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 ring \( R = (R, M, \psi, \Phi) \). The finite alphabet \( V \) is a left module for the ring \( R \) and the biadditive form \( \beta : V \times V \to \mathbb{Q}/\mathbb{Z} \) 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 $R$-module $\rho_\Phi(\Phi)$ which is a certain subgroup of the group of quadratic mappings $V \to \mathbb{Q}/\mathbb{Z}$. A code $C \leq V^N$ is isotropic, if $C \leq C^\perp$ and

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

Given a finite representation $\rho$, one associates a finite subgroup $\mathcal{C}(\rho)$ of $\text{GL}(C[V])$, 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 $\rho$ is 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 $\rho$. 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

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

is exactly the greatest common divisor of the lengths of self-dual isotropic codes of Type $\rho$. 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 $\rho$. Then the quotient representation $\rho/C$ 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 $\rho$. 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 $\rho$ acts linearly on the space $C[V]$ with basis $\{b_v : v \in V\}$. It is generated by

- $m_r : b_v \mapsto b_{rv}$ for $r \in R^*$
- $d_\phi : b_v \mapsto \exp(2\pi i \phi(\psi(v)))b_v$ for $\phi \in \Phi$
- $h_w : b_v \mapsto \frac{1}{\text{id}_{C[V]} - e^2} \sum_{w \in v} \exp(2\pi i \beta(w, v_\psi))b_{w+(1-e)v}$ for $e^2 = e \in R$ symmetric.

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

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

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

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

(1) 

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

...
such that
\[
\begin{pmatrix}
\gamma^J \alpha & \gamma^J \beta \\
\delta^J \alpha & \delta^J \beta
\end{pmatrix} = \psi_2^{-1} \begin{pmatrix}
\lambda(\phi_1) & m \\
\tau(m) & \lambda(\phi_2)
\end{pmatrix}.
\]
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
\[
d((r, \phi)) = \begin{pmatrix}
r^{-J} & r^{-J} \psi^{-1}(\lambda(\phi)) \\
0 & r
\end{pmatrix},
\]
with \(r \in \mathbb{R}^*, \phi \in \Phi\) and
\[
H_{e,v} = \begin{pmatrix}
1 - e^J u_e & v_e \\
-e^{-1} u_e & 1 - e
\end{pmatrix} \begin{pmatrix}
0 & \psi(-\epsilon e) \\
0 & 0
\end{pmatrix},
\]
where \(e = u_v v_e\) runs through the symmetric idempotents of \(R\).

To formalize the proofs we let \(F(R, \Phi)\) denote the free group on
\[
\{d(r, \phi), H_{e,v} | r \in \mathbb{R}^*, \phi \in \Phi, e = u_v v_e\text{ symmetric idempotent in } R\}.
\]

On these generators there are two group epimorphism:
\[
\pi : F(R, \Phi) \rightarrow \mathcal{U}(R, \Phi), d(r, \phi) \mapsto d((r, \phi)), H_{e,v} \mapsto H_{e,v}
\]
and
\[
(2) \quad p : F(R, \Phi) \rightarrow C(\rho); \quad d(r, \phi) \mapsto m, d_\phi, \quad H_{e,v} \mapsto h_{e,v}.
\]

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

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

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

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
\[
\begin{pmatrix}
\alpha & \beta \\
\gamma & \delta
\end{pmatrix} \begin{pmatrix}
\phi_1 & m \\
\phi_2 & \phi_2
\end{pmatrix} = (\alpha z + \beta x, \gamma z + \delta x, q + \rho(\phi_1)(z) + \rho(\phi_2)(x) + \rho_M(m)(z, x)).
\]

If \(\rho\) is a faithful representation, then this action is faithful.

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

**Lemma 4.** For \(r \in \mathbb{R}^*, \phi \in \Phi\) and \((z, x, q) \in \mathcal{E}(V)\) we have
\[
\Delta(d((r, \phi))(z, x, q)) = (m, d_\phi) \Delta((z, x, q))(m, d_\phi)^{-1}.
\]
Proof. The proof is an easy calculation.

d((r, ϕ))(z, x, q) = (r^{-1} z + r^{-1} ψ^{-1} ϕ(x)) x + q + ρ_Φ(x)

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

\[
\exp(2\pi i q + ρ_Φ(x) + ρ_M(\lambda(ϕ))(r^{-1} v, x)) b_v + x
\]

