

CLIFFORD-WEIL GROUPS OF QUOTIENT REPRESENTATIONS.

ANNIKA GÜNTHER

*Lehrstuhl D für Mathematik,
RWTH Aachen University
52056 Aachen, Germany
annika.guenther@math.rwth-aachen.de*

GABRIELE NEBE

*Lehrstuhl D für Mathematik,
RWTH Aachen University
52056 Aachen, Germany
nebe@math.rwth-aachen.de*

ERIC M. RAINS

*Department of Mathematics,
California Institute of Technology,
Pasadena, CA 91125, U.S.A.,
rains@caltech.edu*

ABSTRACT. This note gives an explicit proof that the scalar subgroup of the Clifford-Weil group remains unchanged when passing to the quotient representation filling a gap in [3]. For other current and future errata to [3] see <http://www.research.att.com/~njas/doc/cliff2.html/>.

1. INTRODUCTION

All notations in this paper are introduced in detail in [3] and we refer to this book for their definitions. One main goal of the book is to introduce a unified language to describe the Type of self-dual codes combining the different notions of self-duality and Types, that are well established in coding theory. The Type of a code is a finite representation $\rho = (V, \rho_M, \rho_\Phi, \beta)$ of a finite form ring $\mathcal{R} = (R, M, \psi, \Phi)$. The finite alphabet V is a left module for the ring R and the biadditive form $\beta : V \times V \rightarrow \mathbb{Q}/\mathbb{Z}$ defines the notion of duality. A code C of length N is then an R -submodule of V^N and the dual code is

$$C^\perp = \{v \in V^N \mid \sum_{i=1}^N \beta(v_i, c_i) = 0 \forall c \in C\}.$$

Additional properties of codes of a given Type are encoded in the R -qmodule $\rho_\Phi(\Phi)$ which is a certain subgroup of the group of quadratic mappings $V \rightarrow \mathbb{Q}/\mathbb{Z}$. A code $C \leq V^N$ is *isotropic*, if $C \leq C^\perp$ and

$$\sum_{i=1}^N \rho_\Phi(\phi)(c_i) = 0 \quad \text{for all } \phi \in \Phi \text{ and for all } c \in C.$$

Given a finite representation ρ , one associates a finite subgroup $\mathcal{C}(\rho)$ of $\text{GL}(\mathbb{C}[V])$, called the associated Clifford-Weil group (see Section 2). For certain finite form rings (including direct products of matrix rings over finite Galois rings) it is shown in [3, Theorem 5.5.7] that the ring of polynomial invariants of $\mathcal{C}(\rho)$ is spanned by the complete weight-enumerators of self-dual isotropic codes of Type ρ . We conjecture that this theorem holds for arbitrary finite form rings. It is shown in [3, Theorem 5.4.13, 5.5.3] that in general the order of the scalar subgroup

$$\mathcal{S}(\mathcal{C}(\rho)) = \mathcal{C}(\rho) \cap \mathbb{C}^* \text{id}_{\mathbb{C}[V]}$$

is exactly the greatest common divisor of the lengths of self-dual isotropic codes of Type ρ . The proof of this theorem uses the fact that the scalar subgroup of $\mathcal{C}(\rho)$ remains unchanged when passing to the quotient representation. The aim of the present note is to give a full proof of this statement, Theorem 1.

Throughout the note we fix an isotropic code $C \leq C^\perp \leq V$ in ρ . Then the quotient representation ρ/C is defined by

$$\rho/C := (C^\perp/C, \rho_M/C, \rho_\Phi/C, \beta/C),$$

where $(\rho_M/C(m))(v+C, w+C) = \rho_M(m)(v, w)$, $(\rho_\Phi/C(\phi))(v+C) = \rho_\Phi(\phi)(v)$, and $\beta/C(v+C, w+C) = \beta(v, w)$ for all $v, w \in C^\perp, m \in M, \phi \in \Phi$.

Theorem 1. *Let $\mathcal{R} = (R, M, \psi, \Phi)$ be a finite form-ring and let $\rho = (V, \rho_M, \rho_\Phi, \beta)$ be a finite representation of \mathcal{R} . Let C be an isotropic self-orthogonal code in ρ . Then*

$$\mathcal{S}(\mathcal{C}(\rho)) \cong \mathcal{S}(\mathcal{C}(\rho/C)).$$

2. CLIFFORD-WEIL GROUPS AND HYPERBOLIC COUNITARY GROUPS

The Clifford-Weil group $\mathcal{C}(\rho)$ associated to the finite representation ρ acts linearly on the space $\mathbb{C}[V]$ with basis $[b_v : v \in V]$. It is generated by

$$\begin{aligned} m_r &: b_v \mapsto b_{rv} && \text{for } r \in R^* \\ d_\phi &: b_v \mapsto \exp(2\pi i \rho_\Phi(\phi)(v)) b_v && \text{for } \phi \in \Phi \\ h_{e, u_e, v_e} &: b_v \mapsto \frac{1}{|eV|^{1/2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e v)) b_{w+(1-e)v} && e^2 = e \in R \text{ symmetric.} \end{aligned}$$

Recall that the form-ring structure defines an involution J on R . Then an idempotent $e \in R$ is called *symmetric*, if eR and $e^J R$ are isomorphic as right R -modules, which means that there are $u_e \in eR e^J, v_e \in e^J R e$ such that $e = u_e v_e$ and $e^J = v_e u_e$.

