Automorphism groups of self-dual codes

vorgelegt von

Diplom-Mathematikerin

Annika Günther

aus Neuss

Diese Dissertation ist auf den Internetseiten der Hochschulbibliothek online verfügbar.

Contents

Chapter 1

Introduction

The interest in linear codes began with the papers "Notes on digital coding" by M. J. E. Golay and "Error detecting and error correcting codes" by R. W. Hamming, published in 1949 and 1950, respectively (cf. [10], [15]). In these works it is shown how digital information, given as m-tuples with entries 0 and 1, can be expanded to a tuple of length $N = m + k$, such that the highest possible number of errors in the information can be corrected. The words of length N, obtained by adding k *parity checks* to the original information, form a subspace of $\mathbb{F}_2^N$. Here originates the classical notion of a *binary code*, as a subspace of $\mathbb{F}_2^N$. Algebraic coding theorists began to investigate codes over other alphabets than $\mathbb{F}_2$ as well, also because a larger alphabet allows to correct a greater number of errors occurring in a row in the digital information (*burst errors*). A linear code in the classical sense is hence a subspace of $\mathbb{F}^N$, for a finite field $\mathbb{F}$.

Soon codes with additional algebraic structure received more interest both from algebraists and from coding theorists, since additional structure often gives rise to more efficient decoding algorithms. A well-known example is given by the *cyclic codes*, which are invariant under a cyclic shift of the coordinates. That is, the *automorphism group* of a cyclic code, i.e. the group formed by those coordinate permutations which leave the code invariant, contains a subgroup $\langle (1, \ldots, N) \rangle$ isomorphic to the cyclic group of order N. In her paper "Codes and ideals in group algebras" ([24]), F. J. MacWilliams treats cyclic codes as ideals in the group algebra $\mathbb{F}C_N \cong \mathbb{F}[x]/(x^N - 1)$. A generalization of the cyclic codes are the *group ring codes*, which are right ideals in a group algebra of some finite group and have been investigated by several authors (cf. [27, 2, 19]), using methods of representation theory of finite groups. Among these codes, the *self-dual* codes are of particular interest, for instance since their *weight distribution* has an invariance property given by the famous *MacWilliams identity*.

An interesting connection between the automorphisms of a self-dual linear code and its weight distribution was discovered by N. J. A. Sloane and J. G. Thompson. In their paper "Cyclic self-dual codes" ([40]) they prove that there exists no binary cyclic self-dual code such that the *Hamming weight* of every word is a multiple of 4. Codes whose weight distributions satisfy this divisibility condition are called *doubly-even*, and self-dual doubly-even binary codes are also

called *Type* II codes. The result of Sloane and Thompson has been generalized
by C. Martinez-Peréz and W. Willems in [27], stating that there exists a self-dual
doubly-even binary group ring code for a finite group G if and only if the order
of G is a multiple of 8 and the Sylow 2-subgroups of G are not cyclic.

From the point of view of representation theory, group ring codes are $\mathbb{F}G$-
submodules of the regular permutation module for G. These are linear codes on
which G acts as automorphisms via its regular representation. The present thesis
investigates the existence of codes with prescribed automorphisms which arise
from arbitrary permutation representations, or more generally monomial repre-
sentations, of a finite group. The challenge is hence to decide, given a monomial
permutation group G, whether there exists a self-dual linear code whose auto-
morphism group contains G. This issue is viewed from different perspectives,
allowing different generalizations of the question and the results.

Chapter 3 deduces obvious necessary conditions on G for the existence of a
self-dual G-invariant code. In this chapter monomial permutations are naturally
embedded into the orthogonal group $O(V)$ of a quadratic space V. Hence the
developed theory applies to self-dual codes in odd characteristic, and to gener-
alized Type II codes in characteristic 2. Here a self-dual code C corresponds to a
maximal totally isotropic subspace of V, and G lies in the automorphism group
of C if and only if, as a subgroup of $O(V)$, it lies in the stabilizer S in $O(V)$ of
the corresponding maximal totally isotropic subspace. Depending on the char-
acteristic of $\mathbb{F}$, the determinant or the *Dickson invariant* provides a well-defined
epimorphism $D : O(V) \to C_2$ such that S is always contained in the kernel of D.
On the symmetric group S_N the map D restricts to the sign homomorphism. This
allows to conclude that the automorphism group of a self-dual code in odd char-
acteristic, or of a self-dual Type II code in characteristic 2, is always contained in
the alternating group (see Corollaries 3.2.4, 3.2.5).

In the other chapters of this thesis, a different approach is pursued, following
ideas in [33]. Here G-invariance is part of the definition of a code. A code in
this new sense is a submodule of $\mathbb{F}^N$ for the group algebra $\mathbb{F}G$, where G acts as
coordinate permutations. This opens up the possibility to apply representation
theoretic methods to find criteria for the existence of a self-dual G-invariant code
(see for instance [42]). Moreover, the theory of *Witt groups* can be applied in this
context. The Witt group of the group algebra $\mathbb{F}G$ contains equivalence classes of
$\mathbb{F}G$-modules V which are endowed with a non-degenerate G-invariant form, with
the orthogonal sum as composition (see **Chapter 4**). By definition $\mathbb{F}^N$ contains a
self-dual G-invariant code if and only if it is Witt equivalent with the zero module.
In some cases, for instance in characteristic 2, the theory of Witt groups is rich
enough to characterize the situation where a self-dual G-invariant code exists,
only by the composition factors of the $\mathbb{F}G$-module $\mathbb{F}^N$ (cf. Corollary 4.1.28). Using
in addition the methods from Chapter 3, a characterization of the existence of a
self-dual G-invariant Type II code is proven (cf. Theorem 4.2.19, Theorem 3.2.7),
generalizing the result of Martinez-Peréz and Willems cited above.

A general concept where a code is by definition a module for some ring R

is developed in [33]. There a general notion of the *Type* of a code is introduced. The Type allows to specify important properties of codes, taking as the alphabet a left R-module V, on which there exist biadditive forms to define duality and, where required, quadratic forms which specify additional properties of the code, such as being doubly-even in the case of binary codes. The codes of a Type T and length N form a family of codes, which are self-orthogonal with respect to some non-degenerate biadditive form and isotropic with respect to the above-mentioned quadratic forms. In **Chapter 2** it is shown that the G-invariant linear codes in $V = \mathbb{F}^N$ have a Type with $R = \mathbb{F}G$ and $V = \mathbb{F}^N$.

For every Type T of codes there exists a *neighbor graph*, whose vertices are the self-dual Type T codes and where two vertices C, D are adjacent if and only if $C \cap D$ is a maximal R-submodule of C (cf. Section 2.3). The graph Γ_T is connected whenever R and V are finite, and thus in particular the neighbor graph Γ_G for the Type of G-invariant codes is always connected. This provides an algorithm to find all self-dual G-invariant codes, by starting with one such code and successively computing neighbors in the graph. Moerover, the normalizer $\mathfrak{N} = N_{S_N}(G)$ acts on Γ_G as graph automorphisms. Hence there exists a system of representatives of the $\mathfrak{N}$-orbits of vertices which forms a connected subgraph of Γ_G. This allows to compute only $\mathfrak{N}$-orbit representatives, instead of computing the whole set of all G-invariant self-dual codes. Similar results hold for every finite Type of codes.

If the characteristic of $\mathbb{F}$ does not divide the order of G then the total number M of G-invariant self-dual codes can easily be determined a priori, basically from the composition factors of the $\mathbb{F}G$-module $V = \mathbb{F}^N$. The number of cyclic self-dual codes whose length is coprime to the characteristic of $\mathbb{F}$ is already given in [18]. In this situation V is the regular module over the semisimple group algebra $\mathbb{F}C_N \cong \mathbb{F}[x]/(x^N - 1)$, and the number of self-dual codes is determined via a factorization of $x^N - 1$, which plainly describes the composition factors of V. In **Chapter 6**, formulae are given for the number of self-dual codes over a general finite semisimple associative algebra A. These results are proven via a Morita equivalence $\mathcal{F}$ between the categories of modules for A and for its center $Z(A)$, respectively, where all the modules carry a certain non-degenerate biadditive form to define the orthogonal of a submodule. The Morita equivalence $\mathcal{F}$ is *orthogonality-preserving*, which means that an A-module V contains the same number of self-dual codes as the $Z(A)$-module $\mathcal{F}(V)$. Since A is semisimple, $Z(A)$ is a ringdirect sum of fields. At this point the problem of determining M is settled, since the number of self-dual codes over such a ring can be computed with methods of linear algebra and is well-known (cf. [41], for instance). In the situation where $A = \mathbb{F}G$ is a semisimple group algebra, the orbit lengths under $\mathfrak{N}$ and the total number of self-dual G-invariant codes are related via an obvious *mass formula*, which can be used to prove completeness in a classification of $\mathfrak{N}$-orbit representatives of self-dual G-invariant codes.

In the Type context the *alphabet* of a code is no longer understood as the set $\mathbb{F}$, but as the set V, and it is in this sense that **Chapter 5** asks for the minimum *length* t for which there exists a self-dual G-invariant code. This comprises the question whether there exists a self-dual G-invariant code in $\mathbb{F}^N$, which in this sense has

length 1. The number t is thus the order of the equivalence class of (V, β) in the Witt group of $\mathbb{F}G$. It is shown that t equals the order of the scalar subgroup of the *Clifford-Weil group* $\mathcal{C}(T_G)$, a complex matrix group associated with the Type T_G of G-invariant codes (cf. [33]). A computation of $\mathcal{C}(T_G)$ is possible as soon as the action of the unit group of R on V and the values of the biadditive and quadratic forms associated with T_G are known. Hence t can be a priori be read off from this information (see Section 5.6 for some examples).

Chapter 2

The Type of a code

Classically, a *linear code* is a subspace of $\mathbb{F}^N$, where $\mathbb{F}$ is a finite field. Given a non-degenerate bilinear or Hermitian form $\beta : \mathbb{F}^N \times \mathbb{F}^N \to \mathbb{F}$, the *dual* of a code C is

$$C^\perp = \{v \in \mathbb{F}^N \mid \beta(v, c) = 0 \text{ for all } c \in C\}.$$

If $C = C^\perp$ then C is called *self-dual*. Based on a result of Gleason and Pierce on the divisibility of the *Hamming weight*

$$\mathrm{wt}((c_1, \ldots, c_N)) := |\{i \in \{1, \ldots, N\} \mid c_i \neq 0\}|$$

of the words of a self-dual code (cf. [39]), one classically distinguishes four Types of linear codes, known as Type I, II, III and IV, respectively. For instance, the self-dual Type II codes are those binary self-dual codes in which the weight of every codeword is a multiple of 4, and the self-dual Type III codes are the self-dual subspaces of $\mathbb{F}_3^N$, whose weights are all automatically multiples of 3.

The most interesting of the classical codes over finite fields have some additional structure apart from being vector spaces. For instance, the *cyclic codes* of length N are the submodules of the $\mathbb{F}C_N$-module $\mathbb{F}^N$, where C_N is the cyclic group of order N, which acts on $\mathbb{F}^N$ by a cyclic permutation of the coordinates. These codes also form a Type, in a more general sense. A unifying language to describe the Type of a code is developed in the book "Self-dual codes and invariant theory" ([33]). Here a Type of codes consists of modules over a ring R, for which orthogonality is defined via biadditive forms, and additional properties may be modeled via quadratic forms. The basic concepts are given in Section 2.1.

The unified setting in which the Type of a code is defined allows for instance a uniform approach to prove Theorems like Gleason's famous 1970 Theorem which states that the weight enumerator of a binary Type II code lies in the polynomial ring generated by the weight enumerators of the extended Hamming code of length 8 and the Golay code of length 24. The approach to prove theorems like Gleason's is to compute the invariant ring of the *Clifford-Weil group* $\mathcal{C}(T)$ (cf. Section 5.1), a finite complex matrix group associated with a Type T, such that the weight enumerators of the self-dual Type T codes all lie in the invariant ring of $\mathcal{C}(T)$. Moreover, this general setting allows to define the Type of codes with prescribed automorphisms, in Section 2.2.4 (cf. [14]).

In Section 2.3 a very efficient method is given to compute all self-dual codes of a given Type T. A notion of *neighborhood* of self-dual codes is introduced, following ideas of Kneser in [21], which have been applied to $\mathbb{Z}G$-lattices in [29]. The concept of neighborhood is applied to self-dual codes of arbitrary Type T over a finite ground ring, such that the neighbors of a self-dual Type T code can easily be computed. This leads to the notion of the *neighbor graph*, which has the self-dual Type T codes as vertices, and where two vertices are adjacent if and only if they are neighbors. It is shown that the neighbor graph is connected and hence given a single self-dual Type T code, it is possible to find all self-dual Type T codes by successively computing neighbors (cf. [14]). In Section 2.3.1 it is shown that this method is also appropriate to compute only representatives for the equivalence classes of self-dual codes of a given Type, where the equivalence classes are the orbits of a certain finite group acting on the set of all self-dual Type T code, inducing automorphisms of the neighbor graph. For the Type of classical linear codes over $\mathbb{F}$ of length N, this group is the symmetric group on N points. Hence the neighbor method can be used, for instance, to compute all self-dual codes in $\mathbb{F}^N$ up to permutation equivalence, without computing all self-dual codes in $\mathbb{F}^N$ first.

2.1   Form rings and their representations

In the language of form rings and their representations, the alphabet over which a code is defined is a left module V over a ring R. Throughout this work, R is assumed to be a finite ring with 1, and all R-modules V are assumed to be finite and unitary, i.e. $1 \cdot v = v$ for all $v \in V$. A *form ring* (cf. Definition 2.1.4) is a quadruple basically consisting of algebraic objects which allow homomorphisms to the algebraic objects formed by the biadditive and quadratic forms on V (cf. Examples 2.1.5 and 2.1.5).

Definition 2.1.1. *A* twisted R-module *is a pair* (M, τ) *consisting of a right* $(R \otimes_{\mathbb{Z}} R)$-module M together with a group automorphism τ of M such that $\tau^2 = \mathrm{id}_M$ and $\tau(m(r \otimes s)) = \tau(m)(s \otimes r)$ for all $m \in M$ and $r, s \in R$. A homomorphism $\rho : (M, \tau) \to (M', \tau')$ of twisted R-modules is an $(R \otimes R)$-module homomorphism satisfying $\rho(\tau(m)) = \tau'(\rho(m))$.

Definition 2.1.2. *An* R-qmodule *is an abelian group* Φ *together with a map* $[\ ] : R \to \mathrm{End}(\Phi)$ *such that*

$$[1] = \mathrm{id}_\Phi, \quad [rs] = [r][s], \quad [r + s + t] + [r] + [s] + [t] = [r + s] + [r + t] + [s + t]$$

for all $r, s, t \in R$. *A homomorphism* $\rho_\Phi : \Phi \to \Phi'$ *of* R-qmodules *is a group homomorphism with* $\rho_\Phi(\phi[r]) = \rho_\Phi(\phi)[r]$ *for all* $\phi \in \Phi$ *and* $r \in R$.

Definition 2.1.3. *A* quadratic pair *over* R *is a tuple* $((M, \tau), \Phi)$, *where* (M, τ) *is a twisted* R-module *and* Φ *is an* R-qmodule, *together with structure maps* $\lambda : \Phi \to M$ *and* $\{\ \} : M \to \Phi$ *with*

$$\{\tau(m)\} = \{m\}, \quad \tau(\lambda(\phi)) = \lambda(\phi), \quad \lambda(\{m\}) = m + \tau(m)$$

and

$$\phi[r+s] - \phi[r] - \phi[s] = \{\,\lambda(\phi)(r \otimes s)\,\}.$$

Let $((M', \tau'), \Phi')$ be another R-qmodule with structure maps λ' and $\{\,\}'$. A homomorphism of quadratic pairs is a pair (ρ_M, ρ_Φ), where $\rho_M : (M, \tau) \to (M', \tau')$ is a homomorphism of twisted modules and $\rho_\Phi : \Phi \to \Phi'$ is a homomorphism of R-qmodules such that

$$\rho_\Phi(\{\,m\,\}) = \{\,\rho_M(m)\,\}' \quad and \quad \rho_M(\lambda(\phi)) = \lambda'(\rho_\Phi(\phi)).$$

for all $m \in M$ and $\phi \in \Phi$.

Definition 2.1.4. *The quadruple (R, M, ψ, Φ) is called a* form ring *if $((M, \tau), \Phi)$ is a quadratic pair over R, and $\psi : R \to M$ is an isomorphism of right R-modules such that $\varepsilon := \psi^{-1}(\tau(\psi(1))) \in R^*$, where M is a right R-module via $mr := m(1 \otimes r)$.*

Remark 2.1.5. *Let V be a left R-module and A an abelian group. Let $\mathrm{Bil}(V, A)$ be the set of all $\mathbb{Z}$-bilinear mappings $V \times V \to A$. Define an $(R \otimes R)$-module structure on $\mathrm{Bil}(V, A)$ via*

$$\beta(r \otimes s)(v, w) = \beta(rv, sw)$$

for $r, s \in R$ and $v, w \in V$, and let

$$\tau_{\mathrm{Bil}} : \mathrm{Bil}(V, A) \to \mathrm{Bil}(V, A), \ \ \beta \mapsto ((v, w) \mapsto \beta(w, v)).$$

Then $(\mathrm{Bil}(V, A), \tau_{\mathrm{Bil}})$ is a twisted R-module. An A-valued quadratic map *on V is a map $\phi : V \to A$ such that $\phi(nv) = n^2\phi(v)$ for all integers n and all $v \in V$, and*

$$\phi(u + v + w) + \phi(u) + \phi(v) + \phi(w) = \phi(u + v) + \phi(v + w) + \phi(u + w)$$

for all $u, v, w \in V$, or equivalently, such that

$$\lambda_{\mathrm{Bil}}(\phi) := ((v, w) \mapsto \phi(v + w) - \phi(v) - \phi(w)) \in \mathrm{Bil}(V, A).$$

By $\mathrm{Quad}(V, A)$ denote the set of all A-valued quadratic maps on V. Then $\mathrm{Quad}(V, A)$ is an R-qmodule via $\phi[r](v) = \phi(rv)$, for $r \in R$ and $v \in V$, and the pair $((\mathrm{Bil}(V, A), \tau_{\mathrm{Bil}}), \mathrm{Quad}(V, A))$ is a quadratic pair with the maps λ_{Bil} and

$$\{\,\}_{\mathrm{Bil}} : \mathrm{Bil}(V, A) \to \mathrm{Quad}(V, A), \ \ \beta \mapsto (v \mapsto \beta(v, v)).$$

Definition 2.1.6. *Let $\mathcal{R} = (R, M, \psi, \Phi)$ be a form ring. Let V be a left R-module and let A be an abelian group. The tuple $T = (V, \rho_M, \rho_\Phi, \beta = \rho_M(\psi(1)))$ is called a* representation *of $\mathcal{R}$ if $(\rho_M, \rho_\Phi) : ((M, \tau), \Phi) \to ((\mathrm{Bil}(V, A), \tau_{\mathrm{Bil}}), \mathrm{Quad}(V, A))$ is a homomorphism of quadratic pairs such that β is non-degenerate, i.e.*

$$V \to \mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{Q}/\mathbb{Z}), \ \ v \mapsto (w \mapsto \beta(v, w))$$

is an isomorphism. T is called finite *if V is finite and $A = \mathbb{Q}/\mathbb{Z}$.*

Every form ring structure defines an antiautomorphism of the underlying ring, as follows. For a proof that this is indeed an antiautomorphism we refer to [33, Lemma 1.4.5].

Remark 2.1.7. *Every form ring structure $\mathcal{R} = (R, M, \psi, \Phi)$ on R defines an antiautomorphism ^{J} of R, by $r^J := \psi^{-1}(\psi(1)(r \otimes 1))$. If $(V, \rho_M, \rho_\Phi, \beta)$ is a representation of $\mathcal{R}$ then $\beta(rv, w) = \beta(v, r^J w)$ for all $r \in R$ and $v, w \in V$.*

Example 2.1.8. *(cf. [14]) Let J be an involution of R, i.e. a ring antiautomorphism of order 1 or 2. That is, $(rs)^J = r^J s^J$ and $(r^J)^J = r$ for all $r, s \in R$. Let V be a left R-module and let $\beta : V \times V \to \mathbb{Q}/\mathbb{Z}$ be a biadditive non-degenerate form with*

$$\beta(v, w) = \beta(w, \epsilon v) \quad \text{and} \quad \beta(rv, w) = \beta(v, r^J w)$$

for all $v, w \in V$ and $r \in R$, where ϵ is a unit which lies in the center of R, with $\epsilon \epsilon^J = 1$. To model the Type of submodules of V which are self-orthogonal with respect to β, we define a form ring structure on R (see also [33]), following a construction by Bak in [1]. Let $M = R$ and let $\tau : M \to M$, $m \mapsto \epsilon m^J$. Let

$$\Lambda := \{m - \tau(m) \mid m \in M\}.$$

Then the tuple

$$\mathcal{R}(R, J, \epsilon) = (R, \mathrm{id}, M = R, \Phi = M/\Lambda)$$

is a form ring, where M is an $R \otimes R$-module via $m(r \otimes s) := r^J m s$, Φ is an R-qmodule via $(m + \Lambda)[r] := (r^J m r) + \Lambda$, and well-defined structure maps

$$\{\ \} : M \to \Phi, \ m \mapsto m + \Lambda, \ \lambda : \Phi \to M, \ m + \Lambda \mapsto m + \tau(m).$$

The associated involution of R is the involution J. A representation of $\mathcal{R}(R, J, \epsilon)$ can be defined as follows. Let $T = T(V, \beta) = (V, \rho_M, \rho_\Phi, \beta)$ with

$$\rho_M(m)(v, w) = \beta(v, mw) \quad \text{and} \quad \rho_\Phi(m + \Lambda)(v) = \beta(v, mv).$$

It is straightforward to show that T is a representation of $\mathcal{R}$. Note that ρ_Φ is well-defined since $\beta(v, mv) = 0$ whenever $m = m' - \tau(m') \in \Lambda$ since

$$\beta(v, \tau(m')v) = \beta(v, \epsilon m'^J v) = \beta(\epsilon m'^J v, \epsilon v) = \beta(v, m' \epsilon^J \epsilon v) = \beta(v, m'v)$$

and hence $\beta(v, mv) = \beta(v, m'v) - \beta(v, \tau(m')v) = 0$.

Example 2.1.9. *Let J be an involution on R. Let V be a left R-module and let $q : V \to \mathbb{Q}/\mathbb{Z}$ be a quadratic map such that $\beta := \lambda(q)$ is non-degenerate and satisfies $\beta(rv, w) = \beta(v, r^J w)$ for all $v, w \in V$ and $r \in R$. We want to model the Type of all submodules of V which are isotropic with respect to q. If 2 is a unit in R then the construction in Example 2.1.8 with $\epsilon = 1$ is appropriate, since $q = \frac{1}{2}\{\beta\}$ and hence any submodule C which is self-orthogonal with respect to β satisfies*

$$q(c) = \frac{1}{2}\{\beta\} = \frac{1}{2}\beta(c, c) = \beta(c, \frac{1}{2}c) = 0$$

for all $c \in C$, and every submodule of V which is isotropic with respect to q is self-orthogonal with respect to $\lambda(q)$. If 2 is no unit in R then assume that $\beta(v, rv) = 0$ whenever $r + r^J = 0$. Note that this condition is natural since whenever there exists a

self-dual isotropic code in V, there exists a quotient of V which satisfies this condition and is appropriate to model the self-dual isotropic codes in V (cf. Remark 2.1.10). Define a form ring

$$\mathcal{R} = \mathcal{R}(R, J) = (R, M = R, \mathrm{id}, \Phi = \langle 1, \{\, M \,\} \rangle)$$

with structure maps $\tau = J$, $\lambda = \mathrm{id}$ and $\{\, m \,\} = m + \tau(m)$. Then $T = T(V, q) = (V, \rho_M, \rho_\Phi, \beta)$ is a representation of $\mathcal{R}$, with $\rho_M(m)(v, w) = \beta(v, mw)$ and ρ_Φ defined on generators by

$$\rho_\Phi(1) = q, \quad \rho_\Phi(\{\, m \,\}) = \{\, \rho_M(m) \,\}.$$

To see that the map ρ_Φ is well-defined, note that if $m \in \ker(\{\,\}\,)$ then $\rho_M(m) = 0$ according to our assumption, and if $r^J r = m + \tau(m) \in \langle 1 \rangle \cap \{\, M \,\}$ then

$$\{\, \rho_M(m) \,\}(v) = \beta(v, mv) = \frac{1}{2}(\beta(v, mv) + \beta(v, mv)) = \frac{1}{2}(\beta(v, (m + \tau(m))v)$$

$$= \frac{1}{2}\beta(v, r^J r v) = \frac{1}{2}\beta(rv, rv) = q(rv) = q[r](v)$$

for all $v \in V$.

Remark 2.1.10. *Let the R-module V with the quadratic map $q : V \to \mathbb{Q}/\mathbb{Z}$ and the form ring $\mathcal{R}$ be as in Example 2.1.9. For $r \in R$ with $r + r^J = 0$, the map*

$$\varphi_r : V \to \mathbb{Q}/\mathbb{Z}, \quad v \mapsto \beta(v, rv)$$

is additive and hence due to the non-degeneracy of β, there exists an element $v_r \in V$ such that $\varphi_r(v) = \beta(v_r, v)$ for all $v \in V$. If C is an isotropic code in V then $\beta(v_r, c) = \beta(c, rc) = 0$ for all $c \in C$ and hence $v_r \in C^\perp$. Hence the R-module

$$Y := \langle v_r \mid r + r^J = 0 \rangle$$

generated by the v_r satisfies $Y \subseteq C^\perp$ for every isotropic code C. In particular if C is self-dual then $Y \subseteq C \subseteq Y^\perp$ and hence Y is isotropic. Hence if there exists a self-dual isotropic code in V then the quadratic map

$$q_Y : Y^\perp/Y \to \mathbb{Q}/\mathbb{Z}, \quad y' + Y \mapsto q(y')$$

is well-defined, with polar form $\beta_Y : (y' + Y, y'' + Y) \mapsto \beta(y', y'')$, and the self-dual isotropic subspaces of $Y^\perp/Y$ correspond to the self-dual isotropic subspaces of V. Moreover, if $r + r^J = 0$ then

$$\beta_Y(y' + Y, r(y' + Y)) = \beta(y', r(y' + Y)) = \beta(y', ry') = \beta(v_r, y') = 0$$

for all $y' \in Y^\perp$. Hence according to Example 2.1.9 the representation $T(Y^\perp/Y, \beta_Y)$ is well-defined and appropriate to model the Type of self-dual isotropic codes in V.

In Section 4.3 the following properties and constructions associated with form rings will be needed. For a proof of the following Lemma, the reader is referred to [33, Lemma 1.4.5, Remark 1.4.6].

Lemma 2.1.11. *Let $\mathcal{R} = (R, M, \psi, \Phi)$ be a form ring with associated unit ε and antiautomorphism J, and let $(V, \rho_M, \rho_\Phi, \beta)$ be a representation of $\mathcal{R}$. Then*

(i) $\varepsilon^J \varepsilon = 1$,

(ii) $\psi(r)(s \otimes t) = \psi(s^J r t)$,

(iii) $\tau(\psi(r)) = \psi(r^J \varepsilon)$,

(iv) $\varepsilon^J r^{J^2} \varepsilon = r$,

(v) $\beta(rv, w) = \beta(v, r^J w)$,

(vi) $\beta(v, w) = \beta(w, \varepsilon v)$,

(vii) $v_e^{J^{-1}} v = v_e^{J^{-1}} w$ *if and only if* $ev = ew$

for all $r, s \in R$, $v, w \in V$ and symmetric idempotents $e = u_e v_e \in R$ (cf. Definition 5.1.1) .

Definition 2.1.12. *Let $\mathcal{R}_i = (R_i, M_i, \psi_i, \Phi_i)$ be form rings, for $i = 1, 2$. A form ring homomorphism is a triple $(\alpha_R, \alpha_M, \alpha_\Phi)$, where $\alpha_R : R_1 \to R_2$ is a ring homomorphism and $(\alpha_M, \alpha_\Phi) : (M_1, \Phi_1) \to (M_2, \Phi_2)$ is a homomorphism of quadratic pairs such that*

$$\alpha_\Phi(\phi)[\alpha_R(r)] = \alpha_\Phi(\phi[r]), \quad \alpha_M(m)(\alpha_R(r) \otimes \alpha_R(s)) = \alpha_M(m(r \otimes s))$$

and

$$\psi_2(\alpha_R(r)) = \alpha_M(\psi_1(r))$$

for all $\phi \in \Phi_1$, $m \in M_1$ and $r, s \in R_1$. A form ring automorphism is a form ring homomorphism where the maps $\alpha_R, \alpha_M, \alpha_\Phi$ are bijective.

Definition 2.1.13. *Let $T = (V, \rho_M, \rho_\Phi, \beta)$, $T' = (V', (\rho_M)', (\rho_\Phi)', \beta')$ be representations of the form ring $\mathcal{R} = (R, M, \psi, \Phi)$. A weak form isometry is a tuple $(\alpha_R, \alpha_M, \alpha_\Phi, \alpha)$, where $(\alpha_R, \alpha_M, \alpha_\Phi)$ is a form ring automorphism of $\mathcal{R}$ and $\alpha : V \to V'$ is a bijective additive map such that*

$$\alpha(rv) = \alpha_R(r)\alpha(v), \quad \rho_{M'}(\alpha_M(m))(\alpha(v), \alpha(w)) = \rho_M(m)(v, w)$$

and

$$(\rho_\Phi)'(\alpha_\Phi(\phi))(\alpha(v)) = \rho_\Phi(\phi)(v)$$

for all $r \in R$, $m \in M$, $\phi \in \Phi$ and $v, w \in V$. The map α is called a form isometry if $(\mathrm{id}, \mathrm{id}, \mathrm{id}, \alpha)$ is a weak form isometry.

Definition 2.1.14. *Let $\mathcal{R} = (R, M, \psi, \Phi)$ be a form ring and let $u \in R^*$. Then the map $R \to M$, $r \mapsto \psi_u(r) = \psi(ur)$ is an isomorphism of right R-modules. The tuple $\mathcal{R}_u := (R, M, \psi_u, \Phi)$ is again a form ring, called the rescaling of $\mathcal{R}$ with u.*

Remark 2.1.15. *The involution ^{J_u} associated with the rescaled form ring $\mathcal{R}_u$ is given by $r^{J_u} = u^{-1} r^J u$, and the associated unit is $\varepsilon_u = u^{-1} u^J \varepsilon$.*

Proof. The proof is an easy calculation:

$$r^{J_u} = \psi_u^{-1}(\psi_u(1)(r \otimes 1)) = \psi_u^{-1}(\psi(u)(r \otimes 1)) = \psi_u^{-1}(\psi(r^J u)) = \psi_u^{-1}(\psi_u(u^{-1} r^J u))$$
$$= u^{-1} r^J u,$$

and the unit ε_u is

$$\varepsilon_u = \psi_u^{-1}(\tau(\psi_u(1))) = \psi_u^{-1}(\tau(\psi(u))) = \psi_u^{-1}(\tau(\psi(1)(1 \otimes u))) = \psi_u^{-1}(\tau(\psi(1))(u \otimes 1))$$
$$= \psi_u^{-1}(\psi(\varepsilon)(u \otimes 1)) = \psi_u^{-1}(\psi(u^J \varepsilon)) = \psi_u^{-1}(\psi_u(u^{-1} u^J \varepsilon))$$
$$= u^{-1} u^J \varepsilon.$$

$\square$

In order to define the Type of a code we define the multiple of a representation, via orthogonal sums.

Definition 2.1.16. *Let* $T = (V, \rho_M, \rho_\Phi, \beta)$ *and* $T' = (V', (\rho_M)', (\rho_\Phi)', \beta')$ *be represen-tations of the form ring* $\mathcal{R} = (R, M, \psi, \Phi)$. *Then the* orthogonal sum

$$T \perp T' = (V \perp V', \rho_M \perp (\rho_M)', \rho_\Phi \perp (\rho_\Phi)', \beta \perp \beta')$$

is again a representation of $\mathcal{R}$*, where*

$$\rho_M \perp (\rho_M)'(m) = (((v, v'), (w, w')) \mapsto \beta(v, w) + \beta(v', w')) \quad and$$

$$\rho_\Phi \perp (\rho_\Phi)'(\phi) = ((v, v') \mapsto \rho_\Phi(\phi)(v) + (\rho_\Phi)'(\phi)(v')).$$

For a positive integer N*, the* N-multiple *of* T *is the representation* $T^N = \perp_{i=1}^N T$.

Definition 2.1.17. *Given a representation* $T = (V, \rho_M, \rho_\Phi, \beta)$ *of some form ring, a sub-module* C *of* V^N *is called* isotropic, *or a* Type T code *if*

$$\rho_M^N(m)(c, c') = 0 \quad and \quad \rho_\Phi^N(\phi)(c) = 0$$

for all $m \in M$*,* $\phi \in \Phi$ *and* $c, c' \in C$*. Note that the first condition is fulfilled if and only if always* $\beta(c, c') = 0$*. The integer* N *is called the* length *of* C*.*

2.2 Examples of important Types

This section gives some examples of how to model the properties of codes in the language of form rings and their representations.

2.2.1 Linear self-dual codes over finite fields

These are codes in the classical sense, i.e. subspaces of $\mathbb{F}^N$, where $\mathbb{F}$ is a finite field. The dual of a code is defined with respect to the standard scalar product on

$\mathbb{F}^N$. The Type of these codes is given by the representation $T_q^E := (\mathbb{F}, \rho_M, \rho_\Phi, \beta)$ of the form ring $\mathcal{R}_q^E := (\mathbb{F}, \mathbb{F}, \mathrm{id}, \{\mathbb{F}\})$, where q is the size of $\mathbb{F}$ and

$$\rho_M(m)(v, w) = \frac{1}{p} \mathrm{Tr}(mvw) \in \mathbb{Q}/\mathbb{Z}$$

for all $m \in M = \mathbb{F}$ and $v, w \in V = \mathbb{F}$. Here Tr denotes the trace of $\mathbb{F}$ to its prime field $\mathbb{F}_p$ with p elements, and is understood as a map into $\mathbb{Z}$ in the definition of ρ_M. This determines the map ρ_Φ, since $\{\ \}$ is surjective and $\rho_\Phi(\{m\}) = \{\rho_M(m)\}_{\mathrm{Bil}}$. Hence a Type T_q^E code is just a subspace $C \leq \mathbb{F}^N$ with $\rho_M(m)(c, c') = 0$ for all $c, c' \in C$, i.e. the $\mathbb{F}$-qmodule Φ does not encode any additional properties of C. One easily verifies that indeed, the self-dual Type T_q^E codes are exactly the self-dual linear codes in $\mathbb{F}^N$.

2.2.2   Binary Type II codes

A binary code $C \leq \mathbb{F}_2^N$ is said to be *Type* II, or *doubly-even*, if the *weight*

$$\mathrm{wt}((c_1, \ldots, c_N)) := |\{i \in \{1, \ldots, n\} \mid c_i \neq 0\}|$$

of every word of C is a multiple of 4. By a well-known result of Gleason, self-dual binary Type II codes exist if and only if N is a multiple of 8. These are Type 2_I^E codes (cf. Section 2.2.1) with the additional property of being doubly-even. This property can be modeled via a bigger $\mathbb{F}_2$-qmodule Φ. Type II codes are given by the representation $2_{II}^E = (\mathbb{F}_2, \rho_M, \rho_\Phi, \beta)$ of the form ring

$$\mathcal{R}_{II} = (\mathbb{F}_2, \mathbb{F}_2, \mathrm{id}, \Phi = \mathbb{Z}/4\mathbb{Z}),$$

where $\rho_M(1)(v, w) = \frac{1}{2}vw \in \mathbb{Q}/\mathbb{Z}$ and $\rho_\Phi(1)(v) = \frac{1}{4}v^2 \in \mathbb{Q}/\mathbb{Z}$ for all $m \in M = \mathbb{F}_2$ and $v, w \in V = \mathbb{F}_2$. Alternatively, changing the underlying vector space, the self-dual Type 2_{II}^E codes can be described by a certain quadratic map q, hence via representations of a form ring $\mathcal{R} = \mathcal{R}(\mathbb{F}, \mathrm{id}) = (\mathbb{F}_2, \mathbb{F}_2, \mathrm{id}, \mathbb{F}_2)$. This is done explicitly in Section 2.2.3.

2.2.3   Generalized doubly-even codes

Let $\mathbb{F}$ be a finite field of characterstic 2. There is a notion of *generalized doubly-even* linear codes over $\mathbb{F}$, introduced by Quebbemann (cf. [35]) as follows.

Definition 2.2.1. *A linear code $C \leq \mathbb{F}^N$ is called* generalized doubly-even, *or* Type II, *if*

$$\sum_{i \in \{1, \ldots, N\}} c_i = \sum_{i < j} c_i c_j = 0$$

for all $(c_1, \ldots, c_N) \in C$.

Note that if $\mathbb{F} = \mathbb{F}_2$ then $\sum_{i=1}^{N} c_i = \mathrm{wt}(c)$ and $\sum_{i<j} c_i c_j = \binom{\mathrm{wt}(c)}{2}$ (mod 2), hence the above coincides with the classical notion of binary doubly-even codes in the previous section. Moreover, there is an interesting connection between doubly-even codes over $\mathbb{F}_{2^f}$ and binary doubly-even codes: Let $(t_1, \ldots, t_f)$ be a Trace-orthogonal basis of the vector space $\mathbb{F}_{2^f}$ over $\mathbb{F}_2$, i.e. $\mathrm{Trace}(t_i t_j) = \delta_{ij}$, where $\mathrm{Trace} : \mathbb{F} \to \mathbb{F}_2$ is the usual trace. The *Gray map*

$$\mathcal{G} : \mathbb{F}_{2^f} \to \mathbb{F}_2^f, \quad \sum_{i=1}^{f} \alpha_i t_i \mapsto (\alpha_1, \ldots, \alpha_f)$$

is an isomorphism of vector spaces over $\mathbb{F}_2$, which associates to a code $C \leq \mathbb{F}_{2^f}^N$ a binary code

$$\mathcal{G}(C) := \{(\mathcal{G}(c_1), \ldots, \mathcal{G}(c_N)) \mid (c_1, \ldots, c_N) \in C\} \leq \mathbb{F}_2^{fN},$$

called the *Gray image* of C. It has been shown in [32] that a code $C \leq \mathbb{F}^N$ is generalized doubly-even if and only if $\mathcal{G}(C)$ is doubly-even.

Remark 2.2.2. *Assume that there exists a self-dual generalized doubly-even code in $\mathbb{F}^N$. Then N is even since every self-dual code $C \leq \mathbb{F}^N$ satisfies $2\dim(C) = N$. Moreover, C contains the all-ones vector $\mathbf{1} = (1, \ldots, 1)$. Hence $C/\langle \mathbf{1} \rangle$ is a subspace of $V := \langle \mathbf{1} \rangle^{\perp}/\langle \mathbf{1} \rangle$. The space $\langle \mathbf{1} \rangle^{\perp}$ is given by*

$$\{v \in \mathbb{F}^N \mid \mathrm{wt}(\mathcal{G}(t_i v)) \text{ is even for all } i \in \{1, \ldots, f\}\},$$

since $\mathrm{Trace}(\sum_{i=1}^{N} v_i) = \mathrm{wt}(\mathcal{G}(v))$ for all $v = (v_1, \ldots, v_N) \in \mathbb{F}^N$. Hence we can define a map

$$q : V \to \mathbb{F}, \quad v + \langle \mathbf{1} \rangle \mapsto \sum_{i=1}^{f} \frac{\mathrm{wt}(\mathcal{G}(t_i v))}{2} t_i^2,$$

where the coefficients $\frac{\mathrm{wt}(\mathcal{G}(t_i v))}{2}$ are in $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$. It has been shown in [30] that q is a well-defined quadratic form whose associated bilinear form $\lambda(q)$ is the standard scalar product $(u + \langle \mathbf{1} \rangle, v + \langle \mathbf{1} \rangle) \mapsto \sum_{i=1}^{N} u_i v_i$.

Proposition 2.2.3. *(see [30, Prop. 3.3].) A self-dual code $C \leq \mathbb{F}^N$ is generalized doubly-even if and only if $C/\langle \mathbf{1} \rangle$ is an isotropic subspace of V with respect to q, i.e. $q(c) = 0$ for all $c \in C$.*

The self-dual generalized doubly-even codes are thus in correspondence with the isotropic subspaces of V with respect to the quadratic map q. Since the polar form $\lambda(q)$ satisfies

$$\lambda(q)(v + \mathbf{1}, r(v + \mathbf{1})) = r \sum_{i=1}^{N} v_i^2 = r \left(\sum_{i=1}^{N} v_i \right)^2 = 0$$

for all $r \in \mathbb{F}$ and $v \in \langle \mathbf{1} \rangle^{\perp}$, the self-dual generalized doubly-even codes in $\mathbb{F}^N$ can be modeled through the representation $T = T(V, q)$ of the form ring

$$\mathcal{R} = \mathcal{R}(\mathbb{F}, \mathrm{id}) = (\mathbb{F}, M = \mathbb{F}, \mathrm{id}, \Phi = \langle 1 \rangle = \mathbb{F})$$

given in Example 2.1.9.

2.2.4 Codes with prescribed automorphisms

This section gives an appropriate representation to model self-dual linear codes $C \leq \mathbb{F}^N$, where $\mathbb{F}$ is a finite field, with prescribed automorphisms. The *automorphism group* of C is

$$\mathrm{Aut}(C) = \{\pi \in S_N \mid \pi(C) = C\},$$

where the symmetric group S_N acts on $\mathbb{F}^N$ by permuting the coordinates. For a subgroup $G \leq S_N$, a code $C \leq \mathbb{F}^N$ has $G \leq \mathrm{Aut}(C)$ if and only if it is a G-submodule of $V = \mathbb{F}^N$, i.e. the G-invariant codes are modules over the group algebra $\mathbb{F}G$. The group algebra $\mathbb{F}G$ carries a natural $\mathbb{F}$-linear involution J given by $g^J = g^{-1}$, for $g \in G$. Since $G \leq S_N$, the standard scalar product

$$\beta : \mathbb{F}^N \times \mathbb{F}^N \to \mathbb{F}, \quad ((v_1, \ldots, v_N), (w_1, \ldots, w_N)) \mapsto \sum_{i=1}^{N} v_i w_i$$

is G-invariant, i.e. $\beta(v, w) = \beta(vg, wg)$ for all $v, w \in \mathbb{F}^N$ and $g \in G$, and hence $\beta(av, w) = \beta(v, a^J w)$ for all $a \in \mathbb{F}G$. According to Example 2.1.8 this defines a form ring

$$\mathcal{R}(\mathbb{F}G, J, 1) = (\mathbb{F}G, M = \mathbb{F}G, \mathrm{id}, \Phi = M/\Lambda = M/\{a - a^J \mid a \in \mathbb{F}G\}).$$

with a representation $T_{V,\beta} = (V, \rho_M, \rho_\Phi, \beta)$, where

$$\rho_M(m)(v, w) = \beta(v, mw) \quad \text{and} \quad \rho_\Phi(m + \Lambda)(v) = \beta(v, mv),$$

cf. Example 2.1.8.

2.2.5 Doubly-even codes with prescribed automorphisms

Let $\mathbb{F}$ be a finite field of characteristic 2 and let $G \leq S_N$ be a permutation group. We want to model the Type of self-dual G-invariant codes in $\mathbb{F}^N$ with the additional property of being generalized doubly-even (cf. Section 2.2.3), provided that such a code exists. These codes correspond to the self-dual isotropic submodules of a certain quadratic space, as follows. Every self-dual code over $\mathbb{F}$ contains the all-ones vector $\mathbf{1}$. Moreover, for an involution $\iota \in G$ let $v^\iota \in \mathbb{F}^N$ be the vector with $v_i^\iota = 1$ if $\iota(i) = i$, and $v_i^\iota = 0$ otherwise. If C is a G-invariant self-dual code in $\mathbb{F}^N$ then $0 = \beta(c, \iota c) = \beta(c, v^\iota)^2$ for every $c \in C$, and hence $v^\iota \in C^\perp = C$. Hence the subspace

$$Y := \langle \mathbf{1}, \; v^\iota \mid \iota \in G \; \text{is an involution} \rangle$$

satisfies $Y \subseteq C \subseteq Y^\perp$ (cf. [5]). In particular if C is generalized doubly-even then Y is isotropic with respect to the quadratic form given in Remark 2.2.2. This yields

Corollary 2.2.4. *If $C \leq \mathbb{F}^N$ is a self-dual generalized doubly-even code and $\pi \in \mathrm{Aut}(C)$ is an involution then $\mathrm{sign}(\pi) = 1$.*

It will be shown in Theorem 3.2.4 that even the automorphism group of a self-dual generalized doubly-eben code is always contained in the alternating group.

The code Y is G-invariant since $gv^\iota = v^{g\iota g^{-1}}$ for all involutions ι and all $g \in G$. Hence

Remark 2.2.5. *Assume that there exists a generalized doubly-even code in $\mathbb{F}^N$. Then the space $Y^\perp/Y$ carries a well-defined quadratic form*

$$q: \ v + Y \mapsto \sum_{i=1}^{f} \frac{\mathrm{wt}(\mathcal{G}(t_i v))}{2} \, t_i^2,$$

where $(t_1, \ldots, t_f)$ is a Trace*-orthogonal $\mathbb{F}_2$-basis of $\mathbb{F}$, and $\mathcal{G}$ is the Gray map (see Section 2.2.3). The polar form $\lambda(q)(v + Y, w + Y) = \beta(v, w)$, and the doubly-even self-dual G-invariant codes in $\mathbb{F}^N$ are in correspondence with the G-invariant isotropic self-dual subspaces of $Y^\perp/Y$.*

The Type of doubly-even self-dual codes in $\mathbb{F}^N$ can now be modeled as a representation of the form ring

$$\mathcal{R} = \mathcal{R}(\mathbb{F}G, J) = (R = \mathbb{F}G, M = R, \mathrm{id}, \Phi = \langle 1, \mathrm{Im}(\{ \ \}) \rangle)$$

introduced in Example 2.1.9. It follows already from Remark 2.1.10 that whenever there exists a self-dual doubly-even G-invariant code in $\mathbb{F}^N$ then there exists a representation of $\mathcal{R}$ which models these codes. Here this representation is $T(Y^\perp/Y, q)$, according to Example 2.1.9, since

Remark 2.2.6. *For every $v \in Y^\perp$ and $r = r^J \in R$,*

$$\lambda(q)(v + Y, r(v + Y)) = \beta(v, rv) = 0.$$

Proof. The element $r = r^J$ if and only if r lies in the kernel of $\{ \ \}$, which is generated as an R-qmodule by the elements $g + g^{-1}$, for $g \in G$, and the involutions of G, and it suffices to proof the claim for these generators. For the first kind of generators one calculates that

$$\beta(v, (g + g^{-1})v) = \beta(v, gv) + \beta(v, g^{-1}v) = \beta(v, gv) + \beta(v, gv) = 0$$

For the second kind of generators, note that for all $v \in \mathbb{F}^N$

$$\beta(v, \iota v) = \sum_{i=1}^{N} v_i v_{\iota(i)} = \sum_{i=\iota(i)} v_i^2 + \sum_{\{i, \iota(i)\}, \, i \neq \iota(i)} v_i v_{\iota(i)} + v_{\iota(i)} v_i = \sum_{i=\iota(i)} v_i^2.$$

Clearly the latter is zero whenever $v \in Y^\perp$, which shows the assertion. $\qquad\square$

2.3   The graph Γ_T of self-dual Type T codes

Let $T = (V, \rho_M, \rho_\Phi, \beta)$ be a representation of the form ring $\mathcal{R}$ and let

$$\mathfrak{C}(T) := \{C \leq V \mid C \text{ is a self-dual Type } T \text{ code}\}.$$

This section introduces a graph Γ_T with vertex set $\mathfrak{C}(T)$ and describes a method to find all neighbors in Γ_T of a code $C \in \mathfrak{C}(T)$. It is shown that the graph Γ_T is connected and hence, starting with one self-dual Type T code, one can successively compute neighbors to determine $\mathfrak{C}(T)$ completely.

Definition 2.3.1. *The* length $l(W)$ *of a submodule W of V is the length of a composition series of W. It is well-defined by the Jordan-Hölder Theorem.*

Remark 2.3.2. *Let $C, D \in \mathfrak{C}(T)$. Then $l(C) = l(D)$.*

Proof. The map $^\perp : M \mapsto M^\perp$ is an antiautomorphism of the submodule lattice of V. Hence if

$$\{0\} = M_0 \leq M_1 \leq \ldots \leq M_k = C$$

is a composition series of C then

$$C = M_k^\perp \leq \ldots \leq M_1^\perp \leq M_0^\perp = V$$

is a composition series of V/C. In particular $l(V)$ is even whenever $\mathfrak{C}(T)$ is nonempty, and $l(C) = \frac{l(V)}{2}$ does not depend on $C \in \mathfrak{C}(T)$. $\qquad\square$

Definition 2.3.3. *The* distance *between two vertices $C, D \in \mathfrak{C}(T)$ is $d(C, D) = l(C/C \cap D)$. The codes C, D are called* neighbors *if $d(C, D) = 1$.*

Remark 2.3.4. *The map d is symmetric and satisfies the triangle inequality, i.e.*

$$d(C, D) = d(D, C) \quad \text{and} \quad d(C, D) \leq d(C, E) + d(E, D)$$

for all $C, D, E \in \mathfrak{C}(T)$.

Proof. For the symmetry of d, note that

$$l(C) = d(C, D) + l(C \cap D) \quad \text{and} \quad l(D) = d(D, C) + l(C \cap D).$$

Since $l(C) = l(D)$ by Remark 2.3.2, this yields $d(C, D) = d(D, C)$. For the triangle inequality, note that

$$d(C, D) = l(C/C \cap D) \leq l(C/C \cap D \cap E) = d(D, E) + l(E \cap D/C \cap E \cap D),$$

hence it suffices to show that $l(D \cap E/C \cap D \cap E) \leq d(C, E) = l(E/C \cap E)$. This follows from the elementary observation that for any two submodules $N \leq M \leq V$, a proper inclusion chain $N \cap D \leq X \leq M \cap D$ yields a proper inclusion chain $N \leq X + N \leq M$. $\qquad\square$

Definition 2.3.5. *The* neighbor graph Γ_T *has vertex set* $\mathfrak{C}(T)$, *and two vertices* C, D *are adjacent if and only if they are neighbors.*

Theorem 2.3.6. *The graph* Γ_T *is connected, and the distance of two vertices* C, D *equals* $d(C, D)$.

Proof. Let $C, D \in \mathfrak{C}(T)$ be two vertices of Γ_T. Induction on $k := d(C, D)$ shows that the minimum number $\delta(C, D)$ of edges of a path in Γ_T connecting C and D equals $d(C, D)$. Clearly $k = 0$ if and only if $D = C$. If $k = 1$ then C, D are adjacent in Γ_T, by definition. Hence the claim follows for $k = 0$ and $k = 1$. Assume that $d(C, D) \geq 2$. Then there exists a code $C_1 \in \mathfrak{C}(T)$ with

$$d(C, C_1) = 1 \quad \text{and} \quad d(C_1, D) = d(C, D) - 1,$$

which is constructed as follows. Since $d(C, D) \geq 2$ there exists a submodule $C \cap D \leq X \leq D$ such that $S := X/(C \cap D)$ is simple. Let $C_1 := (C + X)^\perp + X$, then

$$C_1^\perp = (C + X) \cap X^\perp = C \cap X^\perp + X = (C + X)^\perp + X = C_1$$

since $X \leq X^\perp$. It follows that C_1 is Type T, since X and $(C + X)^\perp$ are Type T. Since the map

$$C + X \to X/(C \cap D), \quad c + x \mapsto x + C \cap D$$

is a well-defined group epimorphism with kernel C, the module $(C + X)/C \cong S$ and hence $C/(C+X)^\perp$ is simple. The situation is illustrated by the diagram below.
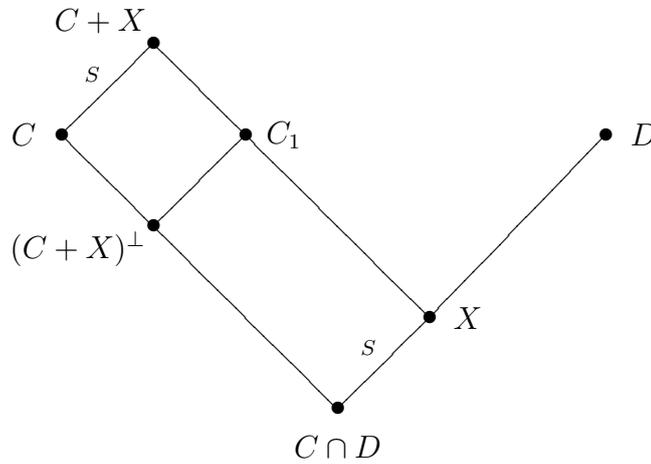
In particular $d(C, C_1) = 1$ since $C \cap C_1 = (C + X)^\perp$, and $d(C_1, D) = d(C, D) - 1$ since $C_1 \cap D = X$. Hence by induction

$$\delta(C, D) \leq \delta(C, C_1) + \delta(C_1, D) = d(C, C_1) + d(C_1, D) = d(C, D).$$

It remains to show that $d(C, D) \leq \delta(C, D)$. Let $(C = C_0, C_1, \ldots, C_t = D)$ be the vertices of a shortest path in Γ_T connecting C and D. This yields a submodule chain

$$C \geq C \cap C_1 \geq \ldots \geq C \cap C_{k-1} \geq C \cap D.$$

The factors

$$C \cap C_i/C \cap C_{i-1} = C \cap C_i/C \cap C_i \cap C_{i+1}$$

are zero or simple, since $C_i/C_i \cap C_{i+1}$ is simple, as observed in the proof of Remark 2.3.4. Hence $d(C, D) \leq \delta(C, D)$.

$\square$

2.3.1   Equivalence of codes and automorphisms of Γ_T

This section defines a finite group $\mathrm{WAut}(T)$ which acts on the set $\mathfrak{C}(T)$ of all self-dual Type T codes, such that the neighbor search given in the previous section can be restricted to the computation of a subset of $\mathfrak{C}(T)$ containing exactly the orbit representatives of this action. In the case of the Type of linear codes $C \leq \mathbb{F}^N$ with $G \leq \mathrm{Aut}(C)$, for a group $G \leq S_N$, we give a subgroup of $\mathrm{WAut}(T)$ which preserves all the properties of codes which are of interest in coding theory, like the weight distribution and the structure of the automorphism group.

Definition 2.3.7. *The weak form isometries (cf. Definition 2.1.13) of T onto itself form a group $\mathrm{WAut}(T)$, called the* weak automorphism group *(cf. [33, Definition 1.11.2]).*

Remark 2.3.8. *For a code $C \in \mathfrak{C}(T)$, let $\mathcal{N}(C)$ be the set of all neighbors of C in the neighbor graph. The weak automorphism group $\mathrm{WAut}(T)$ acts on $\mathfrak{C}(T)$, by $(\Theta, C) := \alpha(C)$, for $\Theta = (\alpha_R, \alpha_M, \alpha_\Phi, \alpha) \in \mathrm{WAut}(T)$ and $C \in \mathfrak{C}(T)$, and $\alpha(\mathcal{N}(C)) = \mathcal{N}(\alpha(C))$.*

   Proof. To see that $\alpha(\mathcal{N}(C)) = \mathcal{N}(\alpha(C))$, let $D \in \mathcal{N}(C)$. The quotient

$$\alpha(C)/(\alpha(C) \cap \alpha(D)) = \alpha(C/\alpha(C \cap D) = \alpha(C/C \cap D)$$

is simple, since $C/C \cap D$ is simple. Hence $\alpha(D) \in \mathcal{N}(\alpha(C))$, which shows the inclusion $\alpha(\mathcal{N}(C)) \subseteq \mathcal{N}(\alpha(C))$. The other inclusion follows by changing to the inverse of α. $\square$

Corollary 2.3.9. *The group $\mathrm{WAut}(T)$ acts on $\mathfrak{C}(T)$ as graph automorphisms of Γ_T, i.e. two vertices C, D are adjacent if and only if $\Theta(C), \Theta(D)$ are adjacent, for every $\Theta \in \mathrm{WAut}(T)$.*

Corollary 2.3.10. *Let $Y \leq \mathrm{WAut}(T)$ be a subgroup. Then there exists a connected subgraph of Γ_T with vertices the orbit representatives of the action of Y on $\mathfrak{C}(T)$. This subgraph is computed by the following algorithm.*

   1. *$L := \{C\}$, $L' := \{C\}$*

   2. *Compute the set $\mathcal{N}_{L'} := \cup_{l' \in L'} \mathcal{N}(l')$ of all neighbors of elements of L'.*

   3. *Choose a subset $L'' \subseteq L \cup \mathcal{N}_{L'}$ such that all codes in L'' lie in different orbits under the action of Y.*

   4. *If $N_{L'} \cap L'' \subseteq L$ then return L.*

5. Go to 2 with $L := L''$, $L' := \mathcal{N}_{L'} \cap L''$.

The theory of weak automorphisms and graph automorphisms is now applied to linear codes over finite fields with prescribed automorphisms. The symmetric group S_N acts naturally on the set of all self-dual linear codes in $\mathbb{F}^N$, but not on the set

$$\mathfrak{C}(\mathbb{F}, G) := \{C = C^\perp \leq \mathbb{F}^N \mid G \leq \mathrm{Aut}(C)\}$$

of all G-invariant self-dual codes for a group $G \leq S_N$, since for $C \in \mathfrak{C}(\mathbb{F}, G)$ and $\pi \in S_N$ the code $\pi(C)$ is not necessarily G-invariant.

Remark 2.3.11. *The normalizer $\mathfrak{N} := N_{S_N}(G)$ acts on $\mathfrak{C}(\mathbb{F}, G)$ by $\eta \cdot C = \eta(C)$, for $\eta \in N$ and $C \in \mathfrak{C}(\mathbb{F}, G)$. Two codes $C, D \in \mathfrak{C}(\mathbb{F}, G)$ are called* normalizer equivalent *if they are in the same orbit under this action.*

Proof. For a code $C \leq \mathbb{F}^N$ and $\eta \in \mathfrak{N}$, the code $\eta \cdot C$ has $\mathrm{Aut}(\eta \cdot C) = \eta \mathrm{Aut}(C) \eta^{-1}$ and hence $G \leq \mathrm{Aut}(\eta \cdot C)$ whenever $G \leq \mathrm{Aut}(C)$. $\qquad \square$

The action of $\mathfrak{N}$ on $\mathfrak{C}(\mathbb{F}, G)$ is the action of some subgroup of the weak automorphism group $\mathrm{WAut}(T(\mathbb{F}, G))$, where $T(\mathbb{F}, G)$ is the Type of self-dual G-invariant codes in $\mathbb{F}^N$: Recall that the underlying form ring is

$$\mathcal{R}(\mathbb{F}, G) = (\mathbb{F}G, \mathbb{F}G, \mathrm{id}, \mathbb{F}G/\Lambda = \mathbb{F}G/\{a - a^J \mid a \in \mathbb{F}G\})$$

(cf. Definition 2.2.4). For every element $\eta \in \mathfrak{N}$, the triple $(\alpha_\eta, \alpha_\eta, \alpha_\eta/\Lambda)$ is a form ring automorphism, where the $\mathbb{F}$-linear map $\alpha_\eta : \mathbb{F}G \to \mathbb{F}G$ is defined by $\alpha_\eta(G) = \eta g \eta^{-1}$, for $g \in G$, and $\alpha_\eta/\Lambda(a + \Lambda) = \alpha_\eta(a) + \Lambda$, for $a \in \mathbb{F}G$. Let $\alpha : \mathbb{F}^N \to \mathbb{F}^N, v \mapsto \eta v$, then $\Theta_\eta := (\alpha_\eta, \alpha_\eta, \alpha_\eta/\Lambda, \alpha)$ is a weak form isometry of $T(\mathbb{F}, G)$. Hence the theory above applies to normalizer equivalence. In particular

Corollary 2.3.12. *The algorithm in Corollary 2.3.10 computes the normalizer equivalence classes of self-dual G-invariant codes in $\mathbb{F}^N$, with $Y = \{\Theta_\eta \mid \eta \in \mathfrak{N}\}$. In particular, for $G = \{1\}$, the algorithm computes the permutation equivalence classes of self-dual codes in $\mathbb{F}^N$.*

Since general the normalizer $\mathfrak{N} = N_{S_N}(G)$ is not so easily computed, one may prefer to compute the orbits of a subgroup of $\mathfrak{N}$ on $\mathfrak{C}(\mathbb{F}, G)$. If G is transitive then the centralizer $C_{S_N}(G) \subseteq \mathfrak{N}$ may be appropriate since it is very easy to compute in this case, as shown in the following theorem.

