Codes and Invariant Theory

G. NEBE, Abteilung Reine Mathematik, Universität Ulm, Germany
E. M. RAINS, Institute for Defense Analyses, Princeton, New Jersey
N. J. A. SLOANE, AT&T Shannon Labs, Florham Park, New Jersey

1 Introduction

One of the most remarkable theorems in coding theory is Gleason’s theorem [7] that the weight enumerator of a binary doubly-even self-dual code is an element of the polynomial ring generated by the weight enumerators of the Hamming code of length 8 and the Golay code of length 24. The authors have recently found a far-reaching generalization of this result that applies to arbitrary-genus weight enumerators of self-dual codes over a large class of finite rings and modules. The purpose of this paper is to give a brief summary of these results.

The main result (Theorem 3.5 below) can be stated informally as follows. Given a quasi-chain ring $R$ and a notion of self-duality for codes over $R$, we construct a “Clifford-Weil” group $G$ such that the vector-invariants of $G$ are spanned by the full weight enumerators of self-dual isotropic codes and the polynomial invariants of $G$ are spanned by the complete weight enumerators of these codes.

In the case of the genus-$m$ weight enumerators of Type I binary self-dual codes and $m \geq 1$, we recover the real Clifford group $C_m$ of our earlier paper [10]. Similarly, if $C$ is a Type II code, $G$ is the complex Clifford group $X_m$ of [10]. The case $m = 1$ gives the original Gleason theorem (except for the specific identification of codes that generate the ring).

For self-dual codes over $\mathbb{F}_p$ containing the all-ones vector ($p$ an odd prime) we recover the group $C_m^{(p)}$ of [10, Section 7].

The proof of the main theorem will be the subject of our forthcoming book [11]. The proof is best carried out via a categorical approach, using the concept of a form ring. However, it is not necessary to understand this theory to state and apply the theorem. For further details the reader is referred to [11].

To illustrate the theorem we will construct the Clifford-Weil groups for generalized doubly-even codes over fields of characteristic 2, doubly-even codes over $\mathbb{Z}/2^t\mathbb{Z}$ and self-dual codes over the noncommutative ring $\mathbb{F}_q + u\mathbb{F}_q$.

2 Self-dual isotropic codes.

Throughout the paper, $R$ will denote a ring (with unit element 1) and $V$ a left $R$-module.

**Definition 2.1.** A (linear) code $C$ of length $N$ over $V$ is an $R$-submodule of the left $R$-module $V^N$. 
Coding theory usually deals with codes over a finite alphabet $V$. Therefore we will assume in the following that $V$ is a finite left $R$-module over the finite ring $R$. In fact, our explicit construction of the Clifford-Weil group only applies to the case of finite modules.

To express self-duality, we need a nonsingular bilinear form $\beta$ on $V$. Since $V$ is finite, $\beta$ can be chosen to have values in $\mathbb{Q}/\mathbb{Z}$. Then

$$\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z}) := \{ \beta : V \times V \to \mathbb{Q}/\mathbb{Z} \mid \beta \text{ is } \mathbb{Z}\text{-bilinear} \}$$

is nonsingular, if $v \mapsto \beta(v, \cdot)$ is an isomorphism of the abelian groups $V$ and $V^* = \text{Hom}(V, \mathbb{Q}/\mathbb{Z})$.

**Definition 2.2.** Let $C \leq V^N$ be a code and $\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$ a nonsingular bilinear form. The dual code (with respect to $\beta$) is

$$C^\perp := \{ x = (x_1, \ldots, x_N) \in V^N \mid \sum_{i=1}^N \beta(x_i, c_i) = 0 \text{ for all } c = (c_1, \ldots, c_N) \in C \}.$$ 

$C$ is called *self-dual* (with respect to $\beta$) if $C = C^\perp$.

To express certain additional constraints on the code (e.g. that weights are divisible by 4 for binary codes, or that the code contains the all-ones vector $1 = (1, \ldots, 1)$, etc.) we use quadratic mappings, which we define to be sums of quadratic forms and linear forms on $V$ with values in $\mathbb{Q}/\mathbb{Z}$:

**Definition 2.3.** Let $\text{Quad}_0(V, \mathbb{Q}/\mathbb{Z}) :=$

$$\{ \phi : V \to \mathbb{Q}/\mathbb{Z} \mid \phi(x + y + z) - \phi(x + y) - \phi(x + z) - \phi(y + z) + \phi(x) + \phi(y) + \phi(z) = 0 \}.$$ 

Let $\Phi \subset \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ and let $C \leq V^N$ be a code. Then $C$ is called *isotropic* (with respect to $\Phi$) if $\phi(c) := \sum_{i=1}^N \phi(c_i) = 0$ for all $c \in C$ and $\phi \in \Phi$.

**Remark.** Let $V$ be a left $R$-module. Then

(a) $\text{Bil}(V, \mathbb{Q}/\mathbb{Z})$ is a right $R \otimes R$-module via $\beta(r \otimes s)(v, w) = \beta(rv, sw)$ for all $\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$, $v, w \in V$, $r, s \in R$.

(b) $\text{Bil}(V, \mathbb{Q}/\mathbb{Z})$ has a natural involution $\tau$ defined by $(\beta^\tau)(v, w) := \beta(w, v)$ for all $\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$, $v, w \in V$.

(c) The group $\text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ is an $R$-module via $\phi[r](v) = \phi(rv)$ for all $\phi \in \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$, $r \in R$ and $v \in V$. This means that the “action” satisfies $[rs] = [r][s]$ and $[r+s+t] - [r+s] - [r+t] - [s+t] + [r] + [s] + [t] = 0$ for all $r, s, t \in R$.

(d) The mapping $[-1]$ is an involution on $\text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$.

(e) There is a mapping $\{\} : \text{Bil}(V, \mathbb{Q}/\mathbb{Z}) \to \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ defined by $\{\beta\}(v) := \beta(v, v)$ for all $\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$, $v \in V$. 

2
(f) There is a mapping $\lambda : \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z}) \to \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$ defined by $(\lambda(\phi))(v, w) := \phi(v + w) - \phi(v) - \phi(w)$ for all $\phi \in \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$, $v, w \in V$.

