_{4p}^{i}}. \end{aligned}$$

which are pure imaginary, so we must have $d = 0$. If D is doubly symmetric, we can apply the same argument on D_1. We would have that $x^i \in D_1 - \langle t \rangle$ implies $x^{2p-i} \in D_1 - \langle t \rangle$. Thus $\sum\{\zeta_{4p}^{i} \mid x^i \in D_1 - \langle t \rangle\}$ is the sum of pure imaginary numbers, so $c + bi = \sum\{\zeta_{4p}^{i} \mid x^i \in D_1\}$ is pure imaginary except for the contribution of either 1 or t, so either $c = 1$ or $c = -1$, and

we have $c^2 = 1$. Since D is a SRHDS for $\mathrm{Dic}_{8\mathrm{p}}$, we have

$$\begin{aligned}
&DD^{(-1)} = (2p-1)(G - \langle t \rangle) + 4p - 1 \\
\implies &\rho(DD^{(-1)}) = \rho((2p-1)(G - \langle t \rangle) + 4p - 1) \\
\implies &\rho(tD^2) = (2p-1)(\rho(G - \langle t \rangle)) + (4p-1)\rho(1) \\
\implies &-\rho(D)^2 = (2p-1)(0) + (4p-1)I_2 \\
\implies &-\begin{bmatrix} ai & -c-bi \\ c-bi & -ai \end{bmatrix}^2 = (4p-1)I_2 \\
\implies &\begin{bmatrix} a^2+b^2+c^2 & 0 \\ 0 & a^2+b^2+c^2 \end{bmatrix} = (4p-1)I_2
\end{aligned}$$

where I_2 is the identity matrix. Thus we have $a^2 + b^2 + c^2 = 4p - 1$, and if $c^2 = 1$, this gives $a^2 + b^2 = 4p - 2$. □

In order to determine when the relation $a^2 + b^2 = 4p - 2$ can be achieved, we shall make use of a bounding theorem of Schmidt [28].

Definition 6.1.6. *[28, Definition 2.2.5, p. 33] Let m, n be positive integers, and let $m = \prod_{i=1}^{t} p_i^{c_i}$ be the prime power decomposition of m. For each prime divisor q of n let*

$$m_q := \begin{cases} \prod_{p_i \neq q} p_i, & \text{if } m \text{ is odd or } q = 2, \\ 4\prod_{p_i \neq 2,q} p_i, & \text{otherwise.} \end{cases}$$

Let $\mathcal{D}(n)$ be the set of prime divisors of n. We define $F(m,n) = \prod_{i=1}^{t} p_i^{b_i}$ to be the minimum multiple of $\prod_{i=1}^{t} p_i$ such that for every pair (i,q), $i \in \{1,\ldots,t\}, q \in \mathcal{D}(n)$, at least one of the following conditions is satisfied.

$$\begin{aligned}
&(a)\ q = p_i \text{ and } (p_i, b_i) \neq (2,1), \\
&(b)\ b_i = c_i, \\
&(c)\ q \neq p_i \text{ and } q^{ord_{m_q}(q)} \not\equiv 1 (\mathrm{mod}\ p_i^{b_i+1}),
\end{aligned}$$

where $ord_x(y)$ denotes the smallest positive integer k such that $y^k \equiv 1 (\mathrm{mod}\ x)$.

Theorem 6.1.7. *[28, Theorem 2.3.2 (F-bound), p. 36] Let $X \in \mathbb{Z}[\zeta_m]$ be of the form*

$$X = \sum_{i=0}^{m-1} a_i \zeta_m^i,$$

with $0 \leq a_i \leq C$ for some constant C and assume that $X\bar{X} = n \in \mathbb{Z}$. Then

$$n \leq \frac{C^2 F(m,n)^2}{4\varphi(F(m,n))},$$

where φ is the Euler totient function.

We can apply this bound to obtain:

Proposition 6.1.8. *Assume that there exists $D = D_0 + D_1 y$, a doubly symmetric SRHDS in* $\mathrm{Dic}_{8\mathrm{p}}$. *Then*

$$4p - 2 \leq \frac{F(4p, 4p-2)^2}{\varphi(F(4p, 4p-2))}.$$

Proof. Given that a doubly symmetric SRHDS exists, by Lemma 6.1.5 we have that $a^2 + b^2 = 4p - 2$ where $ai = \sum\{\zeta_{4p}^i \mid x^i \in D_0\}$ and $c + bi = \sum\{\zeta_{4p}^i \mid x^i \in D_1\}$, with $c = \pm 1$. Thus we have that $a = \sum\{\zeta_{4p}^{3p+i} \mid x^i \in D_0\}$ is a sum of distinct $4p$-th roots of unity. Since $x^i \in D_0$ implies $tx^i = x^{2p+i} \notin D_0$, exactly one of $1 = \zeta_{4p}^0$ or $-1 = \zeta_{4p}^{2p}$ is in the sum $\sum\{\zeta_{4p}^{3p+i} \mid x^i \in D_0\}$. It follows that either