Theorem 2.3.13. *The centralizer $C_{S_N}(G)$ acts as form isometries on $\mathbb{F}^N$, and if G is transitive then $C_{S_N}(G) \cong N_G(H)/H$, where $H = \mathrm{Stab}_G(1)$.*

Proof. The first part of the claim is clear. Assume that G is transitive, then one may define an action of $N_G(H)$ on the set $\{1, \ldots, N\}$ by

$$g(1) * \eta := g(\eta(1)),$$

for $g \in G$ and $\eta \in N_G(H)$. To see that this action is well-defined, i.e. that $g(\eta(1)) = \tilde{g}(\eta(1))$ whenever $g(1) = \tilde{g}(1)$, note that $g^{-1}\tilde{g} \in H$ if and only if $\eta^{-1}g^{-1}\tilde{g}\eta \in H$,

since $\eta \in N_G(H)$. The group homomorphism $\Delta : N_G(H) \to C_{S_N}(G)$ induced by this action has kernel H, and surjectivity can be seen as follows. Due to the transitivity of G, there exists some element $\eta \in G$ with $\eta(1) = \pi(1)$, and since

$$h\eta(1) = h\pi(1) = \pi h(1) = \pi(1) = \eta(1)$$

for all $h \in H$, the element η normalizes H, i.e. $\pi(1) = \eta(1) = 1 * \eta$. Since the action of π and η is determined by $\pi(1)$ and $\eta(1)$, respectively, the claim follows. $\qquad \square$

If G is transitive then the quotient $\mathfrak{N}/C_{S_N}(G)$ is isomorphic to a subgroup of the automorphism group $\mathrm{Aut}(G)$, which is described in the following theorem.

Theorem 2.3.14. *Let G be a transitive permutation group of degree N and let $H :=$ $\mathrm{Stab}_G(1)$. Let $\mathrm{Aut}_H(G)$ be the set of all automorphisms α of G such that H and $\alpha(H)$ are conjugate in G. Then*

$$\mathfrak{N}/C_{S_N}(G) \cong \mathrm{Aut}_H(G).$$

Proof. The normalizer $\mathfrak{N}$ acts as group automorphisms on G, via $(g, \eta) = g^\eta = \eta g \eta^{-1}$. This gives rise to a homomorphism

$$\mathfrak{N} \to \mathrm{Aut}(G), \quad \eta \mapsto (g \mapsto g^\eta),$$

with kernel $C_{S_N}(G)$. The group H is mapped to $\mathrm{Stab}_G(\eta(1))$, which is conjugate to H, due to the transitivity of G. Hence there is a well-defined group monomorphism

$$\varphi : \mathfrak{N}/C_{S_N}(G) \to \mathrm{Aut}_H(G), \quad \eta \cdot C_{S_N}(G) \mapsto (g \mapsto g^\eta).$$

To see that φ is surjective, let $\alpha \in \mathrm{Aut}_H(G)$ and assume without loss of generality that $\alpha(H) = H$. Then α induces a permutation $\pi \in S_N$, given by $\pi(x(1)) = \alpha(x)(1)$, for $x \in G$. This permutation satisfies

$$\pi g \pi^{-1}(x(1)) = \pi g \alpha^{-1}(x)(1) = \alpha(g\alpha^{-1}(x))(1) = \alpha(g)(x(1))$$

for all $g, x \in G$, and hence $\pi g \pi^{-1} = \alpha$, i.e. π is a preimage of α under φ, and the claim follows. $\qquad \square$

Corollary 2.3.15. *If G is a transitive permutation group then $\mathfrak{N} \cong N_G(H)/H \rtimes$ $\mathrm{Aut}_H(G)$, where $H, \mathrm{Aut}_H(G)$ are as above.*

Proof. By Theorem 2.3.13, the quotient $N_G(H)/H \cong C_{S_N}(G)$, and the normal subgroup $C_{S_N}(G)$ of $\mathfrak{N}$ has a complement isomorphic to $\mathrm{Aut}_H(G)$, which is seen as follows. Consider $\mathrm{Aut}_H(G)$ as a subgroup of $\mathfrak{N}$ by means of the embedding

$$\iota : \mathrm{Aut}_H(G) \to \mathfrak{N}, \quad \alpha \mapsto (x(1) \mapsto \alpha(x)(1)), \quad x \in G.$$

To see that ι is injective, note that every element $\alpha \in \ker(\iota)$ maps $\alpha(g) = h_g g$ with some element $h_g \in H$, for all $g \in G$. The identity

$$h_x x h_g g = \alpha(x)\alpha(g) = \alpha(xg) = h_{xg} xg$$

implies that $xh_g x^{-1} \in H$ for all $x, g \in G$, i.e. $h_g \in \cap_{x \in G} x^{-1} H x = \{1\}$. Hence α is the identity, which shows the injectivity of ι. In this sense, $\operatorname{Aut}_H(G) \cap C_{S_N}(G) = \{1\}$, since if $\alpha \in \operatorname{Aut}_H(G) \cap C_{S_N}(G)$ then $\alpha(gx)(1) = g(\alpha(x)(1))$ for all $g, x \in G$ and hence $\alpha(g) = g$ for all $g \in G$. Now the claim follows with Theorem 2.3.14. $\qquad \square$

Remark 2.3.16. *Note that the proof of Theorem 2.3.14 provides an algorithm to compute $\mathfrak{N}$ whenever G is transitive, as follows.*

1. *Determine the subgroup Λ of $\operatorname{Aut}(G)$ containing all automorphisms which leave H invariant.*

2. *For every element α of a generating subset $\mathcal{G}$ of Λ compute the well-defined permutation $\pi_\alpha : \ g(1) \mapsto \alpha(g)(1)$.*

3. *Compute $\mathfrak{N} = \langle G, C_{S_N}(G), \pi_\alpha \mid \alpha \in \mathcal{G} \rangle$.*

In an implementation in Magma ([3]) this algorithm turns out to be fast if $\operatorname{Aut}(G)$ is not too difficult to handle in the first step. In many interesting cases, for instance for $G = M_{12}$, the inner automorphism group has index 2 in $\operatorname{Aut}(G)$ and hence either $\operatorname{Aut}_H(G) = G$ or $\operatorname{Aut}_H(G) = \operatorname{Aut}(G)$. Since the latter is easy to test and $\mathcal{G}$ can easily be determined from a generating subset of $\operatorname{Aut}_H(G)$, the algorithm has a good performance in these cases.

2.3.2 Block decomposition

Let R be a finite ring with unity. An *idempotent* is an element $0 \neq e \in R$ with $e^2 = e$. Two idempotents e, f are called *orthogonal* if $ef = fe = 0$. The idempotent e is called *primitive* if for all orthogonal idempotents $f, g \in R$ with $e = f + g$, either $f = e$ or $g = e$. A *central primitive* idempotent is a primitive idempotent of the center of R. The following is well-known.

Lemma 2.3.17. *(i) Let e, f be central primitive idempotents. Then either $e = f$ or $ef = fe = 0$.*

(ii) There exists a unique decomposition $1 = e_1 + \ldots + e_k$ into central primitive idempotents. This induces a decomposition

$$R = e_1 R \times \ldots \times e_k R$$

into ringdirect summands, called the blocks *of R, and every left R-module V is a direct sum*

$$V = e_1 V \oplus \ldots \oplus e_k V.$$

Remark 2.3.18. *Let $\mathcal{R}$ be a form ring over the ring R, with associated involution J, and let $e \in R$ be a central idempotent with $e^J = e$. Then every finite representation $T = (V, \rho_M, \rho_\Phi, \beta)$ of $\mathcal{R}$ decomposes as $T = eT \perp (1 - e)T$, where*

$$eT = (eV, \rho_M, \rho_\Phi, \beta_e),$$

with $\beta_e(ev, ew) = \beta(ev, ew)$, and $(1-e)T$ is defined similarly. If $C \leq V$ is a submodule then $C = eC \perp (1-e)C$, and $(eC)^{\perp,\beta_e} = (eC)^{\perp,\beta} \cap eV = eC^{\perp,\beta}$. In particular every self-dual Type T code is the orthogonal sum of two self-dual codes of Type eT and $(1-e)T$, respectively.

Remark 2.3.19. *Let $\mathcal{R}$ be a form ring over R and let $1 = e_1 + \ldots + e_k$ be the decomposition into central primitive idempotents. For every finite representation T on the R-module V, the group $\mathrm{WAut}(T)$ acts on the set $\{e_iV \mid i \in \{1, \ldots, k\}\}$, by*

$$(\Theta, e_iV) = \alpha(e_iV) = \alpha_R(e_i)V,$$

for $\Theta = (\alpha_R, \alpha_M, \alpha_\Phi, \alpha) \in \mathrm{WAut}(C)$.

Let $1 = c_1 + \ldots + c_t$ be a decomposition into pairwise orthogonal central idempotents such that $c_i^J = \alpha_R(c_i) = c_i$ for all i and all $\Theta = (\alpha_R, \alpha_M, \alpha_\Phi, \alpha) \in \mathrm{WAut}(T)$. Then $T = \perp_{i=1}^t T_i$, where $T_i = (c_iV, \rho_M, \rho_\Phi, \beta_{c_i})$, and every code $C \in \mathfrak{C}(T)$ decomposes as

$$C = c_1C \perp \ldots \perp c_tC,$$

with summands $c_iC \in \mathfrak{C}(T_i)$. Every subgroup Y of $\mathrm{WAut}(T)$ acts on $\mathfrak{C}(T_i)$ as weak automorphisms, and every element $\Theta \in Y$ satisfies $\Theta \cdot C = D$ if and only if $\Theta \cdot (c_iC) = c_iD$ for all i.

Corollary 2.3.20. *The following modification of the algorithm in Corollary 2.3.10 gives orbit representatives for the action of some subgroup Y of $\mathrm{WAut}(T)$ on $\mathfrak{C}(T)$, performing the neighbor search only on the direct summands c_iV.*

1. *Let $i := 1$, $F := \{0\}$.*

2. *For $C \in F$, find a set O_C of orbit representatives of $\mathfrak{C}(T_i)$ under the action of $\mathrm{Stab}_Y(C)$.*

3. *Go to 1. with $i := i + 1$, $F := \{C \oplus X \mid C \in F, X \in O_C\}$.*

Chapter 7 treats the case where T is the Type of G-invariant codes in $\mathbb{F}^N$, for some subgroup $G \leq S_N$. The underlying ring is the group algebra $\mathbb{F}G$, and on the set $\mathfrak{C}(T)$ the normalizer $N_{S_N}(G)$ acts as weak automorphisms. The following Lemma states that in this case, there exists some non-trivial decomposition $1 = c_1 + \ldots + c_t$ as above.

Lemma 2.3.21. *Let $\mathbb{F}$ be a finite field, let $G \leq S_N$ be a finite group, and let $e \in \mathbb{F}G$ be the central primitive idempotent belonging to the trivial G-module. Then $e^J = e$, and $\eta e \eta^{-1} = e$ for all $\eta \in N_{S_N}(G)$.*

Proof. The element e acts as the identity on the trivial G-module and all other central primitive idempotents annihilate the trivial module. Hence $e = \sum_{g \in G} e_g g$ is the unique central primitive idempotent with $\sum_{g \in G} e_g = 1$. The elements e^J and $\eta e \eta^{-1}$, for $\eta \in N_{S_n}(G)$, are central primitive idempotents which also have this property, hence are equal to e. $\square$

Chapter 3

Permutations and the neighbor graph

This chapter treats *codes* in the classical sense, i.e. a code is a subspace of $\mathbb{F}^N$, for a finite field $\mathbb{F}$. Orthogonality is defined through the standard scalar product

$$\beta: \ \mathbb{F}^N \times \mathbb{F}^N \to \mathbb{F}, \ \ ((v_1, \ldots, v_N), (w_1, \ldots, w_N)) \mapsto \sum_{i=1}^{N} v_i w_i,$$

that is, the *dual* of a code C is

$$C^{\perp} = \{v \in \mathbb{F}^N \mid \beta(v, c) = 0 \ \text{ for all } c \in C\},$$

which is again a code. In this chapter a *self-dual* code (i.e. $C = C^{\perp}$) over a field of odd characteristic, or a self-dual *generalized doubly-even* code (cf. Definition 2.2.1) is viewed as a maximally isotropic subspace of some *quadratic space* (V, q), i.e. V is a vector space over $\mathbb{F}$ and $q : V \to \mathbb{F}$ is a map such that $q(fv) = f^2 q(v)$ for all $f \in \mathbb{F}$ and $v \in V$, and

$$\lambda(q) : V \times V \to \mathbb{F}, \ \ (v, w) \mapsto q(v + w) - q(v) - q(w)$$

is bilinear. Recall that a subspace $U \leq V$ is called isotropic if $q(U) = 0$. The *automorphism group*
$$\mathrm{Aut}(C) := \{\pi \in S_N \mid \pi(C) = C\}$$

is viewed as a subgroup of the *orthogonal group*

$$O(V, q) = \{\varphi \in \mathrm{Aut}(V) \mid q(v) = q(\varphi(v)) \text{ for all } v \in V\}.$$

To state this more precisely, assume first that $\mathbb{F}$ has odd characteristic. Then the quadratic forms on $V = \mathbb{F}^N$ are in correspondence with the symmetric bilinear forms on V, and a code $C \leq V$ is self-dual if and only if $2 \dim(C) = N$ and C is isotropic with respect to the quadratic form $q := \{\beta\} : \ v \mapsto \beta(v, v)$. Moreover, the *orthogonal group*

$$O(V, \beta) = \{\varphi \in \mathrm{Aut}(V) \mid \beta(v, w) = \beta(\varphi(v), \varphi(w)) \text{ for all } v, w \in V\}$$

of the bilinear space (V, β) equals the orthogonal group $O(V, q)$, since $\lambda(\{\beta\}) = 2\beta$. There exists a natural embedding

$$\iota : S_N \hookrightarrow O(V, q), \quad \pi \mapsto (b_i \mapsto b_{\pi(i)}),$$

where $(b_1, \ldots, b_N)$ is the standard orthonormal basis of V. In particular $\mathrm{Aut}(C)$ is isomorphic to a subgroup of $O(V, q)$. Hence for a subgroup $G \leq S_N$, the self-dual G-invariant codes in (V, β) are in correspondence with the $\iota(G)$-invariant isotropic subspaces C of (V, q) which have $2 \dim(C) = N$.

If $\mathbb{F}$ has characteristic 2 then the correspondence between symmetric bilinear and quadratic forms no longer exists, and the isotropic subspaces of $(V, \{\beta\})$ are in general not self-orthogonal with respect to β. However, the generalized doubly-even self-dual codes of length N are in correspondence with the maximally isotropic subspaces of the quadratic space $\tilde{V} := \langle \mathbf{1} \rangle^\perp / \langle \mathbf{1} \rangle$, where $\mathbf{1} \in \mathbb{F}^N$ is the all-ones vector, and the *weight* (cf. Definition 2.2.1) is used to define the appropriate quadratic form. Again, the symmetric group S_N embeds into the orthogonal group of $\tilde{V}$ and $\mathrm{Aut}(C)$ preserves the subspace $C/\langle \mathbf{1} \rangle \leq \tilde{V}$.

This chapter discusses automorphism groups of self-dual codes against the background described above: In either of the two cases, S_N acts as isometries on a quadratic space V, i.e. induces graph automorphisms of the neighbor graph Γ of all self-dual isotropic subspaces of V (cf. Chapter 2). A permutation group leaves a self-dual code invariant if and only if its action on Γ preserves a vertex. From the investigation on the action of transpositions on Γ one concludes that the automorphism group of a self-dual code in odd characteristic, or a generalized doubly-even code, always lies in the alternating group. In characteristic 2, Theorem 3.2.7 characterizes the situation in which there exists a self-dual generalized doubly-even code. The results in this chapter are published in the paper [12].

3.1   Isometries as automorphisms of Γ

Let (V, q) be a *non-degenerate* quadratic space over the finite field $\mathbb{F}$, i.e. the polar form $\lambda(q)$ is non-degenerate. Let $\mathfrak{C}(V, q)$ be the set of all maximally isotropic subspaces of V. Two elements $C, D \in \mathfrak{C}(V, q)$ are called *neighbors* if

$$\dim(C/C \cap D) = 1$$

(cf. Definition 2.3.3). The *neighbor graph* $\Gamma = \Gamma(V, q)$ has the elements of $\mathfrak{C}(V, q)$ as vertices, and two vertices C, D are adjacent if and only if they are neighbors. It follows from Example 2.1.9 that the isotropic subspaces of V form a Type of codes and hence the results in Section 2.3 on the graphs of Type T codes apply to Γ. In particular, Γ is connected and the distance between two vertices C, D in Γ equals $\dim(C/C \cap D) = \dim(D/C \cap D)$. The orthogonal group $O(V) = O(V, q)$ acts transitively on $\mathfrak{C}(V, q)$ by Witt's Theorem (cf. [22, Satz 3.4]). Since

$$\dim(C/C \cap D) = \dim(\varphi(C)/\varphi(C) \cap \varphi(D))$$

for all vertices $C, D \in \mathfrak{C}(V, q)$ and all $\varphi \in O(V)$, the vertices C, D are adjacent if and only if $\varphi(C), \varphi(D)$ are adjacent and hence the action of $O(V)$ on $\mathfrak{C}(V, q)$ induces graph automorphisms of Γ. The following two sections show that Γ is bipartite and that $O(V)$ acts on the set of the two partitions, yielding a group epimorphism $O(V) \to C_2$. To this aim Section 3.1.2 investigates the action of the *reflections* in $O(V)$ on the set $\mathfrak{C}(V, q)$. Recall that the reflection at the hyperplane orthogonal to an anisotropic vector v is the isometry

$$\sigma_v : \ V \to V, \ \ w \mapsto w - \frac{\lambda(q)(v, w)}{q(v)} v.$$

To show that Γ is bipartite, we need another group epimorphism $\delta : O(V) \to C_2$, which is the determinant or the Dickson invariant, depending on the characteristic of $\mathbb{F}$ (cf. Section 3.1.1). We find that every reflection interchanges the partitions of Γ (cf. Theorem 3.1.11). Since every reflection $\sigma \in O(V)$ satisfies $\delta(\sigma) = -1$, this allows to conclude that, whenever $O(V)$ is generated by reflections, the stabilizer in $O(V)$ of a maximally isotropic subspace of V is contained in the kernel of δ.

3.1.1 Determinant and Dickson invariant

If $\mathbb{F}$ has odd characteristic then $O(V)$ is generated by reflections (cf. [22, Satz 3.5]), and the parity of reflections whose product is φ is given by the determinant, for every isometry φ.

Remark 3.1.1. *Assume that $\mathbb{F}$ has odd characteristic and let $\sigma \in O(V)$ be a reflection. Then $\det(\sigma) = -1$. Hence $\varphi \in O(V)$ has $\det(\varphi) = 1$ if and only if it is a product of an even number of reflections, and this parity is well-defined.*

    Proof. Let $v \in V$ be an anisotropic vector such that σ is the reflection at the hyperplane H orthogonal to v. Then $\sigma(v) = -v$, and every element of H is fixed by σ. Hence if $\mathcal{B}$ is a basis of H then $(\mathcal{B}, v)$ is a basis of V, with respect to which σ acts as $\mathrm{diag}(1, \ldots, 1, -1)$, and hence $\det(\sigma) = -1$ as claimed. $\square$

    If $\mathbb{F}$ has characteristic 2 then $O(V)$ is generated by reflections, too, except when V is the orthogonal sum of two hyperbolic planes (cf. [37]). But in characteristic 2 every isometry has determinant 1, i.e. we need a different group epimorphism to describe the parity of reflections whose product is the isometry φ. To this aim Definition 3.1.2 introduces the Clifford algebra $C(V)$ and a certain subalgebra Z of $C(V)$ on which the orthogonal group $O(V)$ acts as automorphisms. It is shown that the automorphism group of Z is cyclic of order 2 (cf. Corollary 3.1.6). Hence the action of $O(V)$ on Z induces a group homomorphism $D : O(V) \to C_2$, which is called the Dickson invariant (cf. Definition 3.1.8).

Definition 3.1.2. *(see [22, Def. 5.3]) A* Clifford algebra *$C(V) = C(V, q)$ is an $\mathbb{F}$-algebra together with a homomorphism $h : V \to C(V)$, such that $h(v)^2 = q(v)$ in $C(V)$ for all $v \in V$, and for every $\mathbb{F}$-algebra B and every homomorphism $g : V \to B$ with $g(v)^2 = q(v)$ for all $v \in V$, there exists a uniquely determined homomorphism $\alpha : C(V) \to B$ with $\alpha(h(v)) = g(v)$ for all $v \in V$.*

It is well-known that for every quadratic space (V, q) there exists a Clifford algebra $C(V, q)$, which is uniquely determined up to isomorphism (cf. [22]), and that the associated map h is always injective. Note that in the Clifford algebra,

$$vw + wv = (v + w)^2 - v^2 - w^2 = q(v + w) - q(v) - q(w) = \lambda(q)(v, w)$$

for all $v, w \in V$.

Remark 3.1.3. *(cf. [22, Satz 5.12]) If the dimension of V is n then the dimension of the Clifford algebra is 2^n. More precisely, if $(e_1, \ldots, e_n)$ is a basis of V then*

$$\mathcal{B} := \{e_{i_1} \cdot \ldots \cdot e_{i_k} \mid i_1 < \ldots < i_k \in \{1, \ldots, n\}\}$$

is a basis of $C(V)$, where the empty product equals 1 and is an element of the basis. As vector spaces, $C(V) = C_0(V) \oplus C_1(V)$, where

$$C_j(V) = \langle e_{i_1} \cdot \ldots \cdot e_{i_k} \in \mathcal{B} \mid k \equiv j \mod 2 \rangle$$

has dimension 2^{n-1}. Then $C_k(V)C_l(V) \subseteq C_{k+l}(V)$, where all indices are modulo 2. Hence $C(V)$ is a graded algebra mod 2. In particular $C_0(V)$ is a subalgebra of $C(V)$, called the even subalgebra.

Theorem 3.1.4. *(see [22, (5.9)]) Let $(V, q) = (V_1, q_1) \perp (V_2, q_2)$ be an orthogonal decomposition. On the vector space $C(V_1, q_1) \otimes C(V_2, q_2)$ define a multiplication by*

$$(v_1 \otimes w_1) \cdot (v_2 \otimes w_2) = (-1)^{ij}(v_1 v_2 \otimes w_1 w_2),$$

where $i = 1$ if $w_1 \in C_1(V_2)$, and $j = 1$ if $v_2 \in C_1(V_1)$, and $i = j = 0$ otherwise. With this multiplication $C(V_1, q_1) \otimes C(V_2, q_2) \cong C(V, q)$, via $(v_1 \otimes v_2) \mapsto v_1 \cdot v_2$.

From now on assume that $\mathbb{F}$ has characteristic 2. Then the non-degenerate symmetric bilinear form $\beta := \lambda(q)$ is symplectic and hence $\dim(V) = 2m$ is even, and there exists a basis $(e_1, \ldots, e_{2m})$ of V such that

$$\beta(e_i, e_j) = 0, \quad \beta(e_{m+i}, e_{m+j}) = 0 \quad \text{and} \quad \beta(e_i, e_{m+j}) = \delta_{ij} \tag{3.1}$$

for $i, j \in \{1, \ldots, m\}$. If the quadratic space (V, q) has Witt defect 0 (cf. Remark 4.2.8) then V is the orthogonal sum of hyperbolic planes, and we may assume that $q(e_i) = q(e_{m+i}) = 0$ for all i. Otherwise, $(V, q) \cong \perp_{i=1}^{m-1} \mathbb{H} \perp V_1$ is the orthogonal sum of hyperbolic planes $\mathbb{H}$ and an anisotropic space (V_1, η), where $V_1 \cong \mathbb{F}_{q^2}$, if $\mathbb{F}$ has q elements, and $\eta : x \mapsto x^{q+1}$ is the Norm form. In this case, we may still assume that $q(e_i) = q(e_{m+i}) = 0$ for all $i \in \{1, \ldots, m-1\}$, and by suitable scaling, that $q(e_m) = 1$ and $\beta(e_m, e_{2m}) = 1$. Note that then the polynomial $x^2 + x + q(e_{2m}) \in \mathbb{F}[x]$ is irreducible since if λ were a root of this polynomial then the vector $v = \lambda e_m + e_{2m}$ would satisfy

$$q(v) = q(\lambda e_m) + \beta(\lambda e_m, e_{2m}) + q(e_{2m}) = \lambda^2 + \lambda + q(e_{2m}) = 0,$$

which contradicts the anisotropy of V_1.

Theorem 3.1.5. *(see [4, p.3]) The center Z of $C_0(V, q)$ is a 2-dimensional vector space over $\mathbb{F}$, generated by the elements 1 and $z := \sum_{i=1}^{m} e_i e_{m+i}$, where $(e_1, \ldots, e_{2m})$ is a basis of V as in (3.1).*

Proof. We proceed by induction on m. If $m = 1$ then $\dim(C_0(V, q)) = 2$, by Remark 3.1.3. Hence it suffices to show that $e_1 e_2 \in Z$, and to this aim it suffices to show that $e_1 e_2$ commutes with the element $e_2 e_1$, which is obvious.

For $m > 1$, let $V = V_1 \perp V_2$ be an orthogonal decomposition into subspaces with symplectic bases $(e_1, \ldots, e_{2m})$ and $(f_1, \ldots, f_{2m})$, respectively. Clearly

$$C_0(V_1) \cdot C_0(V_2) \subseteq C_0(V),$$

and hence every element of Z centralizes the subalgebras $C_0(V_i)$. By induction, the center of $C_0(V_i)$ has a basis $(1, z_i)$, where $z_1 + z_2 = z$. Hence Z is contained in the subalgebra generated by the elements $1, z_1, z_2, z_1 \cdot z_2$, by Theorem 3.1.4. Let

$$x = \lambda_1 + \lambda_2 z_1 + \lambda_3 z_2 + \lambda_4 z_1 \cdot z_2 \in Z,$$

with $\lambda_i \in \mathbb{F}$ for $i \in \{1, \ldots, 4\}$. The element $e_1 \cdot f_1 \in C_0(V, q)$, and an elementary calculation shows that

$$x e_1 \cdot f_1 - e_1 \cdot f_1 x = (\lambda_2 + \lambda_3) e_1 \cdot f_1 + \lambda_4 e_1 \cdot f_1 (1 + z_1 + z_2).$$

Hence if $x \in Z$ then $\lambda_2 = \lambda_3$ and $\lambda_4 = 0$. This yields $x \in \langle 1, z \rangle$. One easily verifies that indeed, $z \in Z$, which proves the assertion. $\square$

Corollary 3.1.6. *If (V, q) has Witt defect 0 then the $\mathbb{F}$-algebra $Z \cong \mathbb{F} \oplus \mathbb{F}$. Otherwise Z is a quadratic field extension of $\mathbb{F}$. In either of the two cases, $\mathrm{Aut}(Z) \cong C_2$ is generated by the automorphism $z \mapsto z + 1$.*

Proof. Let z be as in Theorem 3.1.5. As one easily verifies,

$$z^2 + z = \sum_{i=1}^{m} q(e_i) \, q(e_{m+i}).$$

Hence if V has Witt defect 0 then z has minimal polynomial $x^2 + x$ and hence $Z \cong \mathbb{F}[x]/(x^2 + x) \cong \mathbb{F} z \oplus \mathbb{F}(z + 1)$, and every algebra automorphism of Z either interchanges or fixes the primitive idempotents $z, z + 1$. If V has Witt defect 2 then z has minimal polynomial $x^2 + x + q(e_{2m})$, which is irreducible as remarked above. Hence in this case $Z \cong \mathbb{F}[x]/(x^2 + x + q(e_{2m}))$ is a field, and every algebra automorphism of Z either interchanges or fixes the roots z and $z + 1$ of the polynomial $x^2 + x + q(e_{2m})$ over Z. $\square$

Corollary 3.1.7. *Let $\varphi \in O(V)$. If $h : V \hookrightarrow C(V)$ is the embedding associated with $C(V)$ then $h \circ \varphi : V \hookrightarrow C(V)$ is another embedding and hence by the universal property of the Clifford algebra there exists a unique algebra automorphism c_φ of $C(V)$ with $c_\varphi \circ h = \varphi \circ h$, i.e. which extends φ. The subalgebra Z is left invariant under c_φ, and c_φ either induces the identity on Z or the automorphism of order 2 given by $c_\varphi(z) = z + 1$, where z is as in Theorem 3.1.5.*

Definition 3.1.8. *The* Dickson invariant *is the group homomorphism* $D : O(V, q) \to C_2 = \{1, -1\}$ *with* $D(\varphi) = 1$ *if and only if* φ *induces the identity on* Z.

Remark 3.1.9. *If* σ *is a reflection then* $D(\sigma) = -1$. *Hence if* $O(V)$ *is generated by reflections then an element* $\varphi \in O(V)$ *lies in the kernel of* D *if and only if it is a product of an even number of reflections, and this parity is well-defined since* D *is well-defined.*

Proof. All reflections are conjugate in $O(V)$, since if σ_v, σ_w are reflections at vectors v, w then by suitable scaling one may assume that $q(v) = q(w)$, since every element in $\mathbb{F}$ is a square. By Witt's Theorem there exists an isometry h with $h(v) = w$ and hence $\sigma_w = \sigma_{h(v)} = h\sigma_v h^{-1}$. Hence it suffices to show the claim for the reflection $\sigma = \sigma_{e_1 - e_{m+1}}$ interchanging the basis vectors e_1, e_{m+1} and fixing all other basis vectors. Now

$$c_\sigma(z) = e_{m+1}e_1 + \sum_{i=2}^{m} e_i e_{m+i} = 1 + \sum_{i=1}^{m} e_i e_{m+i} = 1 + z$$

and hence $D(\sigma) = -1$, which shows the assertion. □

The Dickson invariant may also defined in odd characteristic, via the action of $O(V)$ on the centralizer of $C_0(V)$ in $C(V)$, which equals Z if V has even dimension. The Dickson invariant is then equal to the determinant (cf. [22]).

3.1.2　Reflections and the neighbor graph

Let (V, q) be a non-degenerate quadratic space over the finite field $\mathbb{F}$ (of arbitrary characteristic), of dimension $2m$ and Witt defect 0, whose orthogonal group is generated by reflections.

Theorem 3.1.10. *Let* $\varphi \in O(V)$ *such that there exists a maximally isotropic subspace of* V *which is left invariant under* φ. *Then* φ *is a product of an even number of reflections.*

Proof. Let U be a maximally isotropic subspace of V which is left invariant under the isometry φ. Then U has a basis $(e_1, \ldots, e_m)$ such that $(e_1, \ldots, e_{2m})$ is a basis of V as in 3.1. Write $\varphi = \left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix} \right)$ with matrices $A, B, C \in \mathbb{F}^{m \times m}$, i.e.

$$\varphi(e_j) = \sum_{i=1}^{m} A_{ij} e_i \quad \text{and} \quad \varphi(e_{m+j}) = \sum_{i=1}^{m} B_{ij} e_i + C_{ij} e_{m+i}$$

for $j \in \{1, \ldots, m\}$. If $\mathbb{F}$ has odd characteristic then φ is a product of an even number of reflections if and only if its determinant is 1. Since φ is an isometry, the product $AC^{\mathrm{tr}} = I_m$ and hence $\det(\varphi) = \det(A)\det(C) = 1$ as claimed. Now assume that $\mathbb{F}$ has characteristic 2. By Remark 3.1.9, φ is a product of an even number of reflections if and only if $D(\varphi) = 1$. Since φ is an isometry,

$$AB^{\mathrm{tr}} \in \mathrm{Alt}_m(\mathbb{F}) = \{M \in \mathbb{F}^{m \times m} \mid M = M^{\mathrm{tr}} \text{ and } M_{ii} = 0 \text{ for } i \in \{1, \ldots, m\}\}$$

and $AC^{\mathrm{tr}} = I_m$. Let z be as in Theorem 3.1.5, then the automorphism c_φ of $C(V, q)$ induced by φ maps

$$
\begin{aligned}
c_\varphi(z) = c_\varphi(\sum_{i=1}^{m} e_i e_{m+i}) &= \sum_{i=1}^{m} \varphi(e_i)\varphi(e_{m+i}) = \sum_{j=1}^{m}\sum_{i=1}^{m} A_{ij} e_i (\sum_{t=1}^{m} B_{tj} e_t + C_{tj} e_{m+t}) \\
&= \sum_{i,j,t=1}^{m} A_{ij} B_{tj} e_i e_t + A_{ij} C_{tj} e_i e_{m+t} = \sum_{i,j,t=1}^{m} (AB^{\mathrm{tr}})_{it} e_i e_t + (AC^{\mathrm{tr}})_{it} e_i e_{m+t} \\
&= \sum_{1 \leq i < t \leq m} (AB^{\mathrm{tr}})_{it} e_i e_t + (AB^{\mathrm{tr}})_{it} e_t e_i + (AC^{\mathrm{tr}})_{ij} e_i e_{m+j} + \sum_{i,t=1}^{m} (AC^{\mathrm{tr}})_{it} e_i e_{m+t} \\
&= \sum_{i=1}^{m} e_i e_{m+i} = z
\end{aligned}
$$

and hence by definition $D(\varphi) = 1$ (see also [7]). $\square$

Theorem 3.1.11. *Let σ be a reflection, and let C be a maximally isotropic subspace of V. Then $\sigma(C)$ and C are neighbors. Conversely, if D is a neighbor of C then there exists a reflection τ with $C\tau = D$.*

    Proof. To prove the first part of the theorem, let $v \in V$ be an anisotropic vector such that σ is the reflection at the hyperplane H orthogonal to v. Then every vector in H is fixed by σ and hence $C \cap H \subseteq C \cap \sigma(C)$. Now

$$
\begin{aligned}
\dim(C \cap H) = \dim((C + \langle v \rangle)^{\perp}) &= \dim(V) - \dim(C + \langle v \rangle) \\
&= 2m - (m + 1) = m - 1
\end{aligned}
$$

and hence $\dim(C/C \cap \sigma(C)) \leq \dim(C/C \cap H) = 1$. According to the previous theorem, C is not invariant under σ and hence $\dim(C/C \cap \sigma(C)) = 1$. Hence $\sigma(C)$ and C are neighbors. Conversely, let D be a neighbor of C. Then there exist $v_C, v_D \in V$ such that $C = \langle C \cap D, v_C \rangle$ and $D = \langle C \cap D, v_D \rangle$. The vector $v := v_C + v_D$ is anisotropic since $q(v) = \beta(v_C, v_D) \neq 0$. One easily verifies that the reflection at the hyperplane orthogonal to v interchanges v_C, v_D and fixes the space $C \cap D$. Hence $D = \sigma(C)$. $\square$

Corollary 3.1.12. *The neighbor graph Γ is bipartite, and an element $\varphi \in O(V)$ interchanges the two partitions if and only if it is a product of an odd number of reflections. Otherwise both partitions are left invariant under φ.*

Remark 3.1.13. *Note that the assumption that V be of Witt defect 0 is necessary for the theorems in this section. Let for instance V be a quadratic space over the finite field $\mathbb{F} = \mathbb{F}_q$ of characteristic 2, of dimension $2m$ and Witt defect 2. In this case, $V = V_0 \perp V_1$ is an orthogonal sum of a quadratic space V_0 of dimension $2m - 2$ and Witt defect 0, and $V_1 = \mathbb{F}_{q^2}$ with the anisotropic quadratic form $\mathbb{F}_{q^2} \to \mathbb{F}_q$, $x \mapsto x^{q+1}$. Let σ be the isometry which interchanges two nonzero vectors $v, w \in V_1$ and fixes V_0. Then σ is the reflection at the hyperplane orthogonal to $v + w$ and hence $D(\sigma) = -1$, by Remark 3.1.9. On the other hand, every maximally isotropic subspace U of V that is contained in V_0 is left invariant under σ.*

3.2 Automorphisms of codes as isometries

This section shows how linear codes over a finite field can be viewed as subspaces of a quadratic space and investigates which isometries are induced by the symmetric group S_N. To this aim, let $(b_1, \ldots, b_N)$ be the distinguished orthonormal basis of the standard scalar product β with respect to which one defines a code. In odd characteristic, the map $\iota : \pi \mapsto (b_i \mapsto b_{\pi(i)})$ gives an embedding into the orthogonal group of the quadratic space $\mathbb{F}^N$, with the quadratic map $\{\beta\}$ induced by the standard scalar product.

We will now investigate the situation when $\mathbb{F}$ has characteristic 2. Classically, a binary code $C \leq \mathbb{F}_2^N$ is said to be doubly-even if the *weight*

$$\mathrm{wt}(c) = |\{i \in \{1, \ldots, N\} \mid c_i \neq 0\}|$$

is a multiple of 4 for every codeword $c = (c_1, \ldots, c_N) \in C$. Definition 2.2.1 extends the notion of doubly-even codes to arbitrary finite fields of characteristic 2 (cf. [35]).

Assume that $N \geq 4$. The symmetric group S_N acts on $\mathbb{F}^N$ via $\pi \cdot (v_1, \ldots, v_N) = (v_{\pi(1)}, \ldots, v_{\pi(N)})$. Since this action preserves the weight and fixes the vector $\mathbf{1}$, this gives rise to an embedding

$$\tilde{\iota} : \ S_N \hookrightarrow O(\tilde{V}, q), \ \ \pi \mapsto (v + \langle \mathbf{1} \rangle \mapsto \pi \cdot v + \langle \mathbf{1} \rangle).$$

In what follows, an element $\pi \in S_N$ may be identified with its image $\tilde{\iota}(\pi)$, and we may write πU instead of $\tilde{\iota}(\pi)U$, where $U \leq \tilde{V}$ is a subspace. Obviously a code C is preserved by a permutation group G if and only if the space $C/\langle \mathbf{1} \rangle$ is preserved by G. Hence

Remark 3.2.1. *The self-dual doubly-even G-invariant codes $C \leq \mathbb{F}^N$ correspond to the maximally isotropic G-invariant subspaces of $(\tilde{V}, q)$.*

To investigate the image $\tilde{\iota}(\pi)$ of an element $\pi \in S_N$, observe that

Remark 3.2.2. *If v lies in the $\mathbb{F}_2$-span of the $\mathbb{F}$-basis $(b_i + b_N + \langle \mathbf{1} \rangle \mid i \in \{1, \ldots, N-2\})$ of $\tilde{V}$ then $q(v) = \frac{\mathrm{wt}(v)}{2}$ mod 2.*

Proof. It suffices to show the claim for a basis vector $b_i + b_N + \langle \mathbf{1} \rangle$. Since

$$\mathrm{Trace}(t_l \cdot 1) = \mathrm{Trace}(t_l^2) = \mathrm{Trace}(t_l \sum_{k=1}^{f} t_k)$$

for all l and hence $\sum_{k=1}^{f} t_k = 1$, due to the nondegeneracy of the Trace form, one calculates that

$$q(b_i + b_N + \langle \mathbf{1} \rangle) = \sum_{k=1}^{f} \frac{\mathrm{wt}(t_k(b_i + b_N))}{2} t_k^2 = \sum_{k=1}^{f} t_k^2 = (\sum_{k=1}^{f} t_k)^2 = 1,$$

as claimed. $\qquad\square$

Lemma 3.2.3. *Assume that $N \geq 4$ is even. The composition $D \circ \tilde{\iota} = \text{sign}$. More precisely, if $\tau_{ij} \in S_N$ is a transposition then $\tilde{\iota}(\tau_{ij})$ is a reflection.*

Proof. Since all transpositions are conjugate in S_N, and since the conjugate of a reflection is again a reflection, one may assume that $i = 1$ and $j = 2$. Now

$$(v_1, \ldots, v_{N-2}) = (b_1 + b_N + \langle \mathbf{1} \rangle, \ldots, b_{N-2} + b_N + \langle \mathbf{1} \rangle)$$

is a basis of $\tilde{V}$, such that $\tilde{\iota}(\tau_{12})$ interchanges v_1, v_2 and leaves all other basis vectors fixed. Hence $\tilde{\iota}(\tau_{12})$ fixes the hyperplane orthogonal to the vector $v_1 + v_2$, which is anisotropic, according to Remark 3.2.2. Hence $\tilde{\iota}(\tau_{12})$ is the reflection $\sigma_{v_1+v_2}$. $\quad\square$

Corollary 3.2.4. *Let $\pi \in S_N$. If $\text{sign}(\pi) = -1$ then $\tilde{\iota}(\pi)$ interchanges the two partitions of the neighbor graph of all self-dual isotropic subspaces of $(\tilde{V}, q)$. In particular the automorphism group of a self-dual generalized doubly-even code is always contained in the alternating group.*

In odd characteristic, the isometry $\iota(\tau_{ij})$ interchanges the basis vectors b_i and b_j and fixes all other basis vectors. Hence $\iota(\tau_{ij}) = \sigma_{b_i - b_j}$ is the reflection at the hyperplane orthogonal to $b_i - b_j$. An application of Corollary 3.1.12 yields

Corollary 3.2.5. *(see [41, Ch. 11]) Let $\mathbb{F}$ be a finite field of odd characteristic and let $\pi \in S_N$. If $\text{sign}(\pi) = -1$ then π interchanges the two partitions of the neighbor graph of all self-dual codes in $\mathbb{F}^N$. If $\text{sign}(\pi) = 1$ then both partitions are left invariant under π. In particular the automorphism group of a self-dual code is contained in the alternating group A_N.*

Remark 3.2.6. *Assume that $\mathbb{F}$ has odd characteristic. The* monomial group $\mathcal{M}_N$ *is the wreath product $\{1, -1\} \wr S_N$ of S_N with the subgroup of $\mathbb{F}^*$ generated by -1. There exists a natural embedding*

$$\mathcal{M}_N \hookrightarrow O(\mathbb{F}^n), \quad ((\lambda_1, \ldots, \lambda_n) \rtimes \pi) \mapsto (b_i \mapsto \lambda_i b_{\pi(i)})$$

for $\pi \in S_N$ and $\lambda_1, \ldots, \lambda_n \in \{1, -1\}$. The monomial automorphism group *of a code $C \leq \mathbb{F}^N$ is*

$$\text{MAut}(C) := \{\varphi \in \mathcal{M}_N \mid \varphi(C) = C\}.$$

If C is self-dual then it follows immediately from Theorem 3.1.10 and Remark 3.1.1 that $\det(\varphi) = 1$ for every $\varphi \in \text{MAut}(C)$.

In characteristic 2 we can prove the following theorem which characterizes the situation in which there exists a doubly-even self-dual G-invariant code. Apart from the theory developed in this chapter, the proof uses the theory of Witt groups (cf. Chapter 4.1) and a well-known result on the lengths of doubly-even self-dual codes.

Theorem 3.2.7. *Let $G \leq S_N$. There exists a self-dual generalized doubly-even code $C = C^\perp \leq \mathbb{F}^n$ with $G \leq \text{Aut}(C)$ if and only if the following three conditions are fulfilled:*

(a) $8 \mid N$, *or* $[\mathbb{F} : \mathbb{F}_2]$ *is even and* $4 \mid N$,

(b) *every self-dual composition factor of the* $\mathbb{F}G$*-module* $\mathbb{F}^N$ *occurs with even multiplicity,*

(c) $G \leq A_N$.

Proof. Condition (a) is equivalent with the existence of a self-dual doubly-even code in $\mathbb{F}^N$, as shown in [32] and also in Theorem 5.6.1. Condition (b) is equivalent with the existence of a self-dual G-invariant code, by Corollary 4.1.28. Hence if there exists a self-dual G-invariant code then conditions (a) and (b) are fulfilled, and by Corollary 3.2.5 condition (c) is fulfilled as well.

Conversely, assume that the conditions (a),(b) and (c) are satisfied. Then there exists a self-dual G-invariant code C. Assume that C is not doubly-even. The map
$$q|_C : \quad C \to \mathbb{F}, \quad c \mapsto q(c + \langle \mathbf{1} \rangle)$$
is additive since C is self-dual, a G-module homomorphism since $G \leq O(\tilde{V}, q)$, and surjective since $C/\langle \mathbf{1} \rangle$ is not isotropic. Hence $\ker(q|_C) =: C_0$ is a G-module, with $\dim(C/C_0) = 1$ and hence $C_0^\perp/C_0$ is a G-module of dimension 2. Moreover, the quadratic map
$$C_0^\perp/C_0 \to \mathbb{F}, \quad c + C_0 \mapsto q(c + \langle \mathbf{1} \rangle)$$
is well-defined and of Witt defect 0 since $\tilde{V}$ is of Witt defect 0 by condition (a) (cf. Remark 4.2.8). The two maximally isotropic subspaces of $C_0^\perp/C_0$ correspond to the vertices D and E of the neighbor graph of all self-dual isotropic codes in $(\tilde{V}, q)$ which intersect C in its subcode C_0. In particular the D and E are adjacent in the neighbor graph, and hence both left invariant under $\tilde{\iota}(G)$, since $G \leq A_N$ (cf. Corollary 3.2.5). Thus the full preimages of D and E under the epimorphism $\mathbb{F}^N \to \tilde{V}$, $v \mapsto v + \langle \mathbf{1} \rangle$ are doubly-even G-invariant self-dual codes. $\qquad \square$

Chapter 4

Witt groups

This chapter treats *linear codes*, i.e. subspaces of $\mathbb{F}^N$, where $\mathbb{F}$ is a finite field, as modules for a group algebra. Orthogonality is defined via the standard scalar product $\beta^{(1)} : \mathbb{F}^N \times \mathbb{F}^N$, or alternatively, if $\mathbb{F} = \mathbb{F}_{r^2}$ has r^2 elements, by means of the Hermitian scalar product

$$\beta^{(r)} : \mathbb{F}^N \times \mathbb{F}^N \to \mathbb{F}, \quad ((v_1, \ldots, v_N), (w_1, \ldots, w_N)) \mapsto \sum_{i=1}^N v_i w_i^r.$$

The *dual* of a linear code $C \le \mathbb{F}^N$ is

$$C^\perp = C^{\perp, \beta^{(\epsilon)}} = \{v \in \mathbb{F}^N \mid \beta^{(\epsilon)}(v, c) = 0 \text{ for all } c \in C\},$$

for $\epsilon \in \{1, r\}$. The code C is called *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$. The *orthogonal group* is

$$O = O(\mathbb{F}^N, \beta^{(\epsilon)}) := \{\psi \in \mathrm{Aut}(\mathbb{F}^N) \mid \beta^{(\epsilon)}(\psi(v), \psi(w)) = \beta^{(\epsilon)}(v, w) \text{ for all } v, w \in \mathbb{F}^N\}.$$

Clearly O acts on the set of all self-dual codes in $\mathbb{F}^N$. The action of the *monomial subgroup* $\mathcal{M}_N$ of O is of particular interest since it preserves the weight distribution of a code (cf. Section 5.1). The group $\mathcal{M}_N^{(\epsilon)}$ is the wreath product $U \wr S_N$, where $U = \{u \in \mathbb{F}^* \mid u^\epsilon u = 1\}$. In matrices,

$$\mathcal{M}_N^{(\epsilon)} = \{X \in \mathrm{GL}(\mathbb{F}, N) \mid X(X^\epsilon)^{\mathrm{tr}} = I_N\},$$

where the powers in X^ϵ are taken componentwise. We view $\mathcal{M}_N^{(\epsilon)}$ as a subgroup of O, via the natural embedding

$$\mathcal{M}_N^{(\epsilon)} \hookrightarrow O, \quad ((\lambda_1, \ldots, \lambda_N) \rtimes \pi) \mapsto (f_i \mapsto \lambda_i f_{\pi(i)}),$$

where $(f_1, \ldots, f_N)$ is the standard basis of $\mathbb{F}^N$. This chapter investigates the *monomial automorphism group*

$$\mathrm{MAut}(C) := \mathrm{Stab}_{\mathcal{M}_N^{(\epsilon)}}(C) = \{\zeta \in \mathcal{M}_N^{(\epsilon)} \mid \zeta(C) = C\}$$

of a self-dual code $C \leq \mathbb{F}^N$, by an inverse approach: Given a subgroup $G \leq \mathcal{M}_N^{(\epsilon)}$, we investigate whether there exists a G-invariant self-dual code $C \leq \mathbb{F}^N$. To this aim, we view $\mathbb{F}^N$ as a G-module, where G acts as a subgroup of $\mathcal{M}_N^{(\epsilon)}$. The connection between codes and modules is given by the following trivial but important remark.

Remark 4.0.8. *Let $C \leq \mathbb{F}^N$ be a code and let $G \leq \mathcal{M}_N^{(\epsilon)}$ be a subgroup. Then C is G-invariant if and only if C is a G-submodule of $\mathbb{F}^N$.*

The group algebra $A = \mathbb{F}\mathcal{M}_N^{(\epsilon)}$ carries an involution J given by

$$\sum_{M \in \mathcal{M}_N^{(\epsilon)}} f_M M \mapsto \sum_{M \in \mathcal{M}_N^{(\epsilon)}} f_M^\epsilon M^{-1}.$$

That $\mathcal{M}_N^{(\epsilon)}$ consists of isometries means that $\beta^{(\epsilon)}(v, wa) = \beta^{(\epsilon)}(va^J, w)$ for all $v, w \in \mathbb{F}^N$ and $a \in A$, i.e. the module $(\mathbb{F}^N, \beta^{(\epsilon)})$ is *equivariant* (cf. Definition 4.1.1). In Section 4.1 we view equivariant A-modules as elements of the *Witt group*, for a general finite algebra A with involution. The structure of this group allows in many cases, for instance if $\mathbb{F}$ has characteristic 2, to decide from the composition factors of the G-module $\mathbb{F}^N$ whether there exists a self-dual G-invariant code (cf. Theorem 4.1.27).

4.1 The Witt group of an algebra with involution

Let A be a finite algebra with unity over the finite field $\mathbb{F}$. Let J be an *involution* of A, i.e. a bijective additive mapping with $(ab)^J = b^J a^J$ and $(a^J)^J = a$ for all $a, b \in A$. Assume that $\mathbb{F}^J = \mathbb{F}$, where $\mathbb{F}$ is naturally embedded into A via $f \mapsto f \cdot 1$. The restriction of J to $\mathbb{F}$ is either the identity or has order 2. In the latter case $\mathbb{F} = \mathbb{F}_{r^2}$ has r^2 elements and $f^J = f^r$, for $f \in \mathbb{F}$. If J is the identity on $\mathbb{F}$ then it is said to be of the *first kind*, otherwise of the *second kind* (see for instance [37, Ch.8, Remark 7.2]).

Definition 4.1.1. *Let $\varepsilon \in \mathbb{F}^*$. An ε-equivariant* form on V (with respect to J) *is a biadditive mapping $\beta : V \times V \to \mathbb{F}$ such that*

$$\beta(va, w) = \beta(v, wa^J), \quad \beta(v, w) = \varepsilon\beta(w, v)^J \text{ and } \beta(v, w\lambda) = \beta(v, w)\lambda$$

for all $v, w \in V$, $a \in A$ and $\lambda \in \mathbb{F}$. The form β is called non-degenerate *if*

$$\alpha_\beta : V \to \mathrm{Hom}_\mathbb{F}(V, \mathbb{F}), \quad v \mapsto (w \mapsto \beta(w, v))$$

is an isomorphism. If β is non-degenerate then (V, β) is called ε-equivariant.

Note that the existence of an ε-equivariant module (V, β) implies that $\varepsilon\varepsilon^J = 1$ since

$$\beta(v, w) = \varepsilon\beta(w, v)^J = \varepsilon(\varepsilon\beta(v, w)^J)^J = \varepsilon\varepsilon^J\beta(v, w)$$

for all $v, w \in V$. We will sometimes omit the ε in the context of equivariant forms, if it is given by the context or if we do not refer to a specific value of ε. By $\mathfrak{M}(A, J, \varepsilon)$ we denote the set of all ε-equivariant A-modules.

Definition 4.1.2. *Let $(V, \beta) \in \mathfrak{M}(A, J, \varepsilon)$. The* orthogonal *of a submodule $C \leq V$ is*

$$C^{\perp} = \{v \in V \mid \beta(v, c) = 0 \, \text{for all } c \in C\},$$

which is again a submodule of V. If $C \subseteq C^{\perp}$ then C is called self-orthogonal, *and if $C = C^{\perp}$ then C is called a* self-dual code. *If C is self-orthogonal and there exists no self-orthogonal submodule of V which properly contains C then C is called* maximally self-orthogonal. *If the zero module is maximally self-orthogonal then V is called* anisotropic, *and if there exists a self-dual code in V then V is called* metabolic.

The equivariant A-modules form a semigroup with the *orthogonal sum* as multiplication, i.e.

$$(V, \beta) \perp (V', \beta') = (V \oplus V', \beta \perp \beta'),$$

where $(\beta \perp \beta')(v + v', w + w') = \beta(v, w) + \beta'(v', w')$ for $v, w, v', w' \in V$. Define a relation on $\mathfrak{M}(A, J, \varepsilon)$ by letting $(V, \beta) \sim (V', \beta')$ if and only if $(V, \beta) \perp (V', -\beta')$ is metabolic. In this section it is shown that $\sim$ is an equivalence relation (cf. Cor. 4.1.6, [37]), hence modulo this relation $\mathfrak{M}(A, J, \varepsilon)$ is a group.

Definition 4.1.3. *The* Witt group *$\mathcal{W}(A, J, \varepsilon)$ is formed by the $\sim$-equivalence classes $[(V, \beta)]$ of equivariant A-modules, with multiplication*

$$[(V, \beta)] \perp [(V', \beta')] = [(V, \beta) \perp (V', \beta')],$$

which is well-defined, due to the Cancellation Lemma 4.1.5. The class $[(V, \beta)]$ is also called the Witt Type *of (V, β).*

The following two Lemmata aim to show that $\sim$ is an equivalence relation.

Lemma 4.1.4. *Let $(V, \beta) \in \mathfrak{M}(A, J, \varepsilon)$ be metabolic and let M be a self-orthogonal submodule of V. Then there exists a self-dual code in V which contains M.*

Proof. Let C be a self-dual code in of V. Then $C \cap M^{\perp} + M$ has the desired properties since

$$(C \cap M^{\perp} + M)^{\perp} = (C + M) \cap M^{\perp} = C \cap M^{\perp} + M,$$

where the last equality holds due to the inclusion $M \subseteq M^{\perp}$. $\qquad\square$

Lemma 4.1.5. *[Cancellation Lemma] Let $(V, \beta), (V', \beta') \in \mathfrak{M}(A, J, \varepsilon)$ such that (V', β') is metabolic. Then (V, β) is metabolic if and only if $(V, \beta) \perp (V', \beta')$ is metabolic.*

Proof. Clearly if (V, β) is metabolic then so is $(V, \beta) \perp (V', \beta')$. Conversely, if $(V, \beta) \perp (V', \beta')$ is metabolic then so is

$$T := (V, \beta) \perp (V', \beta') \perp (V', -\beta')$$

since $(V', -\beta')$ is metabolic as well. Let $M := \{(0, v', v') \mid v' \in V'\} \leq T$, then $M \leq M^\perp$. Hence there exists a self-dual code C in T which contains M, according to Remark 4.1.4. Since $C \leq M^\perp$, the elements of C must be of the form (v, v', v') for some $v \in V$ and $v' \in V'$. Let $\pi : T \to V$ denote the projection onto the first component, then $\pi(C) = \pi(C)^\perp \leq V$ and hence (V, β) is metabolic. □

Corollary 4.1.6. *The relation $\sim$ is an equivalence relation.*

   Proof. Clearly the relation is symmetric and reflexive. For the transitivity, let

$$(V'', \beta'') \sim (V, \beta) \sim (V', \beta').$$

Then $(V'', \beta'') \perp (V, -\beta) \perp (V, \beta) \perp (V', -\beta')$ is metabolic. Since the summand $(V, -\beta) \perp (V, \beta)$ is metabolic as well, so is the module $(V'', \beta'') \perp (V', -\beta')$, by Lemma 4.1.5, and hence $(V'', \beta'') \sim (V', \beta')$. □

Remark 4.1.7. *Let $(V, \beta), (V', \beta') \in \mathfrak{M}(A, J, \varepsilon)$. An* isometry *is an A-module isomorphism $\varphi : V \to V'$ such that $\beta(v, w) = \beta'(\varphi(v), \varphi(w))$ for all $v, w \in V$. If there exists an isometry $V \to V'$ then V, V' are called* isometric, *and $(V, \beta) \sim (V', \beta')$.*

   In what follows a standard representative of a class in $\mathcal{W}(A, J, \varepsilon)$ will be constructed, which is always semisimple.

Lemma 4.1.8. *Let $(V, \beta) \in \mathfrak{M}(A, J, \varepsilon)$ and let M be a self-orthogonal submodule of V. The form*

$$\beta_M : M^\perp/M \times M^\perp/M \to \mathbb{F}, \quad (m' + M, m'' + M) \mapsto \beta(m', m'')$$

is again equivariant and non-degenerate, i.e. $(M^\perp/M, \beta_M) \in \mathfrak{M}(A, J, \varepsilon)$. Moreover, $(M^\perp/M, \beta_M) \sim (V, \beta)$, i.e. $[(V, \beta)] = [((M^\perp/M, \beta_M))] \in \mathcal{W}(A, J, \varepsilon)$. If M is maximally self-orthogonal then the module $(M^\perp/M, \beta_M)$ is anisotropic.

   Proof. The code

$$\{(m' + M, m') \mid m' \in M^\perp\} \leq (M^\perp/M, \beta_M) \perp (V, -\beta)$$

is self-dual, i.e. $(M^\perp/M, \beta_M) \sim (V, \beta)$. Moreover, if M is maximally self-orthogonal then $(M^\perp/M, \beta_M)$ is anisotropic, since any proper self-orthogonal submodule of $M^\perp/M$ would lift to a self-orthogonal submodule of V properly containing M, which contradicts our assumption. □

Theorem 4.1.9. *For every module $(V, \beta) \in \mathfrak{M}(A, J, \varepsilon)$ there exists an anisotropic representative of $[(V, \beta)]$, which is unique up to isometry.*

   Proof. The existence of an anisotropic representative follows from Lemma 4.1.8. For uniqueness, let $(V_i, \psi_i) \sim (V, \beta)$, $i = 1, 2$, be anisotropic equivariant A-modules. By the transitivity of $\sim$, the sum $M := (V_1, \psi_1) \perp (V_2, -\psi_2)$ is metabolic. Let N be a self-dual code in M. The projections $\pi_i : N \to V_i$ are injective since

$\ker(\pi_1)$ is an isotropic submodule of the anisotropic module V_2, and vice versa. Hence

$$|\pi_1(N)| \cdot |\pi_2(N)| = |N|^2 = |V_1| \cdot |V_2|$$

and hence $|\pi_i(N)| = |V_i|$, i.e. the π_i are isomorphisms. This yields an A-module isomorphism $\alpha := \pi_2 \circ \pi_1^{-1} : V_1 \to V_2$, which satisfies $N = \{(v_1, \alpha(v_1)) \mid v_1 \in V_1\}$. Hence

$$\psi_1(v_1, v_1') - \psi_2(\alpha(v_1, \alpha(v_1'))) = (\psi_1 \perp (-\psi_2))((v_1, \alpha(v_1)), (v_1', \alpha(v_1'))) = 0$$

for all $v_1, v_1' \in V_1$, i.e. α is an isometry, which proves the assertion. $\qquad\square$

Corollary 4.1.10. *Let $(V, \beta) \in \mathfrak{M}(A, J, \varepsilon)$ and let M be a maximally self-orthogonal submodule of V. Let $\beta_M : M^\perp/M \times M^\perp/M \to \mathbb{F}$ be as in Remark 4.3.3. Then the quotient $(M^\perp/M, \beta_M)$ is independent from the choice of M, up to isometry.*

The following Theorem is very useful in the determination of the isomorphism type of $\mathcal{W}(A, J, \varepsilon)$.