(g) Both mappings $\lambda$ and $\beta$ are $R$-module homomorphisms, where $\text{Bil}(V, \mathbb{Q}/\mathbb{Z})$ is regarded as an $R$-module via $\beta[r](v, w) := \beta(rv, rw)$ for all $\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$, $v, w \in V$, $r \in R$.

(h) For all $\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$ and $\phi \in \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ we have

\[
\begin{align*}
\{\beta^r\} &= \{\beta\}, \\
\lambda(\phi)^r &= \lambda(\phi), \\
\lambda(\{\beta\}) &= \beta + \beta^r, \\
\phi[r + s] - \phi[r] - \phi[s] &= \{\lambda(\phi)(r \otimes s)\}.
\end{align*}
\]

(i) For all $\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$ and $\phi \in \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ we have

\[
\lambda(\{\lambda(\phi)\}) = 2\lambda(\phi) \text{ and } \{\lambda(\{\beta\})\} = 2\{\beta\}.
\]

We call $\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$ admissible if $\beta$ is nonsingular and the $(1 \otimes R)$-submodule $M := \beta(1 \otimes R) = \{\beta_r = \beta(1 \otimes r) \mid r \in R\}$ (where $\beta_r(v, w) = \beta(v, rw)$) generated by $\beta$ is closed under $\tau$ and isomorphic to $R$, i.e. if

$$
\psi : r \mapsto \beta_r
$$

defines an isomorphism of right $R$-modules $\psi : R_R \to M_{1 \otimes R}$.

Note that any admissible $\beta$ defines an anti-automorphism $J$ of $R$ by $r \mapsto r^J$ with

$$
\beta(rv, w) = \beta(v, r^Jw) \text{ for all } v, w \in V.
$$

Let $\epsilon \in R$ be defined by $\beta(v, w) = \beta(w, \epsilon v)$ for all $v, w \in V$. Then $\epsilon^J r (r^J) \epsilon = r$ for all $r \in R$. In particular $\epsilon^J \epsilon = 1$ and since $R$ is finite, $\epsilon$ is a unit.

**Definition 2.4.** The quadruple $\rho := (R, V, \beta, \Phi)$ is called a (finite representation of a) *form ring* if $R$ is a finite ring, $V$ is a finite left $R$-module, $\beta \in \text{Bil}(V, \mathbb{Q}/\mathbb{Z})$ is an admissible bilinear form, and $\Phi \leq \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ is a sub-$R$-qmodule such that $\{M\} \leq \Phi$ and $\lambda(\Phi) \leq M$, for $M := \beta(1 \otimes R)$.

If $C \leq V^N$ is self-dual with respect to $\beta$ and isotropic with respect to $\Phi$, $C$ is called a (self-dual isotropic) code of Type $\rho$.

**Remark.** In [11], $\rho$ denotes a finite representation of an abstract form ring. For our purposes here it is enough to work with the above concrete realization of $\rho$, which we will also call a form ring.
3 Weight enumerators and Clifford-Weil groups.

There are many possible notions of weight enumerators of codes (see e.g. [13]). We introduce only the complete weight enumerator of a code $C$, though analogues of our main theorem hold for full weight enumerators and other suitable symmetrizations of the full weight enumerator.

**Definition 3.1.** Let $C \subseteq V^N$ be a code. The complete weight enumerator of $C$ is
\[
\text{cwe}(C) := \sum_{c \in C} \prod_{i=1}^{N} x_{c_i} \in \mathbb{C}[x_v \mid v \in V].
\]
The genus-$m$ complete weight enumerator of $C$ is
\[
\text{cwe}_m(C) := \sum_{\{c^{(1)}, \ldots, c^{(m)}\} \subseteq C^m} \prod_{i=1}^{N} x_{(c^{(1)}_i, \ldots, c^{(m)}_i)} \in \mathbb{C}[x_v \mid v \in V^m].
\]

The genus-$m$ weight enumerator of $C$ can be obtained from the usual weight enumerator of $C(m) := C \otimes R^m \leq V^N \otimes R^m \cong V^m$. Note that $C(m)$ is a code over the ring $\text{Mat}_m(R)$.

**Remark 3.2.** If we identify $V^m \cong (V^m)^N$ and consider $C(m)$ as a code in $(V^m)^N$, then $\text{cwe}_m(C) = \text{cwe}(C(m))$.

This last remark is one of the main reasons why we allow arbitrary (in general noncommutative) ground rings: to handle genus-$m$ weight enumerators even for classical binary codes, $\text{Mat}_m(\mathbb{F}_2)$ arises naturally as a ground ring.

Let $\rho = (R, V, \beta, \Phi)$ be a form ring. Let $C \subseteq V^N$ be a self-dual isotropic code of Type $\rho$. Then the complete weight enumerator $\text{cwe}(C)$ is invariant under the substitutions
\[
\rho(r) : x_v \mapsto x_{rv} \quad \text{for all } r \in R^* \quad \text{(since } C \text{ is a code)},
\]
\[
\rho(\phi) : x_v \mapsto \exp(2\pi i \phi(v)) x_v \quad \text{for all } \phi \in \Phi \quad \text{(since } C \text{ is isotropic)},
\]

as well as the MacWilliams transformation
\[
h : x_v \mapsto \sqrt{|V|}^{-1} \sum_{w \in V} \exp(2\pi i \beta(w, v)) x_w \quad \text{(since } C = C^\perp).\]

If $R = \mathbb{Z}/6\mathbb{Z}$ for example, we have the MacWilliams transformations modulo 2 and modulo 3. For general rings $R$, one can similarly construct further MacWilliams transformations using symmetric idempotents.

**Example 3.3.** Let $V' = \iota R$ for some idempotent $\iota$. Then $V'$ admits a nonsingular $J$-Hermitian form if and only if there is an isomorphism of right $R$-modules
\[
\kappa : \iota R \cong \iota^J R,
\]

4
in which case we say that the idempotent is symmetric. Note that any isomorphism \( \kappa \) has the form
\[
\kappa(\iota x) = v_i x, \quad \kappa^{-1}(\iota' x) = u_i x,
\]
where \( u_i \in i \mathcal{R}_t^J \) and \( v_i \in i^J \mathcal{R}_t \) satisfy \( u_i v_i = \iota, \ v_i u_i = \iota' \).

If \( \iota = u_i v_i \) is a symmetric idempotent in \( \mathcal{R} \), then let
\[
h_{u_i v_i} : x_v \mapsto \sqrt{|\iota V|} \sum_{w \in \iota V} \exp(2\pi i \beta(w, v_i v w)) x_{w + (1 - \iota) w}
\]
be the partial MacWilliams transformation on \( \iota V \).