$$a + bi = -c + \sum\{\zeta_{4p}^{3p+i} \mid x^i \in D_0\} + \sum\{\zeta_{4p}^i \mid x^i \in D_1\}$$

or

$$-a + bi = -c + \sum\{\zeta_{4p}^{p+i} \mid x^i \in D_0\} + \sum\{\zeta_{4p}^i \mid x^i \in D_1\}$$

can be written in the form

$$\sum_{i=0}^{4p-1} a_i \zeta_{4p}^i$$

with $0 \leq a_i \leq 2$. In either case, defining $X = \pm a + bi$ gives $X\bar{X} = a^2 + b^2 = 4p - 2$. The F-bound Theorem 6.1.7 then gives that

$$4p - 2 \leq \frac{2^2 F(4p, 4p-2)^2}{4\varphi(F(4p, 4p-2))} = \frac{F(4p, 4p-2)^2}{\varphi(F(4p, 4p-2))},$$

as desired. □

6.2 Application to generalized quaternion groups

Proposition 6.1.8 gives a means to prove that certain dicyclic groups do not contain a doubly symmetric SRHDS. We will now focus our attention on generalized quaternion groups, where $p = 2^u$ for some $u \in \mathbb{Z}_{\geq 0}$.

Lemma 6.2.1. *If the generalized quaternion group* $\mathrm{Dic}_{2^{u+3}}$*, where* $u \in \mathbb{Z}_{\geq 0}$*, has a doubly symmetric SRHDS, then* $F(2^{u+2}, 2^{u+2} - 2) = 2^l$ *where* $l \geq u + 1$*.*

Proof. We notice from condition (b) in the definition (6.1.6) of $F(m, n)$ that $F(m, n)$ divides m, so $F(2^{u+2}, 2^{u+2} - 2) = 2^l$ for some $l \in \mathbb{Z}_{>0}$. Also note that condition (a) guarantees that $l \geq 2$. By Proposition 6.1.8, we have

$$\begin{aligned} 2^{u+2} - 2 &\leq \frac{F(2^{u+2}, 2^{u+2} - 2)^2}{\varphi(F(2^{u+2}, 2^{u+2} - 2))} \\ &= \frac{(2^l)^2}{\varphi(2^l)} \\ &= \frac{2^{2l}}{2^{l-1}} \\ &= 2^{l+1}. \end{aligned}$$

Since $2 \leq l$, this implies that $u + 2 \leq l + 1$, so $l \geq u + 1$. □

This lemma motivates us to calculate $F(2^{u+2}, 2^{u+2} - 2) = 2^l$ in general. We first find that $F(4, 2) = 4$ and then consider when $u > 1$. Going through Definition 6.1.6, let $2q_1^{n_1} q_2^{n_2} \dots q_r^{n_r}$ be the prime power decomposition of $2^{u+2} - 2$. Then $m_2 = 1$ and $m_{q_i} = 4$ for each other prime q_i. We have that $ord_4(q_i) = 1$ if $q_i \equiv 1 (\mathrm{mod}\ 4)$ and $ord_4(q_i) = 2$ if $q_i \equiv 3 (\mathrm{mod}\ 4)$. Condition (a) guarantees that $l \geq 2$, and condition (b) guarantees that $l \leq u + 2$. Besides that, only condition (c) is relevant to this calculation. Either $l = u + 2$, or we have that

$$q_i^{ord_4(q_i)} \not\equiv 1 (\mathrm{mod}\ 2^{l+1}) \text{ for all } 1 \leq i \leq r.$$

Since $2^{u+2} - 2 = 2q_1^{n_1} q_2^{n_2} \dots q_r^{n_r}$, the maximum possible value a prime q_i can achieve is if $2^{u+2} - 2 = 2q_1$ in which case $q_1 = 2^{u+1} - 1$. Thus no prime factor is larger than 2^{u+1}, so we will always have

$$q_i \not\equiv 1 (\mathrm{mod}\ 2^{u+1}).$$

Thus if we assume that $l \geq u+1$, there must be some prime $q_j \equiv 3 (\text{mod } 4)$ such that

$$\begin{aligned} q_j^{ord_4(q_j)} = q_j^2 &\equiv 1 (\text{mod } 2^l) \\ &\implies q_j^2 \equiv 1 (\text{mod } 2^{u+1}) \\ &\implies q_j^2 - 1 = 2^{u+1}s \quad \text{for some } s \in \mathbb{N} \\ &\implies (q_j+1)(q_j-1) = 2^{u+1}s. \end{aligned}$$

Since $q_j - 1 \equiv 2 (\text{mod } 4)$, only one power of 2 in the product $2^{u+1}s$ can come from $q_j - 1$, so we have

$$q_j + 1 = 2^u t \quad \text{for some } t \in \mathbb{N}.$$

Since the maximum value q_j can be is $2^{u+1} - 1$, we have either $t = 1$ or $t = 2$. But, the $t = 1$ case is impossible because that would imply $q_j = 2^u - 1$ and since

$$4(2^u - 1) + 2 = 2^{u+2} - 2,$$

we would have $2^{u+2} - 2 \equiv 2 (\text{mod } q_j)$, contradicting that q_j divides $2^{u+2} - 2$. Thus the only possibilty is that $q_j = 2^{u+1} - 1$, so $2^{u+2} - 2 = 2q_j$. Therefore we have proved the following:

Lemma 6.2.2. *If $F(2^{u+2}, 2^{u+2} - 2) = 2^l$ where $l \geq u+1$, then $2^{u+2} - 2 = 2q$ where either $q = 1$ or q is an odd prime.*

Finally, we can use these lemmas to classify which generalized quaternion groups contain doubly symmetric SHRDS.