Theorem 4.1.11. *Every anisotropic module $(V, \beta) \in \mathfrak{M}(A, J, \varepsilon)$ is an orthogonal sum of simple equivariant A-modules.*

Proof. For every submodule M of V the submodule $M^\perp$ is a complement, since $M \cap M^\perp = \{0\}$ and $|M||M^\perp| = |V|$. This argument shows that V is the orthogonal sum of its simple summands. In particular, the restriction of β to a simple summand S induces a non-degenerate equivariant form on S. $\qquad\square$

Let $\mathfrak{S}_\varepsilon$ be the set of all simple A-modules carrying a non-degenerate ε-equivariant form. Then $\mathfrak{S}_\varepsilon$ is finite since A is finite, and by Theorem 4.1.11

$$\mathcal{W}(A, J, \varepsilon) \cong \times_{S \in \mathfrak{S}_\varepsilon} \langle [(S, \beta_S)] \mid \beta_S \text{ non-degenerate and } \varepsilon\text{-equivariant} \rangle.$$

To determine the structure of $\mathcal{W}(A, J, \varepsilon)$, the equivariant forms on $S \in \mathfrak{S}_\varepsilon$ will be investigated in Remark 4.1.13.

Definition 4.1.12. *Let $(V, \beta) \in \mathfrak{M}(A, J, \varepsilon)$. Then β induces an involution ad_β on $\mathrm{End}_A(V)$ via $\beta(v, w\alpha) = \beta(v\alpha^{\mathrm{ad}_\beta}, w)$ for $\alpha \in \mathrm{End}_A(V)$ and $v, w \in V$.*

Note that in general the endomorphism ad_β depends on the chosen form β. More precisely, β induces an A-module isomorphism

$$\alpha_\beta : V \to V^*, \ v \mapsto (w \mapsto \beta(v, w)),$$

where $V^* = \mathrm{Hom}_\mathbb{F}(V, \mathbb{F})$ is an A-module via $(\varphi, a)(v) := \varphi(va^J)$ for $\varphi \in V^*, a \in A$ and $v \in V$. If ψ is another non-degenerate equivariant form then $\alpha_\psi = \alpha_\beta \circ \vartheta$ for some $\vartheta \in \mathrm{End}_A(V)$, and hence

$$\psi(v, w) = \alpha_\psi(v)(w) = \alpha_\beta(v\vartheta)(w) = \beta(v\vartheta, w)$$

for all $v, w \in W$. In particular if V is simple then $\mathrm{End}_A(V)$ is a field and hence $\mathrm{ad}_\psi = \mathrm{ad}_\beta$. Hence if V is simple then the involution $\mathrm{ad}_V := \mathrm{ad}_\beta$ does not depend on β, and α^{ad_V} is called the *adjoint* of α.

Remark 4.1.13. *Let $S \in \mathfrak{S}_\varepsilon$ and let $\mathfrak{F} := \{\alpha \in \mathrm{End}_A(S) \mid \alpha^{\mathrm{ad}} = \alpha\}$ be the subfield of $\mathrm{End}_A(S)$ containing the self-adjoint endomorphisms of S. Then the unit group $\mathfrak{F}^*$ acts transitively on the set of all non-degenerate ε-equivariant forms on S, by*

$$\beta \cdot \vartheta : \ (s, s') \mapsto \beta(s\vartheta, s')$$

for a non-degenerate equivariant form β and $\vartheta \in \mathfrak{F}^*$.

Proof. Let β, ψ be two non-degenerate equivariant forms on S. As remarked above, there exists an automorphism ϑ of S such that $\psi(s, s') = \beta \cdot \vartheta(s, s')$. Since both β and ψ are ε-equivariant we have

$$\beta(s\vartheta, s') = \psi(s, s') = \varepsilon \left(\psi(s', s)\right)^J = \varepsilon \left(\beta(s'\vartheta, s)\right)^J = \beta(s, s'\vartheta) = \beta(s\vartheta^{\mathrm{ad}_S}, s')$$

for all $s, s' \in S$ and hence $\vartheta = \vartheta^{\mathrm{ad}_S} \in \mathfrak{F}^*$, and the claim follows. $\qquad\square$

Corollary 4.1.14. *Let $S \in \mathfrak{S}_\varepsilon$ and let $\mathfrak{F}$ be as in Remark 4.1.13. Define a group homomorphism*

$$\theta : \ \mathrm{End}_A(S)^* \to \mathfrak{F}^*, \ \ \alpha \mapsto \alpha\alpha^{\mathrm{ad}_S},$$

where $\mathrm{End}_A(S)^*$ and $\mathfrak{F}^*$ are the unit groups of the fields $\mathrm{End}_A(S)$ and $\mathfrak{F}$, respectively. Then S carries exactly $[\mathfrak{F}^* : \mathrm{Im}(\theta)]$ pairwise non-isometric non-degenerate equivariant forms.

Proof. Let β be a non-degenerate equivariant form on S. According to Remark 4.1.13, every other such form on S is of the form $\beta \cdot \vartheta$ for some $\vartheta \in \mathfrak{F}^*$. Now (S, β) and $(S, \beta \cdot \vartheta)$ are isometric if and only if there exists some $\gamma \in \mathrm{End}_A(S)$ with

$$\beta \cdot \vartheta(s, s') = \beta(s, s'\vartheta) = \beta(s\gamma, s'\gamma) = \beta(s, s'\gamma\gamma^{\mathrm{ad}_S})$$

for all $s, s' \in S$, i.e. if and only if $\vartheta = \theta(\gamma) \in \mathrm{Im}(\theta)$. Hence the stabilizer in $\mathfrak{F}^*$ of an isometry class of equivariant forms is $\mathrm{Im}(\theta)$ and the claim follows. $\qquad\square$

Definition 4.1.15. *For $S \in \mathfrak{S}_\varepsilon$, the involution ad_S on $\mathrm{End}_A(S)$ is either the identity or a field automorphism τ of order 2. Let $\mathfrak{S}_\varepsilon^{\mathrm{id}}, \mathfrak{S}_\varepsilon^\tau$ be the respective subsets of $\mathfrak{S}_\varepsilon$. Clearly $S \in \mathfrak{S}_\varepsilon^\tau$ if J is non-trivial on $\mathbb{F}$, since $f^J = f^{\mathrm{ad}_S}$, with respect to the natural embedding $\mathbb{F} \hookrightarrow \mathrm{End}_A(S)$.*

Corollary 4.1.16. *(i) Let $S \in \mathfrak{S}_\varepsilon^{\mathrm{id}}$. If $\mathbb{F}$ has characteristic 2 then S carries exactly one non-degenerate ε-equivariant form, up to isometry. If $\mathbb{F}$ has odd characteristic then S carries exactly two non-degenerate ε-equivariant forms, up to isometry.*

(ii) Let $S \in \mathfrak{S}_\varepsilon^\tau$, then S carries only one non-degenerate ε-equivariant form, up to isometry.

Proof. Let $S \in \mathfrak{S}_\varepsilon$ and let $\theta : \mathrm{End}_A(S) \to \mathrm{End}_A(S)$, $\alpha \mapsto \alpha\alpha^{\mathrm{ad}_S}$ as in Corollary 4.1.14 and $\mathfrak{F}$ as in Remark 4.1.13.

ad (i): Assume that $S \in \mathfrak{S}_\varepsilon^{\mathrm{id}}$, i.e. $\mathfrak{F} = \mathrm{End}_A(S)$ and $\theta(\alpha) = \alpha^2$, for $\alpha \in \mathrm{End}_A(S)$. If $\mathbb{F}$ has characteristic 2 then θ is a Galois automorphism of $\mathrm{End}_A(S)$. Hence according to Corollary 4.1.14, the module S carries exactly one non-degenerate equivariant form. If $\mathbb{F}$ has odd characteristic then

$$\mathrm{Im}(\theta) = (\mathrm{End}_A(S)^*)^2 \leq \mathrm{End}_A(S)^*$$

is a subgroup of index 2, hence the claim follows with Corollary 4.1.14.

ad (ii): For $S \in \mathfrak{S}_\varepsilon^\tau$, the map ad_S is the Galois automorphism of order 2 of $\mathrm{End}_A(S) = \mathbb{F}_{r^2}$, i.e. $\alpha^{\mathrm{ad}_S} = \alpha^r$, for $\alpha \in \mathrm{End}_A(S)$. Hence the subfield $\mathfrak{F}$ of $\mathrm{End}_A(S)$ containing the self-adjoint endomorphisms has r elements and the map $\theta : \mathbb{F}_{r^2}^* \to \mathbb{F}_r$, $\alpha \mapsto \alpha\alpha^{\mathrm{ad}_S} = \alpha^{r+1}$ is surjective, as one easily verifies. Hence the claim follows with Corollary 4.1.14.

$\square$

Theorem 4.1.17. *The groups* $\mathcal{W}(A, J, \varepsilon) \cong \oplus_{S \in \mathfrak{S}_\varepsilon} \mathcal{W}(L_S, \mathrm{ad}_S, 1)$ *are isomorphic, where* $L_S := \mathrm{End}_A(S)$ *is viewed as an algebra over itself.*

Proof. Every element $(V, \beta) \in \mathcal{W}(A, J, \varepsilon)$ has an anisotropic representative, which is an orthogonal sum of simple equivariant A-modules (cf. Theorems 4.1.9, 4.1.11), and the orthogonal summands are unique up to isometry. On every $S \in \mathfrak{S}_\varepsilon$ fix a non-degenerate ε-equivariant form β_S. Then the isometry classes of simple ε-equivariant modules are represented by

$$((S, \beta_S \cdot \alpha) \mid S \in \mathfrak{S}_\varepsilon, \ \alpha \in \mathfrak{F}^* / \mathrm{Im}(\theta)),$$

where $\mathfrak{F}, \theta$ are as in Corollary 4.1.14. Define a homomorphism

$$\mathcal{W}(A, J, \varepsilon) \to \oplus_{S \in \mathfrak{S}_\varepsilon} \mathcal{W}(L_S, \mathrm{ad}_S, 1), \quad [(S, \beta_S \cdot \alpha)] \mapsto [(L_S, (\alpha))],$$

where $(\alpha) : L_S \times L_S \to L_S$, $(\varphi, \varphi') \mapsto \alpha\varphi^{\mathrm{ad}_S}\varphi'$. This map is obviously injective, and surjective by Remark 4.1.13, which proves the assertion. $\square$

The following Proposition investigates the Witt groups on the right hand side of the above isomorphism.

Proposition 4.1.18. *Let L be a finite field with involution J and consider L as an algebra over itself. Let $\mathfrak{F} := \{l \in L \mid l^J = l\}$, and $\theta : L \to L$, $\alpha \mapsto \alpha\alpha^J$. On the module $V := L$ consider the equivariant form $(l) : (\alpha, \alpha') \mapsto l\alpha^J\alpha'$, for $l \in \mathfrak{F}^*$. In the Witt group $\mathcal{W}(L, J, 1)$, the element $[(V, (l))]$ has order 2 if $-1 \in \mathrm{Im}(\theta)$, and order 4 otherwise.*

Proof. Clearly the order n of $(V, (l))$ is even, since every self-dual code C in $\perp_{i=1}^n (V, (l))$ satisfies $n = 2\dim(C)$. Assume without loss of generality that $l = 1$. If $-1 = \alpha\alpha^J \in \mathrm{Im}(\theta)$ then $\langle(1, \alpha)\rangle$ is a self-dual code of $\perp_{i=1}^2 (V, (1))$ and hence $[(V, (1))]$ has order 2. On the other hand, a self-dual code in $\perp_{i=1}^2 (V, (1))$, provided that it exists, is generated by an element $(1, \alpha)$, where $\alpha\alpha^J = -1$ due to self-orthogonality. Hence if -1 is not in the image of θ then the order of $[(V, (1))]$

is at least 4. Moreover, the involution J must be the identity. Hence since the polynomial $x^2 + y^2 + 1$ has at least one nonzero root (α, α') over L, the code $\langle (1, 0, \alpha, \alpha'), (0, 1, -\alpha', \alpha) \rangle$ of $\perp_{i=1}^4 (V, (1))$ is self-dual, which shows the assertion. $\square$

Corollary 4.1.19. *Let $S \in \mathfrak{S}_\varepsilon$ and let β be a non-degenerate equivariant form on S. If $\mathbb{F}$ has characteristic 2 or if $S \in \mathfrak{S}_\varepsilon^\tau$ then $[(S, \beta)] \in \mathcal{W}(A, J, \varepsilon)$ has order 2. If $\mathbb{F}$ has odd characteristic and $S \in \mathfrak{S}_\varepsilon^{\mathrm{id}}$ then $[(S, \beta)]$ has order 2 if and only if $|\operatorname{End}_A(S)| \equiv_4 1$, and order 4 otherwise.*

    Proof. Let $\theta : \operatorname{End}_A(S)^* \to \operatorname{End}_A(S)^*$, $\alpha \mapsto \alpha\alpha^{\mathrm{ad}}$ be as in Corollary 4.1.14. By Theorem 4.1.17 and Proposition 4.1.18, the element $[(S, \beta)]$ has order 2 if $-1 \in \operatorname{Im}(\theta)$, and order 4 otherwise. Clearly if $\mathbb{F}$ has characteristic 2 then $-1 = 1 \in \operatorname{Im}(\theta)$. If $S \in \mathfrak{S}_\varepsilon^\tau$, i.e. if ad_S is not the identity then $\operatorname{End}_A(S)$ is the field with q^2 elements, and $\alpha^{\mathrm{ad}} = \alpha^q$, for $\alpha \in \operatorname{End}_A(S)$. Hence in this case the subfield of index 2 of $\operatorname{End}_A(S)$ lies in $\operatorname{Im}(\theta)$, and in particular $-1 \in \operatorname{Im}(\theta)$. Thus in this case $[(S, \beta)]$ has order 2 as well. If $S \in \mathfrak{S}_\varepsilon^{\mathrm{id}}$, i.e. if ad_S is the identity then $[(S, \beta)]$ has order 2 if and only if -1 is a square in $\operatorname{End}_A(S)$. The latter is equivalent with $|\operatorname{End}_A(S)| \equiv_4 1$, and hence the claim follows. $\square$

    Putting the results on the number of forms (cf. Lemma 4.1.16) and the orders of the simple equivariant modules (cf. Proposition 4.1.19) together, one obtains the following result on the structure of the Witt group $\mathcal{W}(A, J, \varepsilon)$.

Corollary 4.1.20. *Let $\mathfrak{S}_\varepsilon$ be a system of representatives for the isomorphism classes of simple equivariant A-modules, and let $(\mathfrak{S}_\varepsilon)^{\mathrm{id}}, (\mathfrak{S}_\varepsilon)^\tau$ be the subsets of $\mathfrak{S}_\varepsilon$ containing the simple modules S where $\operatorname{ad}_S = \operatorname{id}$, or $\operatorname{ad}_S \neq \operatorname{id}$, respectively (cf. Definition 4.1.15).*

(i) Assume that J is of the first kind. If $\mathbb{F}$ has characteristic 2 then

$$\mathcal{W}(A, J, \varepsilon) \cong \times_{S \in \mathfrak{S}_\varepsilon} C_2 .$$

If $\mathbb{F}$ has odd characteristic then let $d_S := |\operatorname{End}_A(S)|$, for $S \in \mathfrak{S}_\varepsilon$. Then

$$\mathcal{W}(A, J, \varepsilon) \cong \times_{S \in (\mathfrak{S}_\varepsilon)^{\mathrm{id}}, \, d_S \equiv_4 1}(C_2 \times C_2) \ \times_{S \in (\mathfrak{S}_\varepsilon)^{\mathrm{id}}, \, d_S \equiv_4 -1} C_4 \times_{S \in (\mathfrak{S}_\varepsilon)^\tau} C_2 .$$

(ii) If J is of the second kind then $\mathcal{W}(A, J, \varepsilon) \cong \times_{S \in \mathfrak{S}_\varepsilon} C_2$.

Definition 4.1.21. *The* dual *of an A-module V is $V^* = \operatorname{Hom}_\mathbb{F}(V, \mathbb{F})$, which is a right A-module via $fa(v) := f(va^J)$, for $f \in V^*$, $a \in A$ and $v \in V$. The module V is called* self-dual *if and only if $V \cong V^*$.*

    Note that this thesis uses two different notions of duality. A self-dual code (cf. Definition 4.1.2) is defined with respect to an equivariant form, i.e. using a distinguished basis, whereas the notion of a self-dual module is independent from the choice of a basis. Note that every equivariant A-module (V, φ) is a self-dual module since

$$\alpha_\varphi : V \to V^*, \quad v \mapsto (v' \mapsto \varphi(v', v))$$

is an isomorphism of right A-modules. Conversely, for the simple A-modules the following holds.

Remark 4.1.22. *Let S be a simple A-module and let $\varepsilon \in \mathbb{F}^*$ with $\varepsilon\varepsilon^J = 1$. If S is self-dual then S carries a non-degenerate ε-equivariant form or a non-degenerate $(-\varepsilon)$-equivariant form. In particular if $\mathbb{F}$ has characteristic 2 then S is self-dual if and only if S carries a non-degenerate ε-equivariant form.*

Proof. Let $\alpha : S \to \operatorname{Hom}_{\mathbb{F}}(S, \mathbb{F})$ be an isomorphism, then the biadditive form

$$\beta : S \times S \to \mathbb{F}, \quad (s, s') \mapsto \alpha(s)(s')$$

is non-degenerate and satisfies $\beta(sa, s') = \beta(s, s'a^J)$ and $\beta(s, s'\lambda) = \beta(s, s')\lambda$ for all $s, s' \in S$, $a \in A$ and all $\lambda \in \mathbb{F}$. Define another form

$$\beta' : S \times S \to \mathbb{F}, \quad (s, s') \mapsto \beta(s, s') - \varepsilon\beta(s', s)^J.$$

Then β' is $(-\varepsilon)$-equivariant, since

$$-\varepsilon\beta'(s', s)^J = -\varepsilon(\beta(s', s) - \varepsilon\beta(s, s')^J)^J = -\varepsilon\beta(s', s)^J + \beta(s, s') = \beta'(s, s')$$

for all $s, s' \in S$. The radical $\operatorname{rad}(\beta')$ is a submodule of S and hence either $\operatorname{rad}(\beta') = \{0\}$ or $\operatorname{rad}(\beta') = S$, since S is simple. In the first case, β' is non-degenerate and in the second case, β is ε-equivariant. $\square$

To understand Corollary 4.1.24, note that the involution ad_S on $\operatorname{End}_A(S)$ does not depend on ε, for a simple self-dual module S.

Remark 4.1.23. *Every self-dual simple A-module S defines an automorphism ad_S of $\operatorname{End}_A(S)$, such that $\beta(s, \alpha(s')) = \beta(\alpha^{\mathrm{ad}}(s), s')$ for all $s, s' \in S$, all $\varepsilon \in \mathbb{F}$ with $\varepsilon\varepsilon^J = 1$ and all ε-equivariant forms β.*

Corollary 4.1.24. *Let $\varepsilon \in \mathbb{F}^*$ with $\varepsilon\varepsilon^J = 1$ and let S be a simple self-dual A-module.*

(i) If $\mathbb{F}$ has characteristic 2 or if ad_S is not the identity then S carries both a non-degenerate ε-equivariant and $-\varepsilon$-equivariant form.

(ii) Assume that $\mathbb{F}$ has odd characteristic and that S carries both a non-degenerate ε-equivariant and a $-\varepsilon$-equivariant form. Then ad_S has order 2.

Proof. The claim of (i) is clear in characteristic 2. Assume that ad_S is not the identity, then there exists some element $\alpha \in \operatorname{End}_A(S)$ with $\alpha^{\mathrm{ad}_S} = -\alpha$. One easily verifies that for every ε-equivariant form β, the form $(s, s') \mapsto \beta(s, \alpha s')$ is $-\varepsilon$-equivariant.

Assume that S carries both a non-degenerate 1-equivariant form β and a -1-equivariant form $(v, w) \mapsto \beta(v, \alpha(w))$, for $\alpha \in \operatorname{End}_A(S)$. Then α satisfies $\alpha^{\mathrm{ad}_S} = -\alpha$, hence ad_S is an automorphism of order 2. $\square$

Remark 4.1.25. *Every self-dual simple A-module occurs in the equivariant A-module (V, β) with the same parity as in the anisotropic representative of (V, β).*

Proof. Let C be a maximally self-orthogonal submodule of V and let

$$C = M_k \geq M_{k-1} \geq \ldots \geq M_1 \geq M_0 = \{0\}$$

be a composition series. Then

$$C^\perp = M_k^\perp \leq M_{k-1}^\perp \leq \ldots \leq M_1^\perp \leq M_0 = V$$

is a composition series of $V/C^\perp$, since taking orthogonals yields an antiautomorphism of the submodule lattice of V. The composition factors satisfy

$$M_{i-1}^\perp/M_i^\perp \cong (M_i/M_{i-1})^*,$$

since, due to the non-degeneracy and equivariance of β, the map

$$M_{i-1}^\perp \to (M_i/M_{i-1})^*, \quad v \mapsto (m + M_{i-1} \mapsto \beta(v, m))$$

is an A-module epimorphism, with kernel $M_i^\perp$. Hence every self-dual simple A-module occurs in C with the same multiplicity as in $V/C^\perp$. Since the anisotropic representative of V is isomorphic to $C^\perp/C$, the claim follows. $\square$

Corollary 4.1.26. *If $(V, \beta) \in \mathfrak{M}(A, J, \varepsilon)$ is metabolic then every simple self-dual A-module occurs in V with even multiplicity.*

From Remark 4.1.25 together with Corollary 4.1.20 one obtains, in certain cases, the following characterization of metabolic equivariant modules.

Corollary 4.1.27. *Assume that J is of the second kind or that $\mathbb{F}$ has characteristic 2. Then $(V, \beta) \in \mathfrak{M}(A, J, \varepsilon)$ is metabolic if and only if every simple self-dual A-module occurs in V with even multiplicity.*

4.1.1 Self-dual codes in characteristic 2

Let $\mathbb{F}$ be a finite field of characteristic 2. In this section a *code* is a linear subspace of $\mathbb{F}^N$, and its *dual code* $C^\perp$ is defined through the standard scalar product β on $\mathbb{F}^N$. The code C is called *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$. The *automorphism group* of C is

$$\mathrm{Aut}(C) = \{\pi \in S_N \mid C\pi = C\},$$

where S_N is the symmetric group on N points, which acts naturally on $V = \mathbb{F}^N$ by coordinate permutations. This action induces an $\mathbb{F}G$-module structure on V, for every permutation group $G \leq S_N$, and a code C has $G \leq \mathrm{Aut}(C)$, i.e. C is *G-invariant*, if and only if it is an $\mathbb{F}G$-submodule of V. The group algebra $\mathbb{F}G$ carries a natural $\mathbb{F}$-linear involution J given by $g^J = g^{-1}$, for $g \in G$. The G-invariance of β, i.e. that $\beta(vg, wg) = \beta(v, w)$ for all $v, w \in V$ and $g \in G$, thus means that β is equivariant with respect to J, and hence (V, β) is an equivariant $\mathbb{F}G$-module in the sense of Definition 4.1.1.

In this section we investigate the existence of a G-invariant self-dual code in $\mathbb{F}^N$, for a given permutation group G, using the results developed for general equivariant modules. A first application is the following.

Corollary 4.1.28. *There exists a self-dual G-invariant code $C \leq \mathbb{F}^N$ if and only if every simple self-dual G-module occurs with even multiplicity in a composition series of the G-module $\mathbb{F}^N$.*

Example 4.1.29. *(i) The dihedral group D_N with $2N$ elements acts on the N vertices of a regular polygon. Identifying the vertices with the coordinates defines an $\mathbb{F}D_N$-module structure on $V = \mathbb{F}^N$. If N is even then D_N acts faithfully on the set $\mathcal{L}$ of lines in the polygon intersecting two vertices and the origin. Identification with the coordinates yields a G-invariant self-dual repetition code $C \leq \mathbb{F}^N$. This code is also a self-dual module, since $\mathcal{L}$ is an orthonormal basis of a G-invariant non-degenerate bilinear form on C. In particular every composition factor occurs in V with even multiplicity.*

(ii) Let A_N be the alternating group on N points, where $N \geq 4$ is even. Then the code $C_0 \leq \mathbb{F}_2^N$ generated by the all-ones vector $(1, \ldots, 1)$ is isomorphic to the trivial A_N-module, and

$$C_0^{\perp} = \{v \in \mathbb{F}_2^N \mid \mathrm{wt}(v) \text{ is even}\}$$

has codimension 1 in $\mathbb{F}_2^N$. The A_N-module $C_0^{\perp}/C_0$ is simple (cf. [20]) and hence must be self-dual, since C_0 and $C_0^{\perp}/C_0$ are the only composition factors of $\mathbb{F}_2^N$. In particular C_0 is maximally self-orthogonal with $A_N \leq \mathrm{Aut}(C)$.

(iii) Let C_N be the cyclic group on N points, where N is even. There exists a self-dual code $C \leq \mathbb{F}_2^N$ with $C_N \leq \mathrm{Aut}(C)$, which is seen as follows. As a C_N-module, $\mathbb{F}^N \cong \mathbb{F}C_N \cong \mathbb{F}[x]/(x^N - 1)$. Hence the submodules correspond to the divisors of $x^N - 1$, and the composition factors correspond to the quotients $\frac{p_i}{p_{i+1}}$ in a maximally refined divisor chain

$$p_1 \mid p_2 \mid \ldots \mid p_k = x^N - 1.$$

Since N is even, $x^N - 1$ is a square and hence every quotient occurs with even multiplicity. Hence every simple module occurs in $\mathbb{F}^N$ with even multiplicity, and the claim follows with Corollary 4.1.27.

Since the condition in Corollary 4.1.28 is not so easy to test, we give in Theorem 4.1.30 a sufficient group theoretic condition on a permutation group G to be contained in the automorphism group of a self-dual code $C \leq \mathbb{F}^N$. To this aim write

$$\{1, \ldots, N\} = B_1 \,\dot\cup\, \ldots \,\dot\cup\, B_s$$

as a disjoint union of G-orbits and let $H_i := \mathrm{Stab}_G(n_i)$ be the stabilizer in G of some element $n_i \in B_i$ $(i = 1, \ldots, s)$.

Theorem 4.1.30. *If for all $i = 1, \ldots, s$ the index of H_i in its normalizer $N_G(H_i)$ is even then there is a G-invariant self-dual code $C \leq \mathbb{F}^N$.*

Proof. Let $(f_1, \ldots, f_N)$ be the standard basis of $\mathbb{F}^N$ such that $\pi \in S_N$ maps f_j to $f_{j\pi}$ for all $j = 1, \ldots, N$. For $1 \leq i \leq s$ let $\eta_i \in N_G(H_i) - H_i$ such that $\eta_i^2 \in H_i$. Define

$$C := \langle (f_{n_i} + f_{n_i \eta_i})g : g \in G, 1 \leq i \leq s \rangle.$$

Then C is a G-invariant code in $\mathbb{F}^N$ and $C = \perp_{i=1}^s C_i$, where

$$C_i = \langle (f_{n_i} + f_{n_i \eta_i}) g : g \in G \rangle,$$

since the C_i have disjoint support. It suffices to show that each C_i is a self-dual code in $\mathbb{F}^{B_i}$. To see this let $N_i := \langle H_i, \eta_i \rangle$ and choose $S_i \subset G$ such that

$$G = \dot{\cup}_{s \in S_i} N_i s = \dot{\cup}_{s \in S_i} (H_i s \ \dot{\cup} \ H_i \eta_i s).$$

Then $B_i = n_i S_i \ \dot{\cup} \ n_i \eta_i S_i$ and $(f_{n_i s} + f_{n_i \eta_i s} : s \in S_i)$ is a basis of C_i consisting of $|S_i| = |B_i|/2$ pairwise orthogonal vectors of weight 2. $\square$

Remark 4.1.31. *The converse of Theorem 4.1.30 does not hold: Consider $G := GL_3(\mathbb{F}_2)$. Then the subgroup $H := N_G(S)$, for some $S \in Syl_7(G)$, has index 8 and satisfies $Core_G(H) := \cap_{g \in G} g^{-1} H g = \{1\}$. Hence H yields a transitive permutation representation $\Delta : G \to S_8$ with $G \cong \Delta(G)$ and $H \cong \text{Stab}_{\Delta(G)}(1)$. Observe that H is self-normalizing, i.e. $[N_G(H) : H] = 1$. But $\mathcal{C}_q^k(\Delta(G))$ contains a self-dual code, namely some permutation of the Hamming code of length 8 with generator matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

4.1.2   Self-dual codes in odd characteristic

Let $\mathbb{F}$ be a finite field of odd characteristic. As in the previous section, we consider $V = \mathbb{F}^N$ as a module over the group algebra $\mathbb{F}G$, with $\mathbb{F}$-linear involution J given by $g \mapsto g^{-1}$, for $g \in G$, where G is a permutation group on N points. Again, orthogonality is defined via the standard scalar product, and we investigate the existence of a self-dual G-invariant code via the composition factors of V. Since in odd characteristic, the image of (V, β) in the Witt group $\mathcal{W}(\mathbb{F}G, J)$ can in general not be determined only by the composition factors of V (cf. Theorem 4.1.20), this section provides only necessary group theoretic conditions on G to be contained in the automorphism group of a self-dual code, using Corollary 4.1.26.

Corollary 4.1.32. *Let $G \leq S_N$ be a permutation group such that $char(\mathbb{F}) \nmid |G|$. If the number of orbits of G is odd then there exists no G-invariant self-dual code in $\mathbb{F}^N$.*

   Proof.   The condition that $char(\mathbb{F}) \nmid |G|$ means that V is semisimple, by Maschke's Theorem. Hence the multiplicity of the trivial module in V equals the dimension of the fixed space

$$\mathcal{F}(V) := \{ v \in V \mid vg = v \text{ for all } g \in G \}.$$

Since a vector lies in $\mathcal{F}(V)$ precisely when its coefficients are constant on the orbits of G, the dimension of $\mathcal{F}(V)$ equals the number of orbits of G, which was assumed to be odd. Hence the trivial module occurs in V with odd multiplicity, and hence by Corollary 4.1.26 there exists no self-dual G-invariant code in V. $\square$

Corollary 4.1.33. *Let $G \leq S_N$ be a transitive permutation group. If the stabilizer order $|\operatorname{Stab}_G(\{1\})|$ of a point is odd then there exists no self-dual G-invariant code $C \leq \mathbb{F}^N$.*

Proof. Let S be a Sylow-2-subgroup of G, then S acts on $\mathbb{F}^N$ with orbits of length $|S|$, since $S \cap \operatorname{Stab}_G(\{i\})$ is trivial for every i, as the intersection of a 2-group and a group of odd order. Hence there are

$$t := \frac{N}{|S|} = \frac{|G|}{|\operatorname{Stab}_G(\{1\})| \cdot |S|}$$

orbits, where t is odd since S is a Sylow-2-subgroup. Hence by Corollary 4.1.33 there exists no S-invariant self-dual code in $\mathbb{F}^N$, and hence in particular there exists no G-invariant self-dual code in $\mathbb{F}^N$. $\qquad\square$

In the following Theorem we consider the case where the stabilizer in G of a point is trivial, i.e. $V = \mathbb{F}^{k|G|} \cong \oplus_{i=1}^{k} \mathbb{F}G$ is a k-multiple of the regular $\mathbb{F}G$-module, where k is the number of orbits of G. For $k = 1$, the G-invariant codes in V are right ideals in $\mathbb{F}G$. These codes are called *group ring codes* and have been considered by several authors (cf. [27, 2, 19]). The following Theorem gives, for an arbitrary group G, the minimum number k such that V contains a self-dual G-invariant code. Note that this number is the order of $[(\mathbb{F}G, \beta)]$ in the Witt group $\mathcal{W}(\mathbb{F}G, J, 1)$ and hence is also the greatest common divisor of all numbers k for which V contains a self-dual G-invariant code.

Theorem 4.1.34. *Let the G-module $V = \mathbb{F}^{k|G|} \cong \oplus_{i=1}^{k} \mathbb{F}G$ be as above. If $|\mathbb{F}| \equiv_4 1$ then V contains a self-dual G-invariant code if and only if k is even. If $|\mathbb{F}| \equiv_4 -1$ then V contains a self-dual G-invariant code if and only if k is a multiple of 4.*

Proof. Let S be a Sylow-2-subgroup of G, and consider V as a module over $\mathbb{F}S$. Since S acts on V with orbits of length $|S|$, there are $t = k[G : S]$ orbits, and as an $\mathbb{F}S$-module, $V \cong \perp_{i=1}^{t} \mathbb{F}S$. Assume that there exists a self-dual G-invariant code in V. This code is also S-invariant and hence the $\mathbb{F}S$-module V is metabolic. The trivial module occurs with multiplicity 1 in the semisimple module $\mathbb{F}S$, and is an orthogonal summand of $\mathbb{F}S$, generated by the all-ones vector in $\mathbb{F}S = \mathbb{F}^{|S|}$. Hence t is a multiple of the order of $(\mathbb{F}, \psi)$, where ψ is a non-degenerate symmetric bilinear form on $\mathbb{F}$. By Proposition 4.1.18, the order of $(\mathbb{F}, \psi)$ equals 2 if -1 is a square in $\mathbb{F}$, i.e. if $|\mathbb{F}| \equiv_4 1$, and 4 otherwise. Since $[G : S]$ is odd, this implies that k is even if $|\mathbb{F}| \equiv_4 1$, and that k is a multiple of 4 if $|\mathbb{F}| \equiv_4 -1$. Conversely, the exponent of the Witt group $\mathcal{W}(\mathbb{F}G, J)$ is 2 if $|\mathbb{F}| \equiv_4 1$, 4 if $|\mathbb{F}| \equiv_4 -1$, which shows the assertion. $\qquad\square$

As a corollary we obtain a part of a result by Willems in [27] on group ring codes.

Theorem 4.1.35 (Willems). *Let $\mathbb{F}$ be a finite field and G a finite group.*

(i) If $\mathbb{F}$ has characteristic 2 then $\mathbb{F}G$ contains a self-dual group code if and only if the order of G is even.

(ii) If $\mathbb{F}$ has odd characteristic then no self-dual group code is contained in $\mathbb{F}G$.

Proof. If $\mathbb{F}$ has characteristic 2 and the order of G is even then $\mathbb{F}G$ contains a self-dual code, according to Theorem 4.1.30. Conversely, if $\mathbb{F}G = \mathbb{F}^{|G|}$ contains a self-dual code C then $|G| = 2\dim(C)$ must be even. If $\mathbb{F}$ has odd characteristic then an application of Corollary 4.1.33, or of Theorem 4.1.34 shows that there exists no self-dual group code in $\mathbb{F}G$. $\qquad\square$

4.2   The Witt group of quadratic forms

Let $\mathbb{F}$ be a finite field of characteristic 2, and let G be a finite group. Let V be a right module for the group algebra $\mathbb{F}G$.

Definition 4.2.1. *A* quadratic form *on V is a map $q : V \to \mathbb{F}$ such that $q(v\lambda) = q(v)\lambda^2$ for all $v \in V$ and $\lambda \in \mathbb{F}$, and the* polar form

$$\lambda(q) : \quad V \times V \to \mathbb{F}, \quad (v, w) \mapsto q(v + w) - q(v) - q(w)$$

is bilinear. The form q is called non-degenerate *if its polar form is non-degenerate, i.e. if*

$$\alpha_q : \quad V \mapsto \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}), \quad v \mapsto (w \mapsto \lambda(q)(v, w))$$

is an isomorphism. The form q is called G-invariant if $q(v) = q(vg)$ for all $v \in V$ and $g \in G$. If q is G-invariant and non-degenerate then (V, q) is called a quadratic G-module. *A G-isometry between the quadratic G-modules (V, q) and (V', q') is an $\mathbb{F}G$-module isomorphism $\alpha : V \to V'$ such that $q(v) = q'(\alpha(v))$ for all $v \in V$.*

Remark 4.2.2. *The polarization β of a quadratic form is symmetric and satisfies $\beta(v, v) = 0$ for all $v \in V$. Bilinear forms over a field of characteristic 2 with these properties are called* symplectic. *The dimension of a vector space carrying a non-degenerate symplectic form is always even. In particular every quadratic G-module has even dimension.*

Remark 4.2.3. *A quadratic form q is non-degenerate if and only if the* radical

$$\mathrm{rad}(q) := \mathrm{rad}(\lambda(q)) = \{v \in V \mid \lambda(q)(v, w) = 0 \ \textit{for all } w \in V\}$$

is zero. Moreover, if q is G-invariant then so is $\lambda(q)$, i.e. $(V, \lambda(q)) \in \mathfrak{M}(\mathbb{F}G, J, 1)$ is J-equivariant in the sense of Definition 4.1.1, where J is the $\mathbb{F}$-linear involution on $\mathbb{F}G$ with $g^J = g^{-1}$, for $g \in G$. Hence if q is G-invariant and non-degenerate then the map α_q is an isomorphism of $\mathbb{F}G$-modules, where $\mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$ is a G-module via $fg(v) = f(vg^{-1})$, for $f \in \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$, $g \in G$ and $v \in V$. In particular every quadratic G-module is self-dual in the sense of Definition 4.1.21.

Remark 4.2.4. *In [38], methods of group cohomology are applied to investigate whether a G-invariant symplectic form is the polarization of a G-invariant quadratic form. In*

this context the additive groups of quadratic and symplectic forms on V, respectively, are denoted by $S^2(V^*)$ and $\Lambda^2(V^*)$. These spaces are G-modules, via

$$q[g](v) = q(gv) \quad and \quad \beta[g](v,w) = \beta(gv, gw)$$

for $q \in S^2(V^*)$, $\beta \in \Lambda^2(V^*)$, $v, w \in V$ and $g \in G$. The G-invariant forms $(S^2(V^*))^G$, $(\Lambda^2(V^*))^G$ are the G-fixed points in these modules. Every symplectic form on V is the polarization of a quadratic form, i.e. the map $\lambda : S^2(V^*) \to \Lambda^2(V^*)$ is surjective. (Note that yet, a G-invariant symplectic form is not necessarily the polarization of a G-invariant quadratic form.) The kernel of λ is $\mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}^{(2)})$, where $\mathbb{F}^{(2)}$ is the set $\mathbb{F}$ with scalar multiplication $\alpha \cdot f := \alpha^2 f$, for $\alpha \in \mathbb{F}$, $f \in \mathbb{F}^{(2)}$.

In odd characteristic there is a one-to-one correspondence between G-invariant quadratic forms and G-invariant symmetric forms, since $\lambda(\frac{1}{2}\{\beta\}) = \beta$ and $\{\frac{1}{2}\lambda(q)\} = q$ for every symmetric bilinear form β and every quadratic form q, and the maps λ and $\{\}$ preserve G-invariance. Hence in odd characteristic, the theory of Witt groups of quadratic G-invariant forms developed below is a theory of Witt groups of equivariant forms (cf. Section 4.1).

Definition 4.2.5. *A submodule $C \leq V$ is called* isotropic *if $q(c) = 0$ for all $c \in C$, and* maximally isotropic *if there exists no isotropic submodule of V which properly contains C. If the zero module $\{0\} \leq V$ is maximally isotropic then V is called* anisotropic. *If V contains an isotropic submodule C with $2 \dim(C) = \dim(V)$ then V is called* metabolic.

A theory of the Witt group of non-degenerate quadratic G-modules can be developed analogously to the theory of the Witt group of equivariant G-modules in Section 4.1. The *orthogonal sum* of two quadratic G-modules is

$$(V, q) \perp (V', q') = (V \oplus V', q \perp q'),$$

where $(q \perp q')((v, v')) = q(v) + q'(v')$. This defines a semigroup structure on the set of all quadratic G-modules. Define a relation $\sim$ by letting $(V, q) \sim (V', q')$ if and only if $(V, q) \perp (V', q')$ is metabolic. It can be shown with the methods in Section 4.1 that $\sim$ is an equivalence relation, and that modulo this relation, the quadratic G-modules form a group with the orthogonal sum as composition.

Definition 4.2.6. *The* quadratic Witt group *$\mathcal{W}_q(\mathbb{F}, G)$ consists of the $\sim$-equivalence classes $[(V, q)]$ of quadratic G-modules (V, q), with multiplication*

$$[(V, q)] \perp [(V', q')] = [(V, q) \perp (V', q')].$$

The class $[(V, q)]$ is also called the Witt Type *of (V, q).*

Since always $(V, q) \sim (V, q)$, the abelian group $\mathcal{W}_q(\mathbb{F}G)$ has exponent 2, hence is isomorphic to a direct product of cyclic groups of order 2. To give generators for the Witt group, we first investigate which results on the anisotropic representatives of the equivalence classes of equivariant modules (cf. Section 4.1) carry over. The following is straightforward.

Remark 4.2.7. *Every element of $\mathcal{W}_q(\mathbb{F}G)$ has an anisotropic representative, which is unique up to G-isometry.*

For the convenience of the reader we give a construction of the anisotropic representative, which is analogous to the one in Lemma 4.1.8.

Remark 4.2.8. *Let (V, q) be a quadratic G-module and let $C \leq V$ be an isotropic submodule. Then*
$$C \subseteq C^\perp = \{v \in V \mid \lambda(q)(v, c) = 0 \text{ for all } c \in C\},$$
that is, C is self-orthogonal with respect to the polar form $\lambda(q)$. The module $C^\perp/C$ carries again a non-degenerate G-invariant quadratic form
$$\tau_C(q): \ C^\perp/C \to \mathbb{F}, \ \ v + C \mapsto q(v).$$

The quadratic G-modules (V, q) and $(C^\perp/C, \tau_C(q))$ are of the same Witt type, and $(C^\perp/C, \tau_C(q))$ is anisotropic if and only if C is maximally isotropic. In particular the dimension of a maximally isotropic submodule C of V is independent from the choice of C and called the Witt index *of V. Similarly, $\dim(C^\perp/C)$ does not depend on C and is called the* Witt defect *of V.*

Remark 4.2.9. *Unlike in the case of equivariant forms, an anisotropic quadratic G-module is not necessarily semisimple. Assume for instance that G has a subgroup of index 2, i.e. there exists a group epimorphism $G \to C_2$. The space $U = \mathbb{F}^2$ is then a right G-module, where G acts as $\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right) \rangle \cong C_2$ with respect to a basis (b_1, b_2) of U, and the quadratic form f on U with $f(b_1) = f(b_2) = 0$ and $f(b_1 + b_2) = 1$ is non-degenerate and G-invariant. The only G-invariant proper subspace of U is generated by the anisotropic vector $b_1 + b_2$, and hence (U, f) is anisotropic, but not semisimple.*

Let $e \in \mathbb{F}G$ be the central primitive idempotent belonging to the trivial $\mathbb{F}G$-module. Every quadratic G-module (V, q) decomposes as $V = Ve \perp V(1 - e)$, which yields a decomposition
$$\mathcal{W}_q(\mathbb{F}G) = \mathcal{W}_q^0(\mathbb{F}G) \oplus \mathcal{W}_q^1(\mathbb{F}G)$$
into the subgroups $\mathcal{W}_q^0(\mathbb{F}G)$, generated by the quadratic G-modules on which e acts as the identity, and $\mathcal{W}_q^1(\mathbb{F}G)$, generated by the quadratic G-modules annihilated by e. The structure of an anisotropic quadratic G-module essentially depends on this decomposition.

Remark 4.2.10. *(see [38, Prop. 2.4]) If e acts as zero on V then every G-invariant symplectic form on V is the polarization of a G-invariant quadratic form, which is unique up to G-isometry. This yields an isomorphism*
$$\mathcal{W}_q^1(\mathbb{F}G) \to \mathcal{W}_s((1 - e)\mathbb{F}G, J, 1), \ \ [(V, q)] \mapsto (V, \lambda(q))$$
into the subgroup of $\mathcal{W}((1 - e)\mathbb{F}G, J, 1)$ formed by the symplectic J-equivariant forms, where J is the $\mathbb{F}$-linear involution mapping $g \mapsto g^{-1}$. In particular if (V, q) is anisotropic then it is semisimple, i.e. isomorphic to a direct sum of simple quadratic G-modules.

Proof. The proof is based on ideas in [38], using homological algebra, as follows. The short exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}^{(2)}) \to S^2(V^*) \xrightarrow{\lambda} \Lambda^2(V^*) \to 0$$

gives rise to an exact sequence

$$0 \to (\mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}^{(2)}))^G \to (S^2(V^*))^G \xrightarrow{\lambda} (\Lambda^2(V^*))^G \to H^1(G, \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}^{(2)}))$$

of cohomology groups. If V carries a G-invariant symplectic form then $V \cong \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}) \cong \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}^{(2)})$, and hence since e acts as zero on V, the group

$$H^1(G, \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}^{(2)})) \cong \mathrm{Ext}^1(\mathbb{F}, \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}^{(2)})) \cong \mathrm{Ext}^1(\mathbb{F}, V)$$

is trivial, and so is $(\mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F}^{(2)}))^G = \mathrm{Hom}_{\mathbb{F}G}(V, \mathbb{F}^{(2)}) \cong \mathrm{Hom}_{\mathbb{F}G}(V, \mathbb{F})$. Hence the above is in fact an exact sequence

$$0 \to (S^2(V^*))^G \xrightarrow{\lambda} (\Lambda^2(V^*))^G \to 0$$

and hence λ is an isomorphism. Moreover, if the quadratic G-module (V, q) is anisotropic then so is $(V, \lambda(q))$, since if C were a self-orthogonal submodule of V then q would be linear on C, i.e. $q \in \mathrm{Hom}_{\mathbb{F}G}(C, \mathbb{F}) = \{0\}$, contradicting the anisotropy of q. □

Remark 4.2.11. *Let (V, q) be an anisotropic quadratic G-module and let C be a maximally self-orthogonal submodule of V, with respect to $\lambda(q)$. Then either $C = \{0\}$, i.e. the equivariant module $(V, \lambda(q))$ is anisotropic and hence semisimple (cf. Theorem 4.1.11), or C is isomorphic to the trivial module.*

Proof. The map $C \to \mathbb{F}^{(2)}$, $c \mapsto q(c)$ is linear since C is self-orthogonal with respect to $\lambda(q)$, a G-module homomorphism since q is G-invariant, and bijective whenever C is not the zero module, due to the anisotropy of V. Since $\mathbb{F}^{(2)}$ is isomorphic to the trivial $\mathbb{F}G$-module, the claim follows. □

Proposition 4.2.12. *Let (V, q) be an anisotropic quadratic G-module. The trivial module $\mathbf{1}$ occurs in V with multiplicity 0 or 2. In the first case, V is semisimple and in the second case, V is semisimple if and only if $\mathbf{1}$ is a direct summand of V.*

Proof. Let C be a maximally self-orthogonal submodule of V. If $C = \{0\}$ then the claim follows with Remark 4.2.11. Otherwise $C \cong \mathbf{1}$, again by Remark 4.2.11. In this case $V/C^{\perp} \cong \mathbf{1}$, and $C^{\perp}/C$ is anisotropic with respect to $\lambda(q)$, hence in particular does not contain $\mathbf{1}$. Hence in this case $\mathbf{1}$ occurs in V with multiplicity 2. Assume that $C \cong \mathbf{1}$ is a direct summand in V. Then $C^{\perp}$ is a direct summand as well, due to the non-degeneracy of $\lambda(q)$, and hence there is a decomposition

$$V \cong C \oplus V/C \cong C \oplus C^{\perp}/C \oplus V/C^{\perp},$$

which proves the assertion. □

Definition 4.2.13. *A quadratic G-module (V, q) is called* indecomposable *if and only if there is no proper orthogonal decomposition of (V, q) into quadratic G-modules.*

Remark 4.2.14. *Let S be a simple G-module. If S carries a non-degenerate G-invariant quadratic form q then q is unique, up to G-isometry.*

Proof. Let $\tilde{q}$ be another non-degenerate G-invariant quadratic form on S. By Corollary 4.1.16, the polar forms $\lambda(q), \lambda(\tilde{q})$ are isometric, i.e. there exists some $\alpha \in \mathrm{End}_{\mathbb{F}G}(S)$ with $\lambda(q) = \lambda(\tilde{q})[\alpha]$. Hence $q - \tilde{q}[\alpha] \in \ker(\lambda)$ is linear on S, and hence either $q - \tilde{q}[\alpha] = 0$ or the map $S \to \mathbb{F}$, $s \mapsto q(s) - \tilde{q}[\alpha](s)$ is a G-module epimorphism. The latter does not hold since S is simple and of even dimension. Hence $q = \tilde{q}[\alpha]$, i.e. q and $\tilde{q}$ are isometric. $\square$

Lemma 4.2.15. *Let (V, q) be an anisotropic quadratic G-module. Then there exists an orthogonal decomposition of V into indecomposable quadratic G-modules, which are all indecomposable as $\mathbb{F}G$-modules and of which either all or all except for one are simple. This decomposition is unique up to G-isometry and permutation of the summands.*

Proof. If the trivial module does not occur in V then the claim follows with Proposition 4.2.12. Otherwise there exists an isotropic submodule C of V, which is isomorphic to the trivial module. If D is another submodule of V with these properties then the anisotropy of V enforces that $C \cap D^{\perp} = \{0\} = D \cap C^{\perp}$, and hence $V = (C \oplus D) \perp (C \oplus D)^{\perp}$ is an orthogonal decomposition of V. The summand $C \oplus D$ is indecomposable as a quadratic G-module, but not simple as a G-module, and the summand $(C \oplus D)^{\perp}$ does not contain the trivial module, by Proposition 4.2.12, hence is as in the previous case. It remains to consider the case when C is the unique nonzero self-orthogonal submodule of V. Every other simple submodule S of V has $S \cap S^{\perp} = \{0\}$, hence is an orthogonal summand of V. Hence V is the orthogonal sum of some simple quadratic G-modules and a quadratic G-module with a unique minimal submodule, which in particular is indecomposable, but not semisimple. For the uniqueness, note that this decomposition is unique up to permutation and $\mathbb{F}G$-module isomorphism, due to the Krull-Schmidt Theorem, and the uniqueness up to G-isometry follows from Remark 4.2.14 together with Witt's Theorem on the extension of isometries. $\square$

Remark 4.2.16. *Let (V, q) be an anisotropic indecomposable quadratic G-module. Then one of the following holds:*

(i) *V is simple,*

(ii) *The group G acts trivially on V, and (V, q) has Witt Type $[(\mathbb{F}^2, N)]$, where N is the Norm form, i.e. if $\mathbb{F} = \mathbb{F}_q$ then $q : \mathbb{F}^2 \cong \mathbb{F}_{q^2} \to \mathbb{F}$, $x \mapsto x^{q+1}$,*

(iii) *V contains a unique minimal submodule C, which is isomorphic to the trivial module, and the quotient $C^{\perp}/C$ is a direct sum of simple G-modules with a non-trivial first cohomology group, which carry a non-degenerate G-invariant symplectic form, but no non-degenerate G-invariant quadratic form.*

Proof. Except for the description of the situation (iii), everything has been done in Lemma 4.2.15. Assume that V has a unique minimal submodule C, which is isomorphic to the trivial module. The quotient $C^\perp/C$ is then anisotropic with respect to $\lambda(q)$ and hence semisimple. Moreover, the extension

$$C \to C^\perp \to C^\perp/C$$

does not split since C is the unique minimal submodule of V. Hence all the summands S of $C^\perp/C$ have a non-trivial first cohomology group. Now let $U := S + C$, and consider the commutative diagram

$$\begin{array}{ccc} \{q \in S^2(U^*)^G \mid C \leq \mathrm{rad}(q)\} & \xrightarrow{\lambda} & \{\beta \in \Lambda^2(U^*)^G \mid C \leq \mathrm{rad}(\beta)\} \\ \tau_C \uparrow & & \downarrow \iota_C \\ S^2(S^*)^G & \xrightarrow{\lambda} & \Lambda^2(S^*)^G, \end{array}$$

where τ_C is as in Remark 4.2.8, and $\iota_C(\beta)(v + C, w + C) = \beta(v, w)$ for all $v, w \in U$. Assume that S carries a non-degenerate G-invariant quadratic form f, then by Corollary 4.1.16 we may assume that $\lambda(f) = \iota_C(\lambda(q'))$. Since the vertical arrows in the above diagram are bijections, this implies that $\lambda(\tau_C(f)) = \lambda(q')$. Hence $\tau_C(f) - q'$ is linear on U, and C lies in the kernel of this homomorphism. But $\tau_C(f)(C) = \{0\}$, whereas C is anisotropic with respect to q', a contradiction. Hence there exists no non-degenerate G-invariant quadratic form on S. $\qquad\square$

Example 4.2.17. *If the group G is trivial then $\mathcal{W}_q(\mathbb{F}) = \mathcal{W}_q(\mathbb{F}, G)$ is the classical Witt group of quadratic forms over $\mathbb{F}$. This group is cyclic of order 2, since every anisotropic quadratic G-module has Witt Type $[(\mathbb{F}^2, N)]$ (cf. Remark 4.2.16), and this element has order 2.*

Remark 4.2.18. *(cf. Remark 4.1.25) Every simple self-dual G-module occurs in the quadratic G-module (V, q) with the same parity as in the anisotropic representative of (V, q).*

If the quadratic form q is G-invariant then G is naturally embedded into the orthogonal group $O(V, q)$. In this context one may consider the Dickson invariant of an element of G (cf. Definition 3.1.8), which yields the following generalization of Theorem 3.2.7.

Theorem 4.2.19. *A quadratic G-module (V, q) is metabolic if and only if the following three conditions are fulfilled:*

(a) As a quadratic vector space, (V, q) has Witt defect 0,

(b) every simple self-dual G-module occurs in V with even multiplicity,

(c) G lies in the kernel of the Dickson invariant.

Proof. Assume that (V, q) is metabolic. Then clearly condition (a) is fulfilled, and it follows from the fact that $(V, \lambda(q))$ is metabolic together with Theorem 4.1.27 that condition (b) is also fulfilled. Moreover, there exists a G-invariant isotropic subspace C of V, i.e. $\dim(C/C \cap Cg) = 0$ and hence condition (c) is satisfied as well, by Corollary 3.1.12.

Conversely, assume that all three conditions are satisfied, and let (V', q') be the anisotropic representative of (V, q) in the Witt group $\mathcal{W}_q(\mathbb{F}G)$. If (V', q') is the orthogonal sum of simple equivariant A-modules then every summand occurs with multiplicity 2, by condition (b) and Remark 4.2.18. Due to Remark 4.2.14, in this case (V', q') is zero, i.e. (V, q) is metabolic. Otherwise by Lemma 4.2.15, $V' = V_1' \perp V_2'$ is the orthogonal sum of an indecomposable quadratic G-module V_1' which is not semisimple and a quadratic G-module V_2', which is itself the orthogonal sum of simple quadratic G-modules. By Remark 4.2.16, every simple module which occurs in V_1' does not occur in V_2', and vice versa. Hence due to condition (b), V_2' is zero and either (V', q') is zero or it is isometric to the space (U, f) given in Remark 4.2.9. In the latter case there exists a G-invariant isotropic subspace C of V with $(C^\perp/C, \iota_C(q)) \cong (U, f)$. Again by Remark 4.2.9 there exists a nonzero vector $u \in C^\perp - C$ such that the vector space $E := \langle C, c \rangle$ is isotropic of codimension 2, but $\dim(E/E \cap Eg) = 1$ for some $g \in G$ and hence $D(g) = -1$, contradicting condition (c). Hence (V, q) is metabolic. $\qquad\square$

4.3   The Witt group of a form ring

Let $\mathcal{R} = (R, M, \psi, \Phi)$ be a form ring with associated involution J. Recall that throughout this thesis, the ring R is assumed to be finite. A finite representation of R is given by a finite R-module V, which carries biadditive as well as quadratic forms (cf. Definition 2.1.6). A subspace of V is called isotropic if it is both self-orthogonal with respect to the biadditive forms and isotropic with respect to the quadratic forms (cf. Definition 2.1.17). This notion of isotropy gives rise to the notion of the *Witt group* of a form ring (cf. Definition 4.3.2), for which a theory is developed analogously to the theory for the Witt group of equivariant or quadratic forms (see also [33, Ch. 4]).

The biadditive and quadratic forms in a representation are mapped to each other by the structure maps

$$\lambda: \ \mathrm{Quad}(V, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Bil}(V, \mathbb{Q}/\mathbb{Z}), \ \ q \mapsto ((v, w) \mapsto q(v + w) - q(v) - q(w)),$$

$$\{\,\}: \ \mathrm{Bil}(V, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Quad}(V, \mathbb{Q}/\mathbb{Z}), \ \ \psi \mapsto (v \mapsto \psi(v, v)).$$

If the map $\{\,\}$ is surjective then isotropy is equivalent with self-orthogonality with respect to the biadditive forms. Conversely, if the map λ is surjective then isotropy is defined only through the quadratic forms. It will be shown in Lemma 4.3.6 that if $\mathcal{R}$ is a form ring over a finite field and λ is injective then one of the above structure maps is surjective, and the Witt group of $\mathcal{R}$ is isomorphic to a Witt group of equivariant or quadratic forms, which have been investigated in the preceding two sections.

For general finite rings, it is shown that $\mathcal{W}(R)$ is finite. This shows in particular that if T is a finite representation of $\mathcal{R}$ then there exists some minimal finite length N such that there exists a self-dual Type T code of length N, and every length for which there exists a self-dual Type T code is a multiple of N. Moreover, the finiteness of $\mathcal{W}(\mathcal{R})$ provides a proof of finiteness for the Clifford-Weil group $\mathcal{C}(T)$ in the next chapter.

Definition 4.3.1. *The orthogonal sum (cf. Definition 2.1.16) defines a semigroup structure on the set $\mathcal{T}(\mathcal{R})$ of all finite representations of $\mathcal{R}$. An element $T = (V, \rho_M, \rho_\Phi, \beta) \in \mathcal{T}(\mathcal{R})$ is called* metabolic *if there exists a self-dual Type T code in V. Define a relation on $\mathcal{T}(\mathcal{R})$ by letting $T \sim T'$ if and only if $T \perp -T'$ is metabolic.*

With the same methods as in the case of equivariant forms, one verifies that $\sim$ is an equivalence relation and hence modulo this relation, the set $\mathcal{T}(\mathcal{R})$ is a group.

Definition 4.3.2. *The* Witt group *$\mathcal{W}(\mathcal{R})$ contains the $\sim$-equivalence classes $[T]$ of finite representations $T \in \mathcal{T}(\mathcal{R})$, with multiplication*

$$[T] \perp [T'] = [T \perp T'].$$

The equivalence class $[T]$ is also called the Witt Type *of T.*

In analogy with Lemma 4.1.8 we construct a representative of $[T]$, which is always *anisotropic*, i.e. contains no nonzero isotropic code.

Remark 4.3.3. *Every Type T code C in V induces a well-defined* quotient representation

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

with structure maps

$$\rho_M/C : M \to \mathrm{Bil}(C^\perp/C, \mathbb{Q}/\mathbb{Z}), \quad m \mapsto ((v + C, w + C) \mapsto \rho_M(m)(v, w)),$$

$$\rho_\Phi/C : \Phi \to \mathrm{Quad}(C^\perp/C, \mathbb{Q}/\mathbb{Z}), \quad \phi \mapsto (v + C \mapsto \rho_\Phi(\phi)(v)),$$

$$\beta/C := (\rho_M/C)(\psi(1)).$$

Then $[T] = [T/C]$ in the Witt group $\mathcal{W}(\mathcal{R})$, and T/C is anisotropic if and only if C is maximally Type T, i.e. there exists no Type T code which properly contains C.