The Clifford-Weil group $\mathcal{C}(\rho)$ is a projective representation of the hyperbolic counitary group

$$\mathcal{U}(R, \Phi) = U\left(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \text{Mat}_2(R), \Phi_2\right).$$

The elements of $\mathcal{U}(R, \Phi)$ are of the form

$$(1) \quad X = \left(\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \right) \right) \in \text{Mat}_2(R) \times \Phi_2$$

such that

$$\begin{pmatrix} \gamma^J \alpha & \gamma^J \beta \\ \delta^J \alpha - 1 & \delta^J \beta \end{pmatrix} = \psi_2^{-1} \begin{pmatrix} \lambda(\phi_1) & m \\ \tau(m) & \lambda(\phi_2) \end{pmatrix}.$$

A more detailed definition of $\mathcal{U}(R, \Phi)$ can be found in [3, Chapter 5.2].

It is shown in the book that $\mathcal{U}(R, \Phi)$ is generated by the elements

$$d((r, \phi)) = \left(\begin{pmatrix} r^{-J} & r^{-J} \psi^{-1}(\lambda(\phi)) \\ 0 & r \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ \phi & \phi \end{pmatrix} \right)$$

with $r \in R^*$, $\phi \in \Phi$ and

$$H_{e, u_e, v_e} = \left(\begin{pmatrix} 1 - e^J & v_e \\ -\epsilon^{-1} u_e^J & 1 - e \end{pmatrix}, \begin{pmatrix} 0 & \psi(-\epsilon e) \\ 0 & 0 \end{pmatrix} \right),$$

where $e = u_e v_e$ runs through the symmetric idempotents of R .

To formalize the proofs we let $\mathcal{F}(R, \Phi)$ denote the free group on

$$\{\tilde{d}(r, \phi), \tilde{H}_{e, u_e, v_e} \mid r \in R^*, \phi \in \Phi, e = u_e v_e \text{ symmetric idempotent in } R\}.$$

On these generators there are two group epimorphism:

$$\pi : \mathcal{F}(R, \Phi) \rightarrow \mathcal{U}(R, \Phi), \tilde{d}(r, \phi) \mapsto d((r, \phi)), \tilde{H}_{e, u_e, v_e} \mapsto H_{e, u_e, v_e}$$

and

$$(2) \quad p : \mathcal{F}(R, \Phi) \rightarrow \mathcal{C}(\rho); \quad \tilde{d}(r, \phi) \mapsto m_r d_\phi, \quad \tilde{H}_{e, u_e, v_e} \mapsto h_{e, u_e, v_e}.$$

Theorem 2. $p(\ker(\pi)) \subseteq \mathcal{S}(\mathcal{C}(\rho))$.

If ρ is faithful (i.e. $\text{Ann}_R(V) = 0 = \ker(\rho_\Phi)$), then $p(\ker(\pi)) = \mathcal{S}(\mathcal{C}(\rho))$.

This is essentially [3, Theorem 5.3.2]. However the calculations there were omitted so we take the opportunity to give them here for completeness (also since there are a few typos in the proof there). As in [3, Theorem 5.3.2] we define the associated Heisenberg group $\mathcal{E}(V) := V \times V \times \mathbb{Q}/\mathbb{Z}$ with multiplication

$$(z, x, q) \cdot (z', x', q') = (z + z', x + x', q + q' + \beta(x', z)).$$

Then $\mathcal{E}(V)$ acts linearly on $\mathbb{C}[V]$ by

$$(z, x, q) \cdot b_v = \exp(2\pi i(q + \beta(v, z))) b_{v+x}, \quad (z, x, q) \in \mathcal{E}(V), \quad v \in V.$$

This yields an absolutely irreducible faithful representation $\Delta : \mathcal{E}(V) \rightarrow GL_{|V|}(\mathbb{C})$.

Lemma 3. *The hyperbolic counitary group $\mathcal{U}(R, \Phi)$ acts as group automorphisms on $\mathcal{E}(V)$ via*

$$\begin{aligned} & \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ \phi_2 & \phi_2 \end{pmatrix} \right) (z, x, q) \\ & = (\alpha z + \beta x, \gamma z + \delta x, q + \rho_\Phi(\phi_1)(z) + \rho_\Phi(\phi_2)(x) + \rho_M(m)(z, x)). \end{aligned}$$

If ρ is a faithful representation, then this action is faithful.

Also the associated Clifford-Weil group $\mathcal{C}(\rho) \leq GL(\mathbb{C}[V])$ acts on $\Delta(\mathcal{E}(V)) \cong \mathcal{E}(V)$ by conjugation.

Lemma 4. *For $r \in R^*$, $\phi \in \Phi$ and $(z, x, q) \in \mathcal{E}(V)$ we have*

$$\Delta(d((r, \phi))(z, x, q)) = (m_r d_\phi) \Delta((z, x, q)) (m_r d_\phi)^{-1}.$$

Proof. The proof is an easy calculation.

$$d((r, \phi))(z, x, q) = (r^{-J}z + r^{-J}\psi^{-1}(\lambda(\phi))x, rx, q + \rho_{\Phi}(\phi)(x))$$

maps the basis element b_v ($v \in V$) to

$$\exp(2\pi i(q + \rho_{\Phi}(\phi)(x) + \beta(v, r^{-J}z + r^{-J}\psi^{-1}(\lambda(\phi))x)))b_{v+rx}.$$