Theorem 6.2.3. *Let $G = \text{Dic}_{8 \cdot 2^u}$ be a generalized quaternion group for some $u \in \mathbb{Z}_{\geq 0}$. Then G contains a doubly symmetric SRHDS if and only if $2^{u+1} - 1$ is either prime or 1.*

Proof. If G contains a doubly symmetric SRHDS, then Lemma 6.2.1 requires that

$$F(2^{u+2}, 2^{u+2} - 2) = 2^l$$

where $l \geq u+1$. By Lemma 6.2.2, this implies $2^{u+2} - 2 = 2q$ where either $q = 1$ or q is an odd prime, so $q = 2^{u+1} - 1$ is either prime or 1. For the other implication, if $q = 1$ then $G = \text{Dic}_8$. By Theorem 1.0.3, Dic_8 contains an SHRDS, which will be trivially doubly symmetric since

$D_1 - \langle t \rangle$ is just a single element of order 4 in $\langle x \rangle \cong \mathcal{C}_4$. Otherwise, if $q = 2^{u+1} - 1$ is prime, setting $p = 2^{u-1}$ in Corollary 6.1.4 gives that $\mathrm{Dic}_{16\mathrm{p}} = \mathrm{Dic}_{8 \cdot 2^{\mathrm{u}}}$ contains a doubly symmetric SHRDS. □

As a fun consequence of the results in this chapter, we get the following number theoretic result:

Lemma 6.2.4. *If $2^{u+1} - 1$ is a prime power, then $2^{u+1} - 1$ is prime.*

Proof. If $2^{u+1} - 1$ is a prime power, Corollary 6.1.4 says that there is a doubly symmetric SRHDS in $\mathrm{Dic}_{8 \cdot 2^{\mathrm{u}}}$. Then by Theorem 6.2.3, $2^{u+1} - 1$ is a prime. □

This corollary is also a consequence of Catalan's Conjecture, which was proved in 2004 [23].

Chapter 7. Additional Schur Ring Results

7.1 Preliminaries and lemmas

We begin with preliminary definitions. Let H be a subgroup of a finite group G. Let $\mathbb{C}[G]$ denote the complex group algebra of G. An *H-class* in G is some $\{g^a \ : \ a \in H\}$. Let $\mathbb{C}[G]^H$ be the subalgebra of $\mathbb{C}[G]$ generated by the H-classes in G.

We denote by $\hat{G}$ and $\hat{H}$ the set of irreducible characters of G and H, respectively. Given $\chi \in \hat{G}$, we let χ_H be the restriction of χ to H. Then we can write χ_H as a sum of irreducible characters in $\hat{H}$ with multiplicities $c_{\chi\psi} \in \mathbb{Z}_{\geq 0}$, i.e.

$$\chi_H = \sum_{\psi \in \hat{H}} c_{\chi\psi} \cdot \psi.$$

Given $\chi \in \hat{G}$, let R_χ be the irreducible representation of G with character χ, and let V_χ be the $\mathbb{C}G$-module that R_χ acts on. Let f_χ be the dimension of V_χ. Define R_ψ, V_ψ, and f_ψ similarly for $\psi \in \hat{H}$.

Let $\mathrm{End}(V)$ be the space of endomorphisms of a $\mathbb{C}G$-module V: that is, the space of all $\mathbb{C}$-linear maps from V to V. For a $\mathbb{C}[H]$-module W, let $\mathrm{End}_{\mathrm{H}}(W)$ be the submodule of $\mathrm{End}(W)$ consisting of the endomorphisms that commute with the action of H. Specifically, $T \in \mathrm{End}_{\mathrm{H}}(W)$ if

$$T \circ R_\chi(h) = R_\chi(h) \circ T$$

for all $h \in H$.

Recall from Lemma 3.1.4 that we can construct a commutative Schur ring given an SRHDS group. The following theorem is useful in relating commutative Schur rings and the group algebra. We work towards the following result from Travis [31, Corollary 1, p. 72], with the goal of providing a more accessible proof using modern notation.

Theorem 7.1.1. *Given a subgroup H of a finite group G, we have that (G, H) is a strong*

Gelfand pair if and only if $\mathbb{C}[G]^H$, the ring of H-classes in G, forms a commutative Schur ring.

The remainder of this chapter will build up to this the proof of this theorem in Corollary 7.2.5.