**Definition 3.4.** Let \( \rho = (\mathcal{R}, V, \beta, \Phi) \) be a form ring. Then the associated Clifford-Weil group is
\[
\mathcal{C}(\rho) := \langle \rho(r), \rho(\phi), h_{u_i v_i} \mid r \in R^*, \phi \in \Phi, \ i \text{ symmetric idempotent in } \mathcal{R} \rangle \leq \text{GL}_{|V|}(\mathbb{C}).
\]

The above discussion shows that the complete weight enumerator of a self-dual isotropic code of Type \( \rho \) is invariant under the action of the group \( \mathcal{C}(\rho) \). For a subgroup \( G \leq \text{GL}_n(\mathbb{C}) \) let
\[
\text{Inv}(G) := \{ p \in \mathbb{C}[x_1, \ldots, x_n] \mid p(gX) = p(X) \text{ for all } g \in G \}
\]
denote the invariant ring of \( G \).

Now we can state our main theorem, part (i) of which is clear from the above considerations and the MacWilliams identities. We cannot at present prove part (ii) for arbitrary finite rings, but need to assume (for example) that \( \mathcal{R} \) is a chain ring (i.e. the left ideals in \( \mathcal{R} \) are linearly ordered by inclusion) or, more generally, a quasi-chain ring, by which we mean a direct product of matrix rings over chain rings.

**Theorem 3.5.** Let \( \rho = (\mathcal{R}, V, \beta, \Phi) \) be a form ring.

(i) If \( \mathcal{C} \leq V^N \) be a self-dual isotropic code, \( \text{cwe}(\mathcal{C}) \in \text{Inv}(\mathcal{C}(\rho)) \).

(ii) If \( \mathcal{R} \) is a finite quasi-chain ring, \( \text{Inv}(\mathcal{C}(\rho)) \) is spanned by complete weight enumerators of self-dual isotropic codes of Type \( \rho \):
\[
\text{Inv}(\mathcal{C}(\rho)) = \langle \text{cwe}(\mathcal{C}) \mid \mathcal{C} \text{ self-dual, isotropic code in } V^N, N \in \mathbb{N} \rangle.
\]

To deal with higher-genus weight enumerators we introduce the Clifford-Weil group \( \mathcal{C}_m(\rho) := \mathcal{C}(\rho \otimes \mathbb{R}^m) \) of genus \( m \). By Remark 3.2 the invariant ring of \( \mathcal{C}_m(\rho) \) is spanned by the genus-\( m \) weight enumerators of self-dual codes of Type \( \rho \).

Let \( \rho := (\mathcal{R}, V, \beta, \Phi) \) be a form ring. By Morita theory (see [11]), this corresponds to a unique form ring
\[
\text{Mat}_m(\rho) = \rho \otimes R^m := (\text{Mat}_m(\mathcal{R}), V \otimes R^m, \beta(m), \Phi_m)
\]
which we call a matrix ring for the form ring \( \rho \). Here \( \beta^{(m)} \) is the bilinear form on \( V^m = V \otimes R^m \) (admissible for \( \text{Mat}_m(R) \)) defined by

\[
\beta^{(m)}((v_1, \ldots, v_m), (w_1, \ldots, w_m)) = \sum_{i=1}^{m} \beta(v_i, w_i),
\]

\( \beta^{(m)} \) generates the \( \text{Mat}_m(R) \)-module \( M := \beta^{(m)}(1 \otimes \text{Mat}_m(R)) \), and

\[
\Phi_m = \left\{ \begin{pmatrix} \phi_1 & m_{12} & \ldots & m_{1m} \\ \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & m_{m-1,m} \\ \phi_m & \end{pmatrix} \mid \phi_1, \ldots, \phi_m \in \Phi, m_{ij} \in M \right\},
\]

where

\[
\begin{pmatrix} \phi_1 & m_{12} & \ldots & m_{1m} \\ \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & m_{m-1,m} \\ \phi_m & \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = \sum_{i=1}^{m} \phi_i(v_i) + \sum_{i<j} m_{ij}(v_i, v_j).
\]

One easily sees that \( \Phi_m \) is a sub-\( \text{Mat}_m(R) \)-module of \( \text{Quad}_q(V \otimes R^m) \). Note that the involution \( J^m \) on \( \text{Mat}_m(R) \) acts as componentwise application of \( J \) followed by transposition. The unit \( \epsilon_m \in \text{Mat}_m(R) \) is the scalar matrix \( \epsilon I_m \).

**Definition 3.6.** We call \( C_m(\rho) := C(\rho \otimes R^m) \) the associated Clifford-Weil group of genus \( m \).

4 The structure of the Clifford-Weil groups.

The group \( C(\rho) \) is a projective representation of a so-called hyperbolic co-unitary group \( \mathcal{U}(R, \Phi) \), which can be defined abstractly in terms of \( R \), the involution \( J \), and the \( R \)-qmodule \( \Phi \). \( \mathcal{U}(R, \Phi) \) is an extension of the linear \( R \)-module \( \ker(\lambda) \oplus \ker(\lambda) \) by a certain group \( G \) of \( 2 \times 2 \) matrices over the ring \( R \).

Let \( \rho := (R, V, \beta, \Phi) \) be a form ring and let \( M := \beta(1 \otimes R) \). Then, by the above construction of the \( 2 \times 2 \)-matrix ring for a form ring, \( \Phi_2 \) is a \( \text{Mat}_2(R) \) sub-qmodule of \( \text{Quad}_q(V \otimes R^2) \). In particular, \( \Phi_2 \) is a module for the unit group of \( \text{Mat}_2(R) \) and we can form the semi-direct product \( \text{GL}_2(R) \ltimes \Phi_2 \) of which \( \mathcal{U}(R, \Phi) \) will be a subgroup. Applying \( \lambda \) and \( \psi \) componentwise, we get mappings \( \lambda_2 : \Phi_2 \to \text{Mat}_2(M) \) defined by

\[
\lambda_2\left( \begin{pmatrix} \phi_1 \\ m \\ \phi_2 \end{pmatrix} \right) := \begin{pmatrix} \lambda(\phi_1) \\ m \\ \lambda(\phi_2) \end{pmatrix}
\]