On the other hand

$$\begin{aligned} (m_r d_{\phi})\Delta((z, x, q))(m_r d_{\phi})^{-1}(b_v) &= \\ &= m_r d_{\phi} \exp(2\pi i(q - \rho_{\Phi}(\phi)(r^{-1}v) + \beta(r^{-1}v, z)))(b_{r^{-1}v+x}) \\ &= \exp(2\pi i(q - \rho_{\Phi}(\phi)(r^{-1}v) + \beta(r^{-1}v, z) + \rho_{\Phi}(\phi)(r^{-1}v + x)))(b_{v+rx}) \\ &= \exp(2\pi i(q + \beta(r^{-1}v, z) + \rho_M(\lambda(\phi))(r^{-1}v, x)))(b_{v+rx}) \end{aligned}$$

which is the same as the above, since $\beta(r^{-1}v, z) = \beta(v, r^{-J}z)$ by definition of the involution J and

$$\rho_M(\lambda(\phi))(r^{-1}v, x) = \beta(r^{-1}v, \psi^{-1}(\lambda(\phi))x) = \beta(v, r^{-J}\psi^{-1}(\lambda(\phi))x).$$

□

Lemma 5. For $e = u_e v_e$ a symmetric idempotent in R and $(z, x, q) \in \mathcal{E}(V)$

$$\Delta(H_{e, u_e, v_e}(z, x, q)) = h_{e, u_e, v_e} \Delta((z, x, q)) h_{e, u_e, v_e}^{-1}.$$

Proof. The group $\mathcal{E}(V)$ is generated by $(z, 0, 0)$, $(0, x, 0)$, $(0, 0, q)$ where $z \in e^J V \cup (1 - e^J)V$, $x \in eV \cup (1 - e)V$, $q \in \mathbb{Q}/\mathbb{Z}$ and it is enough to check the lemma for these 5 types of generators. For $(0, 0, q)$ this is clear. Similarly, if $z \in (1 - e^J)V$ and $x \in (1 - e)V$, then both sides yield $\Delta((z, x, q))$ as one easily checks. For $z \in e^J V$, $x \in eV$, $q \in \mathbb{Q}/\mathbb{Z}$

$$H_{e, u_e, v_e}(z, x, q) = (v_e x, -\epsilon^{-1} u_e^J z, q + \beta(z, -\epsilon x)).$$

To calculate the right hand side, we note that according to the decomposition

$$V = eV \oplus (1 - e)V$$

the space $\mathbb{C}[V] = \mathbb{C}[eV] \otimes \mathbb{C}[(1 - e)V]$ is a tensor product and

$$h_{e, u_e, v_e} = (h_{e, u_e, v_e})_{\mathbb{C}[eV]} \otimes \text{id}_{\mathbb{C}[(1 - e)V]}.$$

Moreover, the permutation matrix $\Delta((0, x, 0)) : b_v \mapsto b_{v+x}$ for $x \in eV$ is a tensor product $p_x \otimes \text{id}$ and similarly the diagonal matrix $\Delta((z, 0, 0))$ for $z \in e^J V$ is a tensor product $d_z \otimes \text{id}$. It is therefore enough to calculate the action on elements of $\mathbb{C}[eV]$. For $z = e^J z \in e^J V$, $x = ex \in eV$ and $v = ev \in eV$, we get

$$\begin{aligned} h_{e, u_e, v_e} \circ \Delta((e^J z, 0, 0)) \circ h_{e, u_e, v_e}^{-1} b_v &= \\ &= h_{e, u_e, v_e} (|eV|^{-1/2} \sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1} v_e^J ev, w) + \beta(w, e^J z))) b_w) \\ &= |eV|^{-1} \sum_{w' \in eV} \sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1} v_e^J ev, w) + \beta(w, e^J z) + \beta(w', v_e w))) b_{w'}. \end{aligned}$$

Now $\beta(-\epsilon^{-1} v_e^J ev, w) + \beta(w, e^J z) + \beta(w', v_e w) = \beta(-\epsilon^{-1} v_e^J ev + \epsilon^{-1} z + \epsilon^{-1} v_e^J ew', w)$. Hence the sum over all w is non-zero, only if $-v_e^J ev + z + v_e^J ew' = 0$ which implies

that $w' = v - \epsilon^{-1}u_e^J z$. Hence $h_{e,u_e,v_e} \circ \Delta((e^J z, 0, 0)) \circ h_{e,u_e,v_e}^{-1} b_v = b_{v - \epsilon^{-1}u_e^J z}$. A similar calculation yields

$$\begin{aligned}
& h_{e,u_e,v_e} \circ \Delta((0, ex, 0)) \circ h_{e,u_e,v_e}^{-1} b_v = \\
& = h_{e,u_e,v_e}(|eV|^{-1/2} \sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1}v_e^J \epsilon v, w))) b_{w+ex}) \\
& = h_{e,u_e,v_e}(|eV|^{-1/2} \sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1}v_e^J \epsilon v, w - ex))) b_w) \\
& = h_{e,u_e,v_e} \circ h_{e,u_e,v_e}^{-1} (\exp(2\pi i(\beta(\epsilon^{-1}v_e^J \epsilon v, ex))) b_v) \\
& = \exp(2\pi i(\beta(v, v_e x))) b_v.
\end{aligned}$$

□

Proof. (of Theorem 2) That $p(\ker(\pi)) \subseteq \mathcal{S}(\mathcal{C}(\rho))$ follows from Lemma 4 and 5. Assume now that ρ is faithful. Then by Lemma 3 the action of $\mathcal{U}(R, \Phi)$ on $\mathcal{E}(V)$ is faithful: Let $s \in \mathcal{S}(\mathcal{C}(\rho))$. Then there is some $f \in \mathcal{F}(R, \Phi)$ with $p(f) = s$ since p is surjective. Moreover the action of $\pi(f) \in \mathcal{U}(R, \Phi)$ and $p(f) \in \mathcal{C}(\rho)$ on $\mathcal{E}(V)$ coincide, so $\pi(f)$ acts trivially on $\mathcal{E}(V)$ and therefore $f \in \ker(\pi)$.