Proof. That T/C is well-defined follows immediately from the isotropy of the code C. Since

$$\{(c' + C, c') \mid c' \in C^\perp\} \subseteq C^\perp/C \oplus V$$

is a self-dual Type $(T/C \perp -T)$ code, the elements $[T/C] = [T]$. Moreover, the nonzero Type T/C codes correspond to the Type T codes which properly contain C, hence T/C is anisotropic if and only if C is maximally Type T. $\qquad\square$

In analogy with Theorem 4.1.9, one may show that

Theorem 4.3.4. *Every element of $\mathcal{W}(\mathcal{R})$ has an anisotropic representative, which is unique, up to form isometry.*

In the rest of this section the following theorem is proven, which claims that up to equivalence, the form ring $\mathcal{R}$ has only finitely many representations.

Theorem 4.3.5. $\mathcal{W}(\mathcal{R})$ *is a finite group.*

Theorem 4.3.5 will first be proven for form rings over finite fields, which yields the claim of the theorem for form rings over matrix rings over fields (cf. Theorem 4.3.17), and finally for general finite rings.

Lemma 4.3.6. *If $\mathcal{R}$ is a form ring over a finite field $\mathbb{F}$ such that the associated map λ is injective then $\mathcal{W}(\mathcal{R})$ is a finite group. More precisely, $\mathcal{W}(\mathcal{R})$ is isomorphic to a Witt group of equivariant forms in the sense of Section 4.1, or isomorphic to a Witt group of quadratic forms in the sense of Example 4.2.17.*

Proof. Let $\mathcal{R} = (\mathbb{F}, M = \mathbb{F}, \psi, \Phi)$. If $\Phi = \{0\}$ then the map $\{\ \}$ is surjective, and for a representation $T = (V, \rho_M, \rho_\Phi, \beta)$, isotropy of subspaces is equivalent with self-orthogonality with respect to β. Moreover, in this case

$$\beta(v, fv) = \{\rho_M(\psi(f))\}(v) = \rho_\Phi(\{\psi(f)\})(v) = 0$$

for all $f \in \mathbb{F}$ and all $v \in V$ and hence in this case $\mathcal{R}$ has no nonzero anisotropic representations, i.e. $\mathcal{W}(\mathcal{R})$ is trivial. If $\mathbb{F}$ has odd characteristic then, too, $\{\ \}$ is surjective, which is seen as follows. The associated involution J is a field automorphism of order 1 or 2 of $\mathbb{F}$, since $f^{J^2} = \varepsilon^J f^{J^2} \varepsilon = f$ for all $f \in \mathbb{F}$ (cf. Lemma 2.1.11). If $J : \mathbb{F} = \mathbb{F}_{r^2} \to \mathbb{F}$, $f \mapsto f^r$ has order 2 then the map

$$\theta : \ \mathbb{F} \to \{y \in \mathbb{F} \mid y^J = y\}, \ \ x \mapsto x^J x$$

is surjective, and $\varepsilon = \alpha^{r-1}$, for some $\alpha \in \mathbb{F}$. Since rescaling of $\mathcal{R}$ (cf. Definition 2.1.14) leaves the set $\mathcal{T}(\mathcal{R})$ invariant, we may assume that $\varepsilon = 1$, after rescaling with α^{-1}. Likewise, if J is the identity then ε satisfies $\varepsilon^2 = 1$ and hence $\varepsilon \in \{1, -1\}$. The assumption that $\varepsilon = -1$ yields the contradiction

$$\lambda(\phi) = \tau(\lambda(\phi)) = \tau(\psi(\psi^{-1}(\lambda(\phi)))) = \psi(-\psi^{-1}(\lambda(\phi))) = -\lambda(\phi).$$

Hence we may assume that $\varepsilon = 1$ if $\mathbb{F}$ has odd characteristic. Now assume that J has order 2. Since $\lambda(\{\lambda(\phi')\}) = \lambda(2\phi')$ and λ is injective, $\{\lambda(\phi')\} = 2\phi'$ for all $\phi' \in \Phi$. Hence if $f \in \mathbb{F}$ with $\theta(f) = f^r f = 2^{-1}$ then

$$\{\lambda(\phi'[f])\} = \{2^{-1}\lambda(\phi')\} = \phi',$$

which shows the surjectivity of $\{\ \}$ in this case. If J is the identity then $\tau(\psi(f)) = \tau(\psi(f^J)) = \tau(\psi(f))$ for all $f \in \mathbb{F}$, i.e. τ is the identity on M. This implies $\lambda(\{m\}) = m + \tau(m) = 2m$ for all $m \in M$, i.e. here $\{\ \}$ is surjective, too. Hence in either of the two cases, ρ_Φ is determined by ρ_M, which itself is determined by β. Hence T is uniquely determined by (V, β), and isotropy of subspaces of V is equivalent with self-orthogonality with respect to β. The form β takes values in $\frac{1}{p}\mathbb{Z}/\mathbb{Z} \cong \mathbb{F}_p$, where p is the characteristic of $\mathbb{F}$, and β is $\mathbb{F}_p$-linear since it is biadditive. Since the prime field $\mathbb{F}_p$ is fixed by the automorphism J, the pair (V, β) may

be viewed as an equivariant $\mathbb{F}$-module, where $\mathbb{F}$ is viewed as an $\mathbb{F}_p$-algebra. This yields a group isomorphism

$$\mathcal{W}(\mathcal{R}) \to \mathcal{W}(\mathbb{F}, J, 1), \quad [(V, \rho_M, \rho_\Phi, \beta)] \mapsto [(V, \beta)]$$

into the finite Witt group of equivariant forms over $\mathbb{F}$, which is known to be finite (cf. Corollary 4.1.20). Hence the assumption follows in the case where $\mathbb{F}$ has odd characteristic. Now assume that $\mathbb{F}$ has characteristic 2, and that $\Phi \neq \{0\}$. Then T is uniquely determined by $\rho_\phi(\phi)$, for any nonzero element $\phi \in \Phi$, which is seen as follows. Since

$$\beta(v, w) = \rho_M(\lambda(\phi))(v, (\psi^{-1}(\lambda(\phi)))^{-1} w) = \lambda(\rho_\Phi(\phi))(v, (\psi^{-1}(\lambda(\phi)))^{-1} w)$$

for all $v, w \in V$, the map ρ_M is determined by $\rho_\Phi(\phi)$. Assume that J has order 2, then, as in odd characteristic, we may assume that $\varepsilon = 1$ after rescaling. Moreover, the map θ from above is surjective to the subfield of index 2 of $\mathbb{F}$, and hence

$$\mathrm{Im}(\lambda) \subseteq \{m \in M \mid \tau(m) = m\} = \{\psi(f) \mid f \in \mathbb{F}, \ f^r = f\} = \psi(\mathrm{Im}(\theta)),$$

i.e. $|\Phi| = |\mathrm{Im}(\lambda)| \leq |\mathrm{Im}(\theta)|$. On the other hand,

$$\psi^{-1}(\lambda(\phi[f])) = f^J \psi^{-1}(\lambda(\phi)) f = \theta(f) \psi^{-1}(\lambda(\phi)) \tag{4.1}$$

for every $f \in \mathbb{F}$, i.e. $|\mathrm{Im}(\theta)| \leq |\phi[\mathbb{F}]|$, and hence there is a chain

$$|\mathrm{Im}(\theta)| \leq |\phi[\mathbb{F}]| \leq |\Phi| \leq |\mathrm{Im}(\theta)|,$$

in which equality holds. In particular $\phi[\mathbb{F}] = \Phi$. Moreover,

$$\lambda(\{\psi(f)\}) = \psi(f) + \tau(\psi(f)) = \psi(f + f^r) = \psi(\mathrm{Trace}_{\mathbb{F}/\mathbb{F}_r}(f))$$

and hence $|\mathrm{Im}(\{\ \})| \geq |\mathrm{Im}(\mathrm{Trace}_{\mathbb{F}/\mathbb{F}_r})| = r$. On the other hand,

$$|\mathrm{Im}((\{\ \}))| \leq |\Phi| = |\mathrm{Im}(\theta)| = r$$

and hence $|\mathrm{Im}(\{\ \})| = r = |\Phi|$, i.e. $\{\ \}$ is surjective. Hence again $\mathcal{W}(\mathcal{R})$ is isomorphic to a Witt group of equivariant forms, of the $\mathbb{F}_2$-algebra $\mathbb{F}$, and hence $\mathcal{W}(\mathcal{R})$ is cyclic of order 2.

It remains to consider the case where $\mathbb{F}$ has characteristic 2 and J is the identity. Equation (4.1) shows that $|\Phi| = |\phi[\mathbb{F}]| = |\mathbb{F}| = |M|$, i.e. in this case λ is bijective and, again, $\phi[\mathbb{F}] = \Phi$. Hence T is uniquely determined by the pair $(V, \rho_\Phi(\phi))$, and isotropy of subspaces is equivalent with isotropy with respect to $\rho_\Phi(\phi)$. Moreover, $\varepsilon^2 = 1$ and hence $\varepsilon = 1$, and hence τ is the identity on M, as seen in the case where $\mathbb{F}$ has odd characteristic. This implies $\lambda(\{m\}) = m + \tau(m) = m + m = 0$ for all $m \in M$ and hence $\{M\} = \{0\}$, due to the injectivity of λ. This yields

$$\rho_M(\psi(f))(v, v) = \{\rho_M(\psi(f))\}(v) = \rho_\Phi(\{\psi(f)\})(v) = 0$$

for all $v \in V$ and $f \in \mathbb{F}$. Hence $\rho_\Phi(\phi)$ takes values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z} \cong \mathbb{F}_2$, since

$$2\rho_\Phi(\phi)(v) = \rho_\Phi(\phi)(v) + \rho_\Phi(\phi)(v) = \rho_\Phi(\phi)(v + v) - \lambda(\rho_\Phi(\phi))(v, v) = 0$$

for all $v \in V$. Hence $(V, \rho_\Phi(\phi))$ is a quadratic vector space over $\mathbb{F}_2$. This yields a group monomorphism

$$\mathcal{W}(\mathcal{R}) \to \mathcal{W}_q(\mathbb{F}_2), \quad [(V, \rho_M, \rho_\Phi, \beta)] \mapsto [(V, \rho_\Phi(\phi))]$$

into the Witt group of quadratic forms over $\mathbb{F}_2$. Note that this map is well-defined since the quadratic spaces (V, ϕ) and $(V, \phi' = \phi[f])$ are isometric whenever $\phi' \in \Phi$ is nonzero. Now the quadratic vector space $(\mathbb{F}_{r^2}, N)$ over $\mathbb{F}_2$, with $N(f) = \mathrm{Trace}_{\mathbb{F}_r/\mathbb{F}_2}(x^{r+1})$ for all $f \in \mathbb{F}_{r^2}$, induces a nonzero anisotropic representation $(V, \rho_M, \rho_\Phi, \lambda(q))$ of $\mathcal{R}$, where ρ_M is determined by $\lambda(q)$ and ρ_Φ is given by the condition $\rho_\Phi(\lambda^{-1}(\psi(1))) = q$. Since $\mathcal{W}_q(\mathbb{F}_2)$ is cyclic of order 2, this implies the surjectivity of the above monomorphism. Hence if $\mathbb{F}$ has characteristic 2 and J is the identity then $\mathcal{W}(\mathcal{R})$ is isomorphic to the Witt group of quadratic forms over $\mathbb{F}_2$. $\qquad\square$

In order to generalize Lemma 4.3.6 to arbitrary form rings over finite fields, we change to a quotient form ring $\mathcal{R}/\mathcal{I}_\lambda$, to which Lemma 4.3.6 applies. Lemma 4.3.12 states that $\mathcal{W}(\mathcal{R}/\mathcal{I}_\lambda)$ has finite index in $\mathcal{W}(\mathcal{R})$.

Definition 4.3.7. *A form ideal in $\mathcal{R}$ is a pair $\mathcal{I} = (I, \Gamma)$, where I is an ideal in R and Γ is a submodule of Φ with $\{\psi(I)\} + \Phi[I] \subseteq \Gamma \subseteq \Phi$ and $\lambda(\Gamma) \subseteq \psi(I)$.*

Remark 4.3.8. *Let I be an ideal in R with $I^J = I$. Then $\mathcal{I}_I := (I, \lambda^{-1}(\psi(I)))$ is a form ideal in $\mathcal{R}$. In particular $\mathcal{I}_\lambda := (0, \ker(\lambda))$ is a form ideal. On the other hand, if (I, Γ) is a form ideal then $I^J = I$.*

Proof. Assume that $I^J = I$. The only non-trivial step in showing that $\mathcal{I}_I$ is a form ideal is to show that $\{\psi(I)\} \subseteq \lambda^{-1}(\psi(I))$, as follows. Let $i \in I$, then

$$\tau(\psi(i)) = \tau(\psi(1)(1 \otimes i)) = \tau(\psi(1))(i \otimes 1) = \psi(\epsilon)(i \otimes 1) = \psi(i^J \epsilon) \in \psi(I),$$

and hence $\lambda(\{\psi(i)\}) = \psi(i) + \tau(\psi(i)) \in \psi(I)$ since $i^J \in I$. Conversely, let (I, Γ) be a form ideal and let $i \in I$. Then by definition $\lambda(\{\psi(i)\}) = \psi(i) + \tau(\psi(i)) \in \psi(I)$. Hence $\tau(\psi(i)) = \tau(\psi(1)(i^J \otimes 1)) = \tau(\psi(1))(1 \otimes i^J) \in \psi(I)$ and hence

$$\psi^{-1}(\tau(\psi(1))(1 \otimes i^J)) = \psi^{-1}(\tau(\psi(1)))i^J = \varepsilon i^J \in I.$$

Since $\varepsilon \in R$ is a unit, the latter implies that $i^J \in I$. Hence $I^J = I$, since J is bijective. $\qquad\square$

Example 4.3.9. *Let $\mathrm{rad}\, R$ be the Jacobson radical of R, i.e. the intersection of all maximal right ideals in R. The tuple $\mathrm{rad}(\mathcal{R}) := (\mathrm{rad}\, R, \lambda^{-1}(\psi(\mathrm{rad}\, R)))$ is a form ideal, called the radical of $\mathcal{R}$.*

Proof. The involution J induces a bijection between the set $\mathcal{M}_R$ of all maximal right ideals and the set $_R\mathcal{M}$ of all maximal left ideals in R, and hence

$$(\mathrm{rad}\, R)^J = (\cap_{I \in \mathcal{M}_R} I)^J = \cap_{I \in \mathcal{M}_R} I^J = \cap_{I' \in {_R\mathcal{M}}} I' = \mathrm{rad}\, R.$$

Hence $(\mathrm{rad}\, R)^J = \mathrm{rad}\, R$, and the claim follows with Remark 4.3.8. $\qquad\square$

Definition 4.3.10. *The* quotient form ring *of $\mathcal{R}$ by the form ideal $\mathcal{I} = (I, \Gamma)$ is*

$$\mathcal{R}/\mathcal{I} := (R/I, M/\psi(I), \psi_{\mathcal{I}}, \Phi/\Gamma),$$

where $\psi_{\mathcal{I}} : R/I \to M/\psi(I)$, $r + I \mapsto \psi(r) + \psi(I)$, and structure maps

$$\{\ \}_{\mathcal{I}} : M/\psi(I) \to \Phi/\Gamma, \quad m + \psi(I) \mapsto \{m\} + \Gamma,$$

$$\lambda_{\mathcal{I}} : \Phi/\Gamma \to M/\psi(I), \quad \phi + \Gamma \mapsto \lambda(\phi) + \psi(I).$$

The associated antiautomorphism $J_{\mathcal{I}}$ of R/I is given by $(r + I)^{J_{\mathcal{I}}} = r^J + I$.

Example 4.3.11. *(i) Let the form ideal $\mathcal{I}_\lambda$ be as in Remark 4.3.8. In the quotient form ring $\mathcal{R}/\mathcal{I}_\lambda$, the map $\lambda_{\mathcal{I}_\lambda}$ is injective since $\lambda_{\mathcal{I}_\lambda}(\phi + \ker(\lambda)) = \lambda(\phi)$ for all $\phi \in \Phi$. The representations of $\mathcal{R}/\mathcal{I}_\lambda$ correspond to the representations of $\mathcal{R}$ with $\ker(\lambda) \subseteq \ker(\rho_\Phi)$.*

(ii) The annihilator *$\operatorname{Ann}_{\mathcal{R}}(T) = (\operatorname{Ann}_R(V), \ker(\rho_\Phi))$ of a representation T is a form ideal in $\mathcal{R}$. If $\mathcal{I} \subseteq \operatorname{Ann}_{\mathcal{R}}(T)$ is a form ideal then T is also a representation of the quotient form ring $\mathcal{R}/\mathcal{I}$, sometimes denoted by $T_{\mathcal{I}}$ to indicate the change of form rings. If $\operatorname{Ann}_{\mathcal{R}}(T) = (0, 0)$ then T is called* faithful. *Clearly $T_{\operatorname{Ann}_{\mathcal{R}}(T)}$ is always a faithful representation of $\mathcal{R}/\operatorname{Ann}_{\mathcal{R}(T)}$.*

Lemma 4.3.12. *The Witt group $\mathcal{W}(\mathcal{R})$ has a subgroup isomorphic to $\mathcal{W}(\mathcal{R}/\mathcal{I}_\lambda)$, which is of finite index.*

Proof. Let T be a finite representation of $\mathcal{R}$ and let $\phi' \in \ker(\lambda)$. Then $\lambda(\rho_\Phi(\phi')) = \rho_M(\lambda(\phi')) = 0$, i.e. $\rho_\Phi(\phi')$ is additive on V. Hence due to the non-degeneracy of β, there exists some $\alpha_T(\phi') \in V$ with

$$\rho_\Phi(\phi')(v) = \beta(\alpha_T(\phi'), v)$$

for every $v \in V$. One easily verifies that $\alpha_T(\phi'[r]) = \varepsilon r^J \alpha_T(\phi')$ for every $r \in R$ and hence $\alpha_T(\ker(\lambda))$ is an R-submodule of V. Define an abelian group homomorphism $\zeta : \mathcal{W}(\mathcal{R}) \to \operatorname{Hom}_{\mathbb{Z}}(\Phi, \operatorname{Quad}(\ker(\lambda), \mathbb{Q}/\mathbb{Z}))$ by

$$\zeta([T])(\phi) = \phi' \mapsto \rho_\Phi(\phi)(\alpha_T(\phi')).$$

To show that ζ is well-defined, i.e. that $\rho_\Phi(\phi)(\alpha_T(\phi'))$ does not depend on the chosen representative T, let $T' = (V', \rho'_M, \rho'_\Phi, \beta')$ be another representative of $[T]$. If C is a self-dual Type $T \perp -T'$ code in $V \perp V'$ then

$$(\beta \perp -\beta')((\alpha_T(\phi'), \alpha_{T'}(\phi')), (c, c')) = \beta(\alpha_T(\phi'), c) - \beta'(\alpha_{T'}(\phi'), c')$$
$$= \rho_\Phi(\phi')(c) - \rho'_\Phi(\phi')(c') = (\rho_\Phi \perp -\rho'_\Phi)(\phi')(c, c') = 0$$

for all $(c, c') \in C$, and hence $(\alpha_T(\phi'), \alpha_{T'}(\phi')) \in C$. Hence due to the isotropy of C,

$$\rho_\Phi(\phi)(\alpha_T(\phi')) - \rho'_\Phi(\phi)(\alpha_{T'}(\phi')) = (\rho_\Phi \perp -\rho'_\Phi)(\phi)(\alpha_T(\phi'), \alpha_{T'}(\phi')) = 0.$$

Moreover, ζ respects orthogonal sums since always $\alpha_{T \perp T'}(\phi') = (\alpha_T(\phi'), \alpha_{T'}(\phi'))$, and hence is a well-defined homomorphism. In what follows it is shown that $\ker(\zeta) \cong W(\mathcal{R}/\mathcal{I}_\lambda)$, which proves the assertion since the codomain of ζ is finite. The kernel of ζ consists of those representations with $\rho_\Phi(\phi)(\alpha_T(\phi')) = 0$ for all $\phi \in \Phi$ and $\phi' \in \ker(\lambda)$, i.e. where $\alpha_T(\ker(\lambda))$ is isotropic with respect to the quadratic forms. Now if $\alpha_T(\ker(\lambda))$ is isotropic then it is also Type T, since

$$\beta(\alpha_T(\phi'), \alpha_T(\phi'')) = \rho_\Phi(\phi')(\alpha_T(\phi'')) = 0$$

for all $\phi', \phi'' \in \ker(\lambda)$. In particular, the anisotropic representative T' of $[T]$ has $\alpha_{T'}(\ker(\lambda)) = \{0\}$, i.e. $\mathcal{I}_\lambda \subseteq \mathrm{Ann}_{\mathcal{R}}(T)$. This yields an isomorphism

$$\ker(\zeta) \to \mathcal{W}(\mathcal{R}/\mathcal{I}_\lambda), \quad [T] \mapsto [T'_{\mathcal{I}_\lambda}],$$

which proves the Lemma. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

From Lemma 4.3.6 and Lemma 4.3.12 it follows that $\mathcal{W}(\mathcal{R})$ is finite whenever $\mathcal{R}$ is a form ring over some finite field. In what follows we prove the finiteness of $\mathcal{W}(\mathcal{R})$ in the case where the ground ring is a matrix ring over a finite field. These form rings arise form form rings over finite fields as *matrix form rings*, as follows.

Definition 4.3.13. *For a positive integer n the* matrix form ring *of $\mathcal{R}$ is*

$$\mathrm{Mat}_n(\mathcal{R}) := (R^{n \times n}, M^{n \times n}, \psi^{n \times n}, \Phi^{(n)}),$$

where $\psi^{n \times n}$ is defined componentwise and the $R \otimes R$-module structure on M is given by $\psi(r)(s \otimes t) = \psi(r^{J^{(n)}} st)$, for $r, s, t \in R$, where $(r^{J^{(n)}})_{ij} = (r_{ji})^J$ for $r \in R^{n \times n}$, and $J^{(n)}$ is the involution associated with $\mathrm{Mat}_n(\mathcal{R})$. The set

$$\Phi^{(n)} = \left\{ \begin{pmatrix} \phi_1 & & m_{ij} \\ & \ddots & \\ & & \phi_n \end{pmatrix} \;\Big|\; \phi_1, \ldots, \phi_n \in \Phi, \; m_{i,j} \in M \right\}.$$

is an $R^{n \times n}$-qmodule, by imitating matrix multiplication as follows. Writing $\phi \in \Phi^{(n)}$ as above, we have

$$\phi[r]_{ij} = \begin{cases} \sum\limits_{k=1}^{n} \phi_k[r_{ki}] + \sum\limits_{1 \le k \le l \le n} \{ m_{kl}(r_{ki} \otimes r_{li}) \}, & i = j \\[2em] \sum\limits_{k=1}^{n} \lambda(\phi_k)(r_{ki} \otimes r_{kj}) + \sum\limits_{1 \le k \le l \le n} m_{kl}(r_{li} \otimes r_{kj}) + \tau(m_{lk})(r_{ki} \otimes r_{lj}), & i \ne j. \end{cases}$$

The map $\tau : M^{n \times n} \to M^{n \times n}$ is given by $\tau(m)_{ij} = \tau(m_{ji})$, the map $\lambda^{(n)} : \Phi^{(n)} \to M^{n \times n}$ is given by

$$\lambda^{(n)}\left(\begin{pmatrix} \phi_1 & & m_{ij} \\ & \ddots & \\ & & \phi_n \end{pmatrix} \right) = \begin{pmatrix} \lambda(\phi_1) & & m_{ij} \\ & \ddots & \\ \tau(m_{ij}) & & \lambda(\phi_n) \end{pmatrix},$$

and $\{\ \}^{(n)}$ maps

$$\left\{ \begin{pmatrix} m_{1,1} & \cdots & m_{1,n} \\ \vdots & & \vdots \\ m_{n,1} & \cdots & m_{n,n} \end{pmatrix} \right\}^{(n)} = \begin{pmatrix} \{m_{11}\} & & m_{ij} + \tau(m_{ji}) \\ & \ddots & \\ & & \{m_{nn}\} \end{pmatrix}.$$

Theorem 4.3.14. *Every form ring $\mathcal{R}$ over the matrix ring $\mathbb{F}^{n\times n}$ over the finite field $\mathbb{F}$ is isomorphic to some matrix form ring $\mathrm{Mat}_n(\mathcal{R}_0)$, where $\mathcal{R}_0$ is a form ring over $\mathbb{F}$.*

Proof. Write $\mathcal{R} = (R, M, \psi, \Phi)$ and let J be the antiautomorphism of $\mathbb{F}^{n\times n}$ associated with $\mathcal{R}$. After rescaling, we may assume that $B^J = (B^{J_0})^{\mathrm{tr}}$ for all $B \in \mathbb{F}^{n\times n}$, where J_0 is an automorphism of $\mathbb{F}$ which is applied componentwise (cf. Remark 6.1.3). In particular the idempotent $e = \mathrm{diag}(1, 0, \ldots, 0) \in R$ satisfies $e^{J_0} = e$. Hence one easily verifies that

$$\mathcal{R}_0 := (R_0, \psi(R_0), \psi|_{R_0}, \Phi[R_0])$$

is again a form ring, where $R_0 = e\mathbb{F}^{n\times n}e \cong \mathbb{F}$. In what follows it is shown that $\mathcal{R} \cong \mathrm{Mat}_n(\mathcal{R}_0)$. To this aim, let $e_{i,j} \in \mathbb{F}^{n\times n}$ be the element with its only nonzero entry, which is 1, in its ith row and jth column, and let $P_{i,j} \in \mathbb{F}^{n\times n}$ be the permutation matrix such that left multiplication with $P_{i,j}$ interchanges the ith and jth row. The map

$$\alpha_R : R \to R_0^{n\times n}, \quad \alpha_R(r)_{i,j} = P_{1,i}e_{i,i}re_{j,j}P_{1,j},$$

is well-defined since always $e_{1,1}P_{1,i}e_{i,i} = P_{1,i}e_{i,i}$ and $e_{j,j}P_{1,j}e_{1,1} = e_{j,j}P_{j,1}$ and hence always $P_{1,i}e_{i,i}re_{j,j}P_{1,j} \in e_{1,1}\mathbb{F}^{n\times n}e_{1,1} = R_0$. Similarly, one verifies that the maps

$$\alpha_M : M \to (\psi(R_0))^{n\times n}, \quad \alpha_M(m)_{i,j} = m\,(e_{i,i}P_{1,i} \otimes e_{j,j}P_{1,j})$$

and

$$\alpha_\Phi : \Phi \to (\Phi[R_0])^{(n)}, \quad \alpha_\Phi(\phi)_{i,j} = \begin{cases} \phi[e_{i,i}P_{1,i}] & i = j \\ \lambda(\phi)(e_{i,i}P_{1,i} \otimes e_{j,j}P_{1,j}) & i < j \end{cases}$$

are well-defined. It can be shown by elementary calculations that the triple $(\alpha_R, \alpha_M, \alpha_\Phi)$ is a form ring isomorphism. For reader's convenience we give the inverse maps

$$\alpha_M^{-1} : R_0^{n\times n} \to R, \quad (r_{i,j})_{i,j=1}^n \mapsto \sum_{i,j=1}^n r_{i,j}(P_{1,i} \otimes P_{1,j})$$

and $\alpha_\Phi^{-1} : (\Phi[R_0])^{(n)} \to \Phi$ with

$$\alpha_\Phi^{-1}\left(\begin{pmatrix} \phi_1 & m_{1,2} & \cdots & m_{1,n} \\ & \phi_2 & \ddots & \vdots \\ & & \ddots & m_{n-1,n} \\ & & & \phi_n \end{pmatrix}\right) = \sum_{i=1}^n \phi_i[P_{1,i}] + \sum_{i<j} \{m_{i,j}(P_{1,i} \otimes P_{1,j})\},$$

respectively, which shows that α_M and α_Φ are indeed bijective (for α_R this is obvious). $\qquad\square$

Definition 4.3.15. *For a finite representation $T = (V, \rho_M, \rho_\Phi, \beta)$ of $\mathcal{R}$ we define a representation*

$$T^{(n)} := (V^{(n)}, \rho_{M^{n \times n}}, \rho_{\Phi^{(n)}}, \beta^{(n)})$$

of $\mathrm{Mat}_n(\mathcal{R})$, *which is called the nth power of T. Here $V^{(n)}$ consists of the matrices with the elements of V as rows, which is a left $R^{n \times n}$ by usual matrix multiplication, and*

$$\beta^{(n)}\left(\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \begin{pmatrix} v_1' \\ \vdots \\ v_n' \end{pmatrix} \right) = \sum_{i=1}^n \beta(v_i, v_i')$$

and

$$\rho_{\Phi^{(n)}}\left(\begin{pmatrix} \phi_1 & & m_{ij} \\ & \ddots & \\ & & \phi_n \end{pmatrix} \right)\left(\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right) = \sum_{i=1}^n \rho_\Phi(\phi_i)(v_i) + \sum_{i<j} \rho_M(m_{ij})(v_i, v_j).$$

Theorem 4.3.16. *Every representation of $\mathrm{Mat}_n(\mathcal{R})$ is isomorphic to a representation $T^{(n)}$, where T is a representation of $\mathcal{R}$.*

Proof. Write $\mathcal{R} = (R, M, \psi, \Phi)$ and let $T_n := (V_n, (\rho_{M^{n \times n}})_n, (\rho_{\Phi^{(n)}})_n, \beta_n)$ be a representation of $\mathrm{Mat}_n(\mathcal{R})$. Let e_i be the primitive idempotent of $R^{n \times n}$ with its only nonzero entry, which is 1, in its ith row and column. Then $V_n \cong \oplus_{i=1}^n e_i V_n$ as abelian groups. As R-modules via the natural embedding $R \hookrightarrow Z(R^{n \times n})$, the $e_i V$ are all isomorphic, by

$$e_k V_n \to e_l V_n, \quad e_k v \mapsto M_{k,l} \, e_l \, v,$$

where $M_{k,l}$ is the permutation matrix satisfying $M_{k,l} e_l M_{k,l} = e_k$, and hence

$$\varphi : V_n \to (e_1 V_n)^{(n)}, \quad v \mapsto \begin{pmatrix} e_1 v \\ M_{2,1} e_2 v \\ \vdots \\ M_{n,1} e_n v \end{pmatrix}$$

is an isomorphism of $R^{n \times n}$-modules. Observe that in general, $M_{e,y} e_r$ is not invertible, for $e, y, r \in \{1, \ldots, n\}$.

Define a representation $T := (e_1 V, \rho_M, \rho_\Phi, \beta)$ of $\mathcal{R}$ by

$$\beta : e_1 V_n \times e_1 V_n \to \mathbb{Q}/\mathbb{Z}, \quad (e_1 v, e_1 v') \mapsto \beta_n(e_1 v, e_1 v')$$

and $\rho_\Phi : \Phi \to \mathrm{Quad}(e_1 V_n, \mathbb{Q}/\mathbb{Z}), \quad \phi \mapsto (e_1 v \mapsto (\rho_{\Phi^{(n)}})_n(\mathrm{diag}(\phi, 0, \ldots, 0))(e_1 v))$. Then φ is a form isometry, since

$$\beta^{(n)}(\varphi(v), \varphi(v')) = \sum_{i=1}^n \beta(M_{i,1} e_i v, M_{i,1} e_i v') = \sum_{i=1}^n \beta(e_1 M_{i,1} v, e_1 M_{i,1} v')$$

$$= \sum_{i=1}^n \beta_n(e_1 M_{i,1} v, e_1 M_{i,1} v') = \sum_{i=1}^n \beta_n(e_i v, e_i v')$$

$$= \beta_n(v, v')$$

for all $v, v' \in V$. Moreover, if $(m)^{(i,j)}$ is the matrix with its only nonzero entry $m \in M$ in the ith row and jth column then

$$
\rho_\Phi^{(n)}\left(\begin{pmatrix} \phi_1 & & m_{i,j} \\ & \ddots & \\ & & \phi_n \end{pmatrix}\right)(\varphi(v)) = \sum_{i=1}^n \rho_\Phi(\phi_i)(M_{i,1}e_i v) + \sum_{i<j} \rho_M(m_{i,j})(M_{i,1}e_i v, M_{j,1}e_j v)
$$

$$
= \sum_{i=1}^n \rho_\Phi(\phi_i)(e_1 M_{i,1} v) + \sum_{i<j} \beta(e_1 M_{i,1} v, e_1 M_{j,1} m_{i,j} v)
$$

$$
= \sum_{i=1}^n (\rho_{\Phi^{(n)}})_n(\mathrm{diag}(\phi_i, 0, \dots, 0))(e_1 M_{i,1} v) + \sum_{i<j} \beta_n(e_1 M_{i,1} v, e_1 M_{j,1} m_{i,j} v)
$$

$$
= (\rho_{\Phi^{(n)}})_n(\mathrm{diag}(\phi_1, \dots, \phi_n))(v) + \sum_{i<j}(\rho_{M^{n \times n}})_n((m_{i,j})^{(i,j)})(e_i v, e_i v)
$$

$$
= (\rho_{\Phi^{(n)}})_n(\mathrm{diag}(\phi_1, \dots, \phi_n))(v) + \sum_{i<j}(\rho_{\Phi^{(n)}})_n((m_{i,j})^{(i,j)})(e_i v)
$$

$$
= (\rho_{\Phi^{(n)}})_n\left(\begin{pmatrix} \phi_1 & & m_{i,j} \\ & \ddots & \\ & & \phi_n \end{pmatrix}\right)(v)
$$

for all $v \in V$. Hence $T_n = T^{(n)}$, which proves the assertion. $\qquad\square$

Theorem 4.3.17. *The map $\mathcal{W}(\mathcal{R}) \to \mathcal{W}(\mathrm{Mat}_n(\mathcal{R}))$, $[T] \mapsto [T^{(n)}]$ is a well-defined group isomorphism. Hence $\mathcal{W}(\mathrm{Mat}_n(\mathcal{R}))$ is finite whenever $\mathcal{W}(\mathcal{R})$ is finite. In particular if $\mathcal{R}$ is a form ring over a matrix ring $\mathbb{F}^{n \times n}$, for a finite field $\mathbb{F}$, then $\mathcal{W}(\mathcal{R})$ is finite.*

Proof. Let V be the R-module associated with T. If C is a Type T code in V then the submodule $C^{(n)} \leq V^{(n)}$ consisting of the matrices with the elements of C as rows is a Type $T^{(n)}$ code, which is self-dual if and only if C is self-dual. Hence the above maps metabolic representations to metabolic representations. Since orthogonal sums are mapped to orthogonal sums, the above map is well-defined. The surjectivity follows from Theorem 4.3.16. Similarly, every self-dual code Type $T^{(n)}$ code C_n in $(e_1 V_n)^{(n)}$ is of the form $C^{(n)}$, for some self-dual Type T code C in $e_1 V_n$, which implies the injectivity. $\qquad\square$

Definition 4.3.18. *Let $\mathcal{R}_i = (R_i, M_i, \psi_i, \Phi_i)$, for $i = 1, 2$ be form rings with associated involution J_i. Then the direct sum*

$$
\mathcal{R}_1 \oplus \mathcal{R}_2 := (R_1 \times R_2, M_1 \oplus M_2, \psi, \Phi_1 \oplus \Phi_2)
$$

is again a form ring, where $\psi((r_1, r_2)) = (\psi_1(r_1), \psi_2(r_2))$ for $r_1, r_2 \in R$. The associated involution is given by $(r_1, r_2) \mapsto (r_1^{J_1}, r_2^{J_2})$. Clearly the Witt group $\mathcal{W}(\mathcal{R}_1 \oplus \mathcal{R}_2) \cong \mathcal{W}(\mathcal{R}_1) \oplus \mathcal{W}(\mathcal{R}_2)$.

Now we can prove Theorem 4.3.5 for arbitrary finite form rings.

Proof of Theorem 4.3.5. It suffices to show that $\mathcal{W}(\mathcal{R}/\mathcal{I}_\lambda)$ is finite, according to Lemma 4.3.12, i.e. we may assume that λ is injective. If $\mathrm{rad}\, R$ is nontrivial

then there exists some minimal integer t with $(\operatorname{rad} R)^t = \{0\}$, since R is finite and hence $\operatorname{rad} R$ is nilpotent. Let $I := (\operatorname{rad} R)^{\lceil \frac{t}{2} \rceil}$, then $I^J = I$ according to Example 4.3.9, and hence $I^J I = I^2 = \{0\}$. Let $T = (V, \rho_M, \rho_\Phi, \beta)$ be a representation of $\mathcal{R}$, then

$$\beta(iv, jw) = \beta(j^J iv, w) = 0$$

for all $v, w \in V$ and all $i, j \in I$, i.e. IV is a self-orthogonal code. Moreover,

$$\lambda(\phi[i]) = \lambda(\phi)(i \otimes i) = \psi(\psi^{-1}(\lambda(\phi)))(i \otimes i) = \psi(i^J \psi^{-1}(\lambda(\phi))i) = 0$$

for all $\phi \in \Phi$ and $i \in I$ and hence $\Phi[I] = \{0\}$, since λ is injective. Hence always

$$\rho_\Phi(\phi)(iv) = \rho_\Phi(\phi[i])(v) = 0,$$

and hence the code IV is Type T. In particular if T is anisotropic then $I \subseteq \operatorname{Ann}_R(V)$. Moreover, in this case

$$\rho_\Phi(\{\psi(i)\})(v) = \{\rho_M(\psi(i))\}(v) = \rho_M(\psi(i))(v, v) = \beta(v, iv) = \beta(v, 0) = 0$$

for all $i \in I$ and $v \in V$, and hence $\{\psi(I)\} \subseteq \ker(\rho_\Phi)$. Hence the form ideal $\mathcal{I} = (I, \{\psi(I)\}) \subseteq \operatorname{Ann}_\mathcal{R}(T)$ for every anisotropic representation T, which yields a group isomorphism

$$\mathcal{W}(\mathcal{R}) \to \mathcal{W}(\mathcal{R}/\mathcal{I}), \quad [T] \mapsto [T'_\mathcal{I}],$$

where T' is the anisotropic representative of $[T]$. Iterating these arguments, we may assume that $\operatorname{rad} R = \{0\}$, i.e. that R is semisimple. Let $1 = e_1 + \ldots + e_k$ be an orthogonal decomposition into central idempotents with $e_i = e_i^J$, such that every orthogonal decomposition $e_i = f + g$ with $f^J = f$ and $g^J = g$ is trivial, i.e. $f = 0$ or $g = 0$. Then $\mathcal{R} \cong \oplus_{i=1}^k e_i \mathcal{R}$, where

$$e_i \mathcal{R} = (e_i R, M(1 \otimes e_i), \psi(e_i R), \Phi[e_i]),$$

and hence $\mathcal{W}(\mathcal{R}) \cong \oplus_{i=1}^k \mathcal{W}(e_i \mathcal{R})$. Now either e_i is central primitive or it is the sum of two orthogonal central idempotents $e = f + g$ with $f^J = g$. In the latter case $\mathcal{W}(e_i \mathcal{R})$ is trivial, since if T_i is a representation of $e_i \mathcal{R}$ on the $e_i R$-module then fV_i is a self-dual Type T_i code. Hence we may assume that R is simple. Then $\mathcal{R}$ is isomorphic to a matrix form ring (cf. Theorem 4.3.14), hence we may assume that R is a finite field, by Theorem 4.3.17. In this case, the claim of the Theorem has already been proven in the beginning of this section (cf. Theorem 4.3.17). $\square$

Chapter 5

Scalars in Clifford-Weil groups

For a code C of length N over the alphabet V, the *weight enumerator* $\mathrm{cwe}(C)$ is a homogeneous complex polynomial of degree N with variables indexed by V,

$$\mathrm{cwe}(C) := \sum_{v \in V^N} \prod_{i=1}^{N} x_{v_i} \in \mathbb{C}[x_v \mid v \in V^N] \ .$$

The weight enumerator contains some information on the code C which is of interest in coding theoretic applications. For instance the *minimum weight*

$$\min_{0 \neq c \in C} |\{i \in \{1, \dots, N\} \ : \ c_i \neq 0\}|,$$

which, if the alphabet V is a group, is a measure for the error-correcting properties of C, can be read off from $\mathrm{cwe}(C)$. Conversely, certain properties of the code give rise to invariance properties of its weight enumerator. For instance, it follows from the famous MacWilliams identity that the weight enumerator of every self-dual binary code (Type 2_{I}^E) is invariant under the variable substitution

$$(x_0, x_1) \mapsto (\frac{1}{\sqrt{2}}(x_0 + x_1), \frac{1}{\sqrt{2}}(x_0 - x_1)) \ .$$

The weight enumerators of doubly-even binary self-dual codes (Type 2_{II}^E) are also invariant under the variable substitution $x_1 \mapsto I x_1$, where I is a complex primitive fourth root of unity, since the weight of every codeword is a multiple of 4. More generally, to every Type T of codes in the sense of [33] (cf. Chapter 2.2) one associates a complex matrix group $\mathcal{C}(T)$ which acts on $\mathbb{C}[x_v \mid v \in V]$ by linear variable substitutions, such that the weight enumerators of self-dual Type T codes are left invariant. This group is called the *Clifford-Weil group* for the Type T (cf. Definition 5.1). Scalar elements in this group, i.e. elements φ_ζ which map $x_v \mapsto \zeta x_v$, for all $v \in V$ and some $\zeta \in \mathbb{C}^*$, map every homogeneous polynomial p of degree N to $\zeta^N p$. Hence due to the invariance properties of weight enumerators all the ζ^N must be trivial if there exists a self-dual Type T code of length N, i.e. if $[T^N] = [T]^N$ is zero in the Witt group of the underlying form ring. In this chapter it is shown that the connection between $\mathcal{W}(\mathcal{R})$ and the scalar subgroup of

$\mathcal{C}(T)$ is even stronger for finite form rings $\mathcal{R}$ (recall that finiteness of $\mathcal{R}$ is assumed throughout this thesis). Theorem 5.1.7 states that the order of the scalar subgroup equals the order of $[T] \in \mathcal{W}(\mathcal{R})$, i.e. the minimum length for which there exists a self-dual Type T code can a priori be read off from $\mathcal{C}(T)$. The result is already contained in [33, Cor. 5.5.4]. However, the proof given here covers some gaps in the proof given in [33] and parts of it have been published in [13].

5.1 The Clifford-Weil group $\mathcal{C}(T)$

Let $T = (V, \rho_M, \rho_\Phi, \beta)$ be a finite representation of the finite form ring $\mathcal{R} = (R, M, \psi, \Phi)$. In this section we introduce the Clifford-Weil group $\mathcal{C}(T)$, a complex matrix group such that the weight enumerators of self-dual Type T codes are invariant under the variable substitutions given by $\mathcal{C}(T)$. In order to define $\mathcal{C}(T)$ we need the notion of symmetric idempotents below.

Definition 5.1.1. *A nonzero element $e \in R$ is called an* idempotent *if $e^2 = e$. An idempotent e is called* symmetric *with respect to the involution J of R if $eR \cong e^J R$ as right R-modules.*

Remark 5.1.2. *(i) If $e \in R$ is an idempotent then so is e^J, and there is a decomposition*

$$R = eR \oplus (1-e)R = e^J R \oplus (1-e^J)R$$

of R as a right R-module. Since R is finite, the Krull-Schmidt Theorem applies, i.e. a decomposition of R into indecomposable right R-modules is unique, up to isomorphism and permutation of the summands. Hence e is symmetric if and only if the idempotent $1 - e$ is symmetric.

(ii) Let $e \in R$ be a symmetric idempotent. For an isomorphism $\alpha : eR \to e^J R$, define elements $u_e := \alpha^{-1}(e^J) \in eRe^J$ and $v_e := \alpha(e) \in e^J Re$ with

$$u_e v_e = \alpha^{-1}(e^J)v_e = \alpha^{-1}(e^J v_e) = \alpha^{-1}(v_e) = \alpha^{-1}(\alpha(e)) = e,$$

$$v_e u_e = \alpha(e)u_e = \alpha(eu_e) = \alpha(u_e) = \alpha(\alpha^{-1}(e^J)) = e^J.$$

There is an abelian group decomposition $V = eV \oplus (1-e)V$, and on the summands there are non-degenerate $\mathbb{Z}$-bilinear forms

$$\beta_e : \ eV \times eV \to \mathbb{Q}/\mathbb{Z}, \ \ (v, w) \mapsto \beta(v, v_e w)$$

and β_{1-e}, which is defined similarly. This induces another non-degenerate form

$$\beta_e \perp \beta_{1-e} : V \times V \to \mathbb{Q}/\mathbb{Z}, \ \ (v, w) \mapsto \beta_e(ev, ew) + \beta_{1-e}((1-e)v, (1-e)w),$$

with respect to which V decomposes orthogonally as $V = eV \perp (1-e)V$. Moreover, every self-dual code $C = C^{\perp, \beta}$ in V decomposes into abelian groups $C = eC \oplus (1 - e)C$, where

$$eC = (eC)^{\perp, \beta_e} = \{v \in eV \mid \beta_e(v, c) = 0 \text{ for all } c \in eC\},$$

and likewise, $(1 - e)C = ((1 - e)C)^{\perp, \beta_{1-e}}$.

Proof. To prove (ii), note that due to the identity $\beta_e(ev, ew) = \beta(v, v_e w) = \beta(v_e^J v, w)$, for all $v, w \in V$, shows that an element $ev \in \mathrm{rad}(\beta_e)$ if and only if $v_e^J v \in \mathrm{rad}(\beta) = \{0\}$, i.e. $0 = u_e^J v_e^J v = ev$. Hence β_e is non-degenerate. If C is self-dual with respect to β then by definition n element ev lies in $(eC)^{\perp, \beta_e}$ if and only if $\beta_e(v, c) = \beta(v, v_e c) = 0$ for all $c \in eC$. Now $eC \to e^J C$, $ec \mapsto v_e c$ defines a bijection (with inverse $e^J c \mapsto u_e c$), hence the latter is equivalent with $\beta(v, e^J c) = \beta(ev, c) = \beta(v, c) = 0$ for all $c \in C$, i.e. $v \in eC^\perp = eC$, which proves the assertion. $\qquad\square$

Definition 5.1.3. *Let $\mathbb{C}[b_v \mid v \in V]$ be the complex vector space with basis indexed by the elements of V. The* Clifford-Weil group $\mathcal{C}(T)$ *is the subgroup of* $\mathrm{Aut}(\mathbb{C}[b_v \mid v \in V])$ *generated by the elements*

$$m_r : \ b_v \mapsto b_{rv}, \quad d_\phi : \ b_v \mapsto \exp(2\pi i \rho_\Phi(\phi)(v))b_v,$$

$$h_{e, u_e, v_e} : \ b_v \mapsto |eV|^{-\frac{1}{2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e v))b_{w + (1-e)v},$$

for $r \in R^*$, $\phi \in \Phi$ and symmetric idempotents $e = u_e v_e \in R$.

The calculations with Clifford-Weil groups, for instance in Example 5.1.8, are simplified by the following Lemma.

Lemma 5.1.4. *Due to the obvious identities*

$$d_{\phi + \phi'} = d_\phi d_{\phi'}, \quad d_{\phi[r]} = m_r^{-1} d_\phi m_r, \quad h_{e, u_e, v_e} = h_{e, e, e} m_{v_e},$$

which hold for all $\phi, \phi' \in \Phi$, $r \in R^*$ and symmetric idempotents $e = u_e v_e \in R$ with $e^J = e$, the Clifford-Weil group

$$\mathcal{C}(T) = \langle m_r, d_\phi, h_{e, u_e, v_e} \mid e = u_e = v_e \text{ if } e^J = e \rangle,$$

where r and ϕ run through generating subsets of R^* and Φ, respectively.

The action of $\mathcal{C}(T)$ on $\mathbb{C}[b_v \mid v \in V]$ naturally induces an action on the polynomial ring $\mathbb{C}[x_v \mid v \in V]$, by variable substitutions according to as the basis vectors of $\mathbb{C}[b_v \mid v \in V]$ are mapped. The following is Theorem 5.5.1 in [33].

Theorem 5.1.5. *If C is a self-dual Type T code then $\mathrm{cwe}(C)$ is left invariant under all variable substitutions defined by $\mathcal{C}(T)$.*

Remark 5.1.6. *The* scalar subgroup *of $\mathcal{C}(T)$ is*

$$\mathcal{S}(\mathcal{C}(T)) := \{\varphi_\zeta \in \mathcal{C}(T) \mid \varphi_\zeta(b_v) = \zeta \cdot b_v \text{ for all } v \in V\} = \mathcal{C}(T) \cap \mathbb{C}^* \cdot \mathrm{id}.$$

The weight enumerator of a self-dual Type T code C of length t is homogeneous of degree t and left invariant under every element $\varphi_\zeta \in \mathcal{S}(\mathcal{C}(T))$, i.e.

$$\mathrm{cwe}(C) = \varphi_\zeta(\mathrm{cwe}(C)) = \zeta^t \cdot \mathrm{cwe}(C).$$

Hence $\zeta^t = 1$ whenever there exists a self-dual Type T code of length t, i.e. whenever $[T^t] = [T]^t = 0$. Hence the order of $[T]$ is always a multiple of the order of the scalar element φ_ζ, i.e. $\mathcal{S}(\mathcal{C}(T))$ is isomorphic to a subgroup of $\mathbb{C}^*$ with finite exponent, hence is finite.

Hence the order of the scalar subgroup $\mathcal{S}(\mathcal{C}(T))$ is a multiple of the order of the element $[T] \in \mathcal{W}(\mathcal{R})$. In this section the following stronger result will be proven.

Theorem 5.1.7. *If $\mathcal{R}$ is a finite form ring then the order of the element $[T] \in \mathcal{W}(\mathcal{R})$ equals the order of the scalar subgroup $\mathcal{S}(\mathcal{C}(T))$.*

Example 5.1.8. *We compute the Clifford-Weil groups for some of the representations given in Section 2.2, and verify Theorem 5.1.7 in these cases.*

(i) Self-dual binary codes (Type 2_I^E). *Clearly there exists a self-dual Type 2_I^E code of length N if and only if N is even, i.e. the element $[2_I^E]$ has order 2 in the Witt group of the underlying form ring. The Clifford-Weil group $\mathcal{C}(2_I^E)$ is generated by the elements*

$$d := d_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } h := h_{1,1,1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

where the columns give the images of the variables x_0, x_1, i.e. the variable substitution defined by h is

$$x_0 \mapsto \frac{1}{\sqrt{2}}(x_0 + x_1), \quad x_1 \mapsto \frac{1}{\sqrt{2}}(x_0 - x_1),$$

the MacWilliams transformation for binary codes (see [25, Ch.5 §5]). Since $d^2 = h^2 = (dh)^8 = I_2$, the group $\mathcal{C}(2_I^E) \cong D_{16}$ is isomorphic to the dihedral group of order 16. The scalar subgroup of $\mathcal{C}(2_I^E)$ is generated by $(dh)^4 = -\operatorname{id}$, hence the claim of Theorem 5.1.7 holds in this case. The invariant ring of $\mathcal{C}(2_I^E)$ is a polynomial ring $\mathbb{C}[\operatorname{cwe}(i_2), \operatorname{cwe}(e_8)]$ with variables the weight enumerators of the Type 2_I^E codes $i_2 = \langle (1,1) \rangle$, and the extended Hamming code e_8 of length 8, with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

In particular the weight enumerator of every self-dual Type 2_I^E code is a polynomial in $\operatorname{cwe}(i_2)$ and $\operatorname{cwe}(e_8)$, which is a well-known result by Gleason (cf.[9]).

(ii) Self-dual binary Type II codes (Type 2_{II}^E). *These codes are Type 2_I^E, with the additional property of being doubly-even (cf. Section 2.2.2), which is modeled by an additional quadratic form $\rho_\Phi(1) : \mathbb{F}_2 \to \mathbb{Q}/\mathbb{Z}, \quad v \mapsto \frac{1}{4}v^2$. This yields an additional variable substitution*

$$d' = \operatorname{diag}(1, i) \in \mathcal{C}(2_{II}^E),$$

hence $\mathcal{C}(2_{II}^E) = \langle \mathcal{C}(2_I^E), d' \rangle$. One computes that $\mathcal{C}(2_{II}^E)$ has order 192, and that its invariant ring is a polynomial ring $\mathbb{C}[\operatorname{cwe}(e_8), \operatorname{cwe}(g_{24})]$, where e_8 is as above and g_{24} is the extended Golay code of length 24. Hence there exists a self-dual Type II code of length N if and only if N is a multiple of 8, i.e. $[2_{II}^E]$ has order 8 in the Witt group of the underlying form ring. Again, Theorem 5.1.7 holds true, since $\mathcal{S}(\mathcal{C}(2_{II}^E))$ is generated by the element $(d'h)^3$ of order 8.

(iii) Self-dual binary codes with a fixed-point free automorphism of order 2 (cf. [14]). *Let N be even and let S_N be the symmetric group on N points. The natural action of the element*

$$\sigma := (1,2)(3,4)\ldots(N-1,N) \in S_N$$

on $\mathbb{F}_2^N$ induces a $\langle\sigma\rangle$-module structure on $\mathbb{F}_2^N$. By Remark 4.0.8, a code $C \leq \mathbb{F}_2^N$ is σ-invariant if and only if C is a $\mathbb{F}_2\langle\sigma\rangle$-submodule of $\mathbb{F}_2^N$. Hence the Type of σ-invariant binary codes is given by the representation $T = T(V, \beta)$ of the form ring

$$\mathcal{R}(\mathbb{F}_2 C_2, J = \mathrm{id}, 1) = (\mathbb{F}_2 C_2, \mathbb{F}_2 C_2, \mathrm{id}, \Phi = \mathbb{F}_2 C_2)$$

(see Section 2.2.4), where the generating element of C_2 acts on $V = \mathbb{F}_2^2$ with matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and β is the standard scalar product on V. To give generators of the Clifford-Weil group $\mathcal{C}(T)$, note that the unit group $(\mathbb{F}_2 C_2)^*$ is generated by a and Φ is generated by 1 and a. Moreover, $1 = 1^J$ is the only symmetric idempotent of $\mathbb{F}_2 C_2$. Hence according to Lemma 5.1.4, with respect to the basis $(b_{(0,0)}, b_{(0,1)}, b_{(1,0)}, b_{(1,1)})$ of $\mathbb{C}[b_v \mid v \in V]$, generators of $\mathcal{C}(T)$ are given by

$$d_1 := \mathrm{diag}(1, -1, -1, 1), \quad m_a = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$h_1 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

(note that $d_a = \mathrm{id}$). One computes that $\mathcal{C}(T)$ has order 16 and is isomorphic to the direct product $C_2 \times D_8$, where D_8 is the dihedral group of order 8. The scalar subgroup of $\mathcal{C}(T)$ is trivial, and $\langle(1,1)\rangle$ is a self-dual Type $T(V, \beta)$ code of length 1, hence again, the claim of Theorem 5.1.7 holds true.

The proof of Theorem 5.1.7, in Section 5.4, requires some preparation in the subsequent sections. The proof will first be given for form rings over finite fields, and then successively for general finite rings. To perform this generalization, we use the fact that the order of $\mathcal{S}(\mathcal{C}(T))$ remains unchanged if one passes to a quotient representation T/C. Note that this is plausible, since $[T/C] = [T]$ (cf. Remark 4.3.3). To prove that always $\mathcal{S}(\mathcal{C}(T)) \cong \mathcal{S}(\mathcal{C}(T/C))$, we view the Clifford-Weil group as a projective representation of a *universal hyperbolic counitary group* $\mathcal{U}(R, \Phi)$ in Section 5.2. The group $\mathcal{U}(R, \Phi)$ only depends on the underlying form ring and is finite. Along the way, we define a universal Clifford-Weil group

$$\mathcal{C}(\mathcal{R}) \cong \mathrm{Hom}(\mathcal{W}(\mathcal{R}), \mathbb{C}^*). \mathcal{U}(R, \Phi),$$

which is finite since $\mathcal{U}(R, \Phi)$ and $\mathcal{W}(\mathcal{R})$ are finite. Since $\mathcal{C}(T)$ is always a quotient of $\mathcal{C}(\mathcal{R})$ (cf. Definition 5.5.3), it is finite as well.

5.2 $\mathcal{C}(T)$ **as a projective representation of** $\mathcal{U}(R, \Phi)$

Let $\mathcal{R} = (R, M, \psi, \Phi)$ be a finite form ring and let T be a finite representation of $\mathcal{R}$, over the R-module V. The content of this subsection is basically [33, Theorem 5.3.2], which states that the Clifford-Weil group $\mathcal{C}(T)$ is a projective representation of the universal hyperbolic counitary group $\mathcal{U}(R, \Phi)$ (cf. Remark 5.2.5). This provides a proof of finiteness for $\mathcal{C}(T)$, since $\mathcal{U}(R, \Phi)$ is finite and the scalar subgroup of $\mathcal{C}(T)$ is finite as well, by Remark 5.1.6. Here we give some of the calculations for the proof of [33, Theorem 5.3.2] which were omitted in [33]. The results have been published in [13].

Both $\mathcal{C}(T)$ and the hyperbolic counitary group $\mathcal{U}(R, \Phi)$ act on the *Heisenberg group* $\mathcal{E} = \mathcal{E}(V \oplus V)$ (cf. Definition 5.2.1, [17]), with the same image in $\mathrm{Aut}(\mathcal{E})$. By $\mathcal{U}_T(R, \Phi) \leq \mathrm{Aut}(\mathcal{E})$ we denote the image of the action of $\mathcal{U}(R, \Phi)$. The image of the action of $\mathcal{C}(T)$ isomorphic to $\mathcal{C}(T)/\mathcal{S}(\mathcal{C}(T))$. This yields a group epimorphism $\mathcal{U}(R, \Phi) \to \mathcal{C}(T)/\mathcal{S}(\mathcal{C}(T))$ in Corollary 5.2.11.

In Definition 5.2.1 we will define Heisenberg groups $\mathcal{E}(W)$ for a general R-module W (cf. [17]), which leads to a definition of counitary groups $U(R, \Phi, W)$ for a general R-module W and an R-qsubmodule $\Phi \leq \mathrm{Quad}(W, \mathbb{Q}/\mathbb{Z})$ (cf. Definition 5.2.3). As a special case, the hyperbolic counitary group $\mathcal{U}_T(R, \Phi)$ will be introduced in Definition 5.2.4.

Definition 5.2.1. *Let W be a left R-module and let $\beta \in \mathrm{Bil}_{\mathbb{Z}}(W, \mathbb{Q}/\mathbb{Z})$. Then the associated* Heisenberg group *is*

$$\mathcal{E}(W) = \mathcal{E}(W, \beta) = W \times \mathbb{Q}/\mathbb{Z},$$

with multiplication

$$(w, q)(w', q') := (w + w', q + q' + \beta(w, w')).$$

Consider the central subgroup $S := \{(0, q) \mid q \in \mathbb{Q}/\mathbb{Z}\}$ of $\mathcal{E}(W)$. Clearly Z is isomorphic to $\mathbb{Q}/\mathbb{Z}$. If β is non-degenerate and R is a field whose characteristic is not 2, then S is characteristic since it equals the commutator subgroup $\mathcal{E}(W)'$, and $S = Z(\mathcal{E}(W))$, see [17]. This does not hold over general rings R. However, the group

$$\mathrm{Fix}_{\mathrm{Aut}(\mathcal{E}(W))}(S) = \{\theta \in \mathrm{Aut}(\mathcal{E}(W)) \mid \theta(s) = s \text{ for all } s \in S\}$$

still has an interesting structure.