and \( \psi_2 : \text{Mat}_2(R) \to \text{Mat}_2(M) \). Then \( \mathcal{U}(R, \Phi) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ \phi_2 \end{pmatrix} \} \in \text{GL}_2(R) \ltimes \Phi_2 \mid \psi_2\left( \begin{pmatrix} c^d a & c^d b \\ d^d a & d^d b \end{pmatrix} \right) = \lambda_2\left( \begin{pmatrix} \phi_1 & m \\ \phi_2 \end{pmatrix} \right) \}. \)
Remark. To describe the isomorphism type of \( \mathcal{U}(R, \Phi) \) note that
\[
\pi : \mathcal{U}(R, \Phi) \to \text{GL}_2(R), \quad (u, \phi) \mapsto u,
\]
defines a group homomorphism. The kernel of \( \pi \) is the set of all \((1, \phi) \in \mathcal{U}(R, \Phi)\), i.e.
\[
\ker(\pi) = \{(1, \begin{pmatrix} \phi_1 & 0 \\ \phi_2 & \end{pmatrix}) \mid \phi_1, \phi_2 \in \Phi, \ \lambda(\phi_1) = \lambda(\phi_2) = 0\}
\]
which is naturally isomorphic to \( \ker(\lambda) \times \ker(\lambda) \). The image of \( \pi \) is
\[
\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(R) \mid \left( \begin{array}{cc} a^t & c^t \\ b^t & d^t \end{array} \right) \left( \begin{array}{rr} 0 & 0 \\ 0 & 0 \end{array} \right) - \left( \begin{array}{rr} 0 & 0 \\ \psi^{-1}_2(\lambda_2(\Phi_2)) \end{array} \right) \right\}.
\]
In many important examples it is easy to describe the image of \( \psi^{-1}_2 \lambda_2 \) (e.g. all symmetric, skew-symmetric or hermitian elements) which establishes an isomorphism of \( \mathcal{U}(R, \Phi)/\ker(\pi) \) with (a subgroup of) a classical group.

Example 4.1. Let \( R \) be one of the following finite simple rings with involution. Then \( \mathcal{C}(\rho) = Z \mathcal{U}(R, \Phi) = Z(\ker(\lambda) \oplus \ker(\lambda)) \mathcal{G}(R, \Phi) \) where \( \mathcal{G}(R, \Phi) \) is one of the following classical groups:

\[
\begin{array}{|c|c|c|c|}
\hline
R & J & \epsilon & \mathcal{G}(R, \Phi) \\
\hline
\mathbb{F}_q^{\times n} \oplus \mathbb{F}_q^{\times n} & \langle s, r \rangle^J &=& (s, r) \\
\hline
\mathbb{F}_q^{n \times n} & r^J = (r^t)^{tr} & 1 & \text{GL}_{2n}(\mathbb{F}_q) \\
\hline
\mathbb{F}_q^{n \times n}, p > 2 & r^J = r^{tr} & 1 & \text{Sp}_{2n}(\mathbb{F}_q) \\
\hline
\mathbb{F}_q^{n \times n}, p > 2 & r^J = r^{tr} & -1 & O_{2n}^+(\mathbb{F}_q) \\
\hline
\mathbb{F}_q^{n \times n}, p = 2 & \psi^{-1}(\lambda(\Phi)) = \{r \in R \mid r^J = r\} & \text{Sp}_{2n}(\mathbb{F}_q) \\
\hline
\mathbb{F}_q^{n \times n}, p = 2 & \psi^{-1}(\lambda(\Phi)) = \{0\} & O_{2n}^+(\mathbb{F}_q) \\
\hline
\end{array}
\]

Recall that a ring \( R \) is semiperfect (Lam, [8, page 346]) if \( R/\text{rad}R \) is semisimple and idempotents of \( R/\text{rad}R \) lift to idempotents of \( R \); in particular, all finite rings are semiperfect. One can show the following

Theorem 4.2. (See [11]) If \( R \) is semiperfect, then the hyperbolic co-unitary group \( \mathcal{U}(R, \Phi) \) is generated by
\[
d((u, \phi)) := \left( \begin{array}{cc} u^{-J} & u^{-J}\psi^{-1}(\lambda(\phi)) \\ 0 & \phi \end{array} \right) \left( \begin{array}{cc} 0 & 0 \\ 0 & \phi \end{array} \right).
\]
for all \( u \in R^* \), \( \phi \in \Phi \) and

\[
H_{u, v_i} := \begin{pmatrix}
1 - \varepsilon^I & v_i \\
-\varepsilon^{-1} u_i^J & 1 - \varepsilon
\end{pmatrix}, \quad \left(0 \quad \psi(-\varepsilon)\right)
\]

for all symmetric idempotents \( \varepsilon \in R \).

Then the projective representation \( \mathcal{U}(R, \Phi) \to \mathcal{C}(\rho) \) is defined by

\[
d(u, \phi) \mapsto \rho(u) \rho(\phi)
\]

and

\[
H_{u, v_i} \mapsto h_{v_i}.
\]

Hence \( \mathcal{C}(\rho) \) is an extension

\[
1 \to Z \to \mathcal{C}(\rho) \to \mathcal{U}(R, \Phi) \to 1
\]

where \( Z \) consists of scalar matrices (since the projective representation can be seen to be irreducible). If Theorem 3.5 holds for \( \rho \), then by invariant theory \( Z \cong Z_l \) is cyclic of order \( l \), where \( l = \gcd(\{N \mid \exists C \leq V^N, \text{ of Type } \rho\}) \).

5 **Doubly-even euclidean self-dual codes over** \( \mathbb{F}_{2^f} \).

(For further details about this section see [9].) In [12] Quebbemann defines the notion of an even code over the field \( k := \mathbb{F}_{2^f} \) as follows. \( C \leq k^N \) is called even if

\[
\sum_{i=1}^N c_i = 0 \quad \text{and} \quad \sum_{i<j} c_i c_j = 0, \quad \text{for } c \in C.
\]

One easily sees that even codes are self-orthogonal with respect to the usual bilinear form \( \sum_{i=1}^N c_i c_i^t \). If \( f = 1 \), the even codes are precisely the doubly-even binary codes. Moreover, identifying \( k \) with \( \mathbb{F}_{2^f} \) using a self-complementary (or trace-orthonormal) basis, even codes in this sense remain even over \( \mathbb{F}_2 \). A self-dual even code in this sense is called a **generalized doubly-even self-dual code**. Similarly, over \( \mathbb{F}_4 \), codes of Type \( \rho \) are exactly the Type II codes over \( \mathbb{F}_4 \) considered in [6].