On the other hand

\[
(m_r d_Φ)Δ((z, x, q))(m_r d_Φ)^{-1}(b_v) = \\
= m_r d_Φ \exp(2\pi i q - ρ_Φ(ϕ)(r^{-1} v)) (b_v - v + x)
\]

\[
= \exp(2\pi i q - ρ_Φ(ϕ)(r^{-1} v)) (b_v - v + x)
\]

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

\[
ρ_M(ϕ)(r^{-1} v, x) = β(r^{-1} v, ψ^{-1} ϕ(x)) = β(v, r^{-1} ψ^{-1} ϕ(x)).
\]

□

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

\[
Δ(H_{e, u_e, v_e}(z, x, q)) = h_{e, u_e, v_e} Δ((z, x, q)) h_{e, u_e, v_e}^{-1}.
\]

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

\[
H_{e, u_e, v_e}(z, x, q) = (v_e x, -e^{-1} u_e^j z, q + β(z, -ex)).
\]

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

\[
V = eV ⊕ (1 - eV)
\]

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

\[
h_{e, u_e, v_e} = (h_{e, u_e, v_e})_{eV} : \mathbb{C}[eV] ⊗ \mathbb{C}[(1 - e)V] \rightarrow \mathbb{C}[V].
\]

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

\[
h_{e, u_e, v_e} Δ((e^j z, 0, 0)) h_{e, u_e, v_e}^{-1}(b_v) = \\
= h_{e, u_e, v_e}(eV)|^{-1/2} \sum_{w ∈ eV} \exp(2\pi i(β(-e^{-1} u_e^j e v, w) + β(w, e^j z)) b_w) \\
= |eV|^{-1} \sum_{w' ∈ eV} \sum_{e ∈ eV} \exp(2\pi i(β(-e^{-1} u_e^j e v, w) + β(w, e^j z) + β(w', v_e w)) b_{w'}).
\]

Now \( β(-e^{-1} u_e^j e v, w) + β(w, e^j z) + β(w', v_e w) = β(-e^{-1} u_e^j e v + e^{-1} z + e^{-1} u_e^j e w') \). Hence the sum over all \( w \) is non-zero, only if \(-e^{-1} u_e^j e v + z + e^{-1} u_e^j e w' = 0 \) which implies
that \( w' = v - \epsilon^{-1}u'_e z \). Hence \( h_{e,v_e,v_e} \circ \Delta((e^I z, 0, 0)) \circ h_{e,v_e,v_e}^{-1} b_v = b_{v - \epsilon^{-1}u'_e z} \). A similar calculation yields

\[
\begin{align*}
h_{e,v_e,v_e} \circ \Delta((0, e x, 0)) \circ h_{e,v_e,v_e}^{-1} b_v &= h_{e,v_e,v_e}(\epsilon V)^{-1/2} \sum_{w \in \epsilon V} \exp(2\pi i (\beta(-\epsilon^{-1}v'_e \epsilon v, w)))b_{w + e x} \\
&= h_{e,v_e,v_e}(\epsilon V)^{-1/2} \sum_{w \in \epsilon V} \exp(2\pi i (\beta(-\epsilon^{-1}v'_e \epsilon v, w - e x)))b_w \\
&= h_{e,v_e,v_e} \circ h_{e,v_e,v_e}^{-1}(\exp(2\pi i (\beta(-\epsilon^{-1}v'_e \epsilon v, ex)))b_v) \\
&= \exp(2\pi i (\beta(v, v, x)))b_v.
\end{align*}
\]

\[\Box\]

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

\[\Box\]

**Remark 6.** Let \( \rho \) be faithful. Lemma 4 and 5 show that every element \( a \in C(\rho) \) induces an automorphism \( \alpha \) 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

\[
\nu : C(\rho) \to \mathcal{U}(R, \Phi), \ a \mapsto \alpha.
\]

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

\[
\theta : \mathcal{U}(R, \Phi) \to C(\rho)/\mathcal{S}(C(\rho)), \ u \mapsto p(\pi^{-1}(u))
\]

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 \( R \).

\[\Box\]