Lemma 5.2.2. *The semidirect product* $\mathrm{Aut}(W) \ltimes \mathrm{Quad}(W, \mathbb{Q}/\mathbb{Z})$ *with multiplication*

$$(\alpha, \phi) \cdot (\alpha', \phi') = (\alpha\alpha', \phi[\alpha'] + \phi')$$

acts on $\mathcal{E}(W)$ by

$$(\alpha, \phi)((w, q)) = \psi_{\alpha, \phi}((w, q)) := (\alpha(w), \phi(w) + q).$$

The map $\psi_{\alpha,\phi}$ is a group automorphism if and only if

$$\beta(\alpha(w), \alpha(w')) - \beta(w, w') = \phi(w + w') - \phi(w) - \phi(w') =: \lambda(\phi)(w, w') \quad (5.1)$$

for all $w, w' \in W$, and

$$\{\psi_{\alpha,\phi} \mid (\alpha, \phi) \in \mathrm{Aut}(W) \ltimes \mathrm{Quad}(W, \mathbb{Q}/\mathbb{Z})\} \cap \mathrm{Aut}(\mathcal{E}(W)) = \mathrm{Fix}_{\mathrm{Aut}(\mathcal{E}(W))}(S).$$

Proof. Every element $\psi_{\alpha,\phi} \in \mathrm{Aut}(\mathcal{E}(W))$ satisfies Equation (5.1), since for elements (v, q), $(v', q') \in \mathcal{E}(W)$ we have

$$\psi_{\alpha,\phi}((v, q)(v', q')) = (\alpha((v + v'), q + q' + \beta(v, v') + \phi(v + v'))$$

and this equals

$$\psi_{\alpha,\phi}((v, q))\psi_{\alpha,\phi}((v', q')) = (\alpha(v + v'), q + q' + \phi(v) + \phi(v') + \beta(\alpha(v), \alpha(v'))).$$

Comparing the second components of the right hand sides of the above equations yields that always

$$\beta(v, v') + \phi(v + v') = \phi(v) + \phi(v') + \beta(\alpha(v), \alpha(v')),$$

which is equivalent to equation (5.1). The same argument shows that every pair (α, ϕ) with the property (5.1) induces an endomorphism of $\mathcal{E}(W)$. One easily verifies that this endomorphism has an inverse mapping $\psi_{\alpha^{-1}, -\phi[\alpha^{-1}]}$, hence is indeed an automorphism of $\mathcal{E}(W)$. Hence the pair (α, ϕ) acts as a group automorphism on $\mathcal{E}(W)$ if and only if it satisfies Equation (5.1).

Clearly every automorphism $\psi_{\alpha,\phi}$ fixes the group S, so it remains to show that every $\theta \in \mathrm{Aut}(\mathcal{E}(W))$ which fixes the group S is of the form $\psi_{\alpha,\phi}$, for some $\alpha \in \mathrm{Aut}(W)$ and some ϕ. To this aim, note that

$$\theta((v, q)) = \theta((v, 0) \cdot (0, q)) = \theta((v, 0)) \cdot (0, q)$$

for all $(v, q) \in \mathcal{E}(W)$, and write $\theta((v, 0)) := (\alpha_\theta(v), \phi_\theta(v))$. As one easily verifies, $\alpha_\theta \in \mathrm{Aut}(W)$ and $\phi_\theta \in \mathrm{Quad}(W, \mathbb{Q}/\mathbb{Z})$, and

$$\theta((v, q)) = (\alpha_\theta(v), \phi_\theta(v)) \cdot (0, q) = (\alpha_\theta(v), \phi_\theta(v) + q),$$

hence $\theta = \psi_{\alpha_\theta, \phi_\theta}$. □

Definition 5.2.3. *Let W be an R-module, $\beta \in \mathrm{Bil}_\mathbb{Z}(W, \mathbb{Q}/\mathbb{Z})$ and let Φ be a submodule of $\mathrm{Quad}(W, \mathbb{Q}/\mathbb{Z})$. The semidirect product $R^* \ltimes \Phi$ acts on $\mathcal{E}(W)$ by*

$$(r, \phi)((w, q)) = \psi_{r,\phi}((w, q)) := (rw, \phi(w) + q).$$

The associated counitary *group is*

$$U(R, \Phi, W) := \{\psi_{r,\phi} \mid (r, \phi) \in R^* \ltimes \Phi\} \cap \mathrm{Aut}(\mathcal{E}(W)) \leq \mathrm{Fix}_{\mathrm{Aut}(\mathcal{E}(W))}(S).$$

More explicitly, $U(R, \Phi, W)$ consists of the elements $\psi_{r,\phi}$ with

$$\beta(rw, rw') - \beta(w, w') = \lambda(\phi)(w, w')$$

for all $w, w' \in W$ (cf. Lemma 5.2.2).

In order to define the hyperbolic counitary group, we now return to the context of form rings and their representation – note that some of the structures in form rings already appear in Definition 5.2.3.

In what follows, let $\mathcal{R} = (R, M, \psi, \Phi)$ be a form ring and let $T = (V, \rho_m, \rho_\Phi, \beta)$ be a finite representation of $\mathcal{R}$. Then the direct sum $V^2 = V \oplus V$ is a module over the matrix ring $R^{2 \times 2}$ in the natural way, i.e.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} ((v, w)) = (av + bw, cv + dw).$$

In writing the elements of V^2 as rows and not as columns, we follow the convention that codewords are usually written as rows– remember that a code, in the language of form rings and representations, is an R-submodule of V^t, for some natural number t. The module V^2 carries a $\mathbb{Z}$-bilinear form

$$V^2 \times V^2 \to \mathbb{Q}/\mathbb{Z}, \quad ((v, w), (v', w')) = \beta^2((v', w'), \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} (v, w)) = \beta(w', v),$$

where $\beta^2 : V^2 \times V^2 \to \mathbb{Q}/\mathbb{Z}, \ ((v, w), (v', w')) \mapsto \beta(v, v') + \beta(w, w')$ (cf. Definition 2.1.16). This setting defines a Heisenberg group

$$\mathcal{E} = \mathcal{E}(V^2) = V^2 \times \mathbb{Q}/\mathbb{Z} \tag{5.2}$$

with inner multiplication

$$((v, w), q)((v', w'), q') = ((v + v', w + w'), q + q' + \beta(w', v)),$$

according to Definition 5.2.1. In what follows, we will always write $\mathcal{E}$ for the group in (5.2). To associate a counitary group, let

$$\Phi_2 := \{ \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \mid \phi_1, \phi_2 \in \Phi, \ m \in M \},$$

which is an R-qmodule via

$$\begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right] = \begin{pmatrix} \phi_1' & m' \\ & \phi_2' \end{pmatrix},$$

where

$$\phi_1' := \phi_1[a] + \phi_2[c] + \{ m(a \otimes c) \},$$
$$m' := \lambda(\phi_1)(a \otimes b) + m(a \otimes d) + \lambda(\phi_2)(c \otimes d) + \tau(m)(c \otimes b),$$
$$\phi_2' := \phi_1[b] + \phi_2[d] + \{ m(b \otimes d) \}.$$

The map $\rho_{\Phi_2} : \Phi_2 \to \text{Quad}(V^2, \mathbb{Q}/\mathbb{Z})$ defined by

$$\rho_{\Phi_2}(\begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix})((v, w)) = \rho_\Phi(\phi_1)(v) + \rho_\Phi(\phi_2)(w) + \rho_M(m)(v, w),$$

is a homomorphism of $R^{2 \times 2}$-qmodules. This setting now defines the hyperbolic counitary group as follows.

Definition 5.2.4. *For a finite representation T of $\mathcal{R}$, the* hyperbolic counitary group *is*

$$\mathcal{U}_T(R, \Phi) := U(R^{2\times2}, \rho_{\Phi_2}(\Phi_2), V^2) = \{\psi_{r,\phi} \mid (r, \phi) \in (R^{2\times2})^* \ltimes \rho_{\Phi_2}(\Phi_2)\} \cap \mathrm{Aut}(\mathcal{E}(V^2)).$$

A more explicit description of the elements of $\mathcal{U}_T(R, \Phi)$ is given in the following Remark.

Remark 5.2.5. *Let $\mathcal{R} = (R, M, \psi, \Phi)$ be a form ring and let*

$$(r, \phi) = \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \rho_{\Phi_2}(\begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix}) \right) \in (R^{2\times2})^* \ltimes \rho_{\Phi_2}(\Phi_2).$$

The element $\psi_{r,\phi}$ lies in the hyperbolic counitary group $\mathcal{U}_T(R, \Phi)$ of a representation T of $\mathcal{R}$ if and only if

$$\begin{pmatrix} c^J a & c^J b \\ d^J a - 1 & d^J b \end{pmatrix} = \begin{pmatrix} \psi^{-1}(\lambda(\phi_1)) & \psi^{-1}(m) \\ \psi^{-1}(\tau(m)) & \psi^{-1}(\lambda(\phi_2)) \end{pmatrix}. \tag{$\dagger$}$$

This condition does not depend on the representation T. The subgroup $\mathcal{U}(R, \Phi) \leq (R^{2\times2})^* \ltimes \Phi_2$ formed by the elements which satisfy condition ($\dagger$) is therefore called the universal hyperbolic counitary group.

Proof. By definition $\psi_{r,\phi}$ lies in $\mathcal{U}_T(R, \Phi) = U(R^{2\times2}, \Phi_2, V^2)$ if and only if

$$\beta^2 \left(r \cdot (v', w'), \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot r \cdot (v, w) \right) - \beta^2 \left((v', w'), \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot (v, w) \right)$$
$$= \lambda(\phi) \left(((v, w), (v', w')) \right)$$

for all (v, w) and $(v', w') \in V^2$. Some elementary transformations of the left and the right hand side of this equation yield the equivalent condition

$$\rho_M(\psi(c^J a))(v', v) + \rho_M(\psi(c^J b))(v', w) + \rho_M(\psi(d^J a - 1))(w', v) + \rho_M(\psi(d^J b))(w', w)$$
$$= \rho_M(\lambda(\phi_1))(v', v) \quad + \rho_M(m)(v', w) \quad + \rho_M(\tau(m))(w', v) \quad + \rho_M(\lambda(\phi_2))(w', w).$$

By suitable choices of v, v', w, w' and m one verifies that the latter holds if and only if the four conditions given by the matrix equation ($\dagger$) are fulfilled. $\qquad\square$

The universal hyperbolic counitary group $\mathcal{U}(R, \Phi)$ acts as group automorphisms on $\mathcal{E}(V^2)$ whenever T is a representation on the R-module V, and the hyperbolic counitary group $\mathcal{U}_T(R, \Phi) \leq \mathrm{Aut}(\mathcal{E}(V^2))$ is the image of this action.

The following Theorem gives generators for $\mathcal{U}(R, \Phi)$, under the condition that the ring R be semiperfect, i.e. $R/\mathrm{rad}\, R$ is semisimple and idempotents of $R/\mathrm{rad}\, R$ lift to idempotents of R, where $\mathrm{rad}\, R$ is the Jacobson radical of R, i.e. the intersection of all maximal right ideals in R. This condition is satisfied in all the cases which are of interest in this work since all Artinian rings, and particularly all finite rings, are semiperfect. For a proof of Theorem 5.2.6 we refer to [33, Theorem 5.2.9].

Theorem 5.2.6. *Let $r \in R^*, \phi \in \Phi$ and let $e = u_e v_e$ be a symmetric idempotent. Then the elements*

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

and

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

generate the universal hyperbolic counitary group $\mathcal{U}(R, \Phi)$.

Note that Theorem 5.2.6 provides generators for $\mathcal{U}_T(R, \Phi)$ for every finite representation T of $\mathcal{R}$, since $\mathcal{U}_T(R, \Phi)$ is an epimorphic image of $\mathcal{U}(R, \Phi)$.

The following Theorem 5.2.7 and Lemma 5.2.8 aim to establish a connection between $\mathcal{C}(T)$ and $\mathcal{U}_T(R, \Phi) \leq \operatorname{Aut}(\mathcal{E})$, which we will use to define a projective representation $\rho : \mathcal{U}_T(R, \Phi) \to \mathcal{C}(T)$ in Corollary 5.2.11.

Theorem 5.2.7. *$\mathcal{E}$ acts linearly and faithfully on $\mathbb{C}[b_v \mid v \in V]$ by*

$$((z, x), q) \cdot b_v = \exp(2\pi i(q + \beta(v, z)))b_{v+x}$$

for all $((z, x), q) \in \mathcal{E}$ and $v \in V$, yielding an irreducible representation $\Delta : \mathcal{E} \to \operatorname{GL}_{|V|}(\mathbb{C})$, i.e. the centralizer $C_{\operatorname{GL}(|V|)}(\Delta(\mathcal{E}))$ consists only of scalar matrices.

Proof. It is a straightforward calculation to show that the above induces an action of $\mathcal{E}$ and that this action is faithful. To see that $C_{\operatorname{GL}(|V|)}(\Delta(\mathcal{E})) \cong \mathbb{C}^*$, consider the subgroup $D := \{((z, 0), 0) \mid z \in V\} \leq \mathcal{E}$. Let $d := ((z, 0), 0) \in D$, then

$$\Delta(d) = \operatorname{diag}(\exp(2\pi i \beta(v, z)) \mid v \in V).$$

Since β is non-degenerate, there exists some element of D whose first and second diagonal entry are unequal. Hence the matrix obtained by taking only the first two rows and columns of any centralizing element must be a diagonal matrix. An iteration of this argument shows that $\Delta(D)$ is centralized only by diagonal matrices.

Let $T := \{((0, x), 0) \mid x \in V\} \leq \mathcal{E}$, then $\Delta(T)$ is a transitive subgroup of the group of permutation matrices of rank $|V|$. Hence $\Delta(T)$ is centralized only by those diagonal matrices which are scalar, which now implies that $C_{\operatorname{GL}(|V|)}(\Delta(\mathcal{E})) \cong \mathbb{C}^*$. $\square$

Lemma 5.2.8. *The group $\mathcal{C}(T)$ acts on $\Delta(\mathcal{E})$ by conjugation, yielding a group homomorphism $c : \mathcal{C}(T) \to \operatorname{Aut}(\Delta(\mathcal{E}))$. The kernel $\ker(c) = \mathcal{S}(\mathcal{C}(T))$ consists of the scalar matrices in $\mathcal{C}(T)$, by Theorem 5.2.7.*

The following two Lemmata show that the generators $m_r d_\phi \in \mathcal{C}(T)$ act on $\Delta(\mathcal{E})$ the same way as $d((r, \phi))$, and h_{e,u_e,v_e} acts as H_{e,u_e,v_e}.

Lemma 5.2.9. *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. For the left hand side we calculate

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

hence $\Delta(d((r, \phi))(z, x, q))$ maps the basis element b_v $(v \in V)$ to

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

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 $\beta(r^{-1} v, z) = \beta(v, (r^J)^{-1} z)$ by definition of the involution J and

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

$\square$

Lemma 5.2.10. *For a symmetric idempotent* $e = u_e v_e \in R$ *and* $(z, x, q) \in \mathcal{E}(V)$ *we have*

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

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

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

Moreover the permutation matrix $\Delta((0, x, 0)) : b_v \mapsto b_{v+x}$ for $x \in eV$ is a tensor product $p_x \otimes \mathrm{id}$ and similarly the diagonal matrix $\Delta((z, 0, 0))$ for $z \in e^J V$ is a

tensor product $d_z \otimes \mathrm{id}$. 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

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

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

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

$$\square$$

The preceding two Lemmata show that the action of $\mathcal{C}(T)$ on $\Delta(\mathcal{E})$ induces an embedding $\iota : \mathcal{C}(T)/\mathcal{S}(\mathcal{C}(T)) \to \mathrm{Aut}(\mathcal{E})$ with

$$\iota(m_r \cdot \mathcal{S}(\mathcal{C}(T))) = \psi_{d((r,\phi))} \quad \text{and} \quad \iota(h_{e,u_e,v_e} \cdot \mathcal{S}(\mathcal{C}(T))) = \psi_{H_{e,u_e,v_e}}$$

and hence $\mathrm{Im}(\iota) = \mathcal{U}_T(R, \Phi)$. This induces a group epimorphism

$$\nu_T : \mathcal{U}(R, \Phi) \xrightarrow{\pi} \mathcal{U}_T(R, \Phi) \xrightarrow{\iota^{-1}} \mathcal{C}(T)/\mathcal{S}(\mathcal{C}(T)),$$

where $\pi : (r, \phi) \mapsto \psi_{r,\phi}$ is the obvious epimorphism. Hence

Corollary 5.2.11. *The map $\mathcal{U}(R, \Phi) \to \mathcal{C}(T)$ defined on generators by*

$$d((r, \phi)) \mapsto m_r d_\phi, \; H_{e,u_e,v_e} \mapsto h_{e,u_e,v_e}$$

is a projective representation.

Corollary 5.2.12. *The Clifford-Weil group $\mathcal{C}(T)$ is finite, since $\mathcal{C}(T)/\mathcal{S}(\mathcal{C}(T))$ is the epimorphic image of the finite group $\mathcal{U}(R, \Phi)$, and $\mathcal{S}(\mathcal{C}(T))$ is finite by Remark 5.1.6.*

5.3 Scalar subgroups of quotient representations

In this section we prove the following Theorem needed in the proof of Theorem 5.1.7, filling a gap in [33]. Theorem 5.3.1 and its proof have also been published in [13].

Theorem 5.3.1. *Let C be an isotropic Type T code. Then $\mathcal{S}(\mathcal{C}(T)) \cong \mathcal{S}(\mathcal{C}(T/C))$.*

To prove the above theorem, we need the following well-known results on the lifting of idempotents and units. These results hold over any Artinian ring, hence in particular over finite rings.

Lemma 5.3.2. *Let R be an Artinian ring and let $I \subseteq R$ be an ideal. Then idempotents and units modulo I lift to idempotents and units of R, i.e.*

(i) *for every $e \in R$ with $(e + I)^2 = e + I \in R/I$ there exists some $i \in I$ such that $e + i \in R$ is an idempotent and*

(ii) *for every $x \in R$ with $x + I \in (R/I)^*$ there exists some $i \in I$ such that $x + i \in R^*$.*

Lemma 5.3.3. *Let R be an Artinian ring and let $I \subseteq R$ be an ideal. Let $e \in I + \operatorname{rad} R$ such that $e + \operatorname{rad} R \in R/\operatorname{rad} R$ is an idempotent. Then e lifts to an idempotent in I, i.e. there exists some $x \in \operatorname{rad} R$ such that $(e + x)^2 = e + x \in I$.*

Proof. Let $x_0 \in \operatorname{rad} R$ such that $e_0 := e + x_0 \in I$, then $e_0^2 - e_0 \in \operatorname{rad} R$. Define a sequence $(e_i)_{i \in \mathbb{N}_0}$ recursively by $e_i := e_{i-1}^2(2e_{i-1} - 1)^{-1} \in I$. In what follows we show that for a sufficiently large index i the e_i are idempotents.

To see that the e_i are well-defined, i.e. that always $2e_i - 1 \in R^*$, note that always

$$(2e_i - 1)^2 = 1 + 4(e_i^2 - e_i) \in 1 + \operatorname{rad} R \subseteq R^*$$

since $e_i^2 - e_i \in \operatorname{rad} R$, which can be shown by induction on i as follows. For $i = 0$ the assertion is clear, hence e_1 is well-defined. Now let $i > 1$ and assume that $e_j^2 - e_j \in \operatorname{rad} R$ for all $j \leq i$, then e_i is well-defined and

$$
\begin{aligned}
e_i^2 - e_i &= e_{i-1}^4(2e_{i-1} - 1)^{-2} - e_{i-1}^2(2e_{i-1} - 1)^{-1} \\
&= (e_{i-1}^4 - e_{i-1}^2(2e_{i-1} - 1))(2e_{i-1} - 1)^{-2} \\
&= (e_{i-1}^2 - e_{i-1}(2e_{i-1} - 1)^{-2}.
\end{aligned}
$$

Now by the assumption of our induction, $e_{i-1}^2 - e_{i-1} \in \operatorname{rad} R$ and hence the same holds for e_i. Moreover, this argument shows that $e_i^2 - e_i \in (\operatorname{rad} R)^{2^i}$, which is zero for some finite index since R is Artinian. Hence there exists some index k such that e_k is an idempotent. Now $x := e_k - e = \sum_{i=0}^{k}(e_i - e_{i-1}) \in \operatorname{rad} R$ since always

$$(e_i - e_{i-1})(2e_{i-1} - 1) = e_{i-1} - e_{i-1}^2 \in \operatorname{rad} R,$$

and the proof is complete. $\square$

Lemma 5.3.4. *Let $e \in R$ be an idempotent. If $e + \operatorname{rad} R \in R/\operatorname{rad} R$ is a symmetric idempotent of the form ring $\mathcal{R}/\operatorname{rad}\mathcal{R}$ then e is symmetric, too. More precisely, if*

$$e + \operatorname{rad} R = u_e v_e + \operatorname{rad} R \text{ and } e^J + \operatorname{rad} R = v_e u_e + \operatorname{rad} R$$

for elements $u_e \in eRe^J$, $v_e \in e^J Re$ then there exists an element $\widetilde{u}_e \in eRe^J$ such that $e = \widetilde{u}_e v_e$ and $e^J = v_e \widetilde{u}_e$.

Proof. We have $u_e v_e \in (eRe)^*$ since $u_e v_e - e \in e(\operatorname{rad} R)e = \operatorname{rad}(eRe)$, and similarly $v_e u_e \in (e^J Re^J)^*$. The latter implies that there exists some $x \in R$ with $v_e u_e x = e^J$. Let $\widetilde{u}_e = u_e x$, then $v_e \widetilde{u}_e = e^J$. It remains to prove that $\widetilde{u}_e v_e = e$. Multiplying both sides with v_e yields an equivalent equation $v_e \widetilde{u}_e v_e = v_e$, since v_e has a left inverse in $(eRe)^*$, since $u_e v_e \in (eRe)^*$. Now the latter equation is true since $v_e \widetilde{u}_e v_e = e^J v_e = e^J$, and the claim follows. □

Lemma 5.3.5. *Let $r = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in (R^{2\times 2})^\star$ and let $X = \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \in \Phi_2$ such that $\psi_{m_r,X} \in \mathcal{U}_T(R, \Phi)$. If $\delta^2 = \delta$ then $e := 1 - \delta$ is a symmetric idempotent. More precisely, we have $e = u_e v_e$ and $e^J = v_e u_e$ with $u_e = -e\gamma^J e^J$, $v_e = e^J \beta e$.*

Proof. This is an elementary calculation:

$$
\begin{aligned}
u_e v_e &= -(1-\delta)\epsilon^{-1}\gamma^J(1-\delta^J)\beta(1-\delta) \\
&= -(1-\delta)\epsilon^{-1}\underbrace{\gamma^J\beta}_{=\alpha^J\epsilon\delta-\epsilon}(1-\delta) + (1-\delta)\epsilon^{-1}\gamma^J\underbrace{\delta^J\beta}_{=\beta^J\epsilon\delta}(1-\delta) \\
&= (1-\delta)\epsilon^{-1}\epsilon(1-\delta) \\
&= 1-\delta \\
&= e
\end{aligned}
$$

and

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

□

The following Lemma gives a homomorphism $r : \mathcal{C}(T) \to \mathcal{C}(T/C)$ which restricts to a group isomorphism $\widetilde{r} : \mathcal{S}(\mathcal{C}(T)) \to \mathcal{S}(\mathcal{C}(T/C))$. Injectivity of $\widetilde{r}$ is straightforward; the rest of this section after Lemma 5.3.6 is devoted to the harder part of showing the surjectivity of $\widetilde{r}$.

Lemma 5.3.6. *The group $\mathcal{C}(T)$ acts on a submodule of $\mathbb{C}[V]$ isomorphic to $\mathbb{C}[C^\perp/C]$. This yields a representation*

$$r : \mathcal{C}(T) \to \operatorname{GL}(\mathbb{C}[C^\perp/C])$$

with $r(\mathcal{C}(T)) \le \mathcal{C}(T/C)$. For the scalar subgroups we get $r(\mathcal{S}(\mathcal{C}(T))) \le \mathcal{S}(\mathcal{C}(T/C))$ and $\ker(r) \cap \mathcal{S}(\mathcal{C}(\rho)) = \{1\}$, i.e. r restricts to a group monomorphism $\widetilde{r} : \mathcal{S}(\mathcal{C}(T)) \to \mathcal{S}(\mathcal{C}(T/C))$.

For the proof of Lemma 5.3.6 we need

Remark 5.3.7. *Consider the natural group epimorphism*

$$\theta : \mathcal{U}_T(R, \Phi) \to \mathcal{U}_{T/C}(R, \Phi), \quad \psi_{r, \rho_{\Phi_2}(\phi)} \mapsto \psi_{r, \rho_{(\Phi/C)_2}(\phi)}.$$

Let $(r, \phi) \in (R^{2 \times 2})^* \ltimes \Phi_2$. Then $\psi_{r, \rho_{\Phi_2(\phi)}} \in \ker(\theta)$ if and only if

$$(r, \phi) \in \left(\begin{pmatrix} 1 + I & I \\ I & 1 + I \end{pmatrix}, \begin{pmatrix} \Gamma & \psi(I) \\ & \Gamma \end{pmatrix} \right),$$

where $(I, \Gamma) = \mathrm{Ann}_{\mathcal{R}}(T/C)$.

Proof. Write

$$(r, \phi) = \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & \psi(i) \\ & \phi_2 \end{pmatrix} \right),$$

then for $(c_1' + C, c_2' + C, q) \in \mathcal{E}((C^\perp/C)^2)$ we have

$$\theta(\psi_{r, \rho_{\Phi_2}(\phi)})(c_1' + C, c_2' + C, q)$$
$$= (\alpha c_1' + \beta c_2' + C, \gamma c_1' + \delta c_2' + C, q + \rho_\Phi(\phi_1)(c_1') + \rho_\Phi(\phi_2)(c_2') + \rho_M(m)(c_1', c_2')).$$

By suitable choices of c_1', c_2' one verifies that $\psi_{r, \rho_{\Phi_2}(\phi)} \in \ker(\theta)$ if and only if $\alpha, \delta \in 1 + I$, $\beta, \gamma \in I$, $\phi_1, \phi_2 \in \Gamma$, and $\rho_M(\psi(i))(c_1', c_2') = 0$ for all $c_1', c_2' \in C^\perp$. The latter is equivalent with $i \in I$, since

$$\rho_M(\psi(i))(c_1', c_2') = \rho_M(\psi(1)(1 \otimes i))(c_1', c_2') = \rho_M(\psi(1))(c_1', ic_2') = \beta(c_1', ic_2'),$$

which proves the assertion. $\square$

Proof of Lemma 5.3.6. Let Rep denote a set of coset representatives of $C^\perp/C$, and define a subspace

$$U := \{ \sum_{v \in \mathrm{Rep}} \sum_{c \in C} a_v b_{v+c} \mid a_v \in \mathbb{C} \} \le \mathbb{C}[V].$$

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

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

Hence we can define a group homomorphism

$$r : \mathcal{C}(T) \to \mathrm{Aut}(U), \quad x \mapsto f \circ x \circ f^{-1}$$

which maps $r(s \cdot \mathrm{id}_{\mathbb{C}[V]}) = s \cdot \mathrm{id}_{\mathbb{C}[C^\perp/C]}$. Hence the restriction $\widetilde{r}$ of r to the scalar subgroup of $\mathcal{C}(T)$ is injective. Let φ and φ/C be the projective representations of

$\mathcal{U}_T(R, \Phi)$ associated with the representations T and T/C, respectively (cf. Corollary 5.2.11). We will show that

$$f \circ \varphi(H_{e,u_e,v_e}) \circ f^{-1} = \varphi/C\left(\theta(H_{e,u_e,v_e})\right) \tag{5.3}$$

and

$$f \circ \varphi(d((r,\phi))) \circ f^{-1} = \varphi/C\left((\theta(d((r,\phi))))\right). \tag{5.4}$$

Equations (5.3) and (5.4) imply that $\mathrm{Im}(r) \leq \mathcal{C}(T/C) = \mathrm{Im}(p/C)$, which shows the lemma. To prove Equation (5.3), 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

$$\left(f^{-1} \circ \varphi(H_{e,u_e,v_e}) \circ f\right)(b_{v+C}) = \left(f^{-1} \circ \varphi(H_{e,u_e,v_e})\right)\left(\sum_{c \in C} b_{v+c}\right)$$

$$= f^{-1}\left(\sum_{c \in C} |eV|^{-\frac{1}{2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e(v+c)))b_{w+(1-e)(v+c)}\right)$$

$$\overset{(\star)}{=} f^{-1}\left(|eV|^{-\frac{1}{2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e v)) \sum_{c' \in (1-e)C} \sum_{c \in eC} \exp(2\pi i \beta(w, v_e c))b_{w+(1-e)(v+c')}\right)$$

$$= f^{-1}\left(\frac{|eC|}{|eV|^{\frac{1}{2}}} \sum_{w \in eC^\perp} \sum_{c' \in (1-e)C} \exp(2\pi i \beta(w, v_e v))b_{w+(1-e)(v+c')}\right)$$

$$= f^{-1}\left(\frac{|eC|}{|eV|^{\frac{1}{2}}} \sum_{w \in T} \sum_{c' \in (1-e)C} \sum_{c \in eC} \exp(2\pi i \beta(w, v_e v))b_{w+c+(1-e)(v+c')}\right)$$

$$= f^{-1}\left(\frac{|eC|}{|eV|^{\frac{1}{2}}} \sum_{w \in T} \exp(2\pi i \beta(w, v_e v)) \sum_{c \in C} b_{w+(1-e)v} + c\right)$$

$$|eC^\perp/C|^{-\frac{1}{2}} \sum_{w \in eC^\perp/C} \exp(2\pi i \beta/C(w, v_e(v+C)))b_{w+(1-e)(v+C)}$$

$$= \varphi/C(\theta(H_{e,u_e,v_e}))(b_{v+C}),$$

where $(\star)$ holds due to the fact that

$$\sum_{c \in eC} \exp(2\pi i \beta(w, v_e c)) = \begin{cases} |eC|, & w \in eC^\perp \\ 0 & \text{otherwise} \end{cases}$$

as seen in the proof of Theorem 5.1.5. To prove Equation (5.4) we note that

$\rho_\Phi(\phi)(c) = 0$ for all $c \in C$ and for all $\phi \in \Phi$ and obtain

$$\left(f^{-1} \circ \varphi(d((r,\phi))) \circ f\right)(b_{v+C}) = \left(f^{-1} \circ \varphi(d((r,\phi)))\right)\left(\sum_{c \in C} b_{v+c}\right)$$

$$= f^{-1}(\varphi(d((r,0)))) \sum_{c \in C} \exp(2\pi i \rho_\Phi(\phi)(v+c)) b_{v+c}$$

$$= f^{-1}(\sum_{c \in C} \exp(2\pi i \rho_\Phi(\phi)(v)) b_{rv+rc})$$

$$= f^{-1}(\sum_{c \in C} \exp(2\pi i \rho_\Phi(\phi)(v)) b_{rv+c})$$

$$= \exp(2\pi i \rho_\Phi/C(\phi)(v+C)) b_{r(v+C)})$$

$$= \varphi/C(\theta(d((r,\phi))))(b_{v+C}).$$

$\square$

Remark 5.3.8. *Let $\iota : \mathcal{C}(T)/\mathcal{S}(\mathcal{C}(T)) \to \mathcal{U}_T(R,\Phi)$ be as in Section 5.2. Since $\mathcal{S}(\mathcal{C}(T))$ is a central subgroup of $\mathcal{C}(T)$, this gives rise to a group epimorphism $\nu : \mathcal{C}(T) \to \mathcal{U}_T(R,\Phi)$ with kernel $\mathcal{S}(\mathcal{C}(T))$. Correspondingly, let $\nu/C : \mathcal{C}(T/C) \to \mathcal{U}_{T/C}(R,\Phi)$, then we have a commuting diagram*

$$\begin{array}{ccc} \mathcal{C}(T) & \xrightarrow{\nu} & \mathcal{U}_T(R,\Phi) \\ r \downarrow & & \downarrow \theta \\ \mathcal{C}(T/C) & \xrightarrow{\nu/C} & \mathcal{U}_{T/C}(R,\Phi). \end{array}$$

Let $r, \widetilde{r}$ be as in Lemma 5.3.6, θ as in Remark 5.3.7 let ν and ν/C be as in Remark 5.3.8. Then we have a commuting diagram

$$\begin{array}{ccccccccc} & & & & 1 & & 1 & & \\ & & & & \downarrow & & \downarrow & & \\ & & 1 & \to & \ker(r) & \stackrel{\nu|_{\ker(r)}}{\to} & \ker(\theta) & \to \mathcal{Y}' \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 \to & \mathcal{S}(\mathcal{C}(T)) & \to & \mathcal{C}(T) & \xrightarrow{\nu} & \mathcal{U}_T(R,\Phi) & \to & 1 \\ & \downarrow \widetilde{r} & & \downarrow r & & \downarrow \theta & & & \text{(5.5)} \\ 1 \to & \mathcal{S}(\mathcal{C}(T/C)) & \to & \mathcal{C}(T/C) & \stackrel{\nu/C}{\to} & \mathcal{U}_{T/C}(R,\Phi) & \to & 1 \\ & \downarrow & & \downarrow & & \downarrow & & \\ & \mathcal{Y} & & 1 & & 1 & & \\ & \downarrow & & & & & & \\ & 1 & & & & & & \end{array}$$

where $\mathcal{Y} = \mathcal{S}(\mathcal{C}(T/C))/\widetilde{r}(\mathcal{S}(\mathcal{C}(T)))$ and $\mathcal{Y}' = \ker(\theta)/\nu(\ker(r))$.

Remark 5.3.9. *The rows and columns of diagram (5.5) are exact.*

Proof. The columns of diagram (5.5) are exact by their definition. To see that the first row is exact, note that $\nu_{\ker(r)}$ is injective since $\ker(\nu) \cap \ker(r) = \mathcal{S}(\mathcal{C}(T)) \cap$

$\ker(r) = \{1\}$ (cf. Lemma 5.3.6). The other rows are exact by definition of ν and ν/C. $\qquad\square$

The claim of Theorem 5.3.1 is that $\widetilde{r}$ is surjective, i.e. that $\mathcal{Y}$ is trivial. Since all the rows and columns in diagram (5.5) are exact we have

$$|\mathcal{Y}| = \frac{|\mathcal{S}(\mathcal{C}(T))|}{\widetilde{r}(\mathcal{S}(\mathcal{C}(T)))} = \frac{|\mathcal{C}(T/C)|}{|\mathcal{U}_{T/C}(R,\Phi)|} \cdot \frac{|\mathcal{U}_T(R,\Phi)|}{|\mathcal{C}(T)|} = \frac{\ker(\theta)}{|\ker(r)|} = |\mathcal{Y}'|.$$

Hence Theorem 5.3.1 holds if and only if $\mathcal{Y}'$ is trivial, i.e. if $\nu|_{\ker(r)} : \ker(r) \to \ker(\theta)$ is an isomorphism, which will be proven in the rest of this section.

Lemma 5.3.10. *If $d((r,\phi)) \in \ker(\theta)$, for some $r \in R^*$ and $\phi \in \Phi$ then $d((r,\phi)) \in \mathrm{Im}(\nu|_{\ker(r)})$.*

Proof. That $d((r,\phi)) \in \ker(\theta)$ means that left multiplication with r must yield the identity on $C^\perp/C$, and that $\rho_\Phi/C\left(C^\perp/C\right) = \{0\}$. Hence the elements $m_r, d_\phi \in \mathcal{C}(T)$ lie in the kernel of r. Since $d((r,\phi)) = \nu(m_r d_\phi)$ by Lemma 5.2.9 and definition of ν, the claim follows. $\qquad\square$

Lemma 5.3.11. *Let $r = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in (R^{2\times 2})^\star$ and let $\phi = \left(\begin{smallmatrix} \phi_1 & m \\ & \phi_2 \end{smallmatrix}\right) \in \Phi_2$ such that $\psi_{r,\rho_{\Phi_2}(\phi)} \in \ker(\theta)$. If δ is a unit then there exists $x \in \ker(r)$ with $\nu(x) = \psi_{r,\rho_{\Phi_2}(\phi)}$.*

Proof. Since $\ker(r)$ is a normal subgroup of $\mathcal{C}(T)$ it suffices to show that $\psi_{r,\rho_{\Phi_2}(\phi)}$ is contained in the normal subgroup of $\mathcal{U}_T(R,\Phi)$ generated by the elements of

$$\{d((r,\phi)) \mid r \in R^*, \ \phi \in \Phi\} \cap \ker(\theta),$$

by Lemma 5.3.10. We show that there exists some $\phi_3 \in \Gamma$ such that

$$\psi_{r,\rho_{\Phi_2}(\phi)} = d((\delta,\phi_2))H_{1,1,1}d((1,\phi_3))H_{1,1,1}^{-1}.$$

We have $d((\delta,\phi_2)) = \left(\left(\begin{smallmatrix} (\delta^J)-1 & \beta \\ 0 & \delta \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ & \phi_2 \end{smallmatrix}\right)\right)$ and hence

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

We therefore find $d((\delta,\phi_2))^{-1}\psi_{r,\rho_{\Phi_2}(\phi)} = \psi_{s,\rho_{\Phi_2}(\phi')}$, where

$$(s,\phi') = \left(\left(\begin{array}{cc} \delta^J\alpha - \delta^J\beta\delta^{-1}\gamma & 0 \\ \delta^{-1}\gamma & 1 \end{array}\right), \left(\begin{array}{cc} -\phi_2[\delta^{-1}\gamma] + \phi_1 & \tilde{m} \\ & 0 \end{array}\right)\right)$$

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

$$(s,\phi') = \left(\left(\begin{array}{cc} 1 & 0 \\ \delta^{-1}\gamma & 1 \end{array}\right), \left(\begin{array}{cc} -\phi_2[\delta^{-1}\gamma] + \phi_1 & 0 \\ & 0 \end{array}\right)\right)$$

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 $(d((\delta, \phi_2))^{-1} \psi_{r, \rho_{\Phi_2}(\phi)})^{H_{1,1,1}} = \psi_{t, \rho_{\Phi_2}(\phi'')}$, where

$$(t, \phi'') = \left(\begin{pmatrix} 1 & -\epsilon\delta^{-1}\gamma \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & m' \\ & \phi \end{pmatrix} \right),$$

with some $m' \in M$ and

$$\phi_3 = \left\{ \psi(-\epsilon\delta^{-1}\gamma) \right\} - \phi_2[\delta^{-1}\gamma] + \phi_1 \in \Gamma,$$

since $-\epsilon\delta^{-1}\gamma \in I$ and $\phi_1, \phi_2 \in \Gamma$, according to Remark 5.3.7. Again $m' = 0$ since the lower left entry in the first matrix is 0. Hence

$$H_{1,1,1}^{-1} d((\delta, \phi_2))^{-1} \psi_{r, \rho_{\Phi_2}(\phi)} H_{1,1,1} = d((1, \phi_3)) \in \ker(\theta)$$

as claimed. $\qquad\square$

Lemma 5.3.12 concludes the proof of Theorem 5.3.1.

Lemma 5.3.12. *The map $\nu|_{\ker(r)}$ is surjective, that is, $\mathrm{Im}(\nu|_{\ker(r)}) = \ker(\theta)$.*

Proof. Let $\psi_{r, \rho_{\Phi_2}(\phi)} \in \ker(\theta)$. We show that there exist a symmetric idempotent $e = u_e v_e \in I$ and a pair

$$(s, \phi') = \left(\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}, \begin{pmatrix} \phi_1' & \mu' \\ & \phi_2' \end{pmatrix} \right) \in (R^{2\times 2})^* \times \Phi_2$$

with $\delta' \in R^*$ such that $\psi_{r, \rho_{\Phi_2}(\phi)} \in \mathcal{U}_T(R, \Phi)$ and

$$\psi_{r, \rho_{\Phi_2}(\phi)} = \psi_{s, \rho_{\Phi_2}(\phi')} H_{e, u_e, v_e}.$$

Since $e \in I = \mathrm{Ann}_R(C^\perp/C)$ the set $e(C^\perp/C) = \{0\}$ and hence $h_{e, u_e, v_e} \in \ker(r)$. Hence $H_{e, u_e, v_e} = \nu(h_{e, u_e, v_e}) \in \mathrm{Im}(\nu|_{\ker(r)})$. By Lemma 5.3.11 the element $\psi_{s, \rho_{\Phi_2}(\phi')} \in \mathrm{Im}(\nu|_{\ker(r)})$, so the same holds for $\psi_{r, \rho_{\Phi_2}(\phi)}$.

Now let us construct e. The ring $R/\mathrm{rad}\, R$ 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 $\mathrm{rad}\, R$. After conjugating with u_2 we obtain an idempotent $\tilde{u}\delta + \mathrm{rad}\, R \in R/\mathrm{rad}\, R$ with $\tilde{u} \in R^*$. Since $\tilde{u}\delta + (I + \mathrm{rad}\, R) \in R/(I + \mathrm{rad}\, R)$ is an idempotent as well and $\delta \in 1 + I$ is a unit modulo $I + \mathrm{rad}\, R$, it follows that $\tilde{u} \in 1 + (I + \mathrm{rad}\, R)$. We can even assume that $\tilde{u} \in 1 + I$. If $\tilde{u} = 1 + i + r$ with $i \in I$ and $r \in \mathrm{rad}\, R$ then $(1 + i)\delta = (\tilde{u} - r)\delta$ is an idempotent $\mod \mathrm{rad}\, R$. Additionally, from $\tilde{u} \in R^*$ we get $1 + i \in R^*$, so we can assume $\tilde{u} = 1 + i$. Write

$$(r, \phi) = \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix} \right),$$

then

$$d((\tilde{u},0))\psi_{r,\rho_{\Phi_2}(\phi)} = \left(\begin{pmatrix} (\tilde{u}^J)^{-1}\alpha & (\tilde{u}^J)^{-1}\beta \\ \tilde{u}\gamma & \tilde{u}\delta \end{pmatrix}, \begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix}\right) \in \ker(\theta)$$

since $d((\tilde{u},0)) \in \ker(\theta)$ by Remark 5.3.7. Hence we can assume that $\delta + \operatorname{rad} R \in R/\operatorname{rad} R$ is an idempotent.

Now consider the quotient form ring $\mathcal{R}/\operatorname{rad}\mathcal{R}$ (cf. Example 4.3.9) and a representation over some $(R/\operatorname{rad} R)$-module W. The element

$$\left(\begin{pmatrix} \alpha + \operatorname{rad} R & \beta + \operatorname{rad} R \\ \gamma + \operatorname{rad} R & \delta + \operatorname{rad} R \end{pmatrix}, \begin{pmatrix} \phi_1 + \lambda^{-1}(\psi(\operatorname{rad} R)) & \mu + \psi(\operatorname{rad} R) \\ & \phi_2 + \lambda^{-1}(\psi(\operatorname{rad} R)) \end{pmatrix}\right)$$

lies in the associated counitary group $\mathcal{U}(R/\operatorname{rad} R, \Phi/\lambda^{-1}(\psi(\operatorname{rad} R)), W)$ by Remark 5.2.5, and hence $e := (1-\delta) + \operatorname{rad} R \in R/\operatorname{rad} R$ is a symmetric idempotent with $e = u_e v_e$ for elements

$$u_e = -e\epsilon^{-1}\gamma^J e^J + \operatorname{rad} R \quad \text{and} \quad v_e = e^J \beta e^J + \operatorname{rad} R,$$

by Lemma 5.3.5. By Lemma 5.3.3 there exists some $x \in I \cap \operatorname{rad} R$ such that $e := e + x = 1 - \delta + x \in I$ is a symmetric idempotent. We calculate the projection on the first component

$$\pi(\psi_{r,\rho_{\Phi_2}(\phi)} H^{-1}_{e,u_e,v_e}) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \delta^J - x^J & -v_e^J\epsilon \\ u_e^J & \delta - x \end{pmatrix} = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$$

with $\delta' = -\gamma v_e^J \epsilon + \delta - \delta x$. It remains to show that $\delta' \in R^*$. Lemma 5.3.4 gives $v_e \equiv (1-\delta^J)\beta(1-\delta) \mod \operatorname{rad} R$. Also $\delta x \in \operatorname{rad}(R)$, so it remains to show that

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

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

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

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

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

$\square$

5.4 The order of $[T]$ equals the order of $\mathcal{S}(\mathcal{C}(T))$

In this section Theorem 5.1.7 is proven, which states that the order of an element $[T] \in \mathcal{W}(\mathcal{R})$ equals the order of the scalar subgroup $\mathcal{S}(\mathcal{C}(T))$ of the Clifford-Weil group $\mathcal{C}(T)$, for every finite representation T of the finite form ring $\mathcal{R}$.

The following two lemmata cite constructions of scalar elements in $\mathcal{C}(T)$ given in [33], which are needed in the proof of Theorem 5.1.7. For a proof of the following lemma, the reader is referred to [33, Theorem 5.4.7].

Lemma 5.4.1. *Let $e \in R$ be an idempotent. An element $\phi \in \Phi$ is called* nonsingular *with respect to e if left multiplication by $\psi^{-1}(\lambda(\phi)) \in e^J Re$ yields an isomorphism of the right R-modules eR and $e^J R$. If ϕ is non-singular with respect to e then the* Gauss sum

$$\gamma_{e,\phi}(T) := |eV|^{-\frac{1}{2}} \sum_{v \in eV} \exp(2\pi i \rho_\Phi(\phi)(v))$$

gives rise to a scalar element $\gamma_{e,\phi}(T) \cdot \mathrm{id} \in \mathcal{C}(T)$

Another construction of scalars makes use of the kernel of the map λ associated with $\mathcal{R}$ (for a proof see [33, Lemma 5.4.3]).

Lemma 5.4.2. *Let $T = (V, \rho_M, \rho_\Phi, \beta)$. For all elements $\phi' \in \ker(\lambda)$ the map $\rho_\Phi(\phi')$ is additive since*

$$\rho_\Phi(\phi')(v + w) - \rho_\Phi(\phi')(v) - \rho_\Phi(\phi')(w) = \lambda(\rho_\Phi(\phi'))(v, w) = \rho_M(\lambda(\phi'))(v, w) = 0$$

for all $v, w \in V$. Hence one can define an abelian group homomorphism $\alpha_T : \ker(\lambda) \to V$ by the condition $\beta(v, \alpha_T(\phi')) = \rho_\Phi(\phi')(v)$ for all $v \in V$. Then for $\phi \in \Phi$, the scalar

$$l_{\phi,\phi'}(T) := \exp(2\pi i \rho_\Phi(\phi)(\alpha_T(\phi')))$$

gives rise to a scalar element $l_{\phi,\phi'}(T) \cdot \mathrm{id} \in \mathcal{C}(T)$.

We begin with a proof of Theorem 5.1.7 for form rings over finite fields, where the associated map λ is injective.

Theorem 5.4.3. *If $\mathcal{R}$ is a form ring over a finite field $\mathbb{F}$ such that the associated map λ is injective then the order of every element $[T] \in \mathcal{W}(\mathcal{R})$ equals the order of the scalar subgroup $\mathcal{S}(\mathcal{C}(T))$.*

Proof. Since the order of $[T]$ is always a multiple of the order of $\mathcal{S}(\mathcal{C}(T))$, by Remark 5.1.6, it suffices to find a scalar element in $\mathcal{C}(T)$ which has the same order as $[T]$. If $\Phi = \{0\}$ then $\mathcal{W}(\mathcal{R})$ is trivial, as seen in the proof of Lemma 4.3.6, hence nothing has to be shown in this case. Assume that $\Phi \neq \{0\}$. If $\mathbb{F}$ has odd characteristic then $\mathcal{W}(\mathcal{R}) \cong \mathcal{W}(\mathbb{F}, J, 1)$ is isomorphic to the Witt group of equivariant forms over $\mathbb{F}$, where $\mathbb{F}$ is viewed as an algebra over its prime field $\mathbb{F}_p$, again by the proof of Lemma 4.3.6. Hence if J is not the identity on $\mathbb{F} = \mathbb{F}_{r^2}$ then $\mathcal{W}(\mathcal{R})$ is cyclic of order 2 (cf. Corollary 4.1.20), and generated by some element $[T = (\mathbb{F}, \rho_M, \rho_\Phi, \beta)]$, where $\beta(x, y) = \frac{1}{p} \mathrm{Trace}_{\mathbb{F}_r/\mathbb{F}_p}(x^r y)$. Since $\lambda(\{\psi(1)\}) = 2\psi(1)$

is nonzero and λ is injective, the element $\{\,\psi(1)\,\}) = 2\psi(1) \in \Phi$ is nonzero and hence nonsingular with respect to the idempotent 1. Hence the Gauss sum

$$
\begin{aligned}
\gamma_{1,\{\,\psi(1)\,\}}(T) &= |\mathbb{F}_{r^2}|^{-\frac{1}{2}} \sum_{f \in \mathbb{F}_{r^2}} \exp(\frac{2\pi i}{p} \operatorname{Trace}_{\mathbb{F}_r/\mathbb{F}_p}(f^{r+1})) \\
&= r^{-1}(1 + \sum_{f \in (\mathbb{F}_{r^2})^*} \exp(\frac{2\pi i}{p} \operatorname{Trace}_{\mathbb{F}_r/\mathbb{F}_p}(f^{r+1}))) \\
&= r^{-1}(1 + (r+1) \sum_{f \in \mathbb{F}^*} \exp(\frac{2\pi i}{p} \operatorname{Trace}_{\mathbb{F}_r/\mathbb{F}_p}(f))) \\
&= r^{-1}(1 - (r+1)) = -1
\end{aligned}
$$

induces a scalar of order 2 in $\mathcal{C}(T)$, which shows the assertion in odd characteristic, for non-trivial J. If $\mathbb{F} = \mathbb{F}_r$ has odd characteristic and J is the identity then by Corollary 4.1.20 and Lemma 4.3.6, the Witt group $\mathcal{W}(\mathcal{R})$ is cyclic of order 4 if $r \equiv_4 -1$, and isomorphic to a direct product $C_2 \times C_2$ of two cyclic groups of order 2 if $r \equiv_4 1$. Assume first that $r \equiv_4 -1$, then $\mathcal{W}(\mathcal{R})$ is generated by some element $[T = (\mathbb{F}, \rho_M, \rho_\Phi, \beta)]$, where $\beta(x,y) = \frac{1}{p} \operatorname{Trace}_{\mathbb{F}/\mathbb{F}_p}(xy)$ for all $x, y \in \mathbb{F}$. Let $\zeta \in \mathbb{F}_{r^2}$ such that $\zeta^{r+1} = 1$ and $\zeta + \zeta^r = 0$, then $x^2 + y^2 = (x + \zeta y)^{r+1}$ for all $x, y \in \mathbb{F}$ and hence

$$
\begin{aligned}
(\gamma_{1,\{\,\psi(1)\,\}}(T))^2 &= r^{-1} \sum_{x,y \in \mathbb{F}_r} \exp(\frac{2\pi i}{p} \operatorname{Trace}_{\mathbb{F}_r/\mathbb{F}_p}(x^2 + y^2)) \\
&= r^{-1} \sum_{x,y \in \mathbb{F}_r} \exp(\frac{2\pi i}{p} \operatorname{Trace}_{\mathbb{F}_r/\mathbb{F}_p}((x + \zeta y)^{r+1})) \\
&= r^{-1} \sum_{x \in \mathbb{F}_{r^2}} \exp(\frac{2\pi i}{p} \operatorname{Trace}_{\mathbb{F}_r/\mathbb{F}_p}(x^{r+1})) \\
&= -1
\end{aligned}
$$

gives rise to a scalar of order 4 in $\mathcal{C}(T)$. Now assume that $r \equiv_4 1$. Then

$$
\mathcal{W}(\mathcal{R}) = \{[0], [T], [T_\nu], [T \perp T_\nu]\},
$$

where T is as above and T_ν is given by $\beta_\nu(x,y) = \operatorname{Tr}_{\mathbb{F}_r/\mathbb{F}_p}(\nu xy)$, for some element $\nu \in \mathbb{F}^* - (\mathbb{F}^*)^2$. In this case all nonzero elements of $\mathcal{W}(\mathcal{R})$ have order 2. Let $\phi_1 := \{\,\psi(1)\,\}$ and $\phi_\nu := \{\,\psi(\nu)\,\}$, then elementary calculations show that $\gamma_{1,\phi_1}(T) = -\gamma_{1,\phi_\nu}(T)$ and $\gamma_{1,\phi_1}(T_\nu) = -\gamma_{1,\phi_\nu}(T_\nu)$, hence both cases $\mathcal{C}(T_1)$ and $\mathcal{C}(T_\nu)$ contain a non-trivial scalar, which must have order 2 by Remark 5.1.6. Moreover, the same calculations show that

$$
-1 = \gamma_{1,\phi_1}(T)\gamma_{1,\phi_1}(T_\nu) = \gamma_{1,\phi_1}(T \perp T_\nu),
$$

and hence $\mathcal{C}(T_1 \perp T_\nu)$ contains a scalar element of order 2 as well. If $\mathbb{F} = \mathbb{F}_r$ has characteristic 2 then $\mathcal{W}(\mathcal{R})$ is cyclic of order 2, and generated by some element $[(\mathbb{F}_{r^2}, \rho_M, \rho_\Phi, \lambda(N))]$, where the quadratic form

$$
N : \mathbb{F}_{r^2} \to \mathbb{F}_2, \; f \mapsto \operatorname{Trace}_{\mathbb{F}_r/\mathbb{F}_2}(f^{r+1})
$$

(cf. Example 4.2.17). Let T be a representation of $\mathcal{R}$ with $\rho_\Phi(\phi) = N$, for some element $\phi \in \Phi$. Due to the injectivity of λ, every nonzero element in Φ is non-singular with respect to the idempotent 1 and hence again the Gauss sum

$$\gamma_{1,\phi}(T) = |\mathbb{F}_{r^2}|^{-\frac{1}{2}} \sum_{f \in \mathbb{F}_{r^2}} \exp(\frac{2\pi i}{p} \operatorname{Trace}_{\mathbb{F}_r/\mathbb{F}_2}(f^{r+1})) = -1$$

induces a scalar element of order 2 in $\mathcal{C}(T)$, which shows the assertion. $\qquad\square$

To generalize Theorem 5.4.3 to arbitrary form rings over finite fields, we need the following Remark.

Remark 5.4.4. *Let* $\mathcal{I} \subseteq \operatorname{Ann}_{\mathcal{R}}(T)$ *be a form ideal, and let* $T_\mathcal{I}$ *be the faithful representation of* $\mathcal{R}/\mathcal{I}$ *induced by* T *(cf. Example 4.3.11). Then the element* $[T_\mathcal{I}] \in \mathcal{W}(\mathcal{R}/\mathcal{I})$ *has the same order as* $[T]$*. Moreover, since* R *is finite, idempotents and units lift modulo ideals of* R *(cf. Lemma 5.3.2), and hence*

$$\mathcal{C}(T) \to \mathcal{C}(T_\mathcal{I}), \quad m_r \mapsto m_{r+I}, \quad d_\phi \mapsto d_{\phi+\Gamma}, \quad h_{e,u_e,v_e} \mapsto h_{e+I,u_e+I,v_e+I}$$

is a group isomorphism.

Theorem 5.4.5. *If* $\mathcal{R}$ *is a form ring over a finite field* $\mathbb{F}$ *then the order of an element* $[T] \in \mathcal{W}(\mathcal{R})$ *equals the order of the scalar subgroup* $\mathcal{S}(\mathcal{C}(T))$*.*

Proof. It suffices to show that the order N of $\mathcal{S}(\mathcal{C}(T))$ is a multiple of the order of $[T]$ (cf. Remark 5.1.6). As one easily verifies,

$$\mathcal{C}(T^N) = \{\otimes_{i=1}^N x \mid x \in \mathcal{C}(T)\}$$

consists of Kronecker products of elements of $\mathcal{C}(T)$. Since $\mathcal{S}(\mathcal{C}(T))$ is isomorphic to a finite subgroup of $\mathbb{C}^*$, it is generated by an element ζ, and hence by the above $\mathcal{S}(\mathcal{C}(T^N))$ is generated by ζ^N, hence is trivial. Hence it suffices to show that $[T] = 0$ whenever $\mathcal{S}(\mathcal{C}(T))$ is trivial. Since passing to a quotient representation leaves both the order of $\mathcal{S}(\mathcal{C}(T))$ and the order of $[T]$ unchanged, we may assume that T is anisotropic. By Remark 5.4.4 we may also assume that T is faithful. If $\mathcal{S}(\mathcal{C}(T))$ is trivial then $l_{\phi,\phi'}(T) = 1$ for all $\phi \in \Phi$ and all $\phi' \in \ker(\lambda)$ (cf. Lemma 5.4.2). Hence always $\rho_\Phi(\phi)(\alpha_T(\phi')) = 0$, and in particular

$$\beta(\alpha_T(\phi'), \alpha_T(\phi'')) = \rho_\Phi(\phi')(\alpha_T(\phi'')) = 0$$

for all $\phi', \phi'' \in \ker(\lambda)$. Hence $\alpha_T(\ker(\lambda))$ is a Type T code and hence $\alpha_T(\ker(\lambda)) = \{0\}$, due to the anisotropy of T. This implies that $\ker(\lambda) \subseteq \ker(\rho_\Phi)$, and hence $\ker(\lambda) = \{0\}$, due to the faithfulness of T. Hence λ is injective, and the claim follows with Theorem 5.4.3. $\qquad\square$

In the next step of the proof of Theorem 5.1.7, we generalize the claim to form rings over matrix rings over finite fields.

Theorem 5.4.6. *Let the representation $T^{(n)}$ of $\mathrm{Mat}_n(\mathcal{R})$ be the nth power of T (cf. Definition 4.3.15). Then the element $[T^{(n)}] \in \mathcal{W}(\mathrm{Mat}_n(\mathcal{R}))$ has the same order as the element $[T] \in \mathcal{W}(\mathcal{R})$. Moreover, if $\mathcal{R}$ is a form ring over a finite field then $\mathcal{S}(\mathcal{C}(T)) \cong \mathcal{S}(\mathcal{C}(T^{(n)}))$.*

Proof. That the order of $[T]$ equals the order of $[T]^{(n)}$ follows from Theorem 4.3.17. On generators of $\mathcal{C}(T)$ define a group monomorphism $\iota : \mathcal{C}(T) \to \mathcal{C}(T^{(n)})$ by

$$m_r \mapsto m_{\mathrm{diag}(r,1,\ldots,1)}, \quad d_\phi \mapsto d_{\mathrm{diag}(\phi,0,\ldots,0)}, \quad h_{e,u_e,v_e} \mapsto h_{e^{(n)},u_e^{(n)},v_e^{(n)}}$$

for $r \in R^*$, $\phi \in \Phi$ and a symmetric idempotent $e = u_e v_e \in R$, where $e^{(n)} = \mathrm{diag}(e,0,\ldots,0)$ and u_e, v_e are defined similarly. Then $\iota(x) = x \otimes \mathrm{id}_n$, hence scalars are mapped to scalars of the same order, and hence $\mathcal{S}(\mathcal{C}(T))$ is isomorphic to a subgroup of $\mathcal{S}(\mathcal{C}(T^{(n)}))$. By Remark 5.1.6, the order of $[T^{(n)}]$ is a multiple of the order of $\mathcal{S}(\mathcal{C}(T^{(n)}))$, and hence if $\mathcal{R}$ is a form ring over a finite field then

$$|\mathcal{S}(\mathcal{C}(T^{(n)}))| \leq |\langle[T^{(n)}]\rangle| = |\langle[T]\rangle| = |\mathcal{S}(\mathcal{C}(T))|,$$

by Theorem 5.4.5, hence $\mathcal{S}(\mathcal{C}(T^{(n)}))$ and $\mathcal{S}(\mathcal{C}(T))$ have the same order, and the claim follows. $\qquad\square$

Since every form ring whose ground ring is a matrix ring over a finite field $\mathbb{F}$ is isomorphic to some matrix form ring $\mathrm{Mat}_n(\mathcal{R})$ over $\mathbb{F}$ (cf. Theorem 4.3.14), one obtains Theorem 5.1.7 for form rings over matrix rings.

Corollary 5.4.7. *If $\mathcal{R}$ is a form ring over a matrix ring over a finite field then the order of an element $[T] \in \mathcal{W}(\mathcal{R})$ equals the order of the scalar subgroup $\mathcal{S}(\mathcal{C}(T))$.*

Now we are able to prove Theorem 5.1.7 for form rings over arbitrary finite rings.