The Type of these codes can be specified in the language of form rings as follows: Let \( R = \mathbb{F}_{2^f} \), \( V = R \) and \( \beta : V \times V \to \frac{1}{2} \mathbb{Z}/\mathbb{Z} \) be defined by \( \beta(x, y) := \frac{1}{2} \text{tr}(xy) \), where \( \text{tr} \) denotes the trace from \( \mathbb{F}_{2^f} \) to \( \mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z} \). Then \( \beta \) is admissible and \( M := \beta(1 \otimes R) = \{ \beta_a := \beta(1 \otimes a) \mid a \in R\} \).

To define the quadratic forms, one has to consider values modulo 4. Let \( O := \mathbb{Z}[\mathbb{Z}_{2^f-1}] \) be the ring of integers in the unramified extension of degree \( f \) of the 2-adic numbers. Then \( R \cong O/2O \). If \( x \in R \), then \( x^2 \) is uniquely determined modulo 4, therefore squares
of elements of \( R \) can be considered as elements of \( O/4O \). The usual trace \( \operatorname{Tr} : O \to \mathbb{Z} \) maps \( 4O \) into \( 4\mathbb{Z} \). For \( a \in R \) define

\[
\phi_a : V \to \frac{1}{4}\mathbb{Z}/\mathbb{Z}, \quad \phi_a(x) := \frac{1}{4} \operatorname{Tr}(a^2 x^2) \in \operatorname{Quad}_d(V, \mathbb{Q}/\mathbb{Z})
\]

and let \( \Phi := \{ \phi_a \mid a \in R \} \). Then \( (R, V, \beta, \Phi) \) is a form ring.

**Remark.** The codes of Type \( \rho \) are exactly the generalized doubly-even self-dual codes in the sense of Quebbemann.

**Proof.** Let \( C \subseteq \mathbb{F}_{2^f}^N \) be an even code in the sense of Quebbemann. Since \( \lambda \) is surjective, it is enough to show that \( \sum_{i=1}^N \phi_a(c_i) = 0 \) for all \( c \in C \). Now \( \sum_{i=1}^N c_i = 0 \), therefore as an element of \( O/4O \) the square

\[
\left( \sum_{i=1}^N c_i \right)^2 = \sum_{i=1}^N c_i^2 + 2 \sum_{i<j} c_i c_j = 0 \in O/4O.
\]

Since \( \sum_{i<j} c_i c_j = 0 \) it follows that \( \sum_{i=1}^N c_i^2 = 0 \in O/4O \).

To see the other inclusion let \( C \) be a code of Type \( \rho \). By the nondegeneracy of the trace form, \( \sum_{i=1}^N c_i^2 = 0 \) in \( O/4O \). Therefore by (*) \( (\sum_{i=1}^N c_i)^2 \equiv 0 \) (mod \( 2O \)) and hence also \( \sum_{i=1}^N c_i = 0 \in \mathbb{F}_{2^f} \). Then \( (\sum_{i=1}^N c_i)^2 \equiv 0 \) (mod \( 4O \)) and (*) implies that \( \sum_{i<j} c_i c_j = 0 \).

\[
\square
\]

5.1 **The Clifford-Weil groups for the generalized doubly-even self-dual codes (arbitrary genus)**

**Theorem 5.1.** Let \( C_m(\rho) \) be the Clifford-Weil group of genus \( m \) corresponding to the form ring \( \rho \) above. Then

\[
C(\rho) \cong Z.(k^m \oplus k^m).\operatorname{Sp}_{2m}(k) \cong Z.2^{2m.f}.\operatorname{Sp}_{2m}(2^f)
\]

where \( Z \cong Z_4 \) if \( f := [k : \mathbb{F}_2] \) is even, and \( Z \cong Z_8 \) if \( f := [k : \mathbb{F}_2] \) is odd.

**Proof.** By our general theory \( C_m(\rho) \) has an epimorphic image

\[
\mathcal{U}(\operatorname{Mat}_m(R), \Phi_m) \cong (k^m \oplus k^m).\operatorname{Sp}_{2m}(k).
\]

The kernel \( Z \) of this epimorphism is a cyclic group consisting of scalar matrices. Since the invariant ring of \( C_m(\rho) \) is spanned by weight enumerators of self-dual isotropic codes \( C \), the order of \( Z \) is the greatest common divisor of the lengths of these self-dual isotropic codes. Since the codes are self-dual, they all contain the all-ones vector \( \mathbf{1} \). This vector spans an isotropic \( k \)-space if and only if the length \( N \) of the code is divisible by \( 4 \).
Therefore $|Z|$ is divisible by 4. First consider the case when $f$ is even. The code $Q_4$ with
generator matrix
\[
\begin{pmatrix}
1 & 1 & 1 & 1 \\
0 & 1 & \omega & \omega^2
\end{pmatrix},
\]
where $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$, is an isotropic self-dual code of length 4 over $\mathbb{F}_4$. Extending scalars,
one gets an isotropic self-dual code $k \otimes_{\mathbb{F}_4} Q_4$ of length 4 for all $k$ which are of even degree
over $\mathbb{F}_2$. Hence $Z \cong Z_4$ in this case. If $f$ is odd, then any self-dual isotropic code $C \leq k^N$
gives a doubly-even self-dual binary code $\tilde{C} \leq \mathbb{F}_2^N$. The length $fN$ of $\tilde{C}$ is divisible by
8. Since $f$ is odd, this implies that $N$ is divisible by 8 and hence $Z \cong Z_8$ in this case. □

5.2 The case $k = \mathbb{F}_2$, arbitrary genus.

The codes are the usual doubly-even self-dual binary codes. The Clifford-Weil groups
are the complex Clifford groups of [10].