□

Remark 6. Let ρ be faithful. Lemma 4 and 5 show that every element $a \in \mathcal{C}(\rho)$ induces an automorphism α on $\mathcal{E}(V)$ that is in $\mathcal{U}(R, \Phi)$. The latter group acts faithfully on $\mathcal{E}(V)$ by Lemma 3 hence $\alpha \in \mathcal{U}(R, \Phi)$ is uniquely determined. This defines a group epimorphism

$$\nu : \mathcal{C}(\rho) \rightarrow \mathcal{U}(R, \Phi), \quad a \mapsto \alpha.$$

The kernel of ν is precisely the scalar subgroup $\mathcal{S}(\mathcal{C}(\rho))$. The inverse homomorphism is

$$\theta : \mathcal{U}(R, \Phi) \rightarrow \mathcal{C}(\rho)/\mathcal{S}(\mathcal{C}(\rho)), \quad u \mapsto p(\pi^{-1}(u))$$

which is well defined by Theorem 2.

For the calculations in Section 5 we need the following lemma.

Lemma 7. Let $X \in \mathcal{U}(R, \Phi)$ be as in (1). If $\delta^2 = \delta$ then $\iota := 1 - \delta$ is a symmetric idempotent of R .

Proof. We define $u_\iota = -\iota \gamma^J \iota^J$, $v_\iota = \iota^J \beta \iota$ and calculate

$$\begin{aligned}
u_\iota v_\iota & = -(1 - \delta) \epsilon^{-1} \gamma^J (1 - \delta^J) \beta (1 - \delta) \\
& = -(1 - \delta) \epsilon^{-1} \underbrace{\gamma^J \beta}_{=\alpha^J \epsilon \delta - \epsilon} (1 - \delta) + (1 - \delta) \epsilon^{-1} \gamma^J \underbrace{\delta^J \beta}_{=\beta^J \epsilon \delta} (1 - \delta) \\
& = (1 - \delta) \epsilon^{-1} \epsilon (1 - \delta) = 1 - \delta = \iota
\end{aligned}$$

and

$$\begin{aligned}
v_\iota u_\iota & = -(1 - \delta^J) \beta (1 - \delta) \epsilon^{-1} \gamma^J (1 - \delta^J) \\
& = -(1 - \delta^J) \underbrace{\beta \epsilon^{-1} \gamma^J}_{=\alpha \delta^J - 1} (1 - \delta^J) + (1 - \delta^J) \beta \underbrace{\delta \epsilon^{-1} \gamma^J}_{=\gamma \delta^J} (1 - \delta^J) \\
& = -(1 - \delta^J) (-1) (1 - \delta^J) = 1 - \delta^J = \iota^J.
\end{aligned}$$

□

$$3. \mathcal{S}(\mathcal{C}(\rho)) \leq \mathcal{S}(\mathcal{C}(\rho/C))$$

The Clifford-Weil group $\mathcal{C}(\rho/C)$ can be derived from $\mathcal{C}(\rho)$ by restricting the operation of $\mathcal{C}(\rho)$ to a submodule of $\mathbb{C}[V]$.

Lemma 8. *The group $\mathcal{C}(\rho)$ acts on a submodule of $\mathbb{C}[V]$ isomorphic to $\mathbb{C}[C^\perp/C]$. This yields a representation*

$$\text{res} : \mathcal{C}(\rho) \rightarrow \text{GL}(\mathbb{C}[C^\perp/C])$$

with $\text{res}(\mathcal{C}(\rho)) \leq \mathcal{C}(\rho/C)$. For the scalar subgroups we get $\ker(\text{res}) \cap \mathcal{S}(\mathcal{C}(\rho)) = \{1\}$ and hence $\mathcal{S}(\mathcal{C}(\rho))$ is isomorphic to a subgroup of $\mathcal{S}(\mathcal{C}(\rho/C))$.

Proof. Let Rep denote a set of coset representatives of C^\perp/C . We define a subspace

$$U := \left\{ \sum_{v \in \text{Rep}} \sum_{c \in C} a_v b_{v+c} \mid a_v \in \mathbb{C} \right\} \leq \mathbb{C}[V].$$

This subspace is isomorphic to $\mathbb{C}[C^\perp/C]$ via

$$f : \mathbb{C}[C^\perp/C] \rightarrow U, \quad \sum_{v \in \text{Rep}} a_v b_{v+C} \mapsto \sum_{v \in \text{Rep}} \sum_{c \in C} a_v b_{v+c}.$$

So we have

$$\text{res}(x) = f \circ x \circ f^{-1} \in \text{GL}(U)$$

for $x \in \mathcal{C}(\rho)$. Particularly, if $x = s \cdot \text{id}_{\mathbb{C}[V]}$ then $\text{res}(x) = s \cdot \text{id}_{\mathbb{C}[C^\perp/C]}$ and hence the restriction of res to the scalar subgroup of $\mathcal{C}(\rho)$ is injective.