**Proof.** We define \( u_i = -\iota \gamma_i \iota, \ v_i = \iota \beta \iota \) and calculate

\[
\begin{align*}
u_i u_i &= -(1 - \delta)\epsilon^{-1}\gamma_i(1 - \delta) \beta (1 - \delta) \\
&= -(1 - \delta)\epsilon^{-1} \underbrace{\gamma_i \beta}_{=\alpha \delta} (1 - \delta) + (1 - \delta)\epsilon^{-1} \gamma_i \underbrace{(1 - \delta) \beta}_{=\beta \delta}(1 - \delta) \\
&= (1 - \delta)\epsilon^{-1} (1 - \delta) = 1 - \delta = \iota
\end{align*}
\]

and

\[
\begin{align*}
u_i v_i &= -(1 - \delta)\beta (1 - \delta) \epsilon^{-1} \gamma_i (1 - \delta) \\
&= -(1 - \delta)\beta \epsilon^{-1} \gamma_i (1 - \delta) + (1 - \delta)\beta \epsilon^{-1} \gamma_i (1 - \delta) \\
&= (1 - \delta)(-1)(1 - \delta) = 1 - \delta = \iota.
\end{align*}
\]

\[\Box\]
3. \( S(\mathcal{C}(\rho)) \leq S(\mathcal{C}(\rho/C)) \)

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 \( \mathbb{C}[\mathcal{C}^\perp/C] \). This yields a representation

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

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

**Proof.** Let \( \text{Rep} \) denote a set of coset representatives of \( \mathcal{C}^\perp/C \). We define a subspace

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

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

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

So we have

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

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

We now will show that

\[
*_{H} \quad f \circ p(\check{H}_{e,\alpha,\nu_e}) \circ f^{-1} = p/C(\check{H}_{e,\alpha,\nu_e})
\]

and

\[
*_{d} \quad f \circ p(\check{d}((r, \phi))) \circ f^{-1} = p/C(\check{d}((r, \phi)))
\]

where \( p : \mathcal{F}(R, \Phi) \to \mathcal{C}(\rho) \) and \( p/C : \mathcal{F}(R, \Phi) \to \mathcal{C}(\rho/C) \) 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 \(*_{H}\) let \( v + C \in \mathcal{C}^\perp/C \) and let \( T \) denote a set of coset representatives of \( \epsilon \mathcal{C}^\perp/\epsilon C \cong \epsilon \mathcal{C}^\perp/C \). Then
\[ f^{-1} \circ p(\hat{H}_{e,u,v}) \circ f(b_{v+C}) = f^{-1} \circ p(\hat{H}_{e,u,v})(\sum_{c \in C} b_{v+c}) \]
\[ = f^{-1}(\sum_{c \in C} |eV|^{|c|/2} \sum_{w \in eV} \exp(2\pi i \beta(w,v)\langle v+c \rangle)) \]
\[ = f^{-1}(\sum_{c \in C} \sum_{w \in eC^+} \exp(2\pi i \beta(w,v)\langle v+c \rangle)) \]
\[ = f^{-1}(\sum_{w \in eC^+} \sum_{c \in C} \exp(2\pi i \beta(w,v)\langle v+c \rangle)) \]
\[ = f^{-1}(\sum_{w \in eC^+} \sum_{c \in C} \exp(2\pi i \beta(w,v)\langle v+C \rangle)) \]
\[ = f^{-1}(\sum_{w \in eC^+} \exp(2\pi i \beta(w,v+C)\langle v+C \rangle)) \]
\[ = p/C(\hat{H}_{e,u,v})(b_{v+c}). \]

To show \( \ast_d \) we note that \( \rho \phi(c)(\langle c \rangle) = 0 \) for all \( c \in C \) and for all \( \phi \in \Phi \) and obtain
\[ f^{-1} \circ p(\hat{d}(\langle r, \phi \rangle)) \circ f(b_{v+C}) = f^{-1} \circ p(\hat{d}(\langle r, \phi \rangle))(\sum_{c \in C} b_{v+c}) \]
\[ = f^{-1}(\sum_{c \in C} \exp(2\pi i \rho \phi(c)(v+c)\langle v+c \rangle)) \]
\[ = f^{-1}(\sum_{c \in C} \exp(2\pi i \rho \phi(c)(v+c)\langle v+c \rangle)) \]
\[ = f^{-1}(\sum_{c \in C} \exp(2\pi i \rho \phi(c)(v+c)\langle v+c \rangle)) \]
\[ = f^{-1}(\sum_{c \in C} \exp(2\pi i \rho \phi(c)(v+c)\langle v+c \rangle)) \]
\[ = f^{-1}(\sum_{c \in C} \exp(2\pi i \rho \phi(c)(v+c)\langle v+c \rangle)) \]
\[ = p/C(\hat{d}(\langle r, \phi \rangle))(b_{v+c}). \]

\[ \Box \]