5.3 The case $k = \mathbb{F}_4$.

Let $k = \mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. Then
\[
G := \mathcal{C}(\rho) \cong (Z_4 Y D_8 Y D_8).Alt_5
\]
is generated by $\rho(\omega) = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0
\end{pmatrix}$, $h = \frac{1}{2} \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1
\end{pmatrix}$, and $\rho(\phi) =$
diag(1, −1, i, i). $G$ is a subgroup of index 2 of the complex reflection group $G_{29}$ number
29 in [14]. The Molien series of $G$ is
\[
1 + t^{10} \\
(1 - t^4)(1 - t^8)(1 - t^{12})(1 - t^{20}).
\]
Primary invariants of $G$ (which generate the invariant ring of $G_{29}$) can be taken to be the
complete weight enumerators of the extended quadratic residue codes $Q_i := QR(\mathbb{F}_4, i-1)$
of length $i = 4, 8, 12, 20$. Note that the elements in $G_{29} \setminus G$ act as the Frobenius
automorphism $a \mapsto \bar{a}$ on the weight enumerators of these codes. A weight enumerator $p_C$
is invariant under $G_{29}$ if $p_C = \overline{p_C}$. To get the full invariant ring of $G$, it remains to find
a self-dual even code $C_{40}$ of length 40 over $\mathbb{F}_4$, of which the complete weight enumerator
is not invariant under the Frobenius automorphism. Such a code is constructed in [2].
5.4 The case \( k = \mathbb{F}_8 \).

The Molien series of \( \mathcal{C}(\rho) \) is \( f(t)/g(t) \), where
\[
    f(t) := 1 + 5t^{16} + 77t^{24} + 300t^{32} + 908t^{40} + 2139t^{48} + 3808t^{56} + 5864t^{64} \\
    + 8257t^{72} + 10456t^{80} + 12504t^{88} + 14294t^{96} + 15115t^{104} \\
    + 15115t^{112} + 14294t^{120} + 12504t^{128} + 10456t^{136} + 8257t^{144} \\
    + 5864t^{152} + 3808t^{160} + 2139t^{168} + 908t^{176} + 300t^{184} \\
    + 77t^{192} + 5t^{200} + t^{216}
\]

and
\[
    g(t) := (1 - t^8)(1 - t^{16})^2(1 - t^{24})(1 - t^{48})(1 - t^{56})(1 - t^{72})
\]

6 Doubly-even self-dual codes over \( \mathbb{Z}/2^f\mathbb{Z} \).

Let \( R := \mathbb{Z}/2^f\mathbb{Z} \) and \( C \leq R^N \) be a code. Then the dual code \( C^\perp := \{ x \in R^N \mid \sum_{i=1}^N x_i c_i = 0, \ \forall c \in C \} \). \( C \) is called doubly-even if \( \sum_{i=1}^N c_i^2 \equiv 0 \pmod{2^f+1} \). To express the class of doubly-even self-dual codes over \( R \) in the language of form rings let \( V := R \), and define \( \beta : V \times V \to \frac{1}{2^f}\mathbb{Z}/\mathbb{Z} \) by \( \beta(x, y) := \frac{1}{2^f}xy \) and \( \phi : V \to \frac{1}{2^f+1}\mathbb{Z}/\mathbb{Z} \) by \( \phi(x) := \frac{1}{2^f+1}x^2 \). Let \( \Phi \) be the \( R \)-qmodule generated by \( \phi \) and let
\[
    \rho_a := (R, V, \beta, \Phi).
\]

To express the additional property that \( C \) contains the all-ones vector, let \( \phi_0 : V \to \frac{1}{2^f}\mathbb{Z}/\mathbb{Z} \) be defined by \( \phi_0(x) := \frac{1}{2^f}x \) and let \( \Phi_0 \) be the \( R \)-qmodule spanned by \( \phi \) and \( \phi_0 \). Then
\[
    \rho_b := (R, V, \beta, \Phi_0).
\]

Note that ker(\( \lambda_a \)) \( \cong \mathbb{Z}/2\mathbb{Z} \), whereas ker(\( \lambda_b \)) = \langle \phi_0 \rangle \cong R \), since \( 2^{f-1}\phi_0 = 2^f \phi \). Since the involution on \( R \) is trivial and \( \epsilon = 1 \), one finds that
\[
    \pi(U_m(R, \phi)) = \{ A \in \text{Mat}_{2m}(R) \mid A^T \begin{pmatrix} 0 & -I_m \\ I_m & 0 \end{pmatrix} A = \begin{pmatrix} 0 & -I_m \\ I_m & 0 \end{pmatrix} \} \cong \text{Sp}_{2m}(R).
\]

**Theorem 6.1.** For \( x \in \{ a, b \} \) let \( t_x = \gcd(\{ N \mid \exists C \leq V^N \text{ of Type } \rho_x \}) \). The Clifford-Weil groups of genus \( m \) are extensions
\[
    \mathcal{C}(\rho_a) \cong Z_{t_a}(Z_2^m \times Z_2^m). \text{Sp}_{2m}(R)
\]
and
\[
    \mathcal{C}(\rho_b) \cong Z_{t_b}(R^m \times R^m). \text{Sp}_{2m}(R)
\]
6.1 Doubly-even self-dual codes over $\mathbb{Z}/4\mathbb{Z}$.

We identify $R := \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ and let $\zeta := \exp(2\pi i / 8)$ be a primitive eighth root of unity in $\mathbb{C}$ and $i := \zeta^2$. Then

$$
\mathcal{C}(\rho_a) = \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\
1 & i & -1 & -i \\
1 & 1 & -1 & 1 \\
1 & -i & 1 & -i \end{pmatrix}, \text{diag}(1, \zeta, -1, \zeta) \right\rangle
$$

of order $|\mathcal{C}(\rho_a)| = 1536$, and

$$
\mathcal{C}(\rho_b) = \left\langle \mathcal{C}(\rho_a), \text{diag}(1, i, -1, -i) \right\rangle
$$

of order $|\mathcal{C}(\rho_b)| = 6144$. Note that $\mathcal{C}(\rho_a) \cong Z_8 \times (Z_2 \times Z_2) \cdot SL_2(\mathbb{Z}/4\mathbb{Z})$ and $\mathcal{C}(\rho_b) \cong Z_8 \times (Z_4 \times Z_1) \cdot SL_2(\mathbb{Z}/4\mathbb{Z})$. The Molen series are

$$
\text{Molien}(\mathcal{C}(\rho_a)) = \frac{(1 + t^8)(1 + t^{16})^2}{(1 - t^8)(1 - t^{24})}
$$

and

$$
\text{Molien}(\mathcal{C}(\rho_b)) = \frac{(1 + t^16)(1 + t^{32})}{(1 - t^8)^2(1 - t^{16})(1 - t^{24})}
$$