Proof of Theorem 5.1.7. As already shown in the proof of Theorem 5.4.5, it suffices to show that $[T] = 0$ whenever $\mathcal{S}(\mathcal{C}(T))$ is trivial. Hence assume that $\mathcal{S}(\mathcal{C}(T))$ is trivial. Again by the proof of Theorem 5.4.5, we may assume that T is anisotropic and faithful, which implies that λ is injective. Since R is finite, $\mathrm{rad}\,R$ is nilpotent, i.e. there exists some minimal positive integer t with $(\mathrm{rad}\,R)^t = \{0\}$. Let $I := (\mathrm{rad}\,R)^{\lceil\frac{t}{2}\rceil}$ as in the proof of Theorem 4.3.5, then the form ideal

$$\mathcal{I} := (I, \{\,\psi(I)\,\}) \subseteq \mathrm{Ann}_{\mathcal{R}}(T),$$

as seen in the proof of Theorem 4.3.5, and hence $\mathcal{I} = (0,0)$ since T is faithful. This implies that $t = 1$, i.e. $\mathrm{rad}\,R$ must be trivial. Hence the ring R is semisimple. Let $1 = e_1 + \ldots + e_k$ be an orthogonal decomposition into central idempotents of R such that always $e_i^J = e_i$, and that in every orthogonal decomposition $e_i = f + g$ into central idempotents $f = f^J$ and $g = g^J$, either $f = 0$ or $g = 0$. This induces an orthogonal decomposition

$$T = e_1 T \perp \ldots \perp e_k T,$$

where $[T] = 0$ if and only if always $[e_iT] = 0$ (cf. Remark 2.3.18). Moreover, there is an embedding

$$\varrho : \mathcal{C}(e_iT) \hookrightarrow \mathcal{C}(T), \quad m_{e_ir} \mapsto m_{e_ir+1-e_i}, \quad d_{\phi[e]} \mapsto d_{\phi[e]}, \quad h_{\iota,u_\iota,v_\iota} \mapsto h_{\iota,u_\iota,v_\iota},$$

with $\varrho(x) = x \otimes \mathrm{id}$, for $x \in \mathcal{C}(e_iT)$. In particular all the scalar subgroups $\mathcal{S}(\mathcal{C}(e_iT))$ are trivial since $\mathcal{S}(\mathcal{C}(T))$ is trivial. Now an idempotent e_i in this decomposition is either central primitive, or there exists an orthogonal decomposition $e_i = f + g$ into central primitive idempotents f, g with $f^J = g$. Clearly in the latter case $[e_iT] = 0$, as seen in the proof of Theorem 4.3.5. If e_i is central primitive then we may consider e_iT as a representation of $\mathcal{R}/\mathrm{Ann}_{\mathcal{R}(e_iT)}$, which is a form ring over a matrix ring over a finite field. Since changing to this quotient form ring does not change the order of the scalar subgroup or the order of $[e_iT]$, the claim now follows from Corollary 5.4.7. $\qquad\square$

5.5 The universal Clifford-Weil group

In this section a universal Clifford-Weil group $\mathcal{C}(\mathcal{R})$ is introduced (cf. [33, Remark 5.4.8]), which, if $\mathcal{R}$ is faithful (cf. Definition 5.5.1) is a central extension of $\mathcal{U}(R, \Phi)$ with the Witt group $\mathcal{W}(\mathcal{R})$. For every finite representation T of $\mathcal{R}$, the Clifford-Weil group $\mathcal{C}(T)$ is a quotient of $\mathcal{C}(\mathcal{R})$.

Definition 5.5.1. *$\mathcal{R}$ is called* faithful *if $\cap_{T \in \mathcal{T}(\mathcal{R})} \mathrm{Ann}_{\mathcal{R}}(T) = (0, 0)$.*

Note that with respect to their representations, only the faithful form rings are of interest, since every representation T of $\mathcal{R}$ is also a representation of the faithful form ring $\mathcal{R}/\mathrm{Ann}_{\mathcal{R}}(T)$.

Remark 5.5.2. *If $\mathcal{R}$ is faithful then every element $[T] \in \mathcal{W}(\mathcal{R})$ has a faithful representative.*

Proof. Since $\mathcal{R}$ is faithful, for every element $r \in R - \{0\}$ and $\phi \in \Phi - \{0\}$ there exists some $T_{r,\phi} \in \mathcal{T}(\mathcal{R})$ such that $(r, \phi) \notin \mathrm{Ann}_{\mathcal{R}}(T)$. Let

$$T_f := \perp_{r \in R-\{0\}} \perp_{\phi \in \Phi-\{0\}} T_{r,\phi},$$

then $\mathrm{Ann}_{\mathcal{R}}(T_f) = \cap_{r \in R-\{0\}, \phi \in \Phi-\{0\}} \mathrm{Ann}_{\mathcal{R}}(T_{r,\phi}) = (0, 0)$, i.e. T_f is faithful, and so is every multiple of T_f. Let t be the order of $[T_f]$, then $[T \perp T^t] = [T]$ is faithful, which proves the assertion. $\qquad\square$

By Corollary 5.2.11, the Clifford-Weil group $\mathcal{C}(T)$ of a representation T of $\mathcal{R}$ is a central extension of the hyperbolic counitary group $\mathcal{U}_T(R, \Phi)$,

$$\mathcal{C}(T) \cong \mathcal{S}(\mathcal{C}(T)).\mathcal{U}_T(R, \Phi).$$

Definition 5.5.3. *Let $\mathcal{F}(\mathcal{G}_U)$ be the free group on the generating set*

$$\mathcal{G}_U := \{d((r, \phi)), H_{e,u_e,v_e} \mid r \in R^*, \phi \in \Phi, e \in R \text{ symmetric idempotent}\}$$

of $\mathcal{U}(R, \Phi)$, and let the epimorphism $\nu_T : \mathcal{F}(\mathcal{G}_U) \to \mathcal{C}(T)$ be as in Remark 5.3.8. The universal Clifford-Weil group is

$$\mathcal{C}(\mathcal{R}) := \mathcal{F}(\mathcal{G}_U)/ \cap_{T \in \mathcal{T}} \ker(\nu_T).$$

Clearly $\mathcal{C}(T) \cong \mathcal{F}(\mathcal{G}_U)/ \ker(\nu_T)$ is a quotient of $\mathcal{C}(\mathcal{R})$, for every finite representation T of $\mathcal{R}$.

Theorem 5.5.4. *If $\mathcal{R}$ is faithful then $\mathcal{C}(\mathcal{R}) \cong \operatorname{Hom}(\mathcal{W}(\mathcal{R}), \mathbb{C}^*)$. $\mathcal{U}(R, \Phi)$ is a finite central extension of $\mathcal{U}(R, \Phi)$.*

Proof. Let $\pi : \mathcal{F}(\mathcal{G}_U) \to \mathcal{U}(R, \Phi)$ be the natural group epimorphism. Since $\mathcal{R}$ is faithful, $\cap_{T \in \mathcal{T}(\mathcal{R})} \ker(\nu_T) \subseteq \ker(\pi)$. This induces an epimorphism

$$\widetilde{\pi} :\; \mathcal{C}(\mathcal{R}) = \mathcal{F}(\mathcal{G}_U)/ \cap_{T \in \mathcal{T}} \ker(\nu_T) \to \mathcal{U}(R, \Phi).$$

It remains to show that $\ker(\widetilde{\pi}) \cong \operatorname{Hom}(\mathcal{W}(\mathcal{R}), \mathbb{C}^*)$. Clearly

$$\ker(\widetilde{\pi}) = \ker(\pi)/ \cap_{T \in \mathcal{T}} \ker(\nu_T).$$

Consider the homomorphism

$$\varphi : \ker(\pi) \to \operatorname{Hom}(\mathcal{W}(\mathcal{R}), \mathbb{C}^*), \quad w \mapsto ([T] \mapsto \zeta_T),$$

where $\nu_T(w) = \zeta_T \cdot \operatorname{id} \in \mathcal{C}(T)$. That φ is well-defined, i.e. that ζ_T only depends on the equivalence class $[T]$, follows from the construction and uniqueness of the anisotropic representative of $[T]$, together with Lemma 5.3.6. Clearly the kernel $\ker(\varphi) = \cap_{T \in \mathcal{T}} \ker(\nu_T)$. It remains to show that φ is surjective, i.e. that

$$\operatorname{Im}(\varphi)^{\perp} := \{[T] \in \mathcal{W}(\mathcal{R}) \mid \varphi(u)([T]) = 1 \text{ for all } u \in \ker(\pi)\} = \{0\}.$$

Due to the surjectivity of $\nu_T : \mathcal{F}(R, \Phi) \to \mathcal{C}(T)$, the preimage $\nu_T^{-1}(\mathcal{S}(\mathcal{C}(T))) = \ker(\pi)$. Hence $[T]$ lies in $\operatorname{Im}(\varphi)^{\perp}$ if and only if $\mathcal{S}(\mathcal{C}(T))$ is trivial. According to Theorem 5.1.7, this implies that $[T] = 0$, and hence $\operatorname{Im}(\varphi)^{\perp} = \{0\}$, i.e. φ is surjective, as claimed. $\qquad\square$

5.6   Examples

The theory in this chapter allows to determine the minimum length t for which there exists a self-dual Type T code only from the computation of the Clifford-Weil group $\mathcal{C}(T)$. This is illustrated by the following examples, which give explicit constructions of scalar elements of order t in $\mathcal{C}(T)$.

5.6.1   Doubly-even binary codes

A first application of the theory of Clifford-Weil groups is an alternative proof for the following well-known result by Gleason.

Theorem 5.6.1. *There exists a self-dual doubly-even binary code of length N if and only if N is a multiple of 8.*

Proof. Consider the Type 2_{II}^{E} of doubly-even binary codes defined in Section 2.2.1. The claim is that the element $[2_{\mathrm{II}}^{E}]$ has order 8 in the Witt group of the underlying form ring $\mathcal{R}_{\mathrm{II}}$. By Theorem 5.1.7 this order equals the order of the scalar subgroup of the Clifford-Weil group $\mathcal{C}(2_{\mathrm{II}}^{E})$. As seen in Example 5.1.8, the group $\mathcal{C}(2_{\mathrm{II}}^{E}) \leq \mathrm{GL}(2, \mathbb{C})$ has order 192 and is generated by the elements

$$h = h_{1,1,1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad d = d_1 = \mathrm{diag}(1, i),$$

where i is a root of $x^2 + 1$. The scalar subgroup is generated by $(d \cdot h)^3 = \frac{1+i}{\sqrt{2}} \cdot \mathrm{id}$, which has order 8. $\qquad\square$

5.6.2 Codes with prescribed automorphisms over fields of characteristic 2

Let $\mathbb{F}$ be a finite field of characteristic 2 and let G be a permutation group of degree N. Recall that a linear code $C \leq \mathbb{F}^N$ is called G-invariant if and only if

$$G \subseteq \mathrm{Aut}(C) = \{\pi \in S_N \mid \pi C = C\},$$

where the symmetric group S_N acts naturally on $\mathbb{F}^N$ by coordinate permutations. The G-invariant linear codes in $\mathbb{F}^N$ which are self-dual with respect to the standard scalar product $(\cdot, \cdot)$ are precisely the self-dual Type T codes for the representation $T = T(V = \mathbb{F}^N, \tilde{\beta})$ of the form ring $\mathcal{R} = \mathcal{R}(\mathbb{F}G, J, 1)$, where V is a left $\mathbb{F}G$-module in the natural way, and

$$\beta : \mathbb{F}^N \times \mathbb{F}^N \to \mathbb{Q}/\mathbb{Z}, \quad (v, w) \mapsto \frac{1}{2} \mathrm{Trace}_{\mathbb{F}/\mathbb{F}_2}((v, w)),$$

and J is the $\mathbb{F}$-linear involution of $\mathbb{F}G$ with $g^J = g^{-1}$, for $g \in G$ (cf. Example 2.1.8). The Witt group $\mathcal{W}(\mathcal{R})$ is cyclic of order 2, since

$$\mathcal{W}(\mathbb{F}G, J, 1) \to \mathcal{W}(\mathcal{R}), \quad \mathcal{W}(\mathcal{R}), \quad [(W, \psi)] \mapsto [T(W, \psi)]$$

is a group isomorphism (recall that $\mathcal{W}(\mathbb{F}G, J, 1)$ is the Witt group of equivariant $\mathbb{F}G$-modules introduced in Section 4.1 and that this group is cyclic of order 2 by Corollary 4.1.20). Hence either T is metabolic or $[T]$ has order 2 in $\mathcal{W}(\mathcal{R})$. Note that since in the G-module $V \oplus V$, every simple module occurs with even multiplicity, the latter already follows from Corollary 4.1.27. Hence it follows with Theorem 5.1.7 that either T is metabolic or $\mathcal{S}(\mathcal{C}(T))$ is cyclic of order 2. In the latter case, an explicit construction of a scalar of order 2 is given in Theorem 5.6.3, and prepared in the following lemma.

Lemma 5.6.2. *Let $\mathcal{R}$ be a form ring over a ring R of characteristic 2 with associated unit $\epsilon = 1$, and let $\phi \in \ker(\lambda)$. The element $d((1, \phi))H_{1,1,1}$ in the associated hyperbolic counitary group has order 4, hence $(d_\phi h_{1,1,1})^4$ is a scalar in the Clifford-Weil group of a representation of $\mathcal{R}$.*

Proof. By definition

$$d((1,\phi)) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & \phi \end{pmatrix} \right) \quad \text{and} \quad H_{1,1,1} = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \psi(1) \\ & 0 \end{pmatrix} \right).$$

One calculates that

$$\begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] = \begin{pmatrix} \phi_2 & \tau(m) \\ & \phi_1 \end{pmatrix}$$

for all $\phi_1, \phi_2 \in \Phi$ and $m \in M$, and hence

$$(d((1,\phi))H_{1,1,1})^2 = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \phi & \psi(1) \\ & \phi \end{pmatrix} \right).$$

In particular $d((1,\phi))H_{1,1,1}$ has order greater than 3. Since R has characteristic 2 and $\phi \in \ker(\lambda)$ is a linear R-module, the sum $\phi + \phi = 0$ and hence the above yields

$$(d((1,\phi))H_{1,1,1})^4 = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right),$$

and the claim follows. □

Theorem 5.6.3. *Let V be a left $\mathbb{F}G$-module and let $\beta : V \times V \rightarrow \mathbb{Q}/\mathbb{Z}$ be a non-degenerate, G-invariant, symmetric, biadditive form on V. Let $T = T(V,\beta)$ be the associated representation of the form ring $\mathcal{R} = \mathcal{R}(\mathbb{F}G, J, 1)$ (cf. Example 2.1.8). Then either there exists a self-dual Type T code in V or the element*

$$(d_{\{\psi(1)\}} h_{1,1,1})^4 \in \mathcal{C}(T)$$

is a scalar of order 2.

Proof. Let the code C in V be maximally Type T. Then the quotient representation $T/C = T(C^\perp/C, \beta_C)$ is anisotropic and induced by the G-invariant, non-degenerate, symmetric, biadditive form

$$\beta_C : C^\perp/C \times C^\perp/C \rightarrow \mathbb{Q}/\mathbb{Z}, \quad (c' + C, c'' + C) \mapsto \beta(c', c'').$$

The map $r : \mathcal{C}(T) \rightarrow \mathcal{C}(T/C)$ which maps

$$m_f \mapsto (b_{v+C} \mapsto b_{fv+C}), \quad d_\phi \mapsto (b_{v+C} \mapsto \exp(2\pi i \rho_\Phi(\phi)(v))b_{v+C}),$$

$$h_{e,u_e,v_e} \mapsto (b_{v+C} \mapsto |e(C^\perp/C)|^{-\frac{1}{2}} \sum_{w \in e(C^\perp/C))} \beta(v, v_e w) b_{w+(1-e)v})$$

(cf. Lemma 5.3.6) restricts to an isomorphism of the scalar subgroups, as shown in Section 5.3. Hence it suffices to show the claim for T/C, or alternatively, we may assume that T is anisotropic. Let $\phi := \{\psi(1)\}$ and $h := h_{1,1,1}$. The element $(d_\phi h)^4$ is a scalar by Theorem 5.6.2, since

$$\lambda(\phi) = \lambda(\{\psi(1)\}) = \psi(1) + \tau(\psi(1)) = 1 + 1 = 0,$$

i.e. $\phi \in \ker(\lambda)$. Hence it suffices to show that $(d_\phi h)^4(e_v) = -e_v$ for some $v \in V$. For the following calculations, observe that the map

$$\varphi : V \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}, \quad x \mapsto \beta(x, x)$$

is additive and hence there exists some element $v \in V$ with $\beta(v, x) = \varphi(x)$ for all $x \in V$. In particular $\beta(v, vg) = \varphi(vg) = \beta(vg, vg) = \beta(v, v)$ for all $g \in G$, since β is G-invariant. This implies that $\beta(v, v) \neq 0$ since otherwise $v \in \langle v \rangle^\perp$, i.e. $\langle v \rangle \cap \langle v \rangle^\perp$ is a nonzero isotropic subspace, which contradicts the anisotropy of T. Hence $\beta(v, v) = \frac{1}{2}$. Moreover,

$$d_\phi(e_x) = \exp(2\pi i \beta(x, x))e_x = \exp(2\pi i \beta(v, x))e_x$$

for all $x \in V$. Now

$$
\begin{aligned}
hd_\phi h(e_0) &= hd_\phi(|V|^{-\frac{1}{2}}\sum_{x \in V} e_x) = h(|V|^{-\frac{1}{2}}\sum_{x \in V}\exp(2\pi i \beta(v, x)e_x) \\
&= |V|^{-1}\sum_{w \in V}\sum_{x \in V}\exp(2\pi i \beta(w + v, x))e_w = e_v,
\end{aligned}
$$

since

$$\sum_{x \in V}\exp(2\pi i \beta(w + v, x)) = \begin{cases} |V|, & w = v \\ 0 & \text{otherwise.} \end{cases}$$

Analogously, $hd_\phi h(e_v) = e_0$, and hence

$$(d_\phi h)^4(e_0) = d_\phi(hd_\phi h)d_\phi(e_v) = \exp(2\pi i \beta(v, v))d_\phi(hd_\phi h)(e_v) = -d_\phi(e_0) = -e_0$$

as claimed. $\qquad\square$

5.6.3 Doubly-even codes with prescribed automorphisms

Let G be a permutation group of degree N, where N is a multiple of 8. In the case where there exists no binary G-invariant self-dual code of length N (not necessarily doubly-even), a non-trivial scalar in the appropriate Clifford-Weil group has been constructed in the preceding section. Hence in this section assume that there exists a G-invariant self-dual binary code of length N. Then by Theorem 3.2.7 there exists a G-invariant doubly-even self-dual binary code of length N if and only if G lies in the alternating group A_N. In Lemma 5.6.4 a scalar of order 2 in the Clifford-Weil group of the Type of doubly-even G-invariant self-dual binary codes is constructed in the case where G does not lie in the alternating group. To define this Type, assume that every involution of G acts fixed-point-freely. Let $\mathbf{1} \in \mathbb{F}_2^N$ be the all-ones vector, and on the G-module $V := \langle\mathbf{1}\rangle^\perp/\langle\mathbf{1}\rangle$ consider the G-invariant quadratic form

$$q : V \to \mathbb{F}_2, \quad v + \langle\mathbf{1}\rangle \mapsto \frac{\mathrm{wt}(v)}{2}.$$

The Type $T = T(V, q)$ (cf. Section 2.2.5) models the G-invariant self-dual doubly-even binary codes. Note that the assumption that every involution of G acts fixed-point-freely guarantees that T is well-defined, since it implies that $\lambda(q)(v, aw) = 0$ whenever $a + a^J = 0$, where J is the $\mathbb{F}_2$-linear involution of $\mathbb{F}_2 G$ with $g^J = g^{-1}$ (cf. Example 2.1.9).

Lemma 5.6.4. *Assume that there exists a G-invariant self-dual binary code of length N and that every involution of G acts fixed-point-freely. Let T be the Type of doubly-even G-invariant binary codes as above. If G is not contained in the alternating group A_N then $\mathcal{S}(\mathcal{C}(T))$ is cyclic of order 2. More precisely, for every element $g \in G$ with $\mathrm{sign}(g) = -1$, the element $(h_{1,1,1} \cdot d_{\left\{ \psi(1) \right\}} \cdot d_{\left\{ \psi(g) \right\}})^3$ is a scalar of order 2.*

    Proof. Let the code C in V be maximally Type T. Then the quotient $C^\perp/C$ is nonzero since there exists no self-dual G-invariant doubly-even code of length N, since G is not contained in A_N (cf. Theorem 3.2.7) . The quotient representation $T/C = T(C^\perp/C, q_C)$ is induced by the G-invariant quadratic form

$$q_C : C^\perp/C \to \mathbb{F}_2, \quad c' + C \mapsto q(c')$$

induced by q. With the same argument as in the proof of Theorem 5.6.3, it suffices to show the claim of the lemma for $\mathcal{S}(\mathcal{C}(T/C))$. As seen in the proof of Theorem 4.2.19, the quadratic G-module $(C^\perp/C, q_C)$ is isometric to $(U = \mathbb{F}_2^2, f)$, where $G \cap A_N$ acts trivially on U and every element $g \in G$ with $\mathrm{sign}(g) = -1$ interchanges the basis vectors (u, u') of U, where $f(u) = f(u') = 0$ and $f(u + u') = 1$. Hence with respect to the basis $(b_0, b_u, b_{u'}, b_{u+u'})$ of $\mathbb{C}[b_x \mid x \in U]$, generators of $\mathcal{C}(T/C)$ are

$$d_{\left\{ \psi(1) \right\}} = \mathrm{diag}(1, 1, 1, -1), \quad d_{\left\{ \psi(g) \right\}} = \mathrm{diag}(1, -1, -1, -1),$$

$$m_g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad h_{1,1,1} = \tfrac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

One calculates that the scalar subgroup of this matrix group is cyclic of order 2 and that

$$(h_{1,1,1} \cdot d_{\left\{ \psi(1) \right\}} \cdot d_{\left\{ \psi(g) \right\}})^3 = \mathrm{diag}(-1, -1, -1, -1),$$

which shows the assertion. $\qquad\qquad\square$

Chapter 6

The number of self-dual codes

In this chapter a *code* is a submodule of a finite right A-module V, where A is a finite semisimple algebra over a finite field $\mathbb{F}$. Thus as in the previous chapters, a code has by definition not only the classical structure of a vector space over $\mathbb{F}$, but additional structure is claimed.

It is often additional structure which is of interest in coding theoretic applications. For instance if C_N is the cyclic group of order N then the submodules of the natural $\mathbb{F}C_N$-module $\mathbb{F}^N$ are precisely the famous *cyclic codes* of length N over $\mathbb{F}$, i.e. those codes which are invariant under a cyclic shift of the coordinates. More generally, for a permutation group G of degree N, the G-invariant codes, i.e. those codes C with $Cg = C$ for all $g \in G$, are precisely the submodules of the natural $\mathbb{F}G$-module $V = \mathbb{F}^N$. Such codes have received some attention from several authors (cf. [2, 19, 26]).

The G-invariance of the standard scalar product on $\mathbb{F}^N$ is generalized in Definition 6.1.4 to the notion of *equivariant forms* on an A-module V (see also Definition 4.1.1). The *dual*, or *orthogonal*, of a code C in V with respect to an equivariant form β is

$$C^\perp = C^{\perp,\beta} := \{v \in V \mid \beta(v,c) = 0 \text{ for all } c \in C\} .$$

which is again a submodule of V, due to the equivariance of β. If $C = C^\perp$ then C is called *self-dual*. The existence of a self-dual code in V has been investigated in Chapter 4.1, and some criteria have been given in some special cases where $A = \mathbb{F}G$ is a group algebra in Sections 4.1.1, 4.1.2 (see also [42]). Provided that there exists at least one self-dual code in V, this chapter gives the total number $M_{(V,\beta)}$ of self-dual codes in V, for a semisimple finite algebra A. This was motivated by a question of Cary Huffman, who had already given a formula for the number of self-dual cyclic codes of length N over a field of coprime characteristic, answering this question in the case where $A = \mathbb{F}C_N$ is a semisimple group algebra. In this chapter it is shown for a general semisimple algebra that $M_{(V,\beta)}$ basically depends on the composition factors of V, except if $\mathbb{F}$ has characteristic 2 and β is symmetric. Still, the latter case remains relatively transparent when A is a group algebra – then, $M_{(V,\varphi)}$ additionally depends on the existence of a G-invariant isotropic vector $v \in V$, i.e. $\beta(v,v) = 0$.

The number $M_{(V,\beta)}$ is determined via a Morita equivalence $\mathcal{F}$ given in Section

6.1, which maps (V, β) onto a module (U, β') over the $\mathbb{F}$-algebra $Z(A)$. In the case where $A = \mathbb{F}G$ is a group algebra and $\mathbb{F}$ is a splitting field for G, this corresponds the Morita equivalence given in [43]. It is shown that the equivalence $\mathcal{F}$ preserves the number of self-dual codes. Since A is semisimple, $Z(A)$ is a ringdirect sum of fields. This reduces the determination of $M_{(V,\beta)}$, in Section 6.2.3, basically to an enumeration of all self-dual codes in a vector space endowed with a certain form. This situation is well understood; formulae are given in [41] and [22], for instance, and are cited in Subsection 6.2.2, for the convenience of the reader.

In Section 6.3 we give a group $\mathrm{WAut}(V)$ (cf. Definition 2.3.7) which acts on the set $\mathfrak{C}(V)$ of self-dual codes in V, and define some suitable subgroups $\Gamma \leq \mathrm{WAut}(V)$ which respect certain properties of codes, like the isometry type, or, in the case where V is a permutation module, i.e. has a distinct basis, the weight distribution.

The total number $M_{(V,\beta)}$ of self-dual codes in V is then the sum of the orbit lengths under Γ – the mass formula (Theorem 6.3.2) is a reformulation of this fact, which relates the ratio $\frac{M_{(V,\beta)}}{|\Gamma|}$ to the stabilizer orders of Γ-orbits, hence is a useful tool to prove completeness of a classification of all self-dual codes in V. As an example, we classify in Section 6.3.2 the self-dual binary $[48, 24]$-codes with an automorphism of order 23.

The contents of this chapter have been published in [11].

6.1   Morita theory for codes

Let A be a finite dimensional algebra over the finite field $\mathbb{F}$ and let J be an involution of A, i.e. a bijective additive map satisfying $(ab)^J = b^J a^J$ and $(a^J)^J = a$ for all $a, b \in A$. Morita theory for algebras with involution has been studied in [8] and [16], in particular with regard to the connections between Hermitian modules (cf. Definition 6.1.1) over two different algebras A, E over the same ring, where the Hermitian forms over A factorize through $\otimes_E$. This section studies Hermitian modules V over a semisimple algebra A over a finite field $\mathbb{F}$, with involution, and its center $E = Z(A)$, which is fixed under J, hence naturally carries an involution.

This context naturally arises in the study of codes and their automorphisms, which is resumed in sections 6.2 and 6.3. There the algebra $A = \mathbb{F}G$ is a group algebra, for some subgroup $G \leq S_N$ of the symmetric group on N points such that the characteristic of $\mathbb{F}$ does not divide the order of G. The module $V = \mathbb{F}^N$ is then the associated permutation module over $\mathbb{F}G$. The group algebra $\mathbb{F}G$ carries a natural $\mathbb{F}$-linear involution given by $g \mapsto g^{-1}$, for $g \in G$. We will investigate the number of self-dual codes $C \leq \mathbb{F}^N$ which are G-submodules of V, i.e. $C\pi = C$ for all $\pi \in G$. Orthogonality is in this context defined with respect to the standard scalar product

$$\beta: \ \mathbb{F}^N \times \mathbb{F}^N \to \mathbb{F}, \ \ (v, v') \mapsto \sum_{i=1}^{N} v_i v'_i,$$

which takes values in $\mathbb{F}$ and is G-invariant, i.e. $(v, v') = (vg, v'g)$ for all $v, v' \in V$

and $g \in G$. Hence $(V, \beta) \in \mathrm{Mod}_{\mathbb{F}G}^{(\mathbb{F},1)}$ in the sense of Definition 6.1.4, which introduces the category $\mathrm{Mod}_A^{(\mathbb{F},\varepsilon)}$ of ε-equivariant A-modules for a general finite $\mathbb{F}$-algebra. This category is Morita equivalent to the category $\mathrm{Mod}_A^{(A,\varepsilon)}$ given in Definition 6.1.1. In analogy with the construction given in [8, Th. 8.2] we construct a Morita equivalence $\mathcal{F} : \mathrm{Mod}_A^{(A,\varepsilon)} \to \mathrm{Mod}_E^{(E,\delta)}$ in Theorem 6.1.11, for some suitable $\delta \in \{-1, 1\}$.

Definition 6.1.1. *(i) Let $\varepsilon \in \mathbb{F}^*$. An ε-Hermitian form on a right A-module V is a biadditive mapping $\phi : V \times V \to A$ such that*

$$\phi(v, wa) = \phi(v, w)a \quad \text{and} \quad \phi(v, w) = \varepsilon(\phi(w, v))^J$$

for all $v, w \in V$ and $a \in A$. If ϕ is non-degenerate, i.e. if

$$\mathrm{rad}(\phi) := \{v \in V \mid \phi(v, w) = 0 \text{ for all } w \in V\} = \{0\}$$

then (V, ϕ) is called an ε-Hermitian right A-module. Analogously one defines ε-Hermitian left A-modules.

(ii) Let $\mathrm{Mod}_A^{(A,\varepsilon)}$ be the category of ε-Hermitian right A-modules. The morphisms from the object (V, ϕ) to the object (V', ϕ') are the A-module homomorphisms $\psi : V \to V'$ satisfying $\phi'(\psi(v), \psi(w)) = \phi(v, w)$ for all $v, w \in V$. Since any such homomorphism is injective, the morphisms are also called monometries.

Remark 6.1.2. *If there exists a nonzero ε-Hermitian A-module (V, ϕ) then $\varepsilon^J \varepsilon = 1$, since*

$$\phi(v, w) = \varepsilon\phi(w, v)^J = \varepsilon(\varepsilon\phi(v, w)^J)^J = \varepsilon\varepsilon^J\phi(v, w)$$

for all $v, w \in V$.

Remark 6.1.3. *Write $A = \oplus_{i=1}^t D_i^{n_i \times n_i}$, where the D_i are field extensions of $\mathbb{F}$. Then the involution J preserves the center $Z(A) = \oplus_{i=1}^t D_i$, hence restricts to an automorphism of order 1 or 2 on $Z(A)$. So there are field automorphisms $\alpha_i \in \mathrm{Aut}(D_i)$ and a permutation $\pi \in S_t$ of order 1 or 2 such that*

$$(z_1, \ldots, z_t)^J = (z_{\pi(1)}^{\alpha_1}, \ldots, z_{\pi(t)}^{\alpha_t})$$

for all $(z_1, \ldots, z_t) \in Z(A)$, where always $D_i \cong D_{\pi(i)}$, and α_i and $\alpha_{\pi(i)}$ are of the same order. We extend the automorphism α_i to an involution

$$\alpha_i : D_i^{n_i \times n_i} \to D_i^{n_i \times n_i}, \ M_i \mapsto (M_i^{\alpha_i})^{\mathrm{tr}},$$

where M_i^{tr} is the transpose of the matrix M_i and α_i is applied componentwise. We obtain an involution

$$^- : A \to A, \ (M_1, \ldots, M_t) \mapsto ((M_{\pi(1)}^{\alpha_1})^{\mathrm{tr}}, \ldots, (M_{\pi(t)}^{\alpha_t})^{\mathrm{tr}}).$$

The composition $J \circ {}^- : A \to A$ is an automorphism of A restricting to the identity on the center of A. So by the Theorem of Skolem and Noether (see for instance [23, Th. 1.4]), the composition $J \circ {}^-$ is given by conjugation with a unit $u = (u_1, \ldots, u_t) \in A^*$. Hence

$$(M_1, \ldots, M_t)^J = u\overline{(M_1, \ldots, M_t)}u^{-1} = (u_1(M_{\pi(1)}^{\alpha_1})^{\mathrm{tr}}u_1^{-1}, \ldots, u_t(M_{\pi(t)}^{\alpha_t})^{\mathrm{tr}}u_t^{-1})$$

for all $(M_1, \ldots, M_t) \in A$.

Definition 6.1.4. *An ε-equivariant right A-module is a pair (V, β), where V is a right A-module and $\beta : V \times V \to \mathbb{F}$ is a non-degenerate ε-equivariant form (cf. Section 4.1). Analogously one defines ε-equivariant left A-modules. By $\mathrm{Mod}_A^{(\mathbb{F},\varepsilon)}$ denote the category of ε-equivariant right A-modules, with the monometries as morphisms (cf. Definition 6.1.1).*

The categories $\mathrm{Mod}_A^{(A,\varepsilon)}$ and $\mathrm{Mod}_A^{(F,\varepsilon)}$ are equivalent, which has been shown in [31], for instance. The proof is as follows. Let $\mathrm{Trace}_{\mathrm{reg}} : A \to \mathbb{F}$ be the reduced trace, i.e. if $A = \oplus_{i=1}^t D_i^{n_i \times n_i}$ and $M = (M_1, \ldots, M_t) \in A$ then $\mathrm{Trace}_{\mathrm{reg}}(M) = \sum_{i=1}^t \mathrm{Tr}_{D_i/\mathbb{F}}(\mathrm{Trace}(M_i))$. The functor

$$T : \mathrm{Mod}_A^{(A,\varepsilon)} \to \mathrm{Mod}_A^{(\mathbb{F},\varepsilon)}, \quad (V, \phi) \mapsto (V, \mathrm{Trace}_{\mathrm{reg}}(\phi))$$

establishes an equivalence. Note that $\mathrm{Trace}_{\mathrm{reg}}(\phi)$ is non-degenerate whenever ϕ has this property, since $\mathrm{rad}(\mathrm{Trace}_{\mathrm{reg}}(\phi)) = \mathrm{rad}(\phi)$, due to the non-degeneracy of $\mathrm{Trace}_{\mathrm{reg}} : A \times A \to \mathbb{F}$, $(a, b) \mapsto \mathrm{Trace}_{\mathrm{reg}}(ab)$, cf. [6, Proposition 7.41]. In addition, the functor T preserves orthogonality (cf. Definition 6.1.6). This property ensures that any $(V, \phi) \in \mathrm{Mod}_A^{(A,\varepsilon)}$ contains as many self-dual codes as $T((V, \phi))$.

Remark 6.1.5. *Assume that A is semisimple and that (A, J) is simple, i.e. there exists no nontrivial proper ideal of A which is left invariant under J. Let $(V, \beta) \in \mathrm{Mod}_A^{(\mathbb{F},\varepsilon)}$ such that there exists no proper orthogonal decomposition of (V, β) into other ε-equivariant A-modules. Then one of the following holds.*

(i) *There exists a field extension D of $\mathbb{F}$ such that $A \cong D^{n \times n}$, and $V = D^{1 \times n}$ is the unique simple right A-module. Let $\tilde{\beta} : V \times V \to D$ be a non-degenerate ε-equivariant form such that $(V, \tilde{\beta}) \in \mathrm{Mod}_A^{(D,\varepsilon)}$ and $\beta = \mathrm{Trace}_{D/\mathbb{F}}(\tilde{\beta})$. Let u be a Gram Matrix of $\tilde{\beta}$ with respect to some D-basis of V. Then $u^{\mathrm{tr}} = \varepsilon u^\alpha$, where α is the restriction of J to D, applied componentwise. Let $\Delta : A \to D^{n \times n}$ be the natural embedding. Due to the equivariance of β, $\Delta(a)^\alpha u = u\Delta(a^J)^{\mathrm{tr}}$ for all $a \in A$, i.e. $\Delta(a^J) = u^{\mathrm{tr}}(\Delta(a)^\alpha)^{\mathrm{tr}}(u^{\mathrm{tr}})^{-1}$.*

(ii) *There exists an isomorphism $(\delta_1, \delta_2) : A \to D^{n \times n} \oplus D^{n \times n}$, $a \mapsto (\delta_1(a), \delta_2(a))$, for some field extension D of $\mathbb{F}$, and $V = D^{1 \times n} \oplus D^{1 \times n}$. Let $\Delta : A \hookrightarrow D^{2n \times 2n}$ be the natural embedding as block diagonal matrices. If u is as above then $u = \left(\begin{smallmatrix} 0 & u'^{\mathrm{tr}} \\ \varepsilon u'^\alpha & 0 \end{smallmatrix} \right)$, i.e. again, $u^{\mathrm{tr}} = \varepsilon u^\alpha$ and $\Delta(a^J) = u^{\mathrm{tr}}(\Delta(a)^\alpha)^{\mathrm{tr}}(u^{\mathrm{tr}})^{-1}$ for all $a \in A$.*

Definition 6.1.6. *Let $\mathcal{M}, \mathcal{M}'$ be categories of ε-Hermitian or equivariant modules over the algebras $A_{\mathcal{M}}$ and $A_{\mathcal{M}'}$, respectively. A functor $F : \mathcal{M} \to \mathcal{M}'$, $(V, \beta) \mapsto (F_0(V), F_1(\beta))$ is said to* preserve orthogonality *if*

$$F_0(C^{\perp,\beta}) = F_0(C)^{\perp,F_1(\beta)}$$

for every submodule $C \leq V$.

The main result of this section is the following.

Theorem 6.1.7. *Let $\delta \in \{-1, 1\}$ and assume that every simple self-dual A-module carries a non-degenerate $\delta\varepsilon^J$-Hermitian form. Then there is an orthogonality-preserving equivalence between the categories $\mathrm{Mod}_A^{(\mathbb{F},\varepsilon)}$ and $\mathrm{Mod}_E^{(E,\delta)}$, where $E = Z(A)$ is the center of A, with the restriction of J to E as involution.*

Note that according to Remark 4.1.22, for every semisimple algebra A there exists a decomposition $A = eA \oplus (1 - e)A$ with some central idempotent $e = e^J$ such that the algebras eA and $(1 - e)A$ satisfy the assumption of Theorem 6.1.11 on the simple modules. This decomposition is not necessarily proper (for instance in characteristic 2), nor is it necessarily unique, since a simple self-dual A-module may carry both ε- and $-\varepsilon$-equivariant forms, even in odd characteristic (cf. Corollary 4.1.24).

The equivalence stated in Theorem 6.1.7 will be constructed as a composition

$$\mathrm{Mod}_A^{(\mathbb{F},\varepsilon)} \xrightarrow{T^{-1}} \mathrm{Mod}_A^{(A,\varepsilon)} \xrightarrow{\mathcal{F}} \mathrm{Mod}_E^{(E,\delta)},$$

where T is as above. The functor $\mathcal{F}$ is defined in Theorems 6.1.10 and 6.1.11, respectively. The latter Theorem also states that $\mathcal{F}$ is an equivalence.

Remark 6.1.8. *Let (W, ψ) be a $\delta\varepsilon^J$-Hermitian (resp. $\delta\varepsilon^J$-equivariant) left A-module. Consider W as a right module W_E over $E = Z(A)$ via $we := e^J w$ for $w \in W$ and $e \in E$. Then (W_E, ψ) is also an $\delta\varepsilon^J$-Hermitian (resp. $\delta\varepsilon^J$-equivariant) right E-module, where the involution of E is the restriction of J.*

The functor $\mathcal{F}$ transforms A-valued forms into E-valued forms. For its construction we need the following definition.

Definition 6.1.9. *Let $A \cong \oplus_{i=1}^t D_i^{n_i \times n_i}$, where the D_i are field extensions of $\mathbb{F}$. Define*

$$\mathrm{Trace}_{A/E} : A \to E, \quad (M_1, \ldots, M_t) \mapsto (\mathrm{Trace}(M_1)I_{n_1}, \ldots, \mathrm{Trace}(M_t)I_{n_t}).$$

Theorem 6.1.10. *Let $\delta \in \{1, -1\}$ and let (W, ψ) be a $\delta\varepsilon^J$-Hermitian left A-module such that*

$$\psi(w_1, w_2)w_3 = \mathrm{Trace}_{A/E}(\psi(w_3, w_2))w_1 \qquad (\star\star)$$

for all $w_1, w_2, w_3 \in W$. Consider W as a right module over $E = Z(A)$ as in Remark 6.1.8. Define a functor

$$F_W := F_{(W,\psi)} : \mathrm{Mod}_A^{(A,\varepsilon)} \to \mathrm{Mod}_E^{(E,\delta)}, \quad (V, \phi) \mapsto (V \otimes_A {}_A W_E, \phi \otimes \psi),$$

where $\phi \otimes \psi := \big((v \otimes w, v' \otimes w') \mapsto \mathrm{Trace}_{A/E}(\phi(v', v)\psi(w, w'))\big)$. Then F_W preserves orthogonality.

Proof. To show that $\phi \otimes \psi$ is well-defined one has to check that it is A-balanced, i.e. that

$$\mathrm{Trace}_{A/E}(\phi(v'a', va)\psi(w, w')) = \mathrm{Trace}_{A/E}(\phi(v', v)\psi(aw, a'w'))$$

for all $v, v' \in V$, $w, w' \in W$ and $a \in A$. Since ϕ and ψ are Hermitian, the left hand side of the above equation equals

$$\mathrm{Trace}_{A/E}(\phi(v'a', v)a\psi(w, w')) = \varepsilon\,\mathrm{Trace}_{A/E}(\phi(v, v'a')^J\psi(aw, w')$$
$$= \varepsilon\,\mathrm{Trace}_{A/E}(a'^J\phi(v, v')^J\psi(aw, w')).$$

Due to the elementary properties of the Trace function, the arguments of the latter term may be permuted by a cyclic shift, i.e. the latter equals

$$\varepsilon\,\mathrm{Trace}_{A/E}(\varepsilon^J\phi(v', v)\psi(aw, w')a'^J) = \mathrm{Trace}_{A/E}(\phi(v', v)\delta\varepsilon^J(a'\psi(w', aw))^J)$$
$$= \delta\varepsilon^J\,\mathrm{Trace}_{A/E}(\phi(v', v)\delta\varepsilon\psi(aw, a'w'))$$
$$= \mathrm{Trace}_{A/E}(\phi(v', v)\psi(aw, a'w'))$$

as claimed. It remains to show that F_W preserves orthogonality, i.e. that

$$F_W(C)^{\perp,\phi\otimes\psi} = F_W(C^{\perp,\phi})$$

for all submodules $C \leq V$, where $(V, \phi) \in \mathrm{Mod}_A^{(A,\varepsilon)}$. The inclusion $F_W(C^{\perp,\phi}) \subseteq F_W(C)^{\perp,\phi\otimes\psi}$ follows immediately from the definition of the form $\phi \otimes \psi$. For the inclusion $F_W(C)^{\perp,\phi\otimes\psi} \subseteq F_W(C^{\perp,\phi})$, let $\sum_{i=1}^k v_i \otimes w_i \in F_W(C)^{\perp,\phi\otimes\psi}$. Then

$$\mathrm{Trace}_{A/E}(\sum_{i=1}^k \phi(c, v_i)\psi(w_i, w')) = \mathrm{Trace}_{A/E}(\phi(c, \sum_{i=1}^k v_i\psi(w_i, w'))) = 0$$

for all $c \in C$ and $w' \in W$. Now C is a right A-module and ϕ is Hermitian, hence the latter equation implies that

$$\mathrm{Trace}_{A/E}(\phi(c, \sum_{i=1}^k v_i\psi(w_i, w'))a) = 0$$

for all $c \in C, w' \in W$ and $a \in A$. This implies that always $\phi(c, \sum_{i=1}^k v_i\psi(w_i, w')) = 0$, due to the non-degeneracy of $\mathrm{Trace}_{A/E} : A \times A \to E$, $(x, y) \mapsto \mathrm{Trace}_{A/E}(xy)$. Hence always $\sum_{i=1}^k v_i\psi(w_i, w') \in C^{\perp,\phi}$ and hence

$$\sum_{i=1}^k v_i\psi(w_i, w') \otimes w'' \in F_W(C^{\perp,\phi})$$

for all $w'' \in W$. Choosing $w', w'' \in W$ with $\mathrm{Trace}_{A/E}(\psi(w', w'')) = 1$, this yields

$$\sum_{i=1}^k v_i\psi(w_i, w') \otimes w'' = \sum_{i=1}^k v_i \otimes \psi(w_i, w')w'' = \sum_{i=1}^k v_i \otimes \mathrm{Trace}_{A/E}(\psi(w'', w'))w_i$$
$$= \sum_{i=1}^k v_i \otimes w_i \in F_W(C^{\perp,\phi}).$$

The fact that F_W preserves orthogonality implies that $\phi \otimes \psi$ is non-degenerate since

$$\operatorname{rad}(\phi \otimes \psi) = F_W(V)^{\perp, \phi \otimes \psi} = F_W(V^{\perp, \phi}) = F_W(\operatorname{rad}(\phi)) = \{0\}.$$

$\square$

Note that condition $(\star\star)$ in Theorem 6.1.10 is natural and that, in the situation of Theorem 6.1.11, there always exists a form ψ satisfying this condition: Write $A = \oplus_{i=1}^{t} D_i^{n_i \times n_i}$ and let π be a permutation on t points, $\alpha_i \in \operatorname{Aut}(D_i)$ and $u = (u_1, \ldots, u_t) \in A^*$ with $M_i^J = u_i (M_{\pi(i)}^{\alpha_i})^{\operatorname{tr}} u_i^{-1}$, for $M_i \in D_i^{n_i \times n_i}$ (cf. Remark 6.1.3), and $(u_1, \ldots, u_t) = \delta\varepsilon((u_{\pi(1)}^{\alpha})^{\operatorname{tr}}, \ldots, u_{\pi(t)}^{\alpha})^{\operatorname{tr}})$, according to Remark 6.1.5. On $\mathcal{W} \cong \oplus_{i=1}^{t} D_i^{n_i \times 1}$ there exists a non-degenerate $\delta\varepsilon^J$-Hermitian form

$$\psi : \mathcal{W} \times \mathcal{W} \to A, \quad (\oplus_{i=1}^{t} d_i, \oplus_{i=1}^{t} f_i) \mapsto \oplus_{i=1}^{t} d_i (f_{\pi(i)}^{\alpha_i})^{\operatorname{tr}} u_i^{-1}.$$

We show that ψ satisfies condition $(\star\star)$, i.e. that

$$\psi(d_i, f_{\pi(i)}) g_i = \operatorname{Trace}_{A/E}(\psi(g_i, f_{\pi(i)})) d_i$$

for all $d_i, g_i \in D_i^{n_i \times 1} \le \mathcal{W}$ and $f_{\pi(i)} \in D_{\pi(i)}^{n_{\pi(i)} \times 1} \le \mathcal{W}$ (note that $n_{\pi(i)} = n_i$ and $D_{\pi(i)} = D_i$). The element $(f_{\pi(i)}^{\alpha_i})^{\operatorname{tr}} \in D_i^{1 \times n_i}$ and $u_i^{-1} g_i \in D_i^{n_i \times 1}$, hence

$$(f_{\pi(i)}^{\alpha_i})^{\operatorname{tr}} u_i^{-1} g_i = \operatorname{Trace}(u_i^{-1} g_i (f_{\pi(i)}^{\alpha_i})^{\operatorname{tr}}) = \operatorname{Trace}(g_i (f_{\pi(i)}^{\alpha_i})^{\operatorname{tr}} u_i^{-1}),$$

where $\operatorname{Trace} : D_i^{n_i \times n_i} \to D_i$ denotes the usual trace of a matrix. Hence

$$\psi(d_i, f_{\pi(i)}) g_i = d_i (f_{\pi(i)}^{\alpha_i})^{\operatorname{tr}} u_i^{-1} g_i = d_i \operatorname{Trace}(g_i (f_{\pi(i)}^{\alpha_i})^{\operatorname{tr}} u_i^{-1}) = \operatorname{Trace}_{A/E}(g_i (f_{\pi(i)}^{\alpha_i})^{\operatorname{tr}} u_i^{-1}) d_i$$
$$= \operatorname{Trace}_{A/E}(\psi(g_i, f_{\pi(i)})) d_i,$$

which shows that ψ satisfies condition $(\star\star)$.

The functor $\mathcal{F}$ is now obtained by a particular choice of W in Theorem 6.1.10.

Theorem 6.1.11. *Let $\mathfrak{S}$ be a system of representatives for the isomorphism classes of simple left A-modules, and let $\mathcal{W} := \oplus_{S \in \mathfrak{S}} S$. Assume that there exists some $\delta \in \{1, -1\}$ such that every self-dual simple A-module carries a non-degenerate $\delta\varepsilon^J$-Hermitian form. Fix a non-degenerate $\delta\varepsilon^J$-Hermitian form ψ on $\mathcal{W}$ such that $(\mathcal{W}, \psi)$ satisfies condition $(\star\star)$ from Theorem 6.1.10. Then*

$$\mathcal{F} := F_{(\mathcal{W}, \psi)} : \operatorname{Mod}_A^{(A, \varepsilon)} \to \operatorname{Mod}_E^{(E, \delta)}$$

is an equivalence of categories which preserves orthogonality.

Proof. Let $\mathcal{W}^{op}$ be the set $\mathcal{W}$ with a right A-module structure given by $w * a := a^J w$ for $a \in A$ and $w \in \mathcal{W}$. The form

$$\widehat{\psi} : \mathcal{W}^{op} \times \mathcal{W}^{op} \to A, \quad (w, w') \mapsto \delta\varepsilon\psi(w, w')$$

is then non-degenerate and $\delta\varepsilon$-Hermitian, as one easily verifies. Note that $\mathcal{W}^{op}$ is also a left E-module (since $\mathcal{W}$ is a left A-module). Hence we can define a functor

$$H : \mathrm{Mod}_E^{(E,\delta)} \to \mathrm{Mod}_A^{(A,\varepsilon)}, \quad (U,\beta) \mapsto (U \otimes_E \mathcal{W}^{op}, \beta \otimes \widehat{\psi}),$$

where

$$\beta \otimes \widehat{\psi}(u \otimes w, u' \otimes w') := \beta(u', u)\widehat{\psi}(w, w').$$

To prove that $\beta \otimes \widehat{\psi}$ is well-defined, one has to check that it is E-balanced, i.e. that

$$\beta(u'e', ue)\widehat{\psi}(w, w') = \beta(u', u)\widehat{\psi}(ew, e'w')$$

for all $u, u' \in U$, $w, w' \in \mathcal{W}^{op}$ and $e, e' \in E$. This can be proven by calculations analogous to those in the proof of Theorem 6.1.10, exploiting the fact that $E = Z(A)$. In what follows it is shown that H and F are inverse functors.

(i) First, let $(V, \phi) \in \mathrm{Mod}_A^{(A,\varepsilon)}$ and show that $H(F((V,\phi)))$ and (V,ϕ) are isometric. Clearly, $V \otimes_A \mathcal{W} \otimes_E \mathcal{W}^{op} \cong A$ as right A-modules via $\alpha : (v \otimes w \otimes \hat{w}) \mapsto v\widehat{\psi}(w, \hat{w})$. To see that α is an isometry, we calculate that

$$
\begin{aligned}
(\phi &\otimes \psi) \otimes \widehat{\psi}(v \otimes w \otimes \hat{w}, v' \otimes w' \otimes \hat{w}') \\
&= \phi \otimes \psi(v' \otimes w', v \otimes w)\widehat{\psi}(\hat{w}, \hat{w}') \\
&= \mathrm{Trace}_{A/E}(\phi(v, v')\psi(w', w))\delta\varepsilon\psi(\hat{w}, \hat{w}') \\
&= \delta\varepsilon\psi(\mathrm{Trace}_{A/E}(\phi(v, v')\psi(w', w))\hat{w}, \hat{w}') \\
&= \delta\varepsilon\psi(\mathrm{Trace}_{A/E}(\psi(\phi(v, v')w', w))\hat{w}, \hat{w}') \\
&= \delta\varepsilon\psi(\psi(\hat{w}, w)\phi(v, v')w', \hat{w}') \\
&= \delta\varepsilon\psi(\hat{w}, w)\phi(v, v')\psi(w', \hat{w}') \\
&= \delta\varepsilon\phi(v\psi(\hat{w}, w)^J, v'\psi(w', \hat{w}')) \\
&= \delta\varepsilon\phi(v\delta\varepsilon\psi(w, \hat{w}), v'\psi(w', \hat{w}')) \\
&= \phi(v\psi(w, \hat{w}), v'\psi(w', \hat{w}')) \\
&= \phi(v\widehat{\psi}(w, \hat{w}), v'\widehat{\psi}(w', \hat{w}')) \\
&= \phi(\alpha(v \otimes w \otimes \hat{w}), \alpha(v' \otimes w' \otimes \hat{w}'))
\end{aligned}
$$

for all $(v \otimes w \otimes \hat{w})$, $(v' \otimes w' \otimes \hat{w}') \in U \otimes \mathcal{W} \otimes \mathcal{W}^{op}$.

(ii) Now let $(U, \beta) \in \mathrm{Mod}_E^{(E)}$ and show that $F(H((U,\beta)))$ and (U,β) are isometric. The natural isomorphism

$$\gamma : U \otimes_E \mathcal{W}^{op} \otimes_A \mathcal{W} \to U, \quad (u \otimes \hat{w} \otimes w) \mapsto u\,\mathrm{Trace}_{A/E}(\widehat{\psi}(\hat{w}, w))$$

is an isometry since

$$(\beta \otimes \widehat{\psi}) \otimes \psi(u \otimes \hat{w} \otimes w, u' \otimes \hat{w}' \otimes w')$$
$$= \operatorname{Trace}_{A/E}(\beta \otimes \widehat{\psi}(u' \otimes \hat{w}', u \otimes \hat{w})\psi(w, w'))$$
$$= \operatorname{Trace}_{A/E}(\beta(u, u')\widehat{\psi}(\hat{w}'\hat{w})\psi(w, w'))$$
$$= \beta(u, u') \operatorname{Trace}_{A/E}(\widehat{\psi}(\hat{w}', \psi(w', w)\hat{w}))$$
$$= \beta(u, u') \operatorname{Trace}_{A/E}(\delta\varepsilon\psi(\hat{w}', \hat{w})\psi(w, w'))$$
$$= \delta\varepsilon\beta(u, u') \operatorname{Trace}_{A/E}(\psi(\psi(\hat{w}', \hat{w})w, w'))$$
$$= \delta\varepsilon\beta(u, u') \operatorname{Trace}_{A/E}(\psi(\operatorname{Trace}_{A/E}(\psi(w, \hat{w}))\hat{w}', w'))$$
$$= \delta\varepsilon\beta(u, u') \operatorname{Trace}_{A/E}(\psi(w, \hat{w})) \operatorname{Trace}_{A/E}(\psi(\hat{w}', w'))$$
$$= \delta\varepsilon\beta(u \operatorname{Trace}_{A/E}(\psi(w, \hat{w}))^J), u' \operatorname{Trace}_{A/E}(\psi(\hat{w}', w'))$$
$$= \delta\varepsilon\beta(\delta\varepsilon u \operatorname{Trace}_{A/E}(\psi(\hat{w}, w)), u' \operatorname{Trace}_{A/E}(\psi(\hat{w}', w')))$$
$$= \beta(u \operatorname{Trace}_{A/E}(\psi(\hat{w}, w)), u' \operatorname{Trace}_{A/E}(\psi(\hat{w}', w')))$$
$$= \beta(\gamma(u \otimes \hat{w} \otimes w), \gamma(u' \otimes \hat{w}' \otimes w'))$$

for all $(u \otimes \hat{w} \otimes w)$, $(u' \otimes \hat{w}' \otimes w') \in U \otimes \mathcal{W}^{op} \otimes \mathcal{W}$.

$\square$

Example 6.1.12. *Let $A = \mathbb{F}_3 Q_8$, where $Q_8 = \langle x, y \mid x^4 = 1,\ x^2 = y^2,\ xyx = y \rangle$ is the quaternion group. The group algebra A carries an $\mathbb{F}_3$-linear involution J given by $g \mapsto g^{-1}$, for $g \in G$. Let S be the absolutely irreducible A-module of dimension 2, on which x acts as $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and y acts as $\left(\begin{smallmatrix} 1 & -1 \\ -1 & -1 \end{smallmatrix}\right)$. The module S carries a non-degenerate symplectic Q_8-invariant form (i.e. a -1-equivariant form with respect to J) with Gram matrix $B := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Since $\operatorname{End}_A(S) \cong \mathbb{F}_3$, there exists no symmetric non-degenerate G-invariant form on S (cf. Corollary 4.1.24).*

(i) *To determine the number of self-dual codes in the -1-equivariant module*

$$(V, \varphi) = \perp_{i=1}^{4} (S, B) \perp (\mathbb{F}_3^2, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}),$$

let $e_{\mathbb{F}_3}, e_S$ be the central primitive idempotents belonging to the simple modules $\mathbb{F}_3$ and S, respectively. Consider the first summand of V as a module for the algebra $e_S A$, and the second summand as a module for $e_{\mathbb{F}_3} A = \mathbb{F}_3$. The algebras $e_{\mathbb{F}_3} A, e_S A$ have only one irreducible module and hence satisfy the assumption in Theorem 6.1.11, with $\delta = -1$ for $e_{\mathbb{F}_3} A$ and $\delta = 1$ for $e_S A$. The Morita equivalence from Theorem 6.1.11 maps the first summand to the 1-equivariant $\mathbb{F}_3$-module $\perp_{i=1}^{4} (\mathbb{F}_3, (1))$, which contains 8 self-dual codes (cf. Lemma 6.2.6), and the second summand is mapped to itself. The second summand obviously contains 4 self-dual codes. Hence the number of self-dual codes in (V, φ) equals $8 \cdot 4 = 32$.

(ii) *The module $S \oplus S$ carries a 1-equivariant form with Gram matrix $\left(\begin{smallmatrix} 0 & B \\ -B & 0 \end{smallmatrix}\right)$. An application of Theorem 6.1.11 to $e_S A$, with $\delta = -1$ shows that the number of self-dual codes equals the number of self-dual codes in the $\mathbb{F}_3$-module $(\mathbb{F}_3^2, \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right))$, which is 4.*

6.2   Enumeration of self-dual codes

This section gives explicit formulae for the number of self-dual codes in an ε-equivariant A-module, using the Morita equivalence in Theorem 6.1.11.

There exists a central idempotent $e = e^J$ such the algebras eA and $(1-e)A$ satisfy the assumption in Theorem 6.1.11 on the simple modules. Every equivariant A-module (V, ϕ) is an orthogonal sum $eV \perp (1-e)V$, and every self-dual code $C \subseteq V$ is the orthogonal sum of a self-dual code eC in eV and a self-dual code $(1-e)C$ in $(1-e)V$. The number of self-dual codes in V is hence the product of the number of self-dual codes in eV with the number of self-dual codes in $(1-e)V$.

Hence throughout this section assume that A satisfies the assumption in Theorem 6.1.11, and let $\delta \in \{-1, 1\}$ such that every simple self-dual A-module carries a non-degenerate $\delta\varepsilon^J$-equivariant form. The Morita equivalence $\mathcal{F}$ from Theorem 6.1.11 establishes a bijection between the self-dual codes in (V, ϕ) and the self-dual codes in its Morita equivalent module $\mathcal{F}((V, \phi)) \in \mathrm{Mod}_E^{(E, \delta)}$, where $E = Z(A)$ is a direct sum of finite fields.

Except when q is even and J is the identity, $\mathcal{F}((V, \phi))$ will be determined up to isometry by the composition factors of V in Subsection 6.2.1. For every self-dual code $C \leq V$, the image $\mathcal{F}(C) \leq \mathcal{F}(V)$ is a direct sum of self-dual codes over finite fields, or over a ring $L \oplus L$, where L is a finite field. Formulae for the number of these kinds of codes have been given in [41], e.g. and are reproduced in Subsection 6.2.2. As a corollary, the number of self-dual codes in (V, ϕ) is given in Subsection 6.2.3.