We now will show that

$$\star_H \quad f \circ p(\tilde{H}_{e, u_e, v_e}) \circ f^{-1} = p/C(\tilde{H}_{e, u_e, v_e})$$

and

$$\star_d \quad f \circ p(\tilde{d}((r, \phi))) \circ f^{-1} = p/C(\tilde{d}((r, \phi)))$$

where $p : \mathcal{F}(R, \Phi) \rightarrow \mathcal{C}(\rho)$ and $p/C : \mathcal{F}(R, \Phi) \rightarrow \mathcal{C}(\rho/C)$ denote the group homomorphisms as defined (2). So we have $\text{Im}(\text{res}) \leq \mathcal{C}(\rho/C) = \text{Im}(p/C)$ which shows the lemma.

To prove \star_H let $v + C \in C^\perp/C$ and let T denote a set of coset representatives of $eC^\perp/eC \cong eC^\perp/C$. Then

$$\begin{aligned}
& f^{-1} \circ p(\tilde{H}_{e,u_e,v_e}) \circ f(b_{v+C}) = f^{-1} \circ p(\tilde{H}_{e,u_e,v_e}) \left(\sum_{c \in C} b_{v+c} \right) \\
& = f^{-1} \left(\sum_{c \in C} |eV|^{-\frac{1}{2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e(v+c))) b_{w+(1-e)(v+c)} \right) \\
& = f^{-1} \left(|eV|^{-\frac{1}{2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e v)) \sum_{c' \in (1-e)C} \cdot \right. \\
& \quad \cdot \underbrace{\sum_{c \in eC} \exp(2\pi i \beta(w, v_e c)) b_{w+(1-e)(v+c')}}_{= \begin{cases} |eC|, & w \in eC^\perp, \\ 0 & \text{otherwise.} \end{cases}} \\
& = f^{-1} \left(\frac{|eC|}{|eV|^{\frac{1}{2}}} \sum_{w \in eC^\perp} \sum_{c' \in (1-e)C} \exp(2\pi i \beta(w, v_e v)) b_{w+(1-e)(v+c')} \right) \\
& = f^{-1} \left(\frac{|eC|}{|eV|^{\frac{1}{2}}} \sum_{w \in T} \sum_{c' \in (1-e)C} \sum_{c \in eC} \exp(2\pi i \beta(w, v_e v)) b_{w+c+(1-e)(v+c')} \right) \\
& = f^{-1} \left(\frac{|eC|}{|eV|^{\frac{1}{2}}} \sum_{w \in T} \exp(2\pi i \beta(w, v_e v)) \sum_{c \in C} b_{w+(1-e)v+c} \right) \\
& = |eC^\perp/C|^{-\frac{1}{2}} \sum_{w \in eC^\perp/C} \exp(2\pi i \beta/C(w, v_e(v+C))) b_{w+(1-e)(v+C)} \\
& = p/C(\tilde{H}_{e,u_e,v_e})(b_{v+C}).
\end{aligned}$$

To show \star_d we note that $\rho_\Phi(\phi)(c) = 0$ for all $c \in C$ and for all $\phi \in \Phi$ and obtain

$$\begin{aligned}
& f^{-1} \circ p(\tilde{d}((r, \phi))) \circ f(b_{v+C}) = f^{-1} \circ p(\tilde{d}((r, \phi))) \left(\sum_{c \in C} b_{v+c} \right) \\
& = f^{-1} \left(p(\tilde{d}((r, 0))) \sum_{c \in C} \exp(2\pi i \rho_\Phi(\phi)(v+c)) b_{v+c} \right) \\
& = f^{-1} \left(\sum_{c \in C} \exp(2\pi i \rho_\Phi(\phi)(v)) b_{rv+rc} \right) \\
& = f^{-1} \left(\sum_{c \in C} \exp(2\pi i \rho_\Phi(\phi)(v)) b_{rv+c} \right) \\
& = \exp(2\pi i \rho_\Phi/C(\phi)(v+C)) b_{r(v+C)} \\
& = p/C(\tilde{d}((r, \phi)))(b_{v+C}).
\end{aligned}$$

□

4. THE STRATEGY.

Without loss of generality we now assume that ρ is faithful, that is,

$$\ker(\rho) = (\text{Ann}_R(V), \ker(\rho_\Phi)) = (0, 0)$$

and let $(I, \Gamma) = \ker(\rho/C)$. We then define $\overline{\text{res}} : \mathcal{U}(R, \Phi) \rightarrow \mathcal{U}(R/I, \Phi/\Gamma)$ by

$$\overline{\text{res}} \left(\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \right) \right) = \left(\left(\begin{pmatrix} \alpha + I & \beta + I \\ \gamma + I & \delta + I \end{pmatrix}, \begin{pmatrix} \phi_1 + \Gamma & m + \psi(I) \\ & \phi_2 + \Gamma \end{pmatrix} \right) \right).$$