(see [13]). To interpret these rings in terms of complete weight enumerators of self-dual isotropic codes, we introduce some codes: If $p$ is a prime power $p \equiv \pm 1 \pmod{8}$ then let $\overline{QR}(p)$ be the extended quadratic residue code of length $p + 1$ over $\mathbb{Z}/4\mathbb{Z}$ ([3]). With the correct definition of extension, $\overline{QR}(p)$ contains the all-ones vector. Let $d_8$, $c_{16}$, $d_{16}$ be the codes of Type $\rho_b$ (see [4]) with generator matrices

$$
d_8 = \begin{bmatrix} 13100102 \\ 13010210 \\ 13001021 \\ 22000000 \\ 20222000 \end{bmatrix}, \quad c_{16} = \begin{bmatrix} 1111111111111111 \\ 1011111100010000 \\ 1101010111100100 \\ 11101010101000100 \\ 00001111111100001 \\ 0000020000022002 \\ 000002000022222222 \\ 000002000022222222 \\ 000002000000022222 \\ 000002000000022222 \\ 000000002000022222 \\ 000000002000022222 \\ 0000000000022002 \\ 0000000000220022 \end{bmatrix}, \quad d_{16} = \begin{bmatrix} 1111111111111111 \\ 1110000023000000 \\ 11010000023000000 \\ 11001000222300000 \\ 11000100222300000 \\ 110001022223000000 \\ 1100001022222300000 \\ 10111111022222222 \end{bmatrix}.
$$

Let $p_1 := \text{cwe}(\overline{QR}(7))$, $p_2 := \text{cwe}(d_8)$, $p_3 := \text{cwe}(c_{16})$, $p_4 := \text{cwe}(d_{16})$, and $p_5 := \text{cwe}(\overline{QR}(23))$. Then

$$
\text{Inv}(\mathcal{C}(\rho_b)) = \mathbb{C}[p_1, p_2, p_3, p_5](1 + p_4)(1 + p_6)
$$

12
where \( p_6 \) is the weight enumerator of a suitably chosen random Type \( \rho_b \)-code of length 32.

To find additional generators for the invariant ring of \( \mathcal{C}(\rho_a) \) let \( e^{8'} \) and \( d^{8'} \) be the codes of Type \( \rho_a \) obtained from \( QR(7) \) resp. \( d^8 \) by multiplying one column by \( 3 \in \mathbb{Z}/4\mathbb{Z} \) and let \( p_{1a} := cwe(e^{8'}) \) and \( p_{2a} := cwe(d^{8'}) \) be their complete weight enumerators. Let \( f_1 \) and \( f_2 \) be the complete weight enumerators of two suitably chosen random codes of Type \( \rho_a \) of length 24 and \( f_3 \) the weight enumerator of such a code of length 32. With this notation we find that

\[
\text{Inv}(\mathcal{C}(\rho_b)) = \mathbb{C}[p_1, p_2, p_{1a}, p_{2a}](1 + p_{2a} + p_3 + p_4 + f_1 + f_2 + f_3 + p_{2a}f_3).
\]

7 Self-dual codes over \( \mathbb{F}_{q^2} + \mathbb{F}_{q^2}u \)

In this section we study self-dual codes over the ring \( R = \mathbb{F}_{q^2} + \mathbb{F}_{q^2}u \), for \( q = p^f \), where \( u^2 = 0 \) and \( ua = \alpha a u \) for all \( a \in \mathbb{F}_{q^2} \). These are definitely “non-classical” codes.

Then \( R \cong \mathcal{M}/p\mathcal{M} \), where \( \mathcal{M} \) is the maximal order in the quaternion division algebra over the unramified extension of degree \( f \) of the \( p \)-adic numbers. The most important example is \( q = 2 \). Self-dual codes over this ring have been studied by C. Bachoc [1] in connection with the construction of interesting modular lattices. P. Gaborit [5] found a mass formula.

To construct self-dual codes, we define an \( R \)-valued Hermitian form \( R^N \times R^N \rightarrow R \) by \( (x, y) := \sum_{i=1}^N x_i \overline{y}_i \), where \( \neg : R \rightarrow R \) is the involution defined by \( a + bu := a^q - bu \).

Then

\[
(a' + b'u)(a + bu) = a'a^q + (ab' - ba')u
\]

for all \( a, b, a', b' \in \mathbb{F}_{q^2} \).

To express this self-duality in our language of Types, we need a form ring.

Let \( \beta : R \times R \rightarrow \mathbb{F}_p \cong \mathbb{Z}/Z \) be the bilinear form defined by

\[
\beta(a' + b'u, a + bu) := \frac{1}{p} \text{Tr}(ab' - a'b)
\]

where \( \text{Tr} \) denotes the trace from \( \mathbb{F}_{q^2} \) to \( \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \). Let \( M := \beta(1 \otimes R) \), where the right action of \( R \otimes R \) on \( M \) is left multiplication on the arguments:

\[
m((r + su) \otimes (r' + s'u))(a + bu, a' + b'u) = m((r + su)(a + bu), (r' + s'u)(a' + b'u)).
\]

Let \( \psi : R_R \rightarrow M_{1 \otimes R} \) be the \( R \)-module isomorphism defined by \( \psi(1) := \beta \). The involution \( J \) induced by \( \beta \) is given by \( (r + su)^J = r - s^q u \) and \( \epsilon = -1 \) (since \( \beta \) is skew-symmetric).