Remark 7.1.2. Observe that for $h \in H$ and $\chi \in \hat{G}$,

$$\begin{aligned}\mathrm{Tr}(R_\chi(h)) &= \chi_H(h) \\ &= \sum_{\psi \in \hat{H}} c_{\chi\psi} \cdot \psi(h) \\ &= \sum_{\psi \in \hat{H}} c_{\chi\psi} \cdot \mathrm{Tr}(R_\psi(h)) \\ &= \mathrm{Tr}\left(\sum_{\psi \in \hat{H}} c_{\chi\psi} \cdot R_\psi(h) \right),\end{aligned}$$

and since representations are uniquely determined by characters, we have

$$R_\chi = \sum_{\psi \in \hat{H}} c_{\chi\psi} \cdot R_\psi.$$

Taking the spaces these representations act on, we get

$$V_\chi = \bigoplus_{\psi \in \hat{H}} c_{\chi\psi} \cdot V_\psi,$$

where $c_{\chi\psi} \cdot V_\psi$ denotes the direct sum of $c_{\chi\psi}$ copies of V_ψ. For convenience, we will define

$$V_{\chi\psi} = c_{\chi\psi} \cdot V_\psi,$$

and we naturally associate $V_{\chi\psi}$ with the corresponding subspace of V_χ.

Lemma 7.1.3. *[31, Lemma A, p. 70] Let $\chi \in \hat{G}$, $\psi \in \hat{H}$. Let $T : V_\psi \to V_\chi$ be a $\mathbb{C}H$-module homomorphism. Then the image of T is contained in $V_{\chi\psi}$.*

Proof. We have

$$V_\chi = \bigoplus_{\psi' \in \hat{H}} V_{\chi\psi'}.$$

Applying Schur's Lemma 2.0.2 to T gives that either $\mathrm{Im(T)} = 0$, in which case

$$\mathrm{Im}(T) \subseteq V_{\chi\psi},$$

or T is an isomorphism onto its image. This implies that $\mathrm{Im}(T)$ is $\mathbb{C}[H]$-module isomorphic to V_ψ. Since $V_{\chi\psi}$ contains all $c_{\chi\psi}$ copies of the irreducible V_ψ in V_χ, this implies $\mathrm{Im}(T) \subseteq V_{\chi\psi}$. □

Lemma 7.1.4. *[31, Lemma B, p. 70] Let $\chi \in \hat{G}$ and $T \in \mathrm{End_H}(V_\chi)$. Then T maps $V_{\chi\psi}$ into $V_{\chi\psi}$ for all $\psi \in \hat{H}$.*

Proof. Let $\psi \in \hat{H}$. By Lemma 7.1.3, restricting T to any copy of V_ψ in $V_{\chi\psi}$ results in the image $T(V_\psi)$ being in $V_{\chi\psi}$. Since $V_{\chi\psi} = c_{\chi\psi} \cdot V_\psi$ is generated by the copies of V_ψ, and T is linear, we must have

$$T(V_{\chi\psi}) \subseteq V_{\chi\psi}.$$ □

Corollary 7.1.5. *[31, Corollary 1, p. 70] Let $\chi \in \hat{G}$. If $u \in \mathbb{C}[G]^H$, then $R_\chi(u)$ maps $V_{\chi\psi}$ into $V_{\chi\psi}$ for all $\psi \in \hat{H}$.*

Proof. By Lemma 7.1.4, it suffices to show that $R_\chi(u) \in \mathrm{End_H}(V_\chi)$. We already have that $R_\chi : G \to \mathrm{GL}(V_\chi)$ extends to $R_\chi : \mathbb{C}G \to \mathrm{End}(V_\chi)$ by definition of R_χ as a representation, so $R_\chi(u)$ is linear. Recall that $\mathbb{C}[G]^H$ is the Schur ring generated by the H-classes in $\mathbb{C}[G]$, so u commutes with all elements of H. Given $h \in H, v \in V_\chi$ we have

$$\begin{aligned} R_\chi(u) \circ R_\chi(h)(v) &= R_\chi(uh)(v) \\ &= R_\chi(hu)(v) \\ &= R_\chi(h) \circ R_\chi(u)(v). \end{aligned}$$

So $R_\chi(u) \in \mathrm{End_H}(V_\chi)$. □

Lemma 7.1.6. *[31, Lemma C, p. 70] Let $\chi \in \hat{G}$ and $\psi \in \hat{H}$. Then the ring $\mathrm{End_H}(V_{\chi\psi})$ is isomorphic to $\mathrm{M}_{c_{\chi\psi}}(\mathbb{C})$, the vector space of $c_{\chi\psi} \times c_{\chi\psi}$ matrices with complex coefficients.*

Proof. Let $T \in \mathrm{End_H}(V_{\chi\psi})$. By Schur's Lemma 2.0.2, restricting T to any copy of V_ψ gives a scalar multiple of an identity map onto each copy of V_ψ in the image. Thus the isomorphism is given by $T \to [a_{ij}]$ where T restricted to the ith copy of V_ψ is the map

$\{a_{i1} \cdot id, a_{i2} \cdot id, \ldots, a_{ic_{\chi\psi}} \cdot id\}$ onto $V_{\chi\psi} = V_\psi \bigoplus V_\psi \bigoplus \cdots \bigoplus V_\psi$, where $id : V_\psi \to V_\psi$ is the identity map. □