4. The strategy.

Without loss of generality we now assume that \( \rho \) is faithful, that is,
\[ \ker(\rho) = (\operatorname{Ann}_R(V), \ker(\rho \phi)) = (0,0) \]
and let \( (I, \Gamma) = \ker(\rho/C) \). We then define \( \text{Res} : \mathcal{U}(R, \Phi) \to \mathcal{U}(R/I, \Phi/\Gamma) \) by
\[ \text{Res}(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ \phi_2 & \phi \end{pmatrix}) = \begin{pmatrix} \alpha + I & \beta + I \\ \gamma + I & \delta + I \end{pmatrix}, \begin{pmatrix} \phi_1 + \Gamma & m + \psi(I) \\ \phi_2 + \Gamma \end{pmatrix}). \]
By Remark 6 the epimorphism
\[ \nu : \mathcal{C}(\rho) \to \mathcal{U}(R, \Phi) \] by \( \nu(m, d) = \delta((r, \phi)) \), \( \nu(h, u, \nu) = H_{e, u, \nu} \)
for \( r \in R^*, \phi \in \Phi \) and symmetric idempotents \( e = u, \nu \in R \) is well defined and its kernel is \( S(\mathcal{C}(\rho)) \). Similarly \( \overline{\nu} : \mathcal{C}(\rho/\mathcal{C}) \to \mathcal{U}(R/I, \Phi/\Gamma) \). Then \( \nu \circ p = \pi \) and \( \pi \circ p/C = \pi/C \), where \( \pi/C : \mathcal{F}(R/I, \Phi/\Gamma) \to \mathcal{U}(R/I, \Phi/\Gamma) \) is the analogous group epimorphism. Again the representation \( \rho/C \) of \( (R/I, \Phi/\Gamma) \) is faithful so by Remark 6 the kernel of \( \pi \) is \( S(\mathcal{C}(\rho/C)) \).

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

\[
\begin{array}{ccccccccc}
1 & & 1 & & 1 & & 1 & & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \rightarrow & \ker(\text{res}) & \rightarrow & \ker(\overline{\nu}) & \rightarrow & \mathcal{Y}' & \rightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathcal{S}(\mathcal{C}(\rho)) & \rightarrow & \mathcal{C}(\rho) & \rightarrow & \mathcal{U}(R, \Phi) & \rightarrow & 1 \\
\downarrow & & \downarrow \text{res} & & \downarrow & & \downarrow & & \downarrow \\
\mathcal{S}(\mathcal{C}(\rho/C)) & \rightarrow & \mathcal{C}(\rho/C) & \rightarrow & \mathcal{U}(R/I, \Phi/\Gamma) & \rightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathcal{Y} & & 1 & & 1 & & 1 & & 1 \\
\downarrow & & & & & & & & \\
1 & & & & & & & & \\
\end{array}
\]

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 \( \overline{\nu} \) and res are surjective, since idempotents and units of \( R/I \) lift to idempotents and units of \( R \). Moreover \( \overline{\nu} \circ \text{res} = \overline{\nu} \circ \text{res} \) 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

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

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 \( e^2 \equiv e \mod \text{rad} \ R \) then there exists an idempotent \( e' \in I \) such that \( e' \equiv e \mod \text{rad} \ R \).

**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 \( R \) \cite[Theorem 4.9]{2} 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 \cite[Theorem 4.5]{2} applied to an idempotent \( e \in R \), the right-modules \( eR \) and \( e'R \) 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
\[
e + \text{rad} \ R = u_e v_e + \text{rad} \ R,
\]
\[
e' + \text{rad} \ R = v_e u_e + \text{rad} \ R,
\]
We therefore find $H$.

Furthermore, $U$ for some $\tilde{v}_e \in eR$. If $e \in R$ is an idempotent then $e$ is symmetric as well. More precisely, there exist $\tilde{u}_e \in eR'$, $\tilde{v}_e \in eR$ such that

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

and $\tilde{v}_e \equiv v_e \mod R$.

For the rest of this note, let

$$X := \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right), \quad \left( \begin{array}{c} \phi_1 \\ m \phi_2 \end{array} \right) \in \ker(\mathfrak{res})$$

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 $d(P(R, \Phi)) \cap \ker(\mathfrak{res}) \subseteq \text{Im}(\nu|_{\ker(\text{res})})$.