Define the \( \frac{1}{p}\mathbb{Z}/\mathbb{Z} \)-valued quadratic form \( \phi_0 : R \rightarrow \frac{1}{p}\mathbb{Z}/\mathbb{Z} \) by

\[
\phi_0(a + bu) := \frac{1}{p} \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(aa^q)
\]

13
and let $\Phi := \{ \phi_0[r] \mid r \in R \}$. The mapping $\{ \} : M \to \Phi$ is the obvious diagonal evaluation

$$m_0(1 \otimes (r + su))(a + bu) := m_0(1 \otimes (r + su))(a + bu, a + bu) = - \text{Tr}(saa^q).$$

Since $\{ \}$ is surjective, this defines a unique mapping $\lambda : \Phi \to M$, satisfying

$$\lambda[m] = m + \tau(m)$$

for all $m \in M$. To find $\lambda(\phi_0)$ we choose $\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\omega + \omega^q = -1$. Then $\phi_0 = \{ m_0(1 \otimes \omega u) \}$,

$$\lambda(\phi_0) = m_0(1 \otimes \omega u) + \tau(m_0(1 \otimes \omega u)) = m_0(1 \otimes u)$$

and therefore $\psi^{-1}(\lambda(\phi_0)) = u$. Identifying $\mathbb{F}_p$ with $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$, one obtains $\mathbb{Q}/\mathbb{Z}$-valued quadratic and bilinear forms. Then this defines a form ring $\rho = (R, V, \beta, \Phi)$. The self-dual codes $C \leq R^N$ above are precisely the ones of Type $\rho$.

The hyperbolic co-unitary group $U(R, \Phi)$ contains a normal subgroup

$$N := U((u), \Phi) := \{ (A, \phi) \in U(R, \Phi) \mid A \equiv I_2 \pmod{u} \}$$

where the quotient is a subgroup of $U(\mathbb{F}_{q^2}, \{0\})$. In fact, since $R = \mathbb{F}_{q^2} + \mathbb{F}_{q^2}u$, the hyperbolic co-unitary group $U(R, \Phi)$ has a subgroup $H \cong O_2^+(\mathbb{F}_{q^2})$ consisting of the elements

$$\{ \left( \begin{array}{ccc} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{array} \right), \left( \begin{array}{c} 0 \\ \psi(cb) \\ 0 \end{array} \right) \mid a, b, c, d \in \mathbb{F}_{q^2}, ca = db = 0, cb + da = 1 \}.$$

$H$ is a complement to $N = U((u), \Phi)$ isomorphic to $U(\mathbb{F}_{q^2}, \{0\})$. The normal subgroup $U((u), \Phi)$ given by

$$\{ \left( \begin{array}{ccc} 1 + au & bu & 0 \\ cu & 1 + du & 0 \\ 0 & 0 & 1 \end{array} \right), \text{diag}(\phi_0[c'], \phi_0[b']) \mid c, b \in \mathbb{F}_q, a, d \in \mathbb{F}_{q^2}, a = d^q \}$$

is isomorphic to $\mathbb{F}_{q^2} \oplus \mathbb{F}_q \oplus \mathbb{F}_q$. Therefore

$$U(R, \Phi) \cong (\mathbb{F}_{q^2} \oplus \mathbb{F}_q \oplus \mathbb{F}_q) \rtimes O_2^+(\mathbb{F}_{q^2}).$$

**Example 7.1.** Let $q := 2$, $R = \mathbb{F}_4 + \mathbb{F}_4u$. Then the hyperbolic co-unitary group $U(R, \Phi)$ is generated by

$$g_1 := \left( \begin{array}{ccc} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & 1 \end{array} \right), g_2 := \left( \begin{array}{ccc} 1 + u & 0 & 0 \\ 0 & 1 + u & 0 \\ 0 & 0 & 1 \end{array} \right),$$

$$g_3 := \left( \begin{array}{ccc} 1 & u & 0 \\ 0 & 0 & \phi_0 \\ 0 & 0 & 0 \end{array} \right), h := \left( \begin{array}{ccc} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right).$$
Since $\lambda$ is injective, $U(R, \Phi)$ is isomorphic to its image under the projection of the first component. This image contains a normal subgroup $N \cong \mathbb{F}_1 + \mathbb{F}_2 + \mathbb{F}_2$ generated by

$$\begin{pmatrix} 1 + \omega u & 0 \\ 0 & 1 + \omega^2 u \end{pmatrix}, \begin{pmatrix} 1 + u & 0 \\ 0 & 1 + u \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \end{pmatrix}.$$

The quotient group is isomorphic to $S_3$, generated by the matrices

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence

$$U(R, \Phi) \cong ((C_2)^2 \times (C_2)^2) \rtimes S_3$$

where $S_3$ acts faithfully on one copy $(C_2)^2$ and with kernel $C_3$ on the other copy.

The Molien series of $C(\rho)$ is

$$f(t) = \frac{1 + t + 4t^2 + 3t^3 + 53t^4 + 104t^5 + 458t^6 + 858t^7 + 2474t^8 + 4839t^9 + 10667t^{10} + 19018t^{11} + 34193t^{12} + 55481t^{13} + 86078t^{14} + 125990t^{15} + 173466t^{16} + 230402t^{17} + 287430t^{18} + 346462t^{19} + 393648t^{20} + 431930t^{21} + 450648t^{22} + 450648t^{23} + 431930t^{24} + 393648t^{25} + 346462t^{26} + 287430t^{27} + 230402t^{28} + 173466t^{29} + 125990t^{30} + 86078t^{31} + 55481t^{32} + 34193t^{33} + 19018t^{34} + 10667t^{35} + 4839t^{36} + 2474t^{37} + 858t^{38} + 458t^{39} + 104t^{40} + 53t^{41} + 3t^{42} + 4t^{43} + t^{44} + t^{45}}{(1 - t^2)^2(1 - t^4)(1 - t^6)^2}.$$ 

Various interesting symmetrizations are possible:

a) Symmetrizing by the action of $\mathbb{F}_4 = \langle \omega \rangle$ yields a matrix group $C(7)(\rho) \cong (C_2)^2 \rtimes S_3$ (a non-faithful $S_3$-action) of degree 7 with Molien series

$$\frac{1 + t^2 + 9t^4 + 21t^6 + 41t^8 + 43t^{10} + 43t^{12} + 23t^{14} + 10t^{16}}{(1 - t)(1 - t^2)(1 - t^4)^2(1 - t^6)^2}.$$ 

b) The unit group $R^*$ has three orbits on $R$ namely $\{0\}, R^*, uR^*$. Symmetrizing by $R^*$ gives a matrix group $C(3)(\rho) \cong D_6$ of which the Molien series and invariant ring is described by Bachoc [1, Theorem 4.4].
References

[1] C. Bachoc, Applications of coding theory to the construction of modular lattices, 

[2] K. Betsumiya and Y. J. Choie, Codes over $\mathbb{F}_4$, Jacobi Forms and Hilbert-Siegel modular forms over $\mathbb{Q}(\sqrt{5})$. (Preprint)