To fix some notation, let $\mathfrak{S}$ denote a system of representatives for the isomorphism classes of simple right A-modules. For $S \in \mathfrak{S}$, let $D_S := \mathrm{End}_A(S)$ and let n_S denote the multiplicity of the simple module S in V.

6.2.1   Determination of the Morita equivalent module $\mathcal{F}((V, \phi))$

The module V decomposes into an orthogonal sum, which is respected by the functor $\mathcal{F}$.

Remark 6.2.1. *For $S \in \mathfrak{S}$, denote by V_S the S-homogeneous component of V. Then there is an orthogonal decomposition*

$$V = \perp_{S \in \mathfrak{S}, \, S \cong S^*} V_S \perp_{\{T, T^*\} \subseteq \mathfrak{S}, \, T \not\cong T^*} (V_T \oplus V_{T^*}). \qquad (\star)$$

In particular, the restriction ϕ_U of ϕ to a summand U in $(\star)$ is non-degenerate and equivariant, and if $C \leq V$ is a self-dual code then $C \cap U$ is a self-dual code in U with respect to ϕ_U.

Lemma 6.2.3 gives the images under $\mathcal{F}$ of the orthogonal summands of V. To this aim the following result proven in [34] is useful.

Lemma 6.2.2. *Let $e_S \in Z(A)$ be the central primitive idempotent belonging to the simple module $S \in \mathfrak{S}$. Then $e_S^J = e_{S^*}$. In particular S is self-dual if and only if $e_S^J = e_S$.*

Lemma 6.2.3. *Let $S \in \mathfrak{S}$, and let e_S be the central primitive idempotent belonging to S. Let n be an integer, and by $\mathcal{F}$ denote the Morita equivalence from Theorem 6.1.11.*

(i) *Assume that $S \cong S^*$. There is a natural isomorphism $D_S \cong e_S Z(A)$, of which the image is invariant under J according to Lemma 6.2.2. Thus J induces an involution ad_S on D_S, which will be further investigated in Lemma 6.2.4.*

Assume that S^n carries a non-degenerate ε-equivariant form β. Then $\mathcal{F}((S^n, \beta)) \cong ((D_S)^n, \beta')$, where β' is δ-equivariant with respect to ad_S.

If (S^n, β) contains a self-dual code then so does $((D_S)^n, \beta')$, since $\mathcal{F}$ preserves orthogonality. In odd characteristic, this determines the isometry type of $((D_S)^n, \beta')$, as follows:

   (a) *If $\delta = 1$ then $((D_S)^n, \beta') \cong \perp_{i=1}^{\frac{n}{2}} \mathbb{H}(D_S) \cong \perp_{i=1}^{\frac{n}{2}} ((D_S)^2, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right))$ is an orthogonal sum of hyperbolic planes $\mathbb{H}(D_S)$ (cf. [37, Ch.1, Cor. 3.10, Th.6.4 and Ch.7, Th. 6.3]).*

   (b) *If $\delta = -1$ then $((D_S)^n, \beta') \cong \perp_{i=1}^{\frac{n}{2}} ((D_S)^2, \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right))$.*

Analogously, if $\mathbb{F}$ has characteristic 2 and ad_S is not the identity then $((D_S)^n, \beta')$ is an orthogonal sum of hyperbolic planes.

If $\mathbb{F}$ has characteristic 2 and ad_S is the identity then either $((D_S)^n, \beta')$ is an orthogonal sum of hyperbolic planes as above, or isometric to $\perp_{i=1}^{\frac{n}{2}-1} \mathbb{H}(D_S) \perp W$, where $W \cong (\mathbb{F}^2, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))$.

(ii) *Assume that $S \not\cong S^*$, and consider again the natural isomorphism $D_S \cong e_S Z(A)$. Then $D_S^J = D_{S^*}$ according to Lemma 6.2.2 and hence the sum $D_S \oplus D_{S^*}$ is invariant under J. Clearly with respect to any non-degenerate ε-equivariant form β, the module $(S \oplus S^*)^n$ contains a self-dual code. The Morita equivalent module*

$$\mathcal{F}((S \oplus S^*)^n, \beta) \cong ((D_S)^n \oplus (D_S)^n, \beta') \cong \perp_{i=1}^{n} \mathbb{H}(D_S)$$

is an orthogonal sum of hyperbolic planes, where β' is equivariant with respect to the restriction of J to $D_S \oplus D_{S^*}$. Here $(D_S)^n \oplus (D_{S^*})^n$ is a $(D_S \oplus D_{S^*})$-module in the natural way. Hence the self-dual codes in this module correspond bijectively to the subspaces of $(D_S)^n$.

Lemma 6.2.4. *For a simple self-dual A-module S consider the natural embeddings $\mathbb{F} \hookrightarrow D_S \hookrightarrow Z(A)$. According to Lemma 6.2.3(i) the involution J on A restricts to an involution on D_S. This restriction is either the identity on D_S or a field automorphism of order 2. Clearly the latter holds if J is non-trivial on $\mathbb{F}$.*

Assume that $f^J = f$ for all $f \in \mathbb{F}$. Then the following are equivalent.

(i) *$d^J = d$ for all $d \in D_S$,*

(ii) *if $L \supseteq \mathbb{F}$ is a field extension with $L \cong D_S$ then every composition factor of the right $A \otimes_{\mathbb{F}} L$-module $S \otimes_{\mathbb{F}} L$ is self-dual.*

Proof. Let $A_L := A \otimes_{\mathbb{F}} L$ and let $J^{(L)}$ be the L-linear extension of J to A_L defined by $(a \otimes l)^J := a^J \otimes l$ for all $a \in A$ and $l \in L$, which is well-defined since $\mathbb{F}$ is fixed by J. In particular J is trivial on $D_S \subseteq A$ if and only if $J^{(L)}$ is trivial on $D_S \otimes_{\mathbb{F}} L$. Let $e \in D_S$ be the central primitive idempotent belonging to S, and let $e = e_1 + \ldots + e_n$ be a decomposition into central primitive idempotents e_i of A_L, according to a decomposition of $S \otimes_{\mathbb{F}} L$ into simple modules over $D_S \otimes_{\mathbb{F}} L$. The e_i generate $D_S \otimes_{\mathbb{F}} L$ as a vector space over L and hence $J^{(L)}$ is trivial on $D_S \otimes_{\mathbb{F}} L$ if and only if it fixes all of the e_i, i.e. if and only if every composition factor $e_i A_L$ of $S \otimes_{\mathbb{F}} L$ satisfies $e_i A_L = e_i^J A_L \cong (e_i A_L)^*$ (see Lemma 6.2.2). $\qquad\square$

6.2.2   Enumeration of self-dual codes over finite fields

The formulae in this section are given in [41].

Lemma 6.2.5. *(see Ex. 10.4 of [41]) Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, where $q = r^2$, and let $^r : x \mapsto x^r \in \mathcal{G}al(\mathbb{F}_q/\mathbb{F}_r)$ be the field automorphism of order 2. Let β be a non-degenerate form on $\mathbb{F}^n$ which is equivariant with respect to ^{r}. If $(\mathbb{F}^n, \beta)$ contains a self-dual code then the number of self-dual codes in $\mathbb{F}^n$ equals*

$$\Upsilon_u(n,q) := \prod_{i=1}^{n} (q^{\frac{i}{2}} - (-1)^i) \, (\prod_{j=1}^{\frac{n}{2}} (q^j - 1))^{-1}. \tag{6.3}$$

Lemma 6.2.6. *(see Ex. 11.3 of [41]) Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, where q is odd, and let β be a non-degenerate symmetric bilinear form on $\mathbb{F}^n$. If $(\mathbb{F}^n, \beta)$ contains a self-dual code then the number of self-dual codes in $\mathbb{F}^n$ equals*

$$\Upsilon_{o,1}^+(n,q) := \prod_{i=0}^{\frac{n}{2}-1} (q^i + 1). \tag{6.4}$$

Lemma 6.2.7. *(see Ex. 8.1 of [41]) Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, where q is odd, and let β be a non-degenerate symplectic bilinear form on $\mathbb{F}^n$, i.e. $\beta(v,w) = -\beta(w,v)$ for all $v,w \in \mathbb{F}^n$. Then $(\mathbb{F}^n, \beta)$ contains a self-dual code, and the number of self-dual codes equals*

$$\Upsilon_{o,-1}^+(n,q) := \prod_{i=0}^{\frac{n}{2}-1} (q^{n-2i} - 1)(q^{i+1} - 1)^{-1}. \tag{6.5}$$

Lemma 6.2.8. *(see Ex. 11.3 of [41]) Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, where q is even, and let β be a non-degenerate symmetric bilinear form on $\mathbb{F}^n$ such that $(\mathbb{F}^n, \beta) \cong \perp_{i=1}^{\frac{n}{2}} \mathbb{H}(\mathbb{F})$ is an orthogonal sum of hyperbolic planes, i.e. isotropic. Then the number of self-dual codes in $\mathbb{F}^n$ equals*

$$\Upsilon_o^+(n,q) := \prod_{i=1}^{\frac{n}{2}} (q^i + 1). \tag{6.6}$$

The following lemma is an immediate corollary of Lemma 6.2.8.

Lemma 6.2.9. *Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, where q is even. Let β be a non-degenerate symmetric bilinear form on $\mathbb{F}^n$ such that $(\mathbb{F}^n, \beta) \cong \perp_{i=1}^{\frac{n}{2}-1} \mathbb{H}(\mathbb{F}) \perp W$, where $W \cong (\mathbb{F}^2, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))$. Then the number of self-dual codes in $\mathbb{F}^n$ equals*

$$\Upsilon_o^-(n, q) := \Upsilon_o^+(n - 2, q).$$

Moreover, we need a formula for the number of subspaces of a vector space, cf. Lemma 6.2.3 (ii).

Lemma 6.2.10. *Let U be a vector space over the finite field $\mathbb{F} = \mathbb{F}_q$, $n := \dim(U)$. Then the number of subspaces of U equals*

$$\Xi(n, q) := \sum_{k=0}^n \prod_{i=0}^{n-k-1} \frac{q^{n-i} - 1}{q^{n-k-i} - 1}.$$

6.2.3 Enumeration of self-dual codes in (V, β)

As before, let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements and let A be a finite semisimple algebra over $\mathbb{F}$. Let $\mathfrak{S}$ be a system of representatives for the isomorphism classes of simple right A-modules, and for $S \in \mathfrak{S}$ let $d_S := \dim_\mathbb{F}(\mathrm{End}_A(S))$. By n_S denote the multiplicity of S in V. Recall that we assume the existence of some $\delta \in \{-1, 1\}$ such that every simple self-dual A-module carries a $\delta\varepsilon^J$-equivariant form. The involution J restricts to an involution of the Morita equivalent algebra $E = Z(A) = \oplus_{S \in \mathfrak{S}} \mathrm{End}_A(S)$ (cf. Lemma 6.2.4), and also to a field automorphism of $\mathbb{F}$ (cf. Remark 6.1.3), where $\mathbb{F}$ is naturally embedded into $Z(A)$ by $f \mapsto f \cdot 1$. The restriction to $\mathbb{F}$ is either the identity or a field automorphism of order 2 – we distinguish these two cases to enumerate the self-dual codes in $(V, \beta) \in \mathrm{Mod}_A^{(\mathbb{F}, \varepsilon)}$, which in what follows is assumed to contain at least one such code. As corollaries from the previous Subsections we obtain the following formulae.

Corollary 6.2.11. *If $q = r^2$ and $f^J = f^r$ for all $f \in \mathbb{F}_q$ then the number of self-dual codes in (V, β) equals*

$$M_{(V,\beta)} = \prod_{S \in \mathfrak{S},\, S \cong S^*} \Upsilon_u(n_S, q^{d_S}) \prod_{\{T,T^*\} \subseteq \mathfrak{S},\, T \not\cong T^*} \Xi(n_T, q^{d_T}).$$

Corollary 6.2.12. *Assume that q is odd and $f^J = f$ for all $f \in \mathbb{F}$. This implies $\varepsilon \in \{1, -1\}$. Let*

$$\mathfrak{S}' := \{S \in \mathfrak{S} \mid S \cong S^* \text{ and } e^J = e \text{ for all } e \in \mathrm{End}_A(S)\}.$$

Then the number of self-dual codes in (V, β) equals

$$M_{(V,\beta)} = \prod_{S' \in \mathfrak{S}'} \Upsilon_{o,\delta}^+(n_{S'}, q^{d_{S'}}) \prod_{S \in \mathfrak{S} - \mathfrak{S}',\, S \cong S^*} \Upsilon_u(n_S, q^{d_S}) \prod_{\{T,T^*\} \subseteq \mathfrak{S},\, T \not\cong T^*} \Xi(n_T, q^{d_T}).$$

In the remaining case where q is even and β is symmetric (which implies that $\varepsilon = 1$), it is in general not possible to determine $\mathcal{F}((V, \beta))$ only from the composition factors of V, cf. Lemma 6.2.3(i). Yet this is possible if $A = \mathbb{F}G$ is a group algebra over the finite group G. It is well-known that if the field L, of even characteristic, is a splitting field for the finite group G of odd order then the trivial module is the only self-dual irreducible LG-module. An application of Lemma 6.2.4 then yields that the restriction of J to $Z(A) = E = \oplus_{S \in \mathfrak{S}} \mathrm{End}_A(S)$ is nontrivial on every of these summands, except for the summand belonging to the trivial module. To investigate the number of self-dual codes in this summand under $\mathfrak{F}$ one has to distinguish whether (V, β) is symplectic, i.e. whether $\beta(v, v) = 0$ for all $v \in V$. Note that this only depends on the values of β on the summands of V isomorphic to the trivial module, by the following remark.

Remark 6.2.13. *Let (V, β) be an equivariant $\mathbb{F}G$-module, where $\mathbb{F}$ has characteristic 2 and the associated involution restricts to the identity on $\mathbb{F}$. If the trivial module does not occur in V then β is symplectic.*

Proof. The map $Q : V \to \mathbb{F}$, $v \mapsto \beta(v, v)$ is additive since β is symmetric and $\mathbb{F}$ has characteristic 2. Moreover, $Q(v) = Q(vg)$ for all $v \in V$ and all $g \in G$. Assume that there exists some $v \in V$ with $\beta(v, v) = 1$. Then Q is surjective, and hence there exists an epimorphism of V onto the trivial G-module, which contradicts the assumptions. Hence $Q(V) = \{0\}$, i.e. β is symplectic. $\square$

As an application of Lemma 6.2.3 one obtains

Corollary 6.2.14. *Assume that $A = \mathbb{F}_q G$ is a group algebra over the finite group G, where q is even and G has odd order, and that $f^J = f$ for all $f \in \mathbb{F}$. By $\mathbf{1}$ denote the trivial $\mathbb{F}G$-module. The number of self-dual codes in (V, β) equals*

$$M_{(V, \beta)} = \Upsilon_o^\sigma(n_{\mathbf{1}}, q) \prod_{S \in \mathfrak{S},\, \mathbf{1} \not\cong S \cong S^*} \Upsilon_u(n_S, q^{d_S}) \prod_{\{T, T^*\} \subseteq \mathfrak{S},\, T \not\cong T^*} \Xi(n_T, q^{d_T}),$$

where $\sigma = +$ if (V, β) is symplectic, and $\sigma = -$ otherwise.

6.2.4   Example: Binary extended cyclic codes

Let $\mathbb{F} = \mathbb{F}_2$ and $A = \mathbb{F}C_N$, where C_N is the cyclic group of order N, for some odd integer N. A binary extended cyclic code, as defined in [28], is an A-submodule of

$$V = A \oplus \mathbf{1} = \mathbb{F}^{N+1},$$

where $\mathbf{1}$ is the trivial A-module, i.e. C_N acts on V by cyclic shifts of the first N coordinates and fixes the $(N + 1)$st coordinate. The standard scalar product β on V satisfies $\beta(v, v') = \beta(vg, v'g)$ for all $v, v' \in V$ and $g \in C_N$, hence is equivariant with respect to the $\mathbb{F}$-linear involution on $\mathbb{F}C_N$ given by $g \mapsto g^{-1}$, for $g \in C_N$.

The situation where a self-dual binary extended cyclic code exists has been characterized in [28] as follows.

Theorem 6.2.15. *There exists a self-dual binary extended cyclic code $C \leq V = \mathbb{F}C_N \oplus \mathbf{1}$ if and only if $-1 \notin \langle 2 \rangle \leq (\mathbb{Z}/p\mathbb{Z})^*$ for all prime divisors p of N, i.e. the order of $2 \bmod p$ is odd.*

Remark 6.2.16. *If the order of $2 \bmod p$ is odd then 2 is a square $\bmod p$ and hence $p \equiv_8 \pm 1$ by quadratic reciprocity. If $p \equiv_8 -1$ then -1 is not a square and hence $-1 \notin \langle 2 \rangle \leq (\mathbb{Z}/p\mathbb{Z})^*$. However, if $p \equiv_8 1$ then the order of 2 may be even or odd $\bmod p$. For $p = 41$ the order of 2 is 20, for $p = 73$ the order is 9.*

The structure of the module $V = \mathbb{F}C_N$ is easy to describe and the number of self-dual codes in V is particularly easy to determine, cf. Example 6.2.17. The criterion for the existence of a self-dual binary extended cyclic code in Example 6.2.17 has been given in [27, Th. 3.3] in a more general context.

Example 6.2.17. *There exists a self-dual binary extended cyclic code $C \leq V = \mathbb{F}C_N \oplus \mathbf{1}$ if and only if the trivial module is the only self-dual irreducible $\mathbb{F}C_N$-module. In this case there are*

$$M_{(V,\beta)} = 2^{\frac{|\mathfrak{S}|-1}{2}}$$

such codes, where $\mathfrak{S}$ is a system of representatives for the isomorphism classes of simple right $\mathbb{F}C_N$-modules.

Proof. Assume that there exists a self-dual code $C \leq V$. Then according to [42], Corollary 2.4, every self-dual simple $\mathbb{F}C_N$-module occurs in a composition series of V with even multiplicity. On the other hand, every simple $\mathbb{F}C_N$-module occurs in V with multiplicity 1, except for the trivial module, which occurs in V with multiplicity 2. Hence

$$V \cong \perp_{\{T,T^*\} \subseteq \mathfrak{S},\, T \not\cong \mathbf{1}} (T \oplus T^*) \perp \mathbf{1} \perp \mathbf{1}. \qquad (\bigstar)$$

Conversely, if the trivial module is the only self-dual irreducible $\mathbb{F}C_N$-module then clearly V decomposes as in $(\bigstar)$. Let $T \oplus T^*$ be a summand in $(\bigstar)$ and let e be the central primitive idempotent belonging to T. Then e^J is the central primitive idempotent belonging to T^* according to Remark 6.2.2, hence annihilates T. Thus

$$\beta(t,t') = \beta(te,t') = \beta(t,t'e^J) = \beta(t,0) = 0$$

for all $t, t' \in T$, i.e. $T \subseteq T^\perp$. Choose a subset $\mathcal{T} \subseteq \mathfrak{S} - \{\mathbf{1}\}$ such that for every non-trivial irreducible A-module T, either T or T^* is contained in $\mathcal{T}$. Then

$$C := \langle T \mid T \in \mathcal{T} \rangle + \langle (1, \dots, 1) \rangle$$

is a self-dual code in V. An application of Corollary 6.2.14 then yields

$$M_{(V,\beta)} = \Upsilon_o^-(2,2) \prod_{\{T,T^*\} \subseteq \mathfrak{S},\, T \not\cong \mathbf{1}} \Xi(1, 2^{d_T}) = 2^{\frac{|\mathfrak{S}|-1}{2}},$$

where the value of $d_T = \dim(\mathrm{End}_A(T))$ is irrelevant since $\Xi(1, 2^{d_T})$ counts the number of subspaces of a one-dimensional vector space over a field of size 2^{d_T}. $\square$

Example 6.2.18. *(i)* ***Binary extended cyclic codes of length*** 8***.*** *The order of* 2 *in the unit group* $\mathbb{F}_7^*$ *of* $\mathbb{F}_7$ *equals* 3*. More precisely, the subgroup of* $\mathbb{F}_7^*$ *generated by* 2 *has index* 2 *and the cosets are* $\mathbb{F}_7^* = \{1, 2, 4\} \ \dot{\cup} \ \{3, 5, 6\}$*. This yields central primitive idempotents* $e, f \in \mathbb{F}_2 C_7$*,*

$$e = 1 + a + a^2 + a^4 \quad and \quad f = 1 + a^3 + a^5 + a^6,$$

where a *is a generator of* C_7*. These satisfy* $ef = 0$ *and* $e^J = f$*. Hence* $V = \mathbb{F}_2 C_7 \oplus \mathbb{F}_2 = \mathbb{F}_2^8$ *contains exactly the two self-dual codes*

$$C = \langle Ve, (1, \dots, 1) \rangle \quad and \quad D = \langle Vf, (1, \dots, 1) \rangle$$

with generator matrices

$$M_C := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \quad and \quad M_D := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

These codes are permutation equivalent to the extended Hamming code of length 8*.*

(ii) *Let* p *be a prime with* $p \equiv_8 -1$*. Then there exist exactly* $2^{\frac{t}{2}}$ *self-dual binary extended cyclic codes of length* $p + 1$*, where* $t := [\mathbb{F}_p^* : \langle 2 \rangle]$ *is the index of the subgroup generated by* 2 *in the unit group* $\mathbb{F}_p^*$ *of* $\mathbb{F}_p$*.*

(iii) ***Self-dual binary codes over*** $\mathbb{F}_2(C_3 \wr C_3)$***.*** *The wreath product*

$$G := C_3 \wr C_3 = \langle (1, 2, 3), \ (4, 5, 6), \ (7, 8, 9), \ (1, 4, 7)(2, 5, 8)(3, 6, 9) \rangle$$

acts on 9 *points, hence yields a permutation module* $\widetilde{V}$ *of dimension* 9 *over* $A = \mathbb{F}_2 G$*. Let* $V := \widetilde{V} \oplus \widetilde{V} \oplus \mathbf{1} \oplus \mathbf{1}$*, then* V *decomposes as*

$$V = T_6^2 \perp T_2^2 \perp \mathbf{1}^4,$$

where T_2 *and* T_6 *are irreducible modules of dimension* 2 *and* 6 *over* $\mathbb{F}_2$*, both self-dual with an endomorphism ring isomorphic to* $\mathbb{F}_4$*. Hence the total number of self-dual codes in* V *equals*

$$M_V = \Upsilon_o^-(4, 2) \ \cdot \ \Upsilon_u(2, 4)^2 = 3^3 = 27.$$

6.2.5   Example: Doubly-even binary codes

Recall the notion of doubly-even binary codes in $\mathbb{F}_2^N$, in Section 2.2.2. Assume that N is a multiple of 8, i.e. there exists a self-dual doubly-even binary code of length N. In this section we view a code C as a module over the group algebra $\mathbb{F}_2 G$, where G is a subgroup of the *permutation group*

$$P(C) := \{ \pi \in S_N \mid C\pi = C \}.$$

For a given permutation group $G \leq S_N$, we ask for the number of self-dual doubly-even codes with $G \subseteq P(C)$, i.e. for the doubly-even self-dual codes in the $\mathbb{F}_2 G$-module $V := \mathbb{F}_2^N$. We confine ourselves to the case where the order of G is odd, i.e. the group algebra $\mathbb{F}_2 G$ is semisimple, in order to apply the results of Section 6.1. Hence in what follows assume that the order of G is odd. Theorem 6.2.21 gives the number of G-invariant doubly-even self-dual codes, provided that there exists at least one such code. (Recall that according to Theorem 3.2, such a code exists if and only if N is a multiple of 8 and there exists any self-dual code in $\mathbb{F}_2^N$.)

The group algebra $\mathbb{F}_2 G$ carries an $\mathbb{F}_2$-linear involution given by $g \mapsto g^{-1}$, for $g \in G$, and the standard scalar product β is equivariant with respect to this involution. Recall that the doubly-even codes in $\mathbb{F}_2^N$ correspond to the totally isotropic subspaces of the quadratic space $(\widetilde{V}, q)$, where

$$\widetilde{V} = \langle (1, \ldots, 1) \rangle^{\perp} / \langle (1, \ldots, 1) \rangle = \{v \in \mathbb{F}_2^N \mid \mathrm{wt}(v) \text{ is even}\} / \langle (1, \ldots, 1) \rangle,$$

naturally is a G-module, for every permutation group G of degree N. The quadratic form is

$$q : \widetilde{V} \to \mathbb{F}_2, \quad v + \langle (1, \ldots, 1) \rangle \mapsto \frac{\mathrm{wt}(v)}{2} \mod 2,$$

with polar form

$$(\widetilde{v}, \widetilde{v}') \mapsto q(\widetilde{v} + \widetilde{v}') - q(\widetilde{v}) - q(\widetilde{v}') = \widetilde{\beta}(\widetilde{v}, \widetilde{v}'),$$

where $\widetilde{\beta}$ is the non-degenerate equivariant bilinear form on $\widetilde{V}$ naturally induced by β via

$$\widetilde{\beta} : \widetilde{V} \times \widetilde{V} \to \mathbb{F}_2, \quad (v + \langle (1, \ldots, 1) \rangle, v' + \langle (1, \ldots, 1) \rangle) \mapsto \beta(v, v').$$

As seen in Section 3.2, a self-dual code $C \leq V$ is doubly-even if and only if q vanishes on $C / \langle (1, \ldots, 1) \rangle \leq \widetilde{V}$, i.e. $C / \langle (1, \ldots, 1) \rangle$ is maximally isotropic.

Again, let $\mathfrak{S}$ be a system of representatives for the isomorphism classes of simple right $\mathbb{F}_2 G$-modules. Consider the decomposition

$$\widetilde{V} = \perp_{S \in \mathfrak{S}, \, S \cong S^*} \widetilde{V}_S \perp_{\{T, T^*\} \subseteq \mathfrak{S}, \, T \not\cong T^*} \widetilde{V}_{T \oplus T^*},$$

where $\widetilde{V}_X$ is the X-homogeneous component of $\widetilde{V}$, for $X \in \mathfrak{S}$, and $\widetilde{V}_{T \oplus T^*} = \widetilde{V}_T \oplus \widetilde{V}_{T^*}$. Then every maximally isotropic submodule $\widetilde{C} \leq \widetilde{V}$ is of the form

$$\widetilde{C} = \perp_{S \in \mathfrak{S}, \, S \cong S^*} \left(C \cap \widetilde{V}_S \right) \perp_{\{T, T^*\} \subseteq \mathfrak{S}, \, T \not\cong T^*} \left(C \cap \widetilde{V}_{T \oplus T^*} \right), \qquad (\ast)$$

and every summand $C \cap \widetilde{V}_S$ or $C \cap \widetilde{V}_{T \oplus T^*}$ is a maximally isotropic submodule of $\widetilde{V}_S$ or $\widetilde{V}_{T \oplus T^*}$, respectively, since q is linear on $\widetilde{C}$. Hence the total number of maximally isotropic submodules of $\widetilde{V}$ is the product of the number of maximally isotropic submodules in the summands of $(\ast)$.

Theorem 6.2.19. *Let $U \leq \widetilde{V}$ be a submodule such that the trivial module $\mathbf{1}$ does not occur in U. Then every self-dual code in U is doubly-even.*

Proof. Let $\widetilde{C} = \widetilde{C}^{\perp} \leq U$ be a self-dual code. Then q is linear on $\widetilde{C}$, i.e. $q \in \mathrm{Hom}_{\mathbb{F}_2 G}(\widetilde{C}, \mathbf{1})$ with kernel

$$\ker(q) = \{c \in \widetilde{C} \mid \mathrm{wt}(c) \equiv_4 0\} =: \widetilde{C}_0,$$

the doubly-even subcode of $\widetilde{C}$. The image of q is isomorphic to a factor module of $\widetilde{C}$. Since $\mathbf{1}$ does not occur in $\widetilde{C}$, this enforces that q vanishes on $\widetilde{C}$, i.e. $\widetilde{C} = \widetilde{C}_0$ is doubly-even. $\qquad\square$

Now consider the quadratic space $(\widetilde{V}_{\mathbf{1}}, q_{\mathbf{1}}) \cong (\mathbb{F}_2^n, q_{\mathbf{1}})$, with non-degenerate polar form $\widetilde{\beta}_{\mathbf{1}}$, the restriction of $\widetilde{\beta}$ to $\widetilde{V}_{\mathbf{1}}$. Clearly V contains a doubly-even self-dual code if and only if $(\widetilde{V}_{\mathbf{1}}, q_{\mathbf{1}})$ has Witt defect 0. The total number of maximally isotropic subspaces is then well-known and given in [41], for instance.

Theorem 6.2.20. *(see Ex. 11.3 of [41]) Let $n := \dim(\widetilde{V}_{\mathbf{1}})$. If V contains a doubly-even self-dual code then the number of maximally isotropic subspaces of $(\widetilde{V}_{\mathbf{1}}, q_{\mathbf{1}})$ equals*

$$\varpi(n) := \prod_{i=0}^{\frac{n}{2}-1} (2^i + 1).$$

Theorem 6.2.19 and 6.2.20 now enable us to determine the number of doubly-even self-dual codes in V from the composition factors of V. Again, for a simple module $X \in \mathfrak{S}$, denote by n_X the multiplicity of X in V.

Theorem 6.2.21. *If (V, β) contains a doubly-even self-dual code then the total number of doubly-even self-dual codes in V equals*

$$M_{(V,\beta)}^{\mathrm{II}} = \varpi(n_{\mathbf{1}} - 2) \prod_{S \in \mathfrak{S},\, \mathbf{1} \not\cong S \cong S^*} \Upsilon_u(n_S, q^{d_S}) \prod_{\{T,T^*\} \subseteq \mathfrak{S},\, T \not\cong T^*} \Xi(n_T, q^{d_T}).$$

6.3　The mass formula

For a right A-module V carrying an equivariant form β (cf. Definition 6.1.4), let

$$\mathfrak{C}(V) := \{C \leq V \mid C = C^{\perp} = \{v \in V \mid \beta(v, c) = 0 \text{ for all } c \in C\}\}.$$

One may be interested in an overview of the isometry types or weight distributions which occur here, rather than in the set $\mathfrak{C}(V)$ itself. Hence in what follows, we define a finite group $\mathrm{Aut}(V)$ acting on $\mathfrak{C}(V)$ such that properties like the isometry type of $C \in \mathfrak{C}(V)$ or the weight distribution are left invariant under the operation of suitable subgroups of $\mathrm{Aut}(V)$.

6.3.1 Weak isometries of V and the mass formula

Definition 6.3.1. *A bijective additive map $\psi : V \to V$ is called a* weak isometry *of V if $\beta(v, v') = \beta(\psi(v), \psi(v'))$ and $\psi(va) = \psi(v)a^\alpha$ for some automorphism α of A and all $v, v' \in V$. The weak isometries form a group $\mathrm{WAut}(V)$, with the composition as multiplication, which contains as a subgroup $\mathrm{Aut}(V) := \mathrm{End}_A(V) \cap \mathrm{WAut}(V)$, the isometries of V.*

Clearly $\mathrm{WAut}(V)$ acts on $\mathfrak{C}(V)$. Now consider the action of some subgroup $\Gamma \leq \mathrm{WAut}(V)$. By $[C]$ denote the orbit containing C. If

$$\Gamma(C) = \{\psi \in \Gamma \mid \psi(C) = C\}$$

is the stabilizer of C in Γ then $[C]$ has length $[\Gamma : \Gamma(C)]$ and we obtain

Theorem 6.3.2. (Mass formula)

$$\frac{M_V}{|\Gamma|} = \sum_{[C] \subseteq \mathfrak{C}(V)} \frac{1}{|\Gamma(C)|}.$$

The mass formula gives a method of classifying the self-dual codes in V with respect to a property which is an invariant of the action of Γ on $\mathfrak{C}(V)$ – one may restrict to orbit representatives and weight them by the reciprocal order of their automorphism group, until the value of the left hand side of Theorem 6.3.2 has been reached. For instance, the group $\mathrm{Aut}(V)$ has the isometry type of $C \in \mathfrak{C}(V)$ as an invariant and hence Equation (6.3.2) can be used to classify the self-dual codes in V up to isometry.

6.3.2 Example: Permutation modules

Let $A = \mathbb{F}G$ be a semisimple group algebra over the finite group G and let V be a permutation module for G, i.e. $V = \mathbb{F}^N$ has a distinguished basis, with respect to which G acts as permutations and which we assume to be an orthonormal basis. The existence of a distinguished basis enables us to define the *weight enumerator* of a code $C \leq V$,

$$\mathrm{cwe}(C) = \sum_{(c_1, \ldots, c_N) \in C} \prod_{i=1}^{N} x_{c_i} \ \in \mathbb{C}[x_f : \ f \in \mathbb{F}].$$

The weight enumerator contains information on C which is of interest in coding theory, like the minimum weight of C. It is invariant under permutations of the coordinates of C, that is, $\mathrm{cwe}(C\pi) = \mathrm{cwe}(C)$ for all $C \in \mathfrak{C}(V)$ and $\pi \in S_N$. In general, the permutation equivalent code $C\pi$ is not contained in $\mathfrak{C}(V)$, i.e. S_N does not act on $\mathfrak{C}(V)$.

If V is faithful then the action of G on V induces an embedding $j : G \hookrightarrow S_k$. Let

$$\mathfrak{N} := N_{S_k}(G) \leq \mathrm{WAut}(V)$$

be the normalizer of $j(G)$ in S_k. Every $\eta \in \mathfrak{N}$ naturally induces a bijection $v \mapsto v\eta$ of V. This bijection is a weak automorphism of V since if α_η is the $\mathbb{F}$-linear automorphism of $A = \mathbb{F}G$ given by $g \mapsto \alpha_\eta(g) = \eta^{-1}g\eta$ then

$$v g \eta = v \eta \eta^{-1} g \eta = v \eta \alpha_\eta(g)$$

for all $v \in V$ and $g \in G$. Hence $\mathfrak{N}$ acts on $\mathfrak{C}(V)$, yielding a mass formula

$$\frac{M_V}{|\mathfrak{N}|} = \sum_{[C]_\mathfrak{N} \subseteq \mathfrak{C}(V)} \frac{1}{|\mathfrak{N}(C)|}, \qquad (\ast)$$

where $[C]_\mathfrak{N}$ is the orbit of $\mathfrak{N}$ containing C and $\mathfrak{N}(C)$ is the stabilizer of C under $\mathfrak{N}$. Clearly the weight enumerator is an invariant of this operation. Another invariant is the conjugacy class of $P(C)$ in S_N, since $P(C\eta) = \eta^{-1}P(C)\eta$ for every $\eta \in \mathfrak{N}$. In general there is no larger subgroup $\mathcal{U}$ with $\mathfrak{N} \subsetneq \mathcal{U} \subseteq S_k$ such that $\mathcal{U}$ acts on $\mathfrak{C}(V)$, since every element which acts on $\mathfrak{C}(V)$ normalizes the *Bravais group* $\mathcal{B}(V) := \cap_{C \in \mathfrak{C}(V)} P(C)$, cf. Theorem 6.3.3.

Theorem 6.3.3. *If $\mathcal{B}(V) = G$ then $\mathfrak{N}$ is the largest subgroup of S_k which acts on $\mathfrak{C}(V)$.*

Proof. Let $\pi \in S_k$ such that π acts on $\mathfrak{C}(V)$. Then $\pi \in \mathfrak{N}$ since

$$G = \mathcal{B}(V) = \cap_{C \in \mathfrak{C}(V)} P(C\pi) = \pi^{-1}(\cap_{C \in \mathfrak{C}(V)} P(C))\pi = \pi^{-1}\mathcal{B}(V)\pi = \pi^{-1}G\pi.$$

$\square$

Example 6.3.4. *Self-dual binary codes of length 48 with an automorphism of order 23. The extended quadratic residue code $q_{48} \leq \mathbb{F}_2^{48}$ is, up to permutation equivalence, the only self-dual $[48, 24, 12]$-code, i.e. the only extremal binary self-dual code of length 48, cf. for instance [36]. The code q_{48} has an automorphism $\sigma \in S_{48}$ of order 23 which acts on the coordinates of q_{48} with four orbits. Hence q_{48} is a submodule of*

$$V = \mathbb{F}_2 C_{23} \oplus \mathbb{F}_2 C_{23} \oplus \mathbf{1} \oplus \mathbf{1}$$

over the semisimple algebra $A = \mathbb{F}_2 C_{23}$. The algebra A has three irreducible modules, which are the trivial module $\mathbf{1}$, a module T of dimension 11 and its dual $T^* \not\cong T$ with an endomorphism ring of dimension $d_T = 11$. Hence V has a decomposition $V = \mathbf{1}^4 \perp (T \oplus T^*)^2$ and the total number of self-dual codes in V equals

$$M_V = \Upsilon_o^-(4, 2) \; \Xi(2, 2^{11}) = 3 \cdot (2^{11} + 3) = 6153.$$

Considering normalizer equivalence, i.e. the orbits of $N_{S_{48}}(\sigma)$ on the set $\mathfrak{C}(V)$ of all self-dual codes in V, there are only 14 equivalence classes of codes. Representatives $C_1, \ldots, C_{14}$ for these classes can easily be computed in MAGMA ([3]) using the mass formula $(\ast)$, which then is

$$\frac{6153}{46552} = 4 \cdot \frac{1}{92} + \frac{1}{2024} + 2 \cdot \frac{1}{23276} + \frac{1}{1012} + 4 \cdot \frac{1}{46} + 2 \cdot \frac{1}{11638}.$$

The below-mentioned tabular lists the stabilizer orders $\mathfrak{N}(C_i)$ of the codes $C_1, \ldots, C_{14}$ and gives the number of words of weight 24 in each code, which is helpful to distinguish codes which are not permutation equivalent.

i	$|\mathfrak{N}(C_i)|$	$d(C)$	*Number of words of weight* 24
1	92	2	3754060
2	92	2	3765560
3	92	2	3749000
4	92	2	3759120
5	2024	2	2704156
6	23276	2	3829960
7	23276	2	3829960
8	1012	4	11092764
9	46	8	7691340
10	46	8	7691340
11	46	8	7701000
12	11638	8	7787940
13	11638	8	7787940
14	46	12	7681680

Explicit calculation in MAGMA shows that the codes C_6 and C_7 are permutation equivalent, and the codes C_{12} and C_{13} are permutation equivalent but C_9 and C_{10} are not. Hence there are, up to permutation equivalence, 12 self-dual codes in V.

Chapter 7

Examples

For a finite field $\mathbb{F}$, in this chapter two different scalar products on $\mathbb{F}^N$ are considered to define the dual of a linear code. The *Euclidean scalar product* is given by

$$\beta^1 : \mathbb{F}^N \times \mathbb{F}^N \to \mathbb{F}, \quad ((v_1, \ldots, v_N), (w_1, \ldots, w_N)) \mapsto \sum_{i=1}^{N} v_i w_i,$$

and if $\mathbb{F}$ has r^2 elements then the *Hermitian scalar product* is given by

$$\beta^r : \mathbb{F}^N \times \mathbb{F}^N \to \mathbb{F}, \quad ((v_1, \ldots, v_N), (w_1, \ldots, w_N)) \mapsto \sum_{i=1}^{N} v_i w_i^r.$$

In what follows, fix an element $\nu \in \{1, r\}$. A vector space automorphism $\varphi \in \mathrm{Aut}(\mathbb{F}^N)$ is called *monomial* if its matrix with respect to the standard basis $\mathcal{E} = (e_1, \ldots, e_N)$ of $\mathbb{F}^N$ is monomial, i.e. each column and each row has exactly one nonzero entry. A monomial automorphism is called *transitive* if its natural action on the set $\{\mathbb{F}^* \cdot e_i \mid i \in \{1, \ldots, N\}\}$ is transitive, and *ν-isometric* if $\beta^\nu(\varphi(v), \varphi(w)) = \beta^\nu(v, w)$ for all $v, w \in \mathbb{F}^N$. The *dual* of a linear code $C \leq \mathbb{F}^N$ is

$$C^\perp = C^{\perp,\nu} = \{v \in \mathbb{F}^N \mid \beta^\nu(v, c) = 0 \text{ for all } c \in C\},$$

and C is called *self-dual* if $C = C^\perp$. The group $\mathcal{M}^\nu(\mathbb{F}^N)$ formed by the isometric monomial automorphisms of $\mathbb{F}^N$ acts naturally on the set

$$\mathfrak{C}^\nu = \{C \leq \mathbb{F}^N \mid C = C^{\perp,\nu}\}$$

of all self-dual codes in $\mathbb{F}^N$, preserving for instance the minimum weight and other properties of the code which are of interest in coding theory. The stabilizer of a code C under this action is called the *monomial automorphism group* $\mathrm{MAut}(C)$.

In this chapter we choose some finite group G and ask for all transitive representations $\Delta : G \to \mathcal{M}^\nu(\mathbb{F}^N)$ such that $\Delta(G)$ is contained in the automorphism group of a self-dual code. Note that every such representation is induced from some linear character μ of some subgroup H of G, with $\mu(h)\mu(h)^\nu = 1$ for all $h \in H$ (cf. Remark 7.1.1). The theory developed in the previous chapters is then

applied to investigate the existence of a self-dual $\Delta(G)$-invariant code in $\mathbb{F}^N$. It follows for instance from Chapter 3 that, if $\mathbb{F}$ has odd characteristic, every automorphism of a self-dual code has determinant 1, i.e. if there exists a self-dual $\Delta(G)$-invariant code then $\Delta(G)$ must necessarily be contained in the special orthogonal group

$$\mathrm{SL}(\mathbb{F}^N) = \{X \in \mathrm{GL}(\mathbb{F}^N) \mid \det(X) = 1\},$$

Moreover, since $\Delta(G)$ acts on $\mathbb{F}^N$ as isometries, the pair $(\mathbb{F}^N, \beta^\nu)$ is an equivariant module over the group algebra $\mathbb{F}G$ in the sense of Section 4.1, where the involution on $\mathbb{F}G$ is given by

$$J_\nu : \mathbb{F}G \to \mathbb{F}G, \quad \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g^\nu g^{-1}.$$

Hence if $\mathbb{F}$ has even characteristic or if $\nu = r$ then the theory developed in Section 4.1 enables us to decide from a composition series of the G-module $\mathbb{F}^N$ whether there exists a self-dual $\Delta(G)$-invariant code in $\mathbb{F}^N$. If there exists such a code then the methods developed in Chapter 2.2 can be applied to determine $\mathfrak{C}^\nu$ completely, or up to an appropriate notion of equivalence. This is performed for self-dual binary A_5-invariant codes.

7.1 A_5-invariant self-dual codes

This section gives a classification of all transitive isometric monomial representations Δ of any degree N of the alternating group A_5 such that $\Delta(A_5)$ is contained in the automorphism group of a self-dual code in $\mathbb{F}^N$, where $\mathbb{F}$ is a finite field of characteristic 2,3 or 5. A self-orthogonal code whose automorphism group contains $\Delta(A_5)$ is rightly called A_5-invariant, since $\Delta(A_5) \cong A_5$ whenever Δ is non-trivial, due to the simplicity of A_5. Moreover, if C is a maximally self-orthogonal A_5-invariant code in $\mathbb{F}^N$ then the quotient $C^\perp/C$ is semisimple and does not depend on the choice of C. These quotients are given for every monomial representation of A_5. In terms of Witt groups, these quotients are the anisotropic representatives of the $\Delta(A_5)$-module $\mathbb{F}^N$ in the Witt group $\mathcal{W}(\mathbb{F}A_5, J_\nu, 1)$, which is therefore discussed in Section 7.1.1.

7.1.1   The Witt group of $\mathbb{F}A_5$

Let $\nu \in \{1, r\}$ and let $\Delta : A_5 \to \mathbb{F}^N$ be a transitive ν-isometric monomial representation. Let the involution J_ν be as above and consider $\mathbb{F}^N$ as an $\mathbb{F}A_5$-module via $v \cdot a = v\Delta(a)$, for $v \in \mathbb{F}^N$ and $a \in A$. Then

$$\beta^\nu(v \cdot a, w) = \beta^\nu(v, w \cdot a^{J_\nu}), \quad \beta^\nu(v, w) = \beta^\nu(w, v)^{J_\nu}$$

for all $v, w \in \mathbb{F}^N$ and all $a \in \mathbb{F}A_5$, and hence the pair $(\mathbb{F}^N, \beta^\nu)$ is 1-equivariant in the sense of Definition 4.1.1. In this section we determine the structure of the Witt group $\mathcal{W}(\mathbb{F}A_5, J_\nu, 1)$ and establish a uniform notation to describe the Witt Type of $(\mathbb{F}^N, \beta^\nu)$ in the subsequent section.

$\mathcal{W}(\mathbb{F}A_5, J, 1)$ **in characteristic 2**

Over a field $\mathbb{F} = \mathbb{F}_{2^f}$, for an odd integer f, the group A_5 has three simple modules, namely the trivial module and two 4-dimensional modules S and T. The A_5-module structure on S is given by the homomorphism

$$A_5 \to \text{End}(S), \quad (1,2,3) \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad (3,4,5) \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

and the A_5-module structure on T is given by

$$A_5 \to \text{End}(T), \quad (1,2,3) \mapsto \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad (3,4,5) \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

All three of these modules carry a non-degenerate G-invariant form with respect to the $\mathbb{F}$-linear involution J of $\mathbb{F}G$ given by $g \mapsto g^{-1}$, for $g \in G$. For the non-trivial modules S and T, this is seen as follows. Let

$$\chi_S : \mathbb{F}G \to \mathbb{F}, \quad a \mapsto \text{Trace}_S(a),$$

where Trace denotes the usual trace of a matrix, and define χ_T analogously. The dual module S^* of S is again a simple A_5-module of dimension 4, hence either isomorphic to S or to T, and $\chi_S(g) = \chi_{S^*}(g^{-1})$ for all $g \in G$. Since $\chi_S((1,2,3)) = 1$ and $\chi_T((1,2,3)^{-1}) = 0$, it follows that S is self-dual and, analogously, that T is self-dual. Hence both S and T carry a non-degenerate G-invariant form, by Remark 4.1.22.

The module S is absolutely irreducible, while over a field $\mathbb{F}_{2^f}$ with even f, the module $T = T_1 \oplus T_2$ splits into a direct sum of two modules of dimension 2. The A_5-module structure on T_1 is given by

$$(1,2,3) \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}, \quad (3,4,5) \mapsto \begin{pmatrix} 1 & \zeta \\ \zeta^2 & 0 \end{pmatrix},$$

where ζ is a primitive third root of unity in $\mathbb{F}$. The module T_2 is the algebraic conjugate of T_1 under the Galois automorphism $\mathbb{F} \to \mathbb{F}$, $x \mapsto x^2$, i.e. the A_5-module structure on T_2 is obtained by replacing ζ with ζ^2 above. Let $g := (1,2,3)(3,4,5)$, then

$$\chi_{T_1}(g) = \text{Trace}(\begin{pmatrix} \zeta & \zeta^2 \\ \zeta & 0 \end{pmatrix}) = \zeta, \quad \chi_{T_1}(g^{-1}) = \text{Trace}(\begin{pmatrix} 0 & \zeta^2 \\ \zeta & \zeta \end{pmatrix}) = \zeta$$

and hence $\chi_{T_2}(g) = \chi_{T_2}(g^{-1}) = \zeta^2$. Hence the same argument as above shows that both T_1 and T_2 are self-dual and hence, with respect to J, carry non-degenerate G-invariant forms. Now it follows from Corollary 4.1.16 that up to isometry, every

simple $\mathbb{F}_{2^f} A_5$-module carries exactly one non-degenerate G-invariant form with respect to J, whatever the parity of f. Hence if f is odd then

$$\mathcal{W}(\mathbb{F}_{2^f} A_5, J, 1) \cong \langle [(\mathbb{F}, \beta_\mathbb{F})] \rangle \times \langle [(S, \beta_S)] \rangle \times \langle [(T, \beta_T)] \rangle \cong \times_{i=1}^{3} C_2,$$

and if f is even then

$$\mathcal{W}(\mathbb{F}_{2^f} A_5, J, 1) \cong \langle [(\mathbf{1}, \beta_\mathbf{1})] \rangle \times \langle [(S, \beta_S)] \rangle \times \langle [(T_1, \beta_{T_1})] \rangle \times \langle [(T_2, \beta_{T_2})] \rangle \cong \times_{i=1}^{4} C_2.$$

Now consider the Hermitian case, i.e. assume that $f = 2r$ is even and the involution is given by

$$J_r : \mathbb{F}_{2^f} A_5 \rightarrow \mathbb{F}_{2^f} A_5, \quad \sum_{g \in G} a_g g \mapsto a_g^{2^r} g^{-1}.$$

The same argument as above shows that with respect to J_r, the simple module S carries exactly one non-degenerate G-invariant form, up to isometry, and that T_1 and T_2 carry a non-degenerate G-invariant form if and only if

$$\zeta = \chi_{T_1}(g) = \chi_{T_1}(g^{-1})^{J_r} = \zeta^{2^r},$$

i.e. if and only if f is a multiple of 4. In this case the Witt group

$$\mathcal{W}(\mathbb{F}_{2^f} A_5, J_r, 1) \cong \langle [(\mathbf{1}, \beta_\mathbf{1})] \rangle \times \langle [(S, \beta_S)] \rangle \times_{i=1}^{2} \langle [(T_i, \beta_{T_i})] \cong \times_{i=1}^{4} C_2,$$

and if f is even but no multiple of 4 then the Witt group

$$\mathcal{W}(\mathbb{F}_{2^f} A_5, J_r, 1) \cong \langle [(\mathbf{1}, \beta_\mathbf{1})] \rangle \times \langle [(S, \beta_S)] \rangle \cong \times_{i=1}^{2} C_2.$$

$\mathcal{W}(\mathbb{F} A_5, J, 1)$ in characteristic 3

Over a finite field $\mathbb{F} = \mathbb{F}_{3^f}$, for an odd integer f, the group algebra $\mathbb{F} A_5$ has three simple modules, namely the trivial module, a module U of dimension 4 and a module V of dimension 6. Since all simple modules have different dimension and since the dual of a simple module is again a simple module of the same dimension, all simple modules are self-dual, with respect to either of the two involutions J, J_r. The module U is absolutely irreducible, and the $\mathbb{F} A_5$-module structure on U is given by the homomorphism

$$\varphi : A_5 \rightarrow \operatorname{End}(U), \quad (1,2,3) \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}, \quad (3,4,5) \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

To see that with respect to either of the involutions J, J_r, the module U carries a non-degenerate equivariant form, one calculates that

$$\sum \varphi(g)(\varphi(g)^{\operatorname{tr}})^\nu = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix},$$

where the power $\nu \in \{1, r\}$ is taken componentwise and the sum is over the pairwise different matrices $\varphi(g)\varphi(g)^{\text{tr}}$. By definition the non-degenerate form on U given by this matrix is equivariant.

Over a field $\mathbb{F}_{3^f}$ with even f, the module V splits into two modules V_1, V_2 of dimension 3. The $\mathbb{F}A_5$-module structure on V_1 is given by the homomorphism

$$A_5 \to \text{End}(V_1), \quad (1,2,3) \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad (3,4,5) \mapsto \begin{pmatrix} 1 & \zeta^3 & 2 \\ 1 & \zeta^6 & \zeta^6 \\ 1 & \zeta^5 & \zeta \end{pmatrix},$$

where ζ is a root of unity of order 8. The module V_2 is the algebraic conjugate of V_1 by the Galois automorphism $f \mapsto f^3$, i.e. the $\mathbb{F}A_5$-module structure on V_2 is obtained by replacing ζ with ζ^3 above. Let $g := (1,2,3)(4,5,6)$, then $\chi_{V_1}(g) = \zeta^3 = \chi_{V_1}(g^{-1})$, and hence $\chi_{V_2}(g) = \zeta = \chi_{V_2}(g^{-1})$. Hence with respect to the involution J, both V_1 and V_2 are self-dual. Since these modules have odd dimension, one concludes with Remark 4.1.22 that with respect to J, both V_1 and V_2 carry a non-degenerate 1-equivariant form. This implies that with respect to J, the module V carries a non-degenerate 1-equivariant form, too, as follows. Since V is self-dual, it carries a symplectic or a symmetric non-degenerate G-invariant form. Assume that this form is symplectic. This gives rise to a symplectic G-invariant bilinear form ψ on $V \otimes_{\mathbb{F}} L \cong V_1 \oplus V_2$, where L is a field extension of degree 2 over $\mathbb{F}$. The epimorphism

$$\alpha_\psi : V_1 \oplus V_2 \to \text{Hom}_L(V_1, L), \quad v \mapsto (v_1 \mapsto \psi(v, v_1))$$

has kernel V_2 since V_1 is self-dual. Hence ψ restricts to a non-degenerate G-invariant symplectic bilinear form $V_1 \times V_1 \to_L$, $(v_1, v_1') \mapsto \psi(v_1, v_1')$. But this is a contradiction since V_1 has odd dimension and hence there exists no such form. Hence V must carry a non-degenerate G-invariant symmetric bilinear form.

Now assume that $f = 2r$ is even, and consider the involution J_r on $\mathbb{F}_{3^f}A_5$. The module V_2 is self-dual with respect to J_r if and only if $\zeta^{J_r} = \zeta$. Since $\zeta^{J_r} = \zeta^{3^r}$, this holds if and only if r is even, i.e. if and only if f is a multiple of 4. Hence, again since V_1, V_2 have odd dimension, with respect to J_r, these modules carry a non-degenerate 1-equivariant form if and only if f is a multiple of 4. In conclusion, if f is odd then the Witt group

$$\mathcal{W}(\mathbb{F}_{3^f}A_5, J, 1) \cong \langle[(\mathbf{1}, \beta_\mathbf{1})]\rangle \times \langle[(U, \beta_U)]\rangle \times_{\sigma \in \{1, \epsilon\}} \langle[(V, \sigma\beta_V)]\rangle$$
$$\cong C_4 \times C_4 \times_{\sigma \in \{1, \epsilon\}} (C_2 \times C_2),$$

where the element $\epsilon \in \mathbb{F}^* - (\mathbb{F}^*)^2$. For even f, the Witt group

$$\mathcal{W}(\mathbb{F}_{3^f}A_5, J, 1) \cong \times_{\sigma \in \{1, \epsilon\}} \left(\langle[(\mathbf{1}, \sigma\beta_\mathbf{1})]\rangle \times \langle[(U, \sigma\beta_U)]\rangle \times \times_{i=1}^2 \langle[(V_i, \sigma\beta_{V_i})]\rangle\right)$$
$$\cong \times_{\sigma \in \{1, \epsilon\}} (C_2 \times C_2 \times C_2 \times C_2).$$

In the Hermitian case, the Witt group

$$\mathcal{W}(\mathbb{F}_{3^f}A_5, J_r, 1) \cong \langle[(\mathbf{1}, \beta_\mathbf{1})]\rangle \times \langle[(U, \beta_U)]\rangle \times \times_{i=1}^2 \langle[(V_i, \beta_{V_i})]\rangle \cong \times_{i=1}^3 C_2$$

if f is a multiple of 4, and otherwise

$$\mathcal{W}(\mathbb{F}_{3^f}A_5, J_r, 1) \cong \langle[(\mathbf{1}, \beta_\mathbf{1})]\rangle \times \langle[(U, \beta_U)]\rangle \cong C_2 \times C_2.$$

$\mathcal{W}(\mathbb{F}A_5, J, 1)$ **in characteristic 5**

Over a finite field $\mathbb{F} = \mathbb{F}_{5^f}$, the group algebra $\mathbb{F}A_5$ has three simple modules, namely the trivial module, a module X of dimension 3 and a module Y of dimension 5. As in the case of characteristic 3, one concludes that all these modules are self-dual. Hence with respect to either of the involutions J, J_r of $\mathbb{F}A_5$, these modules carry a non-degenerate 1-equivariant form or a non-degenerate -1-equivariant form, by Remark 4.1.22. But the latter does not hold since the simple modules all have odd dimension. Hence all the simple modules carry a non-degenerate 1-equivariant form. Now it follows from Corollary 4.1.20 that in the Euclidean case,

$$\mathcal{W}(\mathbb{F}_{5^f}A_5, J, 1) \cong \times_{\sigma \in \{1, \epsilon\}} (\langle [(\mathbf{1}, \sigma\beta_{\mathbf{1}})] \rangle \times \langle [(X, \sigma\beta_X)] \rangle \times \langle [(Y, \sigma\beta_Y)] \rangle)$$
$$\cong \times_{\sigma \in \{1, \epsilon\}} (C_2 \times C_2 \times C_2),$$

and in the Hermitian case

$$\mathcal{W}(\mathbb{F}_{5^f}A_5, J, 1) \cong \langle [(\mathbf{1}, \beta_{\mathbf{1}})] \rangle \times \langle [(X, \beta_X)] \rangle \times \langle [(Y, \beta_Y)] \rangle \cong C_2 \times C_2 \times C_2.$$

$\mathcal{W}(\mathbb{F}A_5, J, 1)$ **in coprime characteristic**

Let $\mathbb{F}$ be a finite field whose characteristic does not divide the order of A_5, i.e. $char(\mathbb{F}) \notin \{2, 3, 5\}$. The ordinary character table of A_5 is

Size	1	15	20	12	12
Order	1	2	3	5	5
χ_1	1	1	1	1	1
χ_2	3	-1	0	b_5	b_5°
χ_3	3	-1	0	b_5°	b_5
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

where $b_5 = \frac{1+\sqrt{5}}{2}$ and $b_5^\circ = \frac{1-\sqrt{5}}{2}$. Let Z_i be the simple $\mathbb{C}A_5$-module belonging to the character χ_i. It is well-known that Z_1, Z_4 and Z_5 are realizable over the rationals and hence over every finite field. The modules Z_2, Z_3 are realizable over every finite field which has a root of $x^2 - 5$. If $\mathbb{F}$ has no root of $x^2 - 5$ then there is another irreducible $\mathbb{F}A_5$-module Z_6 of dimension 6, which splits into a direct sum $Z_6 \otimes L \cong (Z_2 \otimes L) \times (Z_3 \otimes L)$ over a field extension L of degree 2 over $\mathbb{F}$. Clearly Z_i is irreducible over $\mathbb{F}$ whenever it is realizable over $\mathbb{F}$, since none of the characters χ_i is the sum of other characters. Since Z_1, Z_4 and Z_5 are the only simple modules of dimension $1, 4$ and 5, respectively, these modules are self-dual. This implies that with respect to either of the involutions J, J_r, the $\mathbb{F}A_5$-modules Z_1 and Z_5 carry a non-degenerate 1-equivariant form (cf. Remark 4.1.22). The same calculations as in the case of characteristic 3 show that Z_4 carries a non-degenerate 1-equivariant form, too, with respect to either of the involutions. Since every element of A_5 is conjugate to its inverse, with respect to the involution J, the modules Z_2 and Z_3 are self-dual, and with respect to the involution J_r these modules are self-dual if

and only if $b_5^{J_r} = b_5$. If Z_2, Z_3 are self-dual then they carry an 1-equivariant form, since they have odd dimension, again by Remark 4.1.22. Now it follows with the same argument as in characteristic 3 that with respect to J, the module Z_6 carries a non-degenerate 1-equivariant form, too. In conclusion, if $x^2 - 5$ has a root in $\mathbb{F} = \mathbb{F}_{p^f}$ and $p^f \equiv_4 1$ then

$$\mathcal{W}(\mathbb{F}_{p^f} A_5, J, 1) \cong \times_{\sigma \in \{1,\epsilon\}} \times_{i=1}^{5} \langle [(Z_i, \sigma \beta_{Z_i})] \rangle \cong \times_{\sigma \in \{1,\epsilon\}} \times_{i=1}^{5} C_2,$$

where $\epsilon \in \mathbb{F}_{p^f}^* - (\mathbb{F}_{p^f}^*)^2$. If $x^2 - 5$ has a root in $\mathbb{F}_{p^f}$ and $p^f \equiv_4 -1$ then

$$\mathcal{W}(\mathbb{F}_{p^f} A_5, J, 1) \cong \times_{i=1}^{5} \langle [(Z_i, \beta_{Z_i})] \rangle \cong \times_{i=1}^{5} C_4.$$

If $x^2 - 5$ has no root in $\mathbb{F}_{p^f}$ and $p^f \equiv_4 1$ then

$$\mathcal{W}(\mathbb{F}_{p^f} A_5, J, 1) \cong \times_{\sigma \in \{1,\epsilon\}} \times_{i \in \{1,4,5,6\}} \langle [(Z_i, \sigma \beta_{Z_i})] \rangle$$
$$\cong \times_{\sigma \in \{1,\epsilon\}} \times_{i \in \{1,4,5,6\}} C_2,$$

and if $x^2 - 5$ has no root in $\mathbb{F}_{p^f}$ and $p^f \equiv_4 -1$ then

$$\mathcal{W}(\mathbb{F}_{p^f} A_5, J, 1) \cong \times_{i \in \{1,4,5\}} \langle [(Z_i, \beta_{Z_i})] \rangle \times_{\sigma \in \{1,\epsilon\}} \langle [(Z_6, \sigma \beta_{Z_6})] \rangle$$
$$\cong \times_{i \in \{1,4,5\}} C_4 \times_{\sigma \in \{1,\epsilon\}} C_2$$

In the Hermitian case, the Witt group

$$\mathcal{W}(\mathbb{F}_{p^f} A_5, J_r, 1) \cong \times_{i \in I} \langle [(Z_i, \beta_{Z_i})] \rangle \cong \times_{i \in I} C_2,$$

where $I = \{1, 2, 3, 4, 5\}$ if $b_5^{J_r} = b_5$, and $I = \{1, 4, 5\}$ otherwise.