By Remark 6 the epimorphism

$$\nu : \mathcal{C}(\rho) \rightarrow \mathcal{U}(R, \Phi) \text{ by } \nu(m_r d_\phi) = d((r, \phi)), \quad \nu(h_{e, u_e, v_e}) = H_{e, u_e, v_e}$$

for $r \in R^*, \phi \in \Phi$ and symmetric idempotents $e = u_e v_e \in R$ is well defined and its kernel is $\mathcal{S}(\mathcal{C}(\rho))$. Similarly $\bar{\nu} : \mathcal{C}(\rho/C) \rightarrow \mathcal{U}(R/I, \Phi/\Gamma)$. Then $\nu \circ p = \pi$ and $\bar{\nu} \circ p/C = \pi/C$, where $\pi/C : \mathcal{F}(R/I, \Phi/\Gamma) \rightarrow \mathcal{U}(R/I, \Phi/\Gamma)$ is the analogous group epimorphism. Again the representation ρ/C of $(R/I, \Phi/\Gamma)$ is faithful so by Remark 6 the kernel of $\bar{\nu}$ is $\mathcal{S}(\mathcal{C}(\rho/C))$.

We then have the following commutative diagram with exact rows and columns

$$\begin{array}{ccccccc}
 & & & 1 & & 1 & \\
 & & & \downarrow & & \downarrow & \\
 & & & \ker(\text{res}) & \xrightarrow{\nu|_{\ker(\text{res})}} & \ker(\bar{\text{res}}) & \rightarrow \mathcal{Y}' \rightarrow 1 \\
 & & 1 & \downarrow & & \downarrow & \\
 1 & \rightarrow & \mathcal{S}(\mathcal{C}(\rho)) & \rightarrow & \mathcal{C}(\rho) & \xrightarrow{\nu} & \mathcal{U}(R, \Phi) \rightarrow 1 \\
 & & \downarrow & & \downarrow \text{res} & & \downarrow \bar{\text{res}} \\
 1 & \rightarrow & \mathcal{S}(\mathcal{C}(\rho/C)) & \rightarrow & \mathcal{C}(\rho/C) & \xrightarrow{\bar{\nu}} & \mathcal{U}(R/I, \Phi/\Gamma) \rightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \mathcal{Y} & & 1 & & 1 \\
 & & \downarrow & & & & \\
 & & 1 & & & &
 \end{array}$$

To see that all sequences are exact, we note that $\nu|_{\ker(\text{res})}$ is injective, since $\ker(\text{res}) \cap \mathcal{S}(\mathcal{C}(\rho)) = 1$. The homomorphisms $\bar{\text{res}}$ and res are surjective, since idempotents and units of R/I lift to idempotents and units of R . Moreover $\bar{\text{res}} \circ \nu = \bar{\nu} \circ \text{res}$ as one checks on the generators.

The claim of Theorem 1 is that \mathcal{Y} is trivial. But this is fulfilled if and only if \mathcal{Y}' is trivial, that is, if $\nu|_{\ker(\text{res})}$ is an isomorphism since

$$|\mathcal{Y}| = \frac{|\mathcal{S}(\mathcal{C}(\rho/C))|}{|\mathcal{S}(\mathcal{C}(\rho))|} = \frac{|\mathcal{C}(\rho/C)| \cdot |\mathcal{U}(R, \Phi)|}{|\mathcal{U}(R/I, \Phi/\Gamma)| \cdot |\mathcal{C}(\rho)|} = \frac{|\ker(\bar{\text{res}})|}{|\ker(\text{res})|} = |\mathcal{Y}'|.$$

5. THE SURJECTIVITY OF $\nu|_{\ker(\text{res})}$

During the proof of Theorem 1 some results on lifting symmetric idempotents are needed, which are stated in the next two lemmata.

Lemma 9. *Let R be an Artinian ring and I an ideal of R . If $e \in I + \text{rad } R \subseteq R$ such that $e^2 \equiv e \pmod{\text{rad } R}$ then there exists an idempotent $e' \in I$ such that $e' \equiv e \pmod{\text{rad } R}$.*

Proof. We choose $x_0 \in \text{rad } R$ such that $e_0 := e + x_0 \in I$. Then $e_0 + \text{rad } R$ is an idempotent in $R/\text{rad } R$. Since $\text{rad } R$ is a nilpotent ideal of R [2, Theorem 4.9] constructs an idempotent $e' = f(e_0) \in I$ for some polynomial $f \in \mathbb{Z}[X]$ with $f(0) = 0$ such that $e' + \text{rad } R = e_0 + \text{rad } R$. \square

By [2, Theorem 4.5] applied to an idempotent $e \in R$, the right-modules eR and $e^J R$ are isomorphic, if and only if their quotients modulo $\text{rad } R$ are isomorphic. Hence we find

Lemma 10. *Let $e + \text{rad } R \in R/\text{rad } R$ be a symmetric idempotent such that*

$$e + \text{rad } R = u_e v_e + \text{rad } R, \quad e^J + \text{rad } R = v_e u_e + \text{rad } R,$$

$u_e + \text{rad } R \in (eRe^J) + \text{rad } R$, $v_e \in (e^JRe) + \text{rad } R$. If $e \in R$ is an idempotent then e is symmetric as well. More precisely, there exist $\tilde{u}_e \in eRe^J$, $\tilde{v}_e \in e^JRe$ such that

$$e = \tilde{u}_e \tilde{v}_e, \quad e^J = \tilde{v}_e \tilde{u}_e$$

and $\tilde{v}_e \equiv v_e \pmod{\text{rad } R}$.