Lemma 7.1.7. *[31, Lemma D, p. 70] Let $\chi \in \hat{G}$. Then the image of $\mathbb{C}[G]^H$ under R_χ is equal to $\mathrm{End_H}(V_\chi)$.*

Proof. In the proof of Corollary 7.1.5, given $u \in \mathbb{C}[G]^H$, we showed that $R_\chi(u) \in \mathrm{End_H}(V_\chi)$. For the reverse inclusion, let $T \in \mathrm{End_H}(V_\chi)$. Since R_χ is irreducible, the Wedderburn decomposition gives that $\mathbb{C}[G]$ acts as the full matrix ring $\mathrm{M_{f_\chi}}(\mathbb{C})$ on V_χ. Therefore, the image of R_χ under $\mathbb{C}[G]$ must be all of $\mathrm{End}(V_\chi)$. Thus there exists some $w \in \mathbb{C}[G]$ such that $R_\chi(w) = T$. Define

$$u = \frac{1}{|H|} \sum_{h \in H} hwh^{-1}.$$

Let $a \in H$. Then,

$$\begin{aligned} aua^{-1} &= a \left(\frac{1}{|H|} \sum_{h \in H} hwh^{-1} \right) a^{-1} \\ &= \frac{1}{|H|} \sum_{h \in H} ahwh^{-1}a^{-1} \\ &= \frac{1}{|H|} \sum_{h \in H} (ah)w(ah)^{-1} \\ &= \frac{1}{|H|} \sum_{h \in H} hwh^{-1} \\ &= u. \end{aligned}$$

Since u commutes with all of H, u is generated by the H-classes of $\mathbb{C}[G]$, so $u \in \mathbb{C}[G]^H$. Then

we have

$$\begin{aligned}
R_\chi(u) &= R_\chi\left(\frac{1}{|H|}\sum_{h\in H} hwh^{-1}\right)\\
&= \frac{1}{|H|}\sum_{h\in H} R_\chi(hwh^{-1})\\
&= \frac{1}{|H|}\sum_{h\in H} R_\chi(h)R_\chi(w)R_\chi(h^{-1})\\
&= \frac{1}{|H|}\sum_{h\in H} R_\chi(h)\circ T\circ R_\chi(h^{-1})\\
&= \frac{1}{|H|}\sum_{h\in H} T\circ R_\chi(h)\circ R_\chi(h^{-1})\\
&= \frac{1}{|H|}\sum_{h\in H} T\circ R_\chi(hh^{-1})\\
&= \frac{1}{|H|}\sum_{h\in H} T = T.
\end{aligned}$$

Thus R_χ maps $\mathbb{C}[G]^H$ onto $\mathrm{End}_{\mathrm{H}}(V_\chi)$, so $\mathrm{End}_{\mathrm{H}}(V_\chi)$ is the complete image of this map. □

Lemma 7.1.8. *[31, Lemma E, p. 71] Let $\chi \in \hat{G}$ and $\psi \in \hat{H}$. Then R_χ restricted to $\mathbb{C}[G]^H$ yields a representation of $\mathbb{C}[G]^H$ on $V_{\chi\psi}$ whose image is isomorphic to $M_{c_{\chi\psi}}(\mathbb{C})$.*

Proof. By Corollary 7.1.5, $R_\chi(u)$ maps $V_{\chi\psi}$ into $V_{\chi\psi}$ for all $u \in \mathbb{C}[G]^H$. Since we also have that $R_\chi(u) \in \mathrm{End}_{\mathrm{H}}(V_\chi)$, we see that $R_\chi(u)$ commutes with the action of H. This implies that the image of R_χ as a representation on $V_{\chi\psi}$ restricted to $\mathbb{C}[G]^H$ is contained in $\mathrm{End}_{\mathrm{H}}(V_{\chi\psi})$.

Now, let $T \in \mathrm{End}_{\mathrm{H}}(V_{\chi\psi})$. Then T extends to an element $\tilde{T}$ of $\mathrm{End}_{\mathrm{H}}(V_\chi)$ by setting $\tilde{T}$ equal to 0 on all $V_{\chi\psi'}$ where $\psi \neq \psi'$. To see this, note that for $v \in V_{\chi\psi}$, and $h \in H$,

$$\begin{aligned}
\tilde{T}\circ R_\chi(h)(v) &= T\circ R_\chi(h)(v)\\
&= R_\chi(h)\circ T(v)\\
&= R_\chi(h)\circ \tilde{T}(v),
\end{aligned}$$

since $R_\chi(h) \in \mathrm{End}_{\mathrm{H}}(V_{\chi\psi})$. For $v \in V_{\chi\psi'}$ with $\psi' \neq \psi$, we have $R_\chi(h)(v) \in V_{\chi\psi'}$ by Corollary

7.1.5, so

$$\begin{aligned}\tilde{T} \circ R_\chi(h)(v) &= \tilde{T}(0) \\ &= 0 \\ &= R_\chi(h)(0) \\ &= R_\chi(h) \circ \tilde{T}(v).\end{aligned}$$

By Lemma 7.1.7, we see that $\tilde{T}$ is in the image of $\mathbb{C}[G]^H$ under R_χ. Thus, by taking the representation R_χ acting on $V_{\chi\psi}$, we have T in the image of R_χ restricted to $\mathbb{C}[G]^H$. Thus, the image of this representation on $V_{\chi\psi}$ is exactly $\mathrm{End}_{\mathrm{H}}(V_{\chi\psi})$, which by Lemma 7.1.6 is isomorphic to $M_{c_{\chi\psi}}(\mathbb{C})$. □

We will denote the representation in Lemma 7.1.8 as $R_{\chi\psi}$.