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

Lemma 12. Let $\delta$ 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 $U(R, \Phi)$ generated by the elements $d(P(R, \Phi)) \cap \ker(\mathfrak{res})$. 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 $d((\delta, \phi_2)) = \left( \begin{array}{cc} \delta^{-J} & \beta \\ 0 & \delta \end{array} \right), \left( \begin{array}{c} 0 \\ \phi_2 \end{array} \right)$ and hence $d((\delta, \phi_2))^{-1} = \left( \begin{array}{cc} \delta^J & -\delta^{-J}\beta^{-1} \\ 0 & \delta^{-1} \end{array} \right), \left( \begin{array}{c} 0 \\ -\phi_2[\delta^{-1}] \end{array} \right)$. We therefore find $d((\delta, \phi_2))^{-1}X = \left( \begin{array}{cc} \delta^J\alpha - \delta^{-J}\beta\delta^{-1}\gamma & 0 \\ \delta^{-1}\gamma & 0 \end{array} \right)$, $\left( \begin{array}{c} -\phi_2[\delta^{-1}] + \phi_1 \tilde{m} \\ 0 \end{array} \right)$ for some $\tilde{m} \in M$. Since the upper right entry in the first matrix of this element of $U(R, \Phi)$ is 0 we obtain $\tilde{m} = 0$ and similarly $\delta^J\alpha - \delta^{-J}\beta\delta^{-1}\gamma = 1$ and we get $d((\delta, \phi_2))^{-1}X = \left( \begin{array}{cc} 1 & 0 \\ \delta^{-1}\gamma & 0 \end{array} \right), \left( \begin{array}{c} -\phi_2[\delta^{-1}] + \phi_1 \\ 0 \end{array} \right)$. Furthermore,

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

Then we have $(d((\delta, \phi_2))^{-1}X)^{H_{1,1,1}} = \left( \begin{array}{cc} 1 & -\epsilon\delta^{-1}\gamma \\ 0 & 1 \end{array} \right), \left( \begin{array}{c} 0 \\ m' \end{array} \right)$, with some $m' \in M$ and $\phi = \{\psi(-\epsilon\delta^{-1}\gamma)\} - \phi_2[\delta^{-1}] + \phi_1 \in \Gamma$, 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 $H_{1,1,1}^{-1}d((\delta, \phi_2))^{-1}XH_{1,1,1} = d((1, \phi)) \in \ker(\mathfrak{res})$.
Lemma 13. The map $\nu|_{\ker(\rho)}$ is surjective, that is, $\text{Im}(\nu|_{\ker(\rho)}) = \ker(\overline{\rho})$.

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

$$X = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}, \begin{pmatrix} \phi_1' & \mu' \\ \phi_2' \end{pmatrix} \right) \in H_{\iota,u,v},$$

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

Now let us construct $\iota$. 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 $\tilde{u}\delta + (I + \text{rad} R) \subseteq R/(I + \text{rad} R)$ 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 $d((\tilde{u}, 0)) \in \ker(\overline{\rho})$, thus

$$X \in \ker(\overline{\rho}) \iff d((\tilde{u}, 0))X \in \ker(\overline{\rho})$$

$$\iff \left( \begin{pmatrix} \tilde{u}^{-1} & 0 \\ 0 & \tilde{u}^{-1} \end{pmatrix}, \begin{pmatrix} \tilde{u}^{-1} & 0 \\ 0 & \tilde{u}^{-1} \end{pmatrix} \right) \in \ker(\overline{\rho})$$

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

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

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

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

$$u_\epsilon = -\epsilon e^{-1} \gamma J e J + \text{rad} R,$$

$$v_\epsilon = e J \beta e J + \text{rad} R.$$ 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

$$\pi(X H_{\iota,u,v}) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

$$\begin{pmatrix} \delta' - x' & -v_\epsilon' \\ u_\epsilon' \delta - x \end{pmatrix} = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$$

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

$$\tilde{\delta}' := -\gamma(1 - \delta J)\beta e(1 - \delta) + \delta \in R^*.$$
We observe that $\tilde{\delta} \delta = -\gamma (1 - \delta^J) \beta^J \epsilon (1 - \delta) \delta + \delta^2 = \delta$ and

$$(1 - \delta) \tilde{\delta} = - (1 - \delta) \gamma (1 - \delta^J) \beta^J \epsilon (1 - \delta) = 0,$$

$$(1 - \delta) \beta^J \epsilon (1 - \delta) + (1 - \delta) \gamma \delta^J \beta^J \epsilon (1 - \delta) = 0,$$

$$(1 - \delta) \gamma \beta^J \epsilon + (1 - \delta) \gamma \delta^J \beta^J \epsilon = 1 - \delta.$$

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

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

□

References