For the rest of this note, let

$$(3) \quad X := \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \right) \in \ker(\overline{\text{res}})$$

and let $(I, \Gamma) := \ker(\rho/C)$. In particular, $\alpha, \delta \in 1 + I$, $\beta, \gamma \in I$, $\phi_1, \phi_2 \in \Gamma$ and $m \in \psi(I)$. We have to find some $x \in \ker(\text{res})$ such that $\nu(x) = X$.

Lemma 11. *We have $d(P(R, \Phi)) \cap \ker(\overline{\text{res}}) \subseteq \text{Im}(\nu|_{\ker(\text{res})})$.*

Proof. Let $r \in R^*$, $\phi \in \Phi$ such that $d((r, \phi)) = \nu(m_r d_\phi) \in \ker(\overline{\text{res}})$. Then $r \in 1 + I$ and $\phi \in \Gamma$. In particular r acts as the identity on C^\perp/C and $\rho_\Phi/C(\phi) = 0$. This implies that both m_r and $d_\phi \in \ker(\text{res})$. \square

Lemma 12. *Let δ be a unit. Then there exists $x \in \ker(\text{res})$ such that $\nu(x) = X$.*

Proof. Since $\ker(\text{res})$ is a normal subgroup of $\mathcal{C}(\rho)$ it suffices to show that X is contained in the normal subgroup of $\mathcal{U}(R, \Phi)$ generated by the elements $d(P(R, \Phi)) \cap \ker(\overline{\text{res}})$. We show that there is $\phi \in \Gamma$ such that

$$X = d((\delta, \phi_2)) H_{1,1,1} d((1, \phi)) H_{1,1,1}^{-1}.$$

We have $d((\delta, \phi_2)) = \left(\begin{pmatrix} \delta^{-J} & \beta \\ 0 & \delta \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & \phi_2 \end{pmatrix} \right)$ and hence

$$d((\delta, \phi_2))^{-1} = \left(\begin{pmatrix} \delta^J & -\delta^J \beta \delta^{-1} \\ 0 & \delta^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & -\phi_2[\delta^{-1}] \end{pmatrix} \right).$$

We therefore find

$$d((\delta, \phi_2))^{-1} X = \left(\begin{pmatrix} \delta^J \alpha - \delta^J \beta \delta^{-1} \gamma & 0 \\ \delta^{-1} \gamma & 1 \end{pmatrix}, \begin{pmatrix} -\phi_2[\delta^{-1} \gamma] + \phi_1 & \tilde{m} \\ & 0 \end{pmatrix} \right)$$

for some $\tilde{m} \in M$. Since the upper right entry in the first matrix of this element of $\mathcal{U}(R, \Phi)$ is 0 we obtain $\tilde{m} = 0$ and similarly $\delta^J \alpha - \delta^J \beta \delta^{-1} \gamma = 1$ and we get

$$d((\delta, \phi_2))^{-1} X = \left(\begin{pmatrix} 1 & 0 \\ \delta^{-1} \gamma & 1 \end{pmatrix}, \begin{pmatrix} -\phi_2[\delta^{-1} \gamma] + \phi_1 & 0 \\ & 0 \end{pmatrix} \right)$$

Furthermore,

$$H_{1,1,1} = \left(\begin{pmatrix} 0 & 1 \\ -\epsilon^J & 0 \end{pmatrix}, \begin{pmatrix} 0 & \psi(-\epsilon) \\ & 0 \end{pmatrix} \right), \quad H_{1,1,1}^{-1} = \left(\begin{pmatrix} 0 & -\epsilon \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \psi(-\epsilon) \\ & 0 \end{pmatrix} \right).$$

Then we have

$$(d((\delta, \phi_2))^{-1} X)^{H_{1,1,1}} = \left(\begin{pmatrix} 1 & -\epsilon \delta^{-1} \gamma \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & m' \\ & \phi \end{pmatrix} \right),$$

with some $m' \in M$ and

$$\phi = \{\psi(-\epsilon \delta^{-1} \gamma)\} - \phi_2[\delta^{-1} \gamma] + \phi_1 \in \Gamma,$$

since $-\epsilon \delta^{-1} \gamma \in I$ and $\phi_1, \phi_2 \in \Gamma$. Again $m' = 0$ since the lower left entry in the first matrix is 0. Hence

$$H_{1,1,1}^{-1} d((\delta, \phi_2))^{-1} X H_{1,1,1} = d((1, \phi)) \in \ker(\overline{\text{res}})$$

as claimed. □

We now conclude the proof of Theorem 1 by showing

Lemma 13. *The map $\nu|_{\ker(\text{res})}$ is surjective, that is, $\text{Im}(\nu|_{\ker(\text{res})}) = \ker(\overline{\text{res}})$.*

Proof. We show that there exists a symmetric idempotent $\iota \in I$ such that

$$X = \underbrace{\left(\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}, \begin{pmatrix} \phi'_1 & \mu' \\ & \phi'_2 \end{pmatrix} \right)}_{=: X'} H_{\iota, u_\iota, v_\iota}$$

and $\delta' \in R^*$. Since $\iota \in I = \ker(\rho/C)$ the set $\iota(C^\perp/C) = \{0\}$ and hence $h_{\iota, u_\iota, v_\iota} \in \ker(\text{res})$. By Lemma 12 $X' \in \text{Im}(\nu|_{\ker(\text{res})})$, so the same holds for X .