7.2 Main results

Theorem 7.2.1. *[31, Theorem 5, p. 71] The representation $R_{\chi\psi}$ of $\mathbb{C}[G]^H$ acting on $V_{\chi\psi}$ decomposes into f_ψ copies of an irreducible representation of dimension $c_{\chi\psi}$.*

Proof. Since $V_{\chi\psi}$ is the direct sum of $c_{\chi\psi}$ copies of V_ψ, the dimension of $V_{\chi\psi}$ over $\mathbb{C}$ is $f_\psi \cdot c_{\chi\psi}$. By Lemma 7.1.8, the representation $R_{\chi\psi}$ acts as the full matrix ring $M_{c_{\chi\psi}}(\mathbb{C})$, so the Wedderburn decomposition gives that $R_{\chi\psi}$ is an irreducible representation of dimension $c_{\chi\psi}$. Thus, when $R_{\chi\psi}$ acts on a space of dimension $f_\psi \cdot c_{\chi\psi}$, it must decompose into f_ψ copies of the irreducible representation. Note in the case that $c_{\chi\psi} = 0$, we have $V_{\chi\psi} = 0$, so in this case we have $R_{\chi\psi} = 0$, the trivial map. □

Lemma 7.2.2. *[31, Theorem 6, p. 71] The $R_{\chi\psi}$ where $\chi \in \hat{G}$ and $\psi \in \hat{H}$ are distinct, excluding the cases where $c_{\chi\psi} = 0$.*

Proof. Let e_χ be the primitive central orthogonal idempotent corresponding to R_χ in the Wedderburn decomposition of $\mathbb{C}[G]$. Similarly, let e_ψ be the primitive central orthogonal

idempotent corresponding to R_ψ in the Wedderburn decomposition of $\mathbb{C}[H]$. Since they are central, e_χ is in the center of $C[G]$ and e_ψ is in the center of $C[H]$. So these idempotents commute with all elements of H, and are thus contained in $\mathbb{C}[G]^H$.

By definition, R_χ maps $\mathbb{C}[G]$ into End(V_χ). If we choose a basis for the vector space V_χ, we have that End(V_χ) is isomorphic to $M_{f_\chi}(\mathbb{C})$. Since $\mathbb{C}[G]$ is semisimple, this matrix ring occurs in the Wedderburn decomposition and corresponds to e_χ. So, up to isomorphism, we can express

$$R_\chi : \mathbb{C}[G] \to \mathbb{C}[G]$$

using e_χ as follows:

$$R_\chi(u) = e_\chi u$$

for $u \in \mathbb{C}[G]$. In particular, this gives that

$$\begin{aligned} R_\chi(e_\chi u) &= e_\chi^2 u \\ &= e_\chi u \\ &= R_\chi(u) \end{aligned} \tag{7.1}$$

since e_χ is idempotent. We can similarly identify

$$R_\psi : \mathbb{C}[H] \to \mathbb{C}[H]$$

as

$$R_\psi(u) = e_\psi u.$$

Now, recall that we obtained $R_{\chi\psi}$ by restricting R_χ to $\mathbb{C}[G]^H$ acting on $V_{\chi\psi}$, namely the copies of V_ψ in V_χ. Rewriting this definition in terms of the idempotents, we get

$$R_{\chi\psi} : \mathbb{C}[G]^H \to \mathbb{C}[G]$$

by

$$R_{\chi\psi}(u) = e_\psi R_\chi(u) = e_\psi e_\chi u.$$

Now, let $\chi' \in \hat{G}$ with $\chi \neq \chi'$. Then,

$$\begin{aligned} R_{\chi\psi}(e_{\chi'}) &= e_\psi R_\chi(e_{\chi'}) \\ &= e_\psi R_\chi(e_\chi e_{\chi'}) \\ &= e_\psi R_\chi(0) \\ &= 0, \end{aligned}$$

by (7.1) and orthogonality. Since the idempotents must sum to 1, that gives

$$\begin{aligned} 1 &= R_{\chi\psi}(1) \\ &= R_{\chi\psi}\left(\sum_{\chi' \in \hat{G}} e_{\chi'}\right) \\ &= \sum_{\chi' \in \hat{G}} R_{\chi\psi}(e_{\chi'}) \\ &= R_{\chi\psi}(e_\chi). \end{aligned}$$

So we have

$$R_{\chi\psi}(e_{\chi'}) = \delta_{\chi\chi'}.$$

Similarly, we see that for $\psi' \neq \psi$ in $\hat{H}$,

$$\begin{aligned} R_{\chi\psi}(e_{\psi'}) &= e_\psi e_\chi e_{\psi'} \\ &= (e_\psi e_{\psi'}) e_\chi \\ &= 0. \end{aligned}$$

So the same argument gives that

$$R_{\chi\psi}(e_{\psi'}) = \delta_{\psi\psi'}.$$

Therefore, each choice of χ and ψ gives a distinct irreducible representation $R_{\chi\psi}$ of $\mathbb{C}[G]^H$ (excluding when $c_{\chi\psi} = 0$). □

Lemma 7.2.3. *[31, Theorem 6, p. 71] Every irreducible representation of $\mathbb{C}[G]^H$ is of the form $R_{\chi\psi}$ for some $\chi \in \hat{G}$ and $\psi \in \hat{H}$.*

Proof. The Schur ring $\mathbb{C}[G]^H$ is generated by the H-classes in $\mathbb{C}[G]$. By the Burnside orbit

formula [9, Exercise 8, pg 877], the number of H-classes is

$$\frac{1}{|H|}\sum_{h\in H}|C_G(h)|,$$

where $C_G(h)$ is the centralizer of h in G. By the Second Orthogonality Relation for group characters (Theorem 2.0.7), this equals

$$\begin{aligned}
\frac{1}{|H|}\sum_{h\in H}\sum_{\chi\in\hat{G}}\chi(h)\overline{\chi(h)} &= \sum_{\chi\in\hat{G}}\left(\frac{1}{|H|}\sum_{h\in H}\chi(h)\overline{\chi(h)}\right)\\
&= \sum_{\chi\in\hat{G}}(\chi,\chi)_H\\
&= \sum_{\chi\in\hat{G}}\left(\sum_{\psi\in\hat{H}}c_{\chi\psi}\psi,\sum_{\psi'\in\hat{H}}c_{\chi\psi}\psi'\right)_H\\
&= \sum_{\chi\in\hat{G}}\left(\sum_{\psi,\psi'\in\hat{H}}c_{\chi\psi}c_{\chi\psi'}(\psi,\psi')_H\right)\\
&= \sum_{\chi\in\hat{G}}\sum_{\psi\in\hat{H}}c_{\chi\psi}^2,
\end{aligned}$$

where $(\cdot,\cdot)_H$ is the standard inner product on H-class functions. Therefore the dimension of $\mathbb{C}[G]^H$ is the sum of the $c_{\chi\psi}^2$. Since the dimension of $\mathbb{C}[G]^H$ is also the sum of the squares of the dimensions of distinct irreducible representations, by Theorem 7.2.1 and Lemma 7.2.2, we have that the $R_{\chi\psi}$ exhaust all irreducible representations of $\mathbb{C}[G]^H$. □

Corollary 7.2.4. *[31, Theorem 7, p. 72] Let $\chi\in\hat{G}$. Restriction of R_χ to $\mathbb{C}[H]$ and $\mathbb{C}[G]^H$ give representations that interchange multiplicity and dimension.*

Proof. If we restrict R_χ to $\mathbb{C}[H]$, we have

$$R_\chi = \sum_{\psi\in\hat{H}}c_{\chi\psi}\cdot R_\psi,$$

so this decomposes into irreducible representations of dimension f_ψ and multiplicity $c_{\chi\psi}$ for all $\psi\in\hat{H}$. See Remark 7.1.2. By Theorem 7.2.1, if we restrict R_χ to $\mathbb{C}[G]^H$, then for each $\psi\in\hat{H}$, the action on $V_{\chi\psi}$ decomposes into irreducible representations of dimension $c_{\chi\psi}$ and multiplicity f_ψ. Thus we have dimensions and multiplicities interchanged. □

Corollary 7.2.5. *[31, Corollary 1, p. 72] The pair (G, H) is a strong Gelfand pair if and only if $\mathbb{C}[G]^H$ is commutative.*

Proof. By definition, (G, H) is a strong Gelfand pair if and only if for all $\chi \in \hat{G}$ and $\psi \in \hat{H}$, we have that $c_{\chi\psi} = (\chi_H, \psi)_H$ is equal to either 0 or 1. By Corollary 7.2.4, this occurs if and only if each nonzero $R_{\chi\psi}$ has dimension 1. By Lemma 7.2.3, the $R_{\chi\psi}$ contain all irreducible representations of $\mathbb{C}[G]^H$. Finally, all irreducible representations have dimension 1 if and only if $\mathbb{C}[G]^H$ is commutative. □

Corollary 7.2.6. *[31, Corollary 1', p. 72] H is commutative if and only if $\mathbb{C}[G]^H$ is multiplicity free in $\mathbb{C}[G]$.*

Proof. The subgroup H is commutative if and only if each irreducible representation R_χ has dimension 1 for all $\psi \in \hat{H}$. That is, if and only if each $f_\psi = 1$. By Corollary 7.2.4, this occurs if and only if the multiplicity of each irreducible representation of $\mathbb{C}[G]^H$ is at most 1, which is exactly the condition for $\mathbb{C}[G]^H$ to be multiplicity free. □

Bibliography

[1] Babai, L. Cameron, P. J *Automorphisms and enumeration of switching classes of tournaments.* Electron. J. Combin. 7 (2000), Research Paper 38, 25 pp.