Now let us construct ι . The ring $R/\text{rad } R$ is a direct sum of matrix rings over skew fields. Thus there exist $u_1, u_2 \in R^*$ such that $u_1 \delta u_2$ is an idempotent modulo $\text{rad } R$. After conjugating with u_2 we obtain an idempotent $\tilde{u} \delta + \text{rad } R \in R/\text{rad } R$ with $\tilde{u} \in R^*$. Since $\tilde{u} \delta + (I + \text{rad } R) \in R/(I + \text{rad } R)$ is an idempotent as well and $\delta \in 1 + I$ is a unit modulo $I + \text{rad } R$, it follows that $\tilde{u} \in 1 + (I + \text{rad } R)$. We can even assume that $\tilde{u} \in 1 + I$. If $\tilde{u} = 1 + i + r$ with $i \in I$ and $r \in \text{rad } R$ then $(1 + i)\delta = (\tilde{u} - r)\delta$ is an idempotent mod $\text{rad } R$. Additionally, from $\tilde{u} \in R^*$ we get $1 + i \in R^*$, so we can assume $\tilde{u} = 1 + i$. Now $d((\tilde{u}, 0)) \in \ker(\overline{\text{res}})$, thus

$$\begin{aligned} X \in \ker(\overline{\text{res}}) &\Leftrightarrow d((\tilde{u}, 0))X \in \ker(\overline{\text{res}}) \\ &\Leftrightarrow \left(\begin{pmatrix} \tilde{u}^{-J} \alpha & \tilde{u}^{-J} \beta \\ \tilde{u} \gamma & \tilde{u} \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix} \right) \in \ker(\overline{\text{res}}) \end{aligned}$$

Thus we can assume that $\delta + \text{rad } R \in R/\text{rad } R$ is an idempotent.

In the hyperbolic unitary group $\mathcal{U}(R/\text{rad } R, \Phi/\tilde{\Gamma})$ there is

$$\tilde{X} := \left(\begin{pmatrix} \alpha + \text{rad } R & \beta + \text{rad } R \\ \gamma + \text{rad } R & \delta + \text{rad } R \end{pmatrix}, \begin{pmatrix} \phi_1 + \tilde{\Gamma} & \mu + \psi(\text{rad } R) \\ & \phi_2 + \tilde{\Gamma} \end{pmatrix} \right)$$

Lemma 7 says that $e := (1 - \delta) + \text{rad } R$ is a symmetric idempotent of $R/\text{rad } R$; more precisely, we may write $e = u_e v_e$ with

$$\begin{aligned} u_e &= -e \epsilon^{-1} \gamma^J e^J + \text{rad } R, \\ v_e &= e^J \beta e^J + \text{rad } R. \end{aligned}$$

By Lemma 9 we obtain a symmetric idempotent

$$\iota := e + x = 1 - \delta + x \in I$$

with $x \in \text{rad } R \cap I$. We calculate the projection on the first component

$$\pi(X H_{\iota, u_\iota, v_\iota}^{-1}) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \delta^J - x^J & -v_\iota^J \epsilon \\ u_\iota^J & \delta - x \end{pmatrix} = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$$

with $\delta' = -\gamma v_\iota^J \epsilon + \delta - \delta x$. It remains to show that $\delta' \in R^*$. Lemma 10 gives $v_\iota \equiv (1 - \delta^J) \beta (1 - \delta) \pmod{\text{rad } R}$. Also $\delta x \in \text{rad}(R)$, so it remains to show that

$$\tilde{\delta}' := -\gamma(1 - \delta^J) \beta^J \epsilon (1 - \delta) + \delta \in R^*.$$

We observe that $\tilde{\delta}'\delta = -\gamma(1 - \delta^J)\beta^J\epsilon \underbrace{(1 - \delta)\delta + \delta^2}_{=0} = \delta$ and

$$\begin{aligned} (1 - \delta)\tilde{\delta}' &= -(1 - \delta)\gamma(1 - \delta^J)\beta^J\epsilon(1 - \delta) = \\ -(1 - \delta)\gamma\beta^J\epsilon(1 - \delta) + \underbrace{(1 - \delta)\gamma\delta^J\beta^J\epsilon(1 - \delta)}_{=0, \text{ since } \gamma\delta^J = \delta\epsilon^J\gamma^J} &= -(1 - \delta)\gamma\beta^J\epsilon + (1 - \delta)\gamma \underbrace{\beta^J\epsilon\delta}_{=\delta^J\beta} = \\ -(1 - \delta) \underbrace{\gamma\beta^J\epsilon}_{=\delta\epsilon^J\alpha^J\epsilon-1} + \underbrace{(1 - \delta)\gamma\delta^J\beta}_{=0} &= 1 - \delta. \end{aligned}$$

Particularly, $(1 - \delta)(2 - \tilde{\delta}') = 1 - \delta$. Now we see that $\tilde{\delta}'$ is a unit since

$$\tilde{\delta}'(2 - \tilde{\delta}') = \tilde{\delta}'(\delta + (1 - \delta))(2 - \tilde{\delta}') = \tilde{\delta}' - \delta\tilde{\delta}' + \delta = 1 - \delta + \delta = 1.$$

□

REFERENCES

- [1] A. Günther, *Self-dual group ring codes*. PhD Thesis, RWTH Aachen University, in preparation
- [2] H. Nagao, Y. Tsushima, *Representations of finite groups*. Academic Press (1988)
- [3] G. Nebe, E.M. Rains, N.J.A. Sloane, *Self-dual codes and invariant theory*. Springer (2006)