[2] W. Bosma and J. Cannon, MAGMA (University of Sydney, Sydney, 1994).

[3] Bruck, R. H. *Difference sets in a finite group.* Trans. Amer. Math. Soc. 78, (1955). 464–481.

[4] *https://cameroncounts.wordpress.com/2011/06/22/groups-with-unique-involution*

[5] Y.Q. Chen, T. Feng, *Abelian and non-abelian Paley type group schemes*, Des. Codes Cryptography. vol. 68 (2013), no. 1-3, 141–154.

[6] Coulter, Robert S., Gutekunst, Todd, *Special subsets of difference sets with particular emphasis on skew Hadamard difference sets.* Des. Codes Cryptogr. 53 (2009), no. 1, 1–12.

[7] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM, vol. 138, Springer, (1996).

[8] Davis, P.J., *Circulant matrices*, Chelsea, New York, (1994).

[9] Dummit, David S.; Foote, Richard M. *Abstract Algebra*, John Wiley and Sons, Inc. 3rd ed (2004), 840–878.

[10] C. Ding, J. Yuan, *A family of skew Hadamard difference sets*, J. Combin. Theory, Ser. A 113 (2006) 1526–1535.

[11] C. Ding, Z. Wang, Q. Xiang, *Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in PG(3,32h+1)*, J. Combin. Theory Ser. A 114 (2007) 867–887.

[12] R.J. Evans, *Nonexistence of twentieth power residue difference sets*, Acta Arith. 84 (1999) 397–402.

[13] T. Feng, Q. Xiang, *Strongly regular graphs from unions of cyclotomic classes*, J.Combin. Theory Ser. B. vol. 102 (2012), no. 4, 982–995 MR2927417

[14] Isaacs, I. M. *Real representations of groups with a single involution.* Pacific J. Math. 71 (1977), no. 2, 463–464.

[15] Ito, Noboru *On Hadamard groups. III.* Kyushu J. Math. 51 (1997), no. 2, 369–379.

[16] James, Gordon; Liebeck, Martin. *Representations and Characters of Groups*, Cambridge University Press. 2nd ed. (2001) 69–80

[17] Leung, Ka Hin; Man, Shing Hing *On Schur rings over cyclic groups* Israel J. Math. 106 (1998) 251–267.

[18] Leung, Ka Hin; Man, Shing Hing *On Schur rings over cyclic groups II* J. Algebra 183 (1996) 273–285

[19] Moore, Emily H.; Pollatsek, Harriet S. *Difference sets. Connecting algebra, combinatorics, and geometry.* Student Mathematical Library, 67. American Mathematical Society, Providence, RI, 2013. xiv+298 pp.

[20] T. Ikuta, A. Munemasa, *Pseudocyclic association schemes and strongly regular graphs*, European J. Combin. 31 (2010) 1513–1519.

[21] Malzan, Jerry, *On groups with a single involution.* Pacific J. Math. 57 (1975), no. 2, 481–489.

[22] Malzan, Jerry, *Corrections to: "On groups with a single involution"* (Pacific J. Math. 57 (1975), no. 2, 481–489). Pacific J. Math. 67 (1976), no. 2, 555.

[23] Mihailescu, Preda, *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*. J. Reine Angew. Math., (2004) 167–195

[24] Isaacs, I. Martin *Finite group theory*. Graduate Studies in Mathematics, 92. American Mathematical Society, Providence, RI, (2008) xii+350

[25] Kesava Menon, P. *On difference sets whose parameters satisfy a certain relation.* Proc. Amer. Math. Soc. 13, (1962) 739–745.

[26] Muzychuk, Mikhail; Ponomarenko, Ilia, *Schur rings.* European J. Combin. 30 (2009), no. 6, 1526-1539.

[27] Pott, Alexander *Finite geometry and character theory.* Lecture Notes in Mathematics, 1601. Springer-Verlag, Berlin, 1995. viii+181 pp.

[28] Schmidt, Bernhard *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Mathematics, vol 1797, (2002), 31–37

[29] Schmidt, Bernhard *Williamson matrices and a conjecture of Ito's.* Des. Codes Cryptogr. 17 (1999), no. 1-3, 61–68.

[30] Schur I., *Zur Theorie der einfach transitiven Permutationsgruppen*, Sitz. Preuss. Akad. Wiss. Berlin, Phys-math Klasse, (1933), 598–623.

[31] Travis, Dennis, *Spherical Functions on Finite Groups*, Journal of Algebra, vol. 29, (1974), 65–78.

[32] Wielandt, Helmut, *Finite permutation groups*, Academic Press, New York-London, (1964), x+114 pages.

[33] Wielandt, Helmut. *Zur theorie der einfach transitiven permutationsgruppen II.* Math. Z., 52:384–393, (1949).