7.1.2 Classification of all transitive monomial representations of A_5

The following Remark gives an outline of the characterization of all transitive monomial representations of A_5.

Remark 7.1.1. *Let G be a finite group and let $\Delta : G \to \mathrm{Aut}(\mathbb{F}^N)$ be a transitive monomial representation. Let $V = \mathbb{F}^N$ be the corresponding $\mathbb{F}G$-module. Then there exist a subgroup H of G and a linear character $\mu : H \to \mathbb{F}^*$ such that V is isomorphic to the $\mathbb{F}G$-module W_μ^G induced from the $\mathbb{F}H$-module $W_\mu = \mathbb{F}$, where $h \cdot w = \mu(h)w$, for $h \in H$ and $w \in W_\mu$. Moreover, $\Delta(G)$ is isometric with respect to the form β^ν if and only if $\mu(h)\mu(h)^\nu = 1$ for all $h \in H$.*

Proof. Let $\mathcal{E} = (e_1, \dots, e_N)$ be the standard basis of $\mathbb{F}^N$ and let $H := \mathrm{Stab}_{\Delta(G)}(\mathbb{F}^* e_1)$. Define a linear character $\mu : H \to \mathbb{F}^*$ by $e_1 h = e_1 \mu(h)$. In what follows, bases of V and W_μ^G are constructed such that there exists a G-module isomorphism which maps basis vectors to basis vectors. To this aim choose elements $g_1, \dots, g_N \in G$ with $e_1 g_i = e_i$. Then $G = \dot\cup \, H g_i$ is a disjoint union of right cosets. For every element $x \in G$ and every i there exists a uniquely determined

element $h_{x,i} \in H$ and an integer $\pi_x(i) \in \{1, \ldots, N\}$ such that $g_i x = h_{x,i} g_{\pi_x(i)}$. Choose an element $w \in W_\mu^G$ such that $wH \subseteq \mathbb{F}^* w$, and with respect to the basis $\mathcal{B} = (bg_1, \ldots, bg_N)$ of W_μ^G, G acts as monomial permutations, via

$$bg_i \cdot x = bg_{\pi_x(i)} \mu(h_{i,x}).$$

Then the linear map $V \to W_\mu^G$, $e_1 g_i \mapsto bg_i$ is an isomorphism of G-modules. If $\Delta(G)$ is isometric then

$$1 = \beta(e_1, e_1) = \beta(e_1 h, e_1 h) = \beta(e_1 \mu(h), e_1 \mu(h)) = \mu(h)\mu(h)^\nu$$

for all $h \in H$. Conversely, if always $\mu(h)\mu(h)^\nu = 1$ then

$$\begin{aligned}
\beta(e_i x, e_i x) &= \beta(e_1 g_i x, e_1 g_i x) = \beta(e_1 g_{\pi_x(i)} \mu(h_{i,x}), e_1 g_{\pi_x(i)} \mu(h_{i,x})) \\
&= \mu(h_{i,x})\mu(h_{i,x})^\nu \beta(e_1 g_{\pi_x(i)}, e_1 g_{\pi_x(i)}) = \beta(e_{\pi_x(i)}, e_{\pi_x(i)}) = \beta(e_i, e_i)
\end{aligned}$$

for all $i \in \{1, \ldots, N\}$ and all $x \in G$, and hence $\Delta(G)$ is isometric. $\square$

Table 7.1 gives all linear characters of subgroups H of A_5 and the composition factors of the induced modules. By the above Remark this is a classification of all transitive isometric monomial representations Δ of A_5. It follows immediately from Corollary 4.1.20 that in characteristic 2 as well as in Hermitian geometry, the group $\Delta(A_5)$ is contained in the automorphism group of a self-dual linear code in $\mathbb{F}^N$ if and only if all self-dual composition factors occur with even multiplicity in the $\Delta(A_5)$-module $V = \mathbb{F}^N$. In Euclidean geometry, if $\mathbb{F}$ has odd characteristic, it is in general not possible to decide only from the composition factors of V whether there exists a self-dual code C in V with $\Delta(A_5) \subseteq \mathrm{Aut}(C)$. In this case we use the following algorithm to compute a maximally self-orthogonal $\Delta(A_5)$-invariant code, with $A = \mathbb{F}A_5$.

Remark 7.1.2. *(cf. Lemma 4.1.8, Theorem 4.1.9) For a finite $\mathbb{F}$-algebra A with involution J, the following algorithm computes a maximally self-orthogonal submodule of an equivariant A-module (V, β).*

1. *Compute the set $\mathcal{S}$ of all minimal submodules of V.*

2. *If there exists some element $S \in \mathcal{S}$ with $S \subseteq S^{\perp,\beta}$ then go to (1) with $(S^\perp/S, \beta_S)$, where*
   $$\beta_S : \ S^\perp/S \times S^\perp/S \to \mathbb{F}, \ \ (s' + S, s'' + S) \mapsto \beta(s', s'').$$
   Otherwise return V.

Note that the quotient $(C^\perp/C, \beta_C)$ is anisotropic and hence semisimple, and independent from the choice of C, up to isometry. Clearly V contains a self-dual code if and only if this quotient is zero. Tables 7.2, 7.3, 7.4, 7.5, 7.6 lists the quotients $C^\perp/C$ for the transitive monomial $\mathbb{F}A_5$-modules, using the notation from Section 7.1.1. This yields the following enumeration of all transitive monomial representations Δ of A_5 such that $\Delta(A_5)$ is contained in the automorphism group of a self-dual code.

Theorem 7.1.3. *Let $\Delta : A_5 \to \mathbb{F}_{p^f}^N$ be a transitive isometric monomial representation. Let $H := \mathrm{Stab}_{\Delta(G)}(\mathbb{F}_{p^f}^* e_1)$, and define a linear character $\mu : H \to \mathbb{F}^*$, $h \mapsto \mu(h)$, where $e_1 h = e_1 \mu(h)$. There exists a self-dual code C in $\mathbb{F}^N$ with $\Delta(A_5) \subseteq \mathrm{Aut}(C)$ if and only if one of the following holds.*

1. *$H = \{1\}$ and $p = 2$,*

2. *$H \cong C_2$, μ is the trivial character and $p = 2$,*

3. *$H \cong C_2$, μ is the sign character, and $p = 3$ and f is even, or $p = 5$,*

4. *$H \cong C_3$, μ is trivial and $p = 2$ in Euclidean geometry, or $p = 5$ in Hermitian geometry,*

5. *$H \cong C_5$, μ is trivial and $p = 2$,*

6. *$H \cong S_3$, μ is trivial and $p = 3$ in Hermitian geometry,*

7. *$H \cong D_{10}$, μ is trivial and $p = 2$ and $f \equiv_4 2$ in Hermitian geometry,*

8. *$H \cong D_{10}$, μ is the sign character and $p = 5$, or the geometry is Hermitian and $p = 3$ and $f \equiv_4 2$.*

Table 7.1: Composition factors of transitive monomial A_5-modules

Subgroup	Linear character	Induced character	Composition factors over				
			$\mathbb{F}_{2f}$, f even $(1, T_1, T_2, S)$	$\mathbb{F}_{2f}$, f odd $(1, T, S)$	$\mathbb{F}_{3f}$, f even $(1, V_1, V_2, U)$	$\mathbb{F}_{3f}$, f odd $(1, V, U)$	$\mathbb{F}_{5f}$ $(1, X, Y)$
1	(1)	$(60,0,0,0,0)$	$(12,8,8,4)$	$(12,8,4)$	$(6,3,3,9)$	$(6,3,9)$	$(5,10,5)$
C_2	$(1,1)$	$(30,2,0,0,0)$	$(6,4,4,2)$	$(6,4,2)$	$(4,1,1,5)$	$(4,1,5)$	$(3,4,3)$
	$(1,-1)$	$(30,-2,0,0,0)$	$-$	$-$	$(2,2,2,4)$	$(2,2,4)$	$(2,6,2)$
C_3	$(1,1,1)$	$(20,0,2,0,0)$	$(4,2,2,2)$	$(4,2,2)$	$(2,1,1,3)$	$(2,1,3)$	$(3,4,1)$
	$(1,\zeta_3,\zeta_3^2)$	$(20,0,-1,0,0)$	$(4,3,3,1)$	$-$	$-$	$-$	$(1,3,2)$
	$(1,\zeta_3^2,\zeta_3)$	$(20,0,-1,0,0)$	$(4,3,3,1)$	$-$	$-$	$-$	$(1,3,2)$
C_5	$(1,1,1,1,1)$	$(12,0,0,2,2)$	$(4,2,2,0)$	$(4,2,0)$	$(2,1,1,1)$	$(2,1,1)$	$(1,2,1)$
	$(1,\zeta_5,\zeta_5^2,\zeta_5^3,\zeta_5^4)$	$(12,0,0,\zeta_5+\zeta_5^4,\zeta_5^2+\zeta_5^3)$	$(2,2,1,1)$	$-$	$(1,0,1,2)$	$-$	$-$
	$(1,\zeta_5^2,\zeta_5^4,\zeta_5,\zeta_5^3)$	$(12,0,0,\zeta_5^2+\zeta_5^3,\zeta_5+\zeta_5^4)$	$(2,1,2,1)$	$-$	$(1,1,0,2)$	$-$	$-$
	$(1,\zeta_5^3,\zeta_5,\zeta_5^4,\zeta_5^2)$	$(12,0,0,\zeta_5^2+\zeta_5^3,\zeta_5+\zeta_5^4)$	$(2,1,2,1)$	$-$	$(1,1,0,2)$	$-$	$-$
	$(1,\zeta_5^4,\zeta_5^3,\zeta_5^2,\zeta_5)$	$(12,0,0,\zeta_5+\zeta_5^4,\zeta_5^2+\zeta_5^3)$	$(2,2,1,1)$	$-$	$(1,0,1,2)$	$-$	$-$
$C_2 \times C_2$	$(1,1,1,1)$	$(15,3,0,0,0)$	$(3,2,2,1)$	$(3,2,1)$	$(3,0,0,3)$	$(3,0,3)$	$(2,1,2)$
	$(1,-1,1,-1)$	$(15,-1,0,0,0)$	$-$	$-$	$(1,1,1,2)$	$(1,1,2)$	$(1,3,1)$
	$(1,1,-1,-1)$	$(15,-1,0,0,0)$	$-$	$-$	$(1,1,1,2)$	$(1,1,2)$	$(1,3,1)$
	$(1,-1,-1,1)$	$(15,-1,0,0,0)$	$-$	$-$	$(1,0,1,2)$	$(1,1,2)$	$(1,3,1)$
S_3	$(1,1,1)$	$(10,2,1,0,0)$	$(2,1,1,1)$	$(2,1,1)$	$(2,0,0,2)$	$(2,0,2)$	$(2,1,1)$
	$(1,-1,1)$	$(10,-2,1,0,0)$	$-$	$-$	$(0,1,1,1)$	$(0,1,1)$	$(1,3,0)$
D_{10}	$(1,1,1,1)$	$(6,2,0,1,1)$	$(2,1,1,0)$	$(2,1,0)$	$(2,0,0,1)$	$(2,0,1)$	$(1,0,1)$
	$(1,-1,1,1)$	$(6,-2,0,1,1)$	$-$	$-$	$(0,1,1,0)$	$(0,1,0)$	$(0,2,0)$
A_4	$(1,1,1,1)$	$(5,1,2,0,0)$	$(1,0,0,1)$	$(1,0,1)$	$(1,0,0,1)$	$(1,0,1)$	$(2,1,0)$
	$(1,1,\zeta_3,\zeta_3^2)$	$(5,1,-1,0,0)$	$(1,1,1,0)$	$-$	$-$	$-$	$(0,0,1)$
	$(1,1,\zeta_3^2,\zeta_3)$	$(5,1,-1,0,0)$	$(1,1,1,0)$	$-$	$-$	$-$	$(0,0,1)$

Table 7.2: Witt Type of transitive monomial A_5-modules, Euclidean geometry, characteristic 2

Subgroup	Linear character	Witt Type of induced module, Euclidean geometry	
		$\mathbb{F}_{2^f}$, f even	$\mathbb{F}_{2^f}$, f odd
1	(1)	0	0
C_2	$(1,1)$	0	0
	$(1,-1)$	$-$	$-$
C_3	$(1,1,1)$	0	0
	$(1,\zeta_3,\zeta_3^2)$	$[\perp_{M\in\{T_1,T_2,S\}} (M,\beta_M)], \quad f \equiv_4 0$ $[S,\beta_S], \qquad\qquad f \equiv_4 2$	$-$
	$(1,\zeta_3^2,\zeta_3)$	$[\perp_{M\in\{T_1,T_2,S\}} (M,\beta_M)], \quad f \equiv_4 0$ $[S,\beta_S], \qquad\qquad f \equiv_4 2$	$-$
C_5	$(1,1,1,1,1)$	0	0
	$(1,\zeta_5,\zeta_5^2,\zeta_5^3,\zeta_5^4)$	$[\perp_{M\in\{T_2,S\}} (M,\beta_M)]$	$-$
	$(1,\zeta_5^2,\zeta_5^4,\zeta_5,\zeta_5^3)$	$[\perp_{M\in\{T_1,S\}} (M,\beta_M)]$	$-$
	$(1,\zeta_5^3,\zeta_5,\zeta_5^4,\zeta_5^2)$	$[\perp_{M\in\{T_1,S\}} (M,\beta_M)]$	$-$
	$(1,\zeta_5^4,\zeta_5^3,\zeta_5^2,\zeta_5)$	$[\perp_{M\in\{T_2,S\}} (M,\beta_M)]$	$-$
$C_2 \times C_2$	$(1,1,1,1)$	$[\perp_{M\in\{\mathbf{1},S\}} (M,\beta_M)]$	$[\perp_{M\in\{\mathbf{1},S\}} (M,\beta_M)]$
	$(1,-1,1,-1)$	$-$	$-$
	$(1,1,-1,-1)$	$-$	$-$
	$(1,-1,-1,1)$	$-$	$-$
S_3	$(1,1,1)$	$[\perp_{M\in\{T_1,T_2,S\}} (M,\beta_M)]$	$[\perp_{M\in\{T,S\}} (M,\beta_M)]$
	$(1,-1,1)$	$-$	$-$
D_{10}	$(1,1,1,1)$	$[\perp_{i\in\{1,2\}} (T_i,\beta_{T_i})]$	$[(T,\beta_T)]$
	$(1,-1,1,1)$	$-$	$-$
A_4	$(1,1,1,1)$	$[\perp_{M\in\{\mathbf{1},S\}} (M,\beta_M)]$	$[\perp_{M\in\{\mathbf{1},S\}} (M,\beta_M)]$
	$(1,1,\zeta_3,\zeta_3^2)$	$[\perp_{M\in\{\mathbf{1},T_1,T_2\}} (M,\beta_M)]$	$-$
	$(1,1,\zeta_3^2,\zeta_3)$	$[\perp_{M\in\{\mathbf{1},T_1,T_2\}} (M,\beta_M)]$	$-$

Table 7.3: Witt Type of transitive monomial A_5-modules, Euclidean geometry, characteristic 3

Subgroup	Linear character	Witt Type of induced module, Euclidean geometry	
		$\mathbb{F}_{3f}$, f even	$\mathbb{F}_{3f}$, f odd
1	(1)	$[\perp_{M\in\{U,V_1,V_2\}} (M,\beta_M)]$	$[\perp_{M\in\{U,V\}} (M,\beta_M) \perp_{i=1}^2 (\mathbf{1},\beta_\mathbf{1})]$
C_2	$(1,1)$	$[\perp_{M\in\{V_1,V_2,U\}} (M,\beta_M)]$	$[\perp_{M\in\{V,U\}} (M,\beta_M)$ $\perp_{i\in\{1,2\}} (\mathbf{1},\beta_\mathbf{1})]$
	$(1,-1)$	0	$[\perp_{i\in\{1,2\}} (\mathbf{1},\beta_\mathbf{1})]$
C_3	$(1,1,1)$	$[\perp_{M\in\{V_1,V_2,U\}} (M,\beta_M)]$	$[\perp_{M\in\{V,U\}} (M,\beta_M) \perp_{i\in\{1,2\}} (\mathbf{1},\beta_\mathbf{1})]$
	$(1,\zeta_3,\zeta_3^2)$	—	—
	$(1,\zeta_3^2,\zeta_3)$	—	—
C_5	$(1,1,1,1,1)$	$[\perp_{M\in\{V_1,V_2,U\}} (M,\beta_M)]$	$[\perp_{M\in\{V,U\}} (M,\beta_M)]$
	$(1,\zeta_5,\zeta_5^2,\zeta_5^3,\zeta_5^4)$	$[\perp_{M\in\{1,V_2\}} (M,\beta_M)]$	—
	$(1,\zeta_5^2,\zeta_5^4,\zeta_5,\zeta_5^3)$	$[\perp_{M\in\{1,V_1\}} (M,\beta_M)]$	—
	$(1,\zeta_5^3,\zeta_5,\zeta_5^4,\zeta_5^2)$	$[\perp_{M\in\{1,V_1\}} (M,\beta_M)]$	—
	$(1,\zeta_5^4,\zeta_5^3,\zeta_5^2,\zeta_5)$	$[\perp_{M\in\{1,V_2\}} (M,\beta_M)]$	—
$C_2\times C_2$	$(1,1,1,1)$	$[\perp_{M\in\{1,U\}} (M,\beta_M)]$	$[\perp_{M\in\{1,U\}} (M,\beta_M)]$
	$(1,-1,1,-1)$	$[\perp_{M\in\{1,V_1,V_2\}} (M,\beta_M)]$	$[\perp_{M\in\{1,V\}} (M,\beta_M)]$
	$(1,1,-1,-1)$	$[\perp_{M\in\{1,V_1,V_2\}} (M,\beta_M)]$	$[\perp_{M\in\{1,V\}} (M,\beta_M)]$
	$(1,-1,-1,1)$	$[\perp_{M\in\{1,V_1,V_2\}} (M,\beta_M)]$	$[\perp_{M\in\{1,V\}} (M,\beta_M)]$
S_3	$(1,1,1)$	0	$[\perp_{i\in\{1,2\}} (\mathbf{1},\beta_\mathbf{1})]$
	$(1,-1,1)$	$[\perp_{M\in\{V_1,V_2,U\}} (M,\beta_M)]$	$[\perp_{M\in\{V,U\}} (M,\beta_M)]$
D_{10}	$(1,1,1,1)$	$[(U,\beta_U)]$	$[(U,\beta_U)]$
	$(1,-1,1,1)$	$[\perp_{i\in\{1,2\}} (V_i,\beta_{V_i})]$	$[(V,\beta_V)]$
A_4	$(1,1,1,1)$	$[\perp_{M\in\{1,U\}} (M,\beta_M)]$	$[\perp_{M\in\{1,U\}} (M,\beta_M)]$
	$(1,1,\zeta_3,\zeta_3^2)$	—	—
	$(1,1,\zeta_3^2,\zeta_3)$	—	—

Table 7.4: Witt Type of transitive monomial A_5-modules, Euclidean geometry, characteristic 5

Subgroup	Linear character	Witt Type of induced module, Euclidean geometry over $\mathbb{F}_{5^f}$
1	(1)	$[\perp_{M \in \{\mathbf{1}, Y\}} (M, \beta_M)]$
C_2	$(1, 1)$	$[\perp_{M \in \{\mathbf{1}, Y\}} (M, \beta_M)]$
	$(1, -1)$	0
C_3	$(1, 1, 1)$	$[\perp_{M \in \{\mathbf{1}, Y\}} (M, \beta_M) \perp_{\sigma \in \{1, \epsilon\}} (X, \sigma\beta_X)], \quad f \equiv_2 1$ $[\perp_{M \in \{\mathbf{1}, Y\}} (M, \beta_M)], \qquad f \equiv_2 0$
	$(1, \zeta_3, \zeta_3^2)$	$[\perp_{M \in \{\mathbf{1}, X\}} (M, \beta_M)]$
	$(1, \zeta_3^2, \zeta_3)$	$[\perp_{M \in \{\mathbf{1}, X\}} (M, \beta_M)]$
C_5	$(1, 1, 1, 1, 1)$	$[\perp_{M \in \{\mathbf{1}, Y\}} (M, \beta_M)]$
	$(1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4)$	$-$
	$(1, \zeta_5^2, \zeta_5^4, \zeta_5, \zeta_5^3)$	$-$
	$(1, \zeta_5^3, \zeta_5, \zeta_5^4, \zeta_5^2)$	$-$
	$(1, \zeta_5^4, \zeta_5^3, \zeta_5^2, \zeta_5)$	$-$
$C_2 \times C_2$	$(1, 1, 1, 1)$	$[(X, \beta_X) \perp_{\sigma \in \{1, \epsilon\}} (Y, \sigma\beta_Y), \quad f \equiv_2 1$ $[(X, \beta_X)], \qquad f \equiv_2 0$
	$(1, -1, 1, -1)$	$[\perp_{M \in \{\mathbf{1}, X, Y\}} (M, \beta_M)]$
	$(1, 1, -1, -1)$	$[\perp_{M \in \{\mathbf{1}, X, Y\}} (M, \beta_M)]$
	$(1, -1, -1, 1)$	$[\perp_{M \in \{\mathbf{1}, X, Y\}} (M, \beta_M)]$
S_3	$(1, 1, 1)$	$[\perp_{M \in \{X, Y\}} (M, \beta_M)]$
	$(1, -1, 1)$	$[\perp_{M \in \{\mathbf{1}, X\}} (M, \beta_M)]$
D_{10}	$(1, 1, 1, 1)$	$[\perp_{M \in \mathbf{1}, Y} (M, \beta_M)]$
	$(1, -1, 1, 1)$	0
A_4	$(1, 1, 1, 1)$	$[(X, \beta_X)]$
	$(1, 1, \zeta_3, \zeta_3^2)$	$[(Y, \beta_Y)]$
	$(1, 1, \zeta_3^2, \zeta_3)$	$[(Y, \beta_Y)]$

Table 7.5: Witt Type of transitive monomial A_5-modules, Hermitian geometry, characteristic 2

Subgroup	Linear character	Witt Type of induced module, Hermitian geometry over $\mathbb{F}_{2^f}$, f even
1	(1)	0
C_2	$(1,1)$	0
	$(1,-1)$	–
C_3	$(1,1,1)$	0
	$(1,\zeta_3,\zeta_3^2)$	$[(S,\beta_S)]$
	$(1,\zeta_3^2,\zeta_3)$	$[(S,\beta_S)]$
C_5	$(1,1,1,1,1)$	0
	$(1,\zeta_5,\zeta_5^2,\zeta_5^3,\zeta_5^4)$	$[\perp_{M\in\{T_2,S\}} (M,\beta_M)]$
	$(1,\zeta_5^2,\zeta_5^4,\zeta_5,\zeta_5^3)$	$[\perp_{M\in\{T_1,S\}} (M,\beta_M)]$
	$(1,\zeta_5^3,\zeta_5,\zeta_5^4,\zeta_5^2)$	$[\perp_{M\in\{T_1,S\}} (M,\beta_M)]$
	$(1,\zeta_5^4,\zeta_5^3,\zeta_5^2,\zeta_5)$	$[\perp_{M\in\{T_2,S\}} (M,\beta_M)]$
$C_2 \times C_2$	$(1,1,1,1)$	$[\perp_{M\in\{\mathbf{1},S\}} (M,\beta_M)]$
	$(1,-1,1,-1)$	–
	$(1,1,-1,-1)$	–
	$(1,-1,-1,1)$	–
S_3	$(1,1,1)$	$[\perp_{M\in\{T_1,T_2,S\}} (M,\beta_M)]$, $f \equiv_4 0$ $[(S,\beta_S)]$, $f \equiv_4 2$
	$(1,-1,1)$	–
D_{10}	$(1,1,1,1)$	$[\perp_{M\in\{T_1,T_2\}} (M,\beta_M)]$, $f \equiv_4 0$ 0, $f \equiv_4 2$
	$(1,-1,1,1)$	–
A_4	$(1,1,1,1)$	$[\perp_{M\in\{\mathbf{1},S\}} (M,\beta_M)]$
	$(1,1,\zeta_3,\zeta_3^2)$	$[(\mathbf{1},\beta_{\mathbf{1}})]$, $f \equiv_4 2$ $[\perp_{M\in\{\mathbf{1},T_1,T_2\}} (M,\beta_M)]$, $f \equiv_4 0$
	$(1,1,\zeta_3^2,\zeta_3)$	$[(\mathbf{1},\beta_{\mathbf{1}})]$, $f \equiv_4 2$ $[\perp_{M\in\{\mathbf{1},T_1,T_2\}} (M,\beta_M)]$, $f \equiv_4 0$

Table 7.6: Witt Type of transitive monomial A_5-modules, Hermitian geometry, characteristic 3 and 5

Subgroup	Linear character	Witt Type of induced module, Hermitian geometry	
		$\mathbb{F}_{3^2}$	$\mathbb{F}_{5^2}$
1	(1)	$[\perp_{M\in\{V_1,V_2,U\}} (M,\beta_M)], \quad f \equiv_4 0$ $[(U,\beta_U)], \qquad f \equiv_4 2$	$[\perp_{M\in\{\mathbf{1},Y\}} (M,\beta_M)]$
C_2	$(1,1)$	$[\perp_{M\in\{V_1,V_2,U\}} (M,\beta_M)], \quad f \equiv_4 0$ $[(U,\beta_U)], \qquad f \equiv_4 2$	$[\perp_{M\in\{\mathbf{1},Y\}} (M,\beta_M)]$
	$(1,-1)$	0	0
C_3	$(1,1,1)$	$[\perp_{M\in\{V_1,V_2,U\}} (M,\beta_M)], \quad f \equiv_4 0$ $[(U,\beta_U)], \qquad f \equiv_4 2$	$[\perp_{M\in\{\mathbf{1},Y\}} (M,\beta_M)]$
	$(1,\zeta_3,\zeta_3^2)$	$-$	$[\perp_{M\in\{\mathbf{1},X\}} (M,\beta_M)]$
	$(1,\zeta_3^2,\zeta_3)$	$-$	$[\perp_{M\in\{\mathbf{1},X\}} (M,\beta_M)]$
C_5	$(1,1,1,1,1)$	$[\perp_{M\in\{V_1,V_2,U\}} (M,\beta_M)], \quad f \equiv_4 0$ $[(U,\beta_U)], \qquad f \equiv_4 2$	$[(\mathbf{1},\beta_{\mathbf{1}}) \perp (Y,\beta_Y)]$
	$(1,\zeta_5,\zeta_5^2,\zeta_5^3,\zeta_5^4)$	$[\perp_{M\in\{\mathbf{1},V_2\}} (M,\beta_M)]$	$-$
	$(1,\zeta_5^2,\zeta_5^4,\zeta_5,\zeta_5^3)$	$[\perp_{M\in\{\mathbf{1},V_1\}} (M,\beta_M)]$	$-$
	$(1,\zeta_5^3,\zeta_5,\zeta_5^4,\zeta_5^2)$	$[\perp_{M\in\{\mathbf{1},V_1\}} (M,\beta_M)]$	$-$
	$(1,\zeta_5^4,\zeta_5^3,\zeta_5^2,\zeta_5)$	$[\perp_{M\in\{\mathbf{1},V_2\}} (M,\beta_M)]$	$-$
$C_2 \times C_2$	$(1,1,1,1)$	$[\perp_{M\in\{\mathbf{1},U\}} (M,\beta_M)]$	$[(X,\beta_X)]$
	$(1,-1,1,-1)$	$[\perp_{M\in\{\mathbf{1},V_1,V_2\}} (M,\beta_M)], \quad f \equiv_4 0$ $[(\mathbf{1},\beta_{\mathbf{1}})], \qquad f \equiv_4 2$	$[\perp_{M\in\{\mathbf{1},X,Y\}} (M,\beta_M)]$
	$(1,1,-1,-1)$	$[\perp_{M\in\{\mathbf{1},V_1,V_2\}} (M,\beta_M)], \quad f \equiv_4 0$ $[(\mathbf{1},\beta_{\mathbf{1}})], \qquad f \equiv_4 2$	$[\perp_{M\in\{\mathbf{1},X,Y\}} (M,\beta_M)]$
	$(1,-1,-1,1)$	$[\perp_{M\in\{\mathbf{1},V_1,V_2\}} (M,\beta_M)], \quad f \equiv_4 0$ $[(\mathbf{1},\beta_{\mathbf{1}})], \qquad f \equiv_4 2$	$[\perp_{M\in\{\mathbf{1},X,Y\}} (M,\beta_M)]$
S_3	$(1,1,1)$	0	$[\perp_{M\in\{X,Y\}} (M,\beta_M)]$
	$(1,-1,1)$	$[\perp_{M\in\{V_1,V_2,U\}} (M,\beta_M)], \quad f \equiv_4 0$ $[(U,\beta_U)], \qquad f \equiv_4 2$	$[\perp_{M\in\{\mathbf{1},X\}} (M,\beta_M)]$
D_{10}	$(1,1,1,1)$	$[(U,\beta_U)]$	$[\perp_{M\in\{\mathbf{1},Y\}} (M,\beta_M)]$
	$(1,-1,1,1)$	$0, \qquad f \equiv_4 2$ $[\perp_{M\in\{V_1,V_2\}} (M,\beta_M)], \quad f \equiv_4 0$	0
A_4	$(1,1,1,1)$	$[\perp_{M\in\{\mathbf{1},U\}} (M,\beta_M)]$	$[(X,\beta_X)]$
	$(1,1,\zeta_3,\zeta_3^2)$	$-$	$[(Y,\beta_Y)]$
	$(1,1,\zeta_3^2,\zeta_3)$	$-$	$[(Y,\beta_Y)]$

7.2 G-invariant binary codes for some simple groups G

For a simple group $G \in \{A_5, \mathrm{GL}_3(\mathbb{F}_2), \mathrm{PGL}_3(\mathbb{F}_3), \mathrm{PGL}_2(\mathbb{F}_8), \mathrm{PSL}_2(\mathbb{F}_{11}), M_{11}, M_{12}\}$, this section classifies all maximally isotropic $\Delta(G)$-invariant binary codes of length $N \leq 200$, where $\Delta : G \to S_N$ is a group homomorphism whose image

$\Delta(G)$ is transitive. Note that then Δ is injective, for every simple group G and every $N > 1$, due to the simplicity of G. Hence the $\Delta(G)$-invariant codes considered in this section will sometimes shortly be called *G-invariant codes*.

Section 7.2.1 cites a construction in [5] of a self-orthogonal G-invariant code $D(\Delta, G)$ such that $C \subset D(\Delta, G)^\perp$ whenever C is a self-orthogonal G-invariant code. In some cases $\dim_{\mathbb{F}_2}(D(\Delta, G)^\perp/C)$, which does not depend on the chosen maximally self-orthogonal code C, turns out to be quite small, and hence there exist few maximally self-orthogonal G-invariant binary codes.

Section 7.2.2 describes how information on $D(\Delta, G)^\perp$ can be read off a priori from the *table of marks* of G. In Section 7.2.3, the number of $\Delta(G)$-invariant codes is given, along with some further information, for instance on the code $D(G, \Delta)$ and the normalizer $\mathfrak{N} = N_{S_N}(\Delta(G))$, which acts on the set of all $\Delta(G)$-invariant maximally self-orthogonal codes.

7.2.1   A G-invariant code generated by involutions

Let G be a transitive permutation group of degree N. An interesting construction of a G-invariant self-orthogonal code in $\mathbb{F}_2^N$ is given in [5], as follows (see also Section 2.2.5). For an involution $\iota \in G$ let $v^\iota \in \mathbb{F}_2^N$ be the vector with $v_i^\iota = 1$ if $\iota(i) = 1$, and $v_i^\iota = 0$ otherwise. Then $(v, \iota(v)) = (v, v^\iota)$ for all $v \in F_2^N$. This yields the following easy but important remark.

Remark 7.2.1. *Let $C(G, N) := \langle v^\iota \mid \iota \in G$ is an involution$\rangle$. Then $C(G, N) \subseteq C^\perp$ for every self-orthogonal G-invariant code in $\mathbb{F}_2^N$. In particular $C(G, N)$ is contained in every self-dual G-invariant code in $\mathbb{F}_2^N$, provided that such a code exists. The code $C(G, N)$ is G-invariant, since $v^\iota g = v^{g\iota g^{-1}} \in C(G, N)$ for every involution ι and all $g \in G$.*

Example 7.2.2. *Let $\Delta : \mathrm{GL}_3(\mathbb{F}_2) \to S_{14}$ be the transitive permutation representation with $H := \mathrm{Stab}_{\Delta(G)}(\{1\}) \cong C_7 \in \mathrm{Syl}_7(\Delta(\mathrm{GL}_3(\mathbb{F}_2)))$. Let $G := \mathrm{Im}(\Delta) \cong \mathrm{GL}_3(\mathbb{F}_2)$. Since $[N_G(H) : H] = 2$, there exists a self-dual G-invariant code $D \leq \mathbb{F}_2^{14}$, namely some repetition code of minimum weight 2 (cf. Theorem 4.1.30). Hence every self-dual G-invariant code contains $C := C(G, 14)$. In particular C is self-orthogonal.*

To construct C, note that all involutions are conjugate in G and hence as a G-module, C is generated by v^ι, where $\iota \in G$ is an arbitrary involution. Every involution in G has two fixed points, hence $\mathrm{wt}(v^\iota) = 2$. Assume that $v_1^\iota = 1$, and for every $i \in \{1, \dots, 14\}$ choose an element $g_i \in G$ with $g_i(1) = i$. The elements $v^\iota g_i = v^{g_i \iota g_i^{-1}} \in C$ all have weight 2 and hence two different elements $v^\iota g_i, v^\iota g_j$ have disjoint support. Since always $(v^\iota g_i)_i = 1$, this implies

$$\{v^\iota g_i \mid i \in \{1, \dots, 14\}\} = C = D.$$

Hence by Remark 7.2.1, the code $C = D$ is the only self-dual G-invariant code in $\mathbb{F}_2^{14}$.

Examples like the following are also in [5].

Example 7.2.3. *Let Δ be the permutation representation of degree 104 of the simple group $\mathrm{PGL}_3(\mathbb{F}_3) \cong \mathrm{GL}_3(\mathbb{F}_3)/Z(\mathrm{GL}_3(\mathbb{F}_3))$, with $H := \mathrm{Stab}_{\Delta(\mathrm{PGL}_3(\mathbb{F}_3))} \cong S \rtimes C_2$, where $S \in \mathrm{Syl}_3(\mathrm{PGL}_3(\mathbb{F}_3))$. Let $G := \Delta(\mathrm{PGL}_3(\mathbb{F}_3))$, then G is contained in the alternating group A_{104}. Again, since $[N_G(H) : H] = 2$, there exists some G-invariant self-dual repetition code $D \leq \mathbb{F}_2^{104}$, of minimum weight 2. Every involution in G has 8 fixed points and hence $C := C(G, 104)$ is a self-orthogonal doubly-even code. Explicit calculations show that C is the doubly-even subcode of D, hence has codimension 1 in D. The two neighbors E, F of D which intersect D in its doubly-even subcode are doubly-even, since 104 is a multiple of 8. Since $G \leq A_{104}$, the codes E and F are G-invariant, by Theorem 3.2.7. According to Remark 7.2.1, C, D and E are the only self-dual G-invariant codes in $\mathbb{F}_2^{104}$.*

7.2.2   Information from tables of marks

The *table of marks* of a finite group G contains information on the transitive permutation representations Δ of G. This section shows how this information can be used to determine a priori some properties of self-dual $\Delta(G)$-invariant codes.

Remark 7.2.4. *For a subgroup H of G, let $\Delta_H : G \to S_{[G:H]}$, $g \mapsto (Hx \mapsto Hxg)$ be the natural permutation representation. Every transitive permutation representation is of the form Δ_H for some subgroup H (cf. Remark 7.1.1).*

By $\mathfrak{C}_H(G)$ denote the set of all self-dual $\Delta_H(G)$-invariant codes in $\mathbb{F}_2^{[G:H]}$. For every automorphism α of G, there exists a bijection $\mathfrak{C}_H(G) \to \mathfrak{C}_{\alpha(H)}(G)$ which maps every code to a permutation equivalent code.

Definition 7.2.5. *For two subgroups H, U of G let $m_{H,U}$ be the number of fixed points of $\Delta_H(U)$. This number is called the* mark *of U with respect to H. Clearly if $T = \{t_1, \ldots, t_N\}$ is a set of left coset representatives of H in G then*

$$m_{H,U} = |\{i \in \{1, \ldots, N\} \mid U \subseteq t_i H t_i^{-1}\}| = \frac{|\{g \in G \mid U \subseteq gHg^{-1}\}|}{|H|}.$$

In particular $m_{H,U} = 0$ whenever $|H| < |U|$, and $m_{H,H} = [N_G(H) : H]$. Let $H_1, \ldots, H_t$ be representatives for the conjugacy classes of subgroups of G, such that $|H_1| \leq \ldots \leq |H_t|$. Then the lower diagonal matrix M with $M_{ij} = m_{H_i, H_j}$ is called the table of marks *of G.*

Remark 7.2.6. *Let $\iota \in G$ be an involution and let H be a subgroup of G, of index N. The number of fixed points of $\Delta_H(\iota)$ equals the mark $m_{H,\langle\iota\rangle}$. Hence the mimimum weight of the binary code $C(\Delta_H(G), N)$ generated by the involutions of G (cf. Remark 7.2.1) is at most $m_{H,\langle\iota\rangle}$. In particular every $\Delta_H(G)$-invariant self-dual code in $\mathbb{F}_2^N$ has minimum weight at most $m_{H,\langle\iota\rangle}$. A $\Delta_H(G)$-invariant self-dual code in $\mathbb{F}_2^N$ exists for instance if $m_{H,H}$ is even (cf. Theorem 4.1.30). Note that $m_{H,\langle\iota\rangle}$, as every mark $m_{H,U}$, is always a multiple of $m_{H,H} = [N_G(H) : H]$.*

7.2.3 The G-invariant codes

Let $G \in \{A_5, \mathrm{GL}_3(\mathbb{F}_2), \mathrm{PGL}_3(\mathbb{F}_3), \mathrm{PGL}_2(\mathbb{F}_8), \mathrm{PSL}_2(\mathbb{F}_{11}), M_{11}, M_{12}\}$ and let Δ be a transitive permutation representation of G of degree $N \leq 200$. Tables 7.7 to 7.13 list the number of maximally self-orthogonal G-invariant codes in $\mathbb{F}_2^N$, along with some further information described below.

The set $\mathfrak{C}$ of all maximally self-orthogonal G-invariant codes has been determined as follows. The algorithm in Remark 7.1.2 has been implemented to find one such code. A system of representatives for the normalizer equivalence classes of codes has then be computed using the neighbor search algorithm in Remark 2.3.10. Recall that two codes C, D are called normalizer equivalent if there exists some element $\eta \in \mathfrak{N} = N_{S_N}(\Delta(G))$ with $C\eta = D$ (cf. Remark 2.3.11). The total number of G-invariant codes is then

$$|\mathfrak{C}| = \sum_{[C] \in \mathfrak{C}/\sim_{\mathfrak{N}}} \frac{|[C]|}{|\mathfrak{N} \cap \mathrm{Aut}(C)|},$$

where $[C]$ denotes the equivalence class of an element $C \in \mathfrak{C}$. The entries in Tables 7.7 to 7.13 are as follows.

1. $\mathrm{Stab}_{\Delta(G)}(1)$: The subgroup H of G such that the action of G on the H-cosets induces the permutation representation Δ. If required, additional information is given to distinguish H from other subgroups, up to automorphisms of G (cf. Remark 7.2.4).

2. $\mathfrak{N}$: The isomorphism type of $\mathfrak{N}$, which is $N_G(H)/H \rtimes \mathrm{Aut}_H(G)$ (cf. Section 2.3.1).

3. $D(G, \Delta)$: The length, dimension and minimum weight of the code $C(\Delta(G), [G : H]) \cap C(\Delta(G), [G : H])^\perp$, which is self-orthogonal and contained in the orthogonal of every code in $\mathfrak{C}$ (cf. Section 7.2.1). If the minimum weight is a multiple of 4, an upper index $^+$ or $^-$ indicates that the code is doubly-even, or singly-even, respectively.

4. C: The length and dimension of a maximally self-orthogonal $\Delta(G)$-invariant code.

5. d: The minimum weights of the maximally self-orthogonal G-invariant codes.

6. $|\mathfrak{C}/\sim\mathfrak{N}|$: The number of normalizer equivalence classes of elements of $\mathfrak{C}$.

7. $|\mathfrak{C}|$: The cardinality of $\mathfrak{C}$, as a sum of orbit lengths. The bold numbers indicate the number of orbits of a certain length.

8. $\mathcal{B}(\Delta(G))$ (for small lengths): The Bravais group for $\mathfrak{C}$. Note that whenever this group equals $\Delta(A_5)$, the normalizer $\mathfrak{N}$ is the largest subgroup of S_N which acts on $\mathfrak{C}$ (cf. Theorem 6.3.3).

Table 7.7: $G = A_5$

$\mathrm{Stab}_{\Delta(G)}(1)$	$\mathfrak{R}$	$D(\Delta,G)$	C	d	$\lvert\mathfrak{C}/\sim_{\mathfrak{R}}\rvert$	$\lvert\mathfrak{C}\rvert$	$\mathcal{B}(\Delta(G))$
1	$G \rtimes \mathrm{Aut}(G)$	$[60,0]$	$[60,30]$	2	1	15	G
				4^-	91	$1\cdot 120 + 1\cdot 60 + \mathbf{81}\cdot 30 + \mathbf{8}\cdot 15 = 2730$	
				6	38	$\mathbf{11}\cdot 60 + \mathbf{27}\cdot 120 = 3900$	
				8^-	71	$\mathbf{71}\cdot 120 = 8520$	
				10	16	$\mathbf{16}\cdot 120 = 1920$	
				12^-	2	$\mathbf{2}\cdot 120 = 240$	
					$\sum = 219$	$\sum = 17325$	
C_2	$C_2 \rtimes \mathrm{Aut}(G)$	$[30,15,2]$	$[30,15]$	2	1	$1\cdot 1 = 1$	$C_2 \wr S_{15}$
C_3	$C_2 \rtimes \mathrm{Aut}(G)$	$[20,0]$	$[20,10]$	2	1	$1\cdot 1 = 1$	G
				4^-	3	$1\cdot 4 + \mathbf{2}\cdot 2$	
					$\sum = 4$	$\sum = 9$	
$C_2 \times C_2$	$C_3 \rtimes \mathrm{Aut}(G)$	$[15,0]$	$[15,5]$	6	1	$1\cdot 3 = 3$	G
C_5	$C_2 \rtimes \mathrm{Aut}(G)$	$[12,0]$	$[12,6]$	2	1	$1\cdot 1 = 1$	$(C_2 \wr S_6) \cap A_{12}$
				4^-	1	$1\cdot 2 = 2$	
S_3	$\mathrm{Aut}(G)$	$[10,1,10]$	$[10,1]$	10	1	$1\cdot 1 = 1$	S_{10}
D_{10}	$\mathrm{Aut}(G)$	$[6,1,6]$	$[6,1]$	7	1	$1\cdot 1 = 1$	S_6
A_4	$\mathrm{Aut}(G)$	$[5,0]$	$[5,0]$	0	1	$1\cdot 1 = 1$	S_5

Table 7.8: $G = \mathrm{GL}_3(\mathbb{F}_2)$

$\mathrm{Stab}_{\Delta(G)}(1)$	$\mathfrak{N}$	$D(\Delta, G)$	C	d	$|\mathfrak{C}/\sim_{\mathfrak{N}}|$	$|\mathfrak{C}|$	$\mathcal{B}(\Delta(G))$
C_2	$(C_2 \times C_2) \rtimes \mathrm{Aut}(G)$	$[84, 21, 4]^+$	$[84, 42]$	2	2	$\mathbf{1} \cdot 1 + \mathbf{1} \cdot 2 = 3$	$C_2^{42} \rtimes G$
				4	112	$\mathbf{2} \cdot 1 + \mathbf{110} \cdot 2 = 222$	
					$\sum = 114$	$\sum = 225$	
C_3	$C_2 \rtimes \mathrm{Aut}(G)$	$[56, 0]$	$[56, 28]$	2	1	$\mathbf{1} \cdot 1 = 1$	G
				4^-	3	$\mathbf{3} \cdot 2 = 6$	
				4^+	15	$\mathbf{8} \cdot 2 + \mathbf{7} \cdot 4 = 44$	
				6	4	$\mathbf{4} \cdot 2 = 8$	
				8^-	10	$\mathbf{2} \cdot 2 + \mathbf{8} \cdot 4 = 36$	
				8^+	37	$\mathbf{9} \cdot 2 + \mathbf{28} \cdot 4 = 130$	
					$\sum = 70$	$\sum = 225$	
$C_2 \times C_2$	G	$[42, 7, 6]$	$[42, 21]$	2	1	$\mathbf{1} \cdot 3 = 3$	G
				4	1	$\mathbf{1} \cdot 3 = 3$	
				6	1	$\mathbf{1} \cdot 6 = 6$	
					$\sum = 3$	$\sum = 12$	
C_4	$C_2 \rtimes \mathrm{Aut}(G)$	$[42, 21, 2]$	$[42, 21]$	2	1	$\mathbf{1} \cdot 1 = 1$	$C_2 \wr S_{21}$
S_3	$\mathrm{Aut}(G)$	$[28, 7, 12]^+$	$[28, 10]$	4	1	$\mathbf{1} \cdot 2 = 2$	G
C_7	$C_3 \rtimes \mathrm{Aut}(G)$	$[24, 0]$	$[24, 12]$	8	1	$\mathbf{1} \cdot 6 = 6$	G
D_8	$\mathrm{Aut}(G)$	$[21, 6, 8]^+$	$[21, 6]$	8	1	$\mathbf{1} \cdot 1 = 1$	$\mathfrak{N}$
A_4	G	$[14, 7, 2]$	$[14, 7]$	2	1	$\mathbf{1} \cdot 1 = 1$	$C_2 \wr S_7$
H_{21}	$\mathrm{Aut}(G)$	$[8, 0]$	$[8, 4]$	4	1	$\mathbf{1} \cdot 2 = 2$	G
S_4	G	$[7, 3, 4]^+$	$[7, 3]$	4	1	$\mathbf{1} \cdot 1 = 1$	$\mathfrak{N}$

Table 7.9: $G = \mathrm{PGL}_3(\mathbb{F}_3)$

$\mathrm{Stab}_{\Delta(G)}(1)$	$\mathfrak{N}$	$D(\Delta, G)$	C	d	$\lvert \mathcal{C}/\sim_{\mathfrak{N}} \rvert$	$\lvert \mathcal{C} \rvert$
$C_{13} \rtimes C_3$	$\mathrm{Aut}(G)$	$[144, 0]$	$[144, 40]$	32^-	4	$3 \cdot 1 + 1 \cdot 2 = 5$
$(C_3 \times C_3) \rtimes C_4$	G	$[156, 13, 12]^+$	$[156, 78]$	2 4^-	3 24	$3 \cdot 1 = 3$ $24 \cdot 1 = 24$
$(C_3 \times C_3) \rtimes (C_2 \times C_2)$	G	$[156, 65, 8]^+$	$[156, 78]$	2 4^- 6 8^-	1 2 2 4	$1 \cdot 1 = 1$ $2 \cdot 1 = 2$ $2 \cdot 1 = 2$ $4 \cdot 1 = 4$
$S \rtimes C_2,\ S \in \mathrm{Syl}_3(G)$	$C_2 \rtimes \mathrm{Aut}(G)$	$[104, 51, 4]^+$	$[104, 52]$	2 4^+	1 2	$1 \cdot 1 = 1$ $2 \cdot 1 = 2$
$S \rtimes C_2,\ S \in \mathrm{Syl}_3(G)$	G	$[104, 13, 8]^+$	$[104, 52]$	2 4^- 4^+ 8^+	1 2 8 4	$1 \cdot 1 = 1$ $2 \cdot 1 = 2$ $8 \cdot 1 = 8$ $4 \cdot 1 = 4$
$(Q_8 \rtimes C_3) \rtimes C_2$	$\mathrm{Aut}(G)$	$[117, 38, 16]^+$	$[117, 39]$	16^-	3	$3 \cdot 1 = 3$
$((C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_2$	G	$[78, 39, 2]$	$[78, 39]$	2	1	$1 \cdot 1 = 1$
$((C_3 \times C_3) \rtimes C_4).C_2$	G	$[78, 13, 6]$	$[78, 39]$	2	3	$3 \cdot 1 = 3$
$((C_3 \times C_3) \rtimes C_4).C_2$	G	$[78, 13, 6]$	$[78, 39]$	2	1	$1 \cdot 1 = 1$
$N_G(S),\ S \in \mathrm{Syl}_3(G)$	$\mathrm{Aut}(G)$	$[52, 1, 52]^+$	$[52, 13]$	4^+	2	$1 \cdot 2 + 1 \cdot 1 = 3$
$(((C_3 \times C_3) \rtimes C_4).C_2) \rtimes C_2$	G	$[39, 0]$	$[39, 0]$	$-$	1	$1 \cdot 1 = 1$
$(((C_3 \times C_3) \rtimes C_4).C_2) \rtimes C_2$	G	$[26, 13, 2]$	$[26, 13]$	2	1	$1 \cdot 1 = 1$
$((((C_3 \times C_3) \rtimes C_4).C_2) \rtimes C_2) \rtimes C_2$	G	$[13, 0]$	$[13, 0]$	$-$	1	$1 \cdot 1 = 1$

Table 7.10: $G = \mathrm{PGL}_2(\mathbb{F}_8)$

$\mathrm{Stab}_{\Delta(G)}(1)$	$\mathfrak{R}$	$D(\Delta,G)$	C	d	$|\mathfrak{C}/\sim_{\mathfrak{R}}|$	$|\mathfrak{C}|$	$\mathcal{B}(\Delta(G))$
S_3	$\mathrm{Aut}(G)$	$[84,28,14]$	$[84,29]$	12^-	1	3	G
C_7	$C_2 \rtimes \mathrm{Aut}(G)$	$[72,0]$	$[72,36]$	2	1	$\mathbf{1}\cdot 1 = 1$	G
				4^+	3	$\mathbf{1}\cdot 2 + \mathbf{2}\cdot 1 = 4$	
				6	1	$\mathbf{1}\cdot 2 = 2$	
				8^+	17	$\mathbf{2}\cdot 1 + \mathbf{5}\cdot 2 + \mathbf{4}\cdot 3 + \mathbf{6}\cdot 6 = 60$	
				8^-	4	$\mathbf{2}\cdot 3 + \mathbf{2}\cdot 6 = 18$	
				12^+	2	$\mathbf{1}\cdot 2 + \mathbf{1}\cdot 6 = 8$	
					$\sum = 28$	$\sum = 93$	
$C_2 \times C_2 \times C_2$	$C_7 \rtimes \mathrm{Aut}(G)$	$[63,0]$	$[63,27]$	16^+	3	$\mathbf{1}\cdot 7 + \mathbf{2}\cdot 1 = 9$	G
				14	4	$\mathbf{2}\cdot 21 + \mathbf{2}\cdot 7 = 56$	
				12^+	7	$\mathbf{1}\cdot 1 + \mathbf{6}\cdot 7 = 43$	
				12^-	3	$\mathbf{2}\cdot 21 + \mathbf{1}\cdot 7 = 49$	
				4^+	2	$\mathbf{2}\cdot 1 = 2$	
					$\sum = 19$	$\sum = 159$	
C_9	$C_2 \rtimes \mathrm{Aut}(G)$	$[56,0]$	$[56,28]$	2	1	$\mathbf{1}\cdot 1 = 1$	G
				4^+	2	$\mathbf{1}\cdot 1 + \mathbf{1}\cdot 1 = 2$	
				8^+	7	$\mathbf{2}\cdot 1 + \mathbf{4}\cdot 3 + \mathbf{1}\cdot 6 = 21$	
				8^-	2	$\mathbf{1}\cdot 3 + \mathbf{1}\cdot 3 = 6$	
				12^+	1	$\mathbf{1}\cdot 2 = 2$	
					$\sum = 13$	$\sum = 32$	
D_{14}	$\mathrm{Aut}(G)$	$[36,7,16]^+$	$[36,8]$	14	1	$\mathbf{1}\cdot 3 = 3$	G
D_{18}	$\mathrm{Aut}(G)$	$[28,7,12]^+$	$[28,8]$	10	1	$\mathbf{1}\cdot 3 = 3$	G
$N_G(C_2 \times C_2 \times C_2)$	$\mathrm{Aut}(G)$	$[9,0]$	$[9,0]$	0	1	$\mathbf{1}\cdot 1 = 1$	S_9

Table 7.11: $G = \mathrm{PSL}_2(\mathbb{F}_{11})$

$\mathrm{Stab}_{\Delta(G)}(1)$	$\mathfrak{R}$	$D(\Delta,G)$	C	d	$\lvert \mathfrak{C}/\sim_{\mathfrak{R}} \rvert$	$\lvert \mathfrak{C} \rvert$	$\mathcal{B}(\Delta(G))$
C_5	$C_2 \rtimes \mathrm{Aut}(G)$	$[132,0]$	$[132,66]$	2	1	$\mathbf{1} \cdot 1 = 1$	
				4^-	7	$\mathbf{7} \cdot 2 = 14$	
				6	2	$\mathbf{2} \cdot 2 = 4$	
				8^-	4	$4 \cdot 2 = 8$	
				10	5	$1 \cdot 4 + \mathbf{4} \cdot 2 = 12$	
				12^-	59	$\mathbf{43} \cdot 4 + \mathbf{16} \cdot 2 = 204$	
				16^-	6	$\mathbf{6} \cdot 4 = 24$	
				18	10	$\mathbf{10} \cdot 4 = 40$	
				20^-	2	$\mathbf{2} \cdot 4 = 8$	
					$\sum = 96$	$\sum = 315$	
S_3	G	$[110,45,6]$	$[110,55]$	2	1	$\mathbf{1} \cdot 1 = 1$	S_{11}
				6	1	$\mathbf{1} \cdot 2 = 2$	
$C_2 \times C_3$	$C_2 \rtimes \mathrm{Aut}(G)$	$[110,55,2]$	$[110,55]$	2	1	$\mathbf{1} \cdot 1 = 1$	$C_2 \wr S_{55}$
C_{11}	$C_5 \rtimes \mathrm{Aut}(G)$	$[60,0]$	$[60,25]$	12^+	1	$\mathbf{1} \cdot 5 = 5$	$\mathrm{Aut}(\Delta(G))$
D_{10}	$\mathrm{Aut}(G)$	$[66,11,20]^-$	$[66,21]$	6	1	$\mathbf{1} \cdot 2 + 1 \cdot 1 = 3$	$\Delta(G)$
$C_{11} \times C_5$	$\mathrm{Aut}(G)$	$[12,0]$	$[12,1]$	12^+	1	$\mathbf{1} \cdot 1 = 1$	$\mathfrak{R}$
A_4	$\mathrm{Aut}(G)$	$[55,10,20]^+$	$[55,10]$	20^+	1	$\mathbf{1} \cdot 1 = 1$	$\mathfrak{R}$
D_{12}	$\mathrm{Aut}(G)$	$[55,10,20]^+$	$[55,10]$	20^+	1	$\mathbf{1} \cdot 1 = 1$	$\mathfrak{R}$
A_5	G	$[11,0]$	$[11,0]$	$-$	1	$\mathbf{1} \cdot 1 = 1$	S_{11}

Table 7.12: $G = M_{11}$

$\text{Stab}_{\Delta(G)}(1)$	$\mathfrak{N}$	$D(\Delta, G)$	C	d	$|\mathfrak{C}/\sim_{\mathfrak{N}}|$	$|\mathfrak{C}|$
$(Q_8 \rtimes C_3) \rtimes C_2$	G	$[165, 54, 20]^+$	$[165, 55]$	18 $\\ 20^-$	1 $\\ 2$	$\mathbf{1} \cdot 1 = 1$ $\\ \mathbf{2} \cdot 1 = 2$
$Q_8 \rtimes C_3$	$C_2 \times G$	$[330, 165, 2]$	$[330, 165]$	2	1	$\mathbf{1} \cdot 1 = 1$
S_5	G	$[66, 1, 66]$	$[66, 11]$	20^-	1	$\mathbf{1} \cdot 1 = 1$
$A_5,\ [N_G(H):H] = 2$	$C_2 \times G$	$[132, 65, 4]^+$	$[132, 66]$	2 $\\ 4^-$	1 $\\ 2$	$\mathbf{1} \cdot 1 = 1$ $\\ \mathbf{2} \cdot 1 = 2$
$PSL_2(\mathbb{F}_{11})$	G	$[12, 1, 12]^+$	$[12, 1]$	12^+	1	$\mathbf{1} \cdot 1 = 1$
$A_5,\ [N_G(H):H] = 1$	G	$[132, 65, 12]^+$	$[132, 66]$	12^- $\\ 6$	2 $\\ 1$	$\mathbf{2} \cdot 1 = 2$ $\\ \mathbf{1} \cdot 1 = 1$
$N_G(S),\ S \in \text{Syl}_{11}(G)$	G	$[144, 0]$	$[144, 56]$	12^+ $\\ 20^-$ $\\ 20^+$	3 $\\ 1$ $\\ 1$	$\mathbf{3} \cdot 1 = 3$ $\\ \mathbf{1} \cdot 1 = 1$ $\\ \mathbf{1} \cdot 1 = 1$
$A_6.C_2$	G	$[11, 0]$	$[11, 0]$	-	1	$\mathbf{1} \cdot 1 = 1$
$(C_3 \times C_3) \rtimes Q_8$	$C_2 \times G$	$[110, 45, 6]$	$[110, 55]$	6 $\\ 2$	1 $\\ 1$	$\mathbf{1} \cdot 2 = 2$ $\\ \mathbf{1} \cdot 1 = 1$
A_6	$C_2 \times G$	$[22, 11, 2]$	$[22, 11]$	2	1	$\mathbf{1} \cdot 1 = 1$
$N_G(S),\ S \in \text{Syl}_3(G)$	G	$[55, 0]$	$[55, 0]$	2	1	$\mathbf{1} \cdot 1 = 1$
$(C_3 \times C_3) \rtimes C_8$	$C_2 \times G$	$[110, 45, 6]$	$[110, 55]$	2	1	$\mathbf{1} \cdot 1 = 1$
$(C_3 \times C_3) \rtimes D_8$	$C_2 \times G$	$[110, 55, 2]$	$[110, 55]$	2	1	$\mathbf{1} \cdot 1 = 1$

Table 7.13: $G = M_{12}$

$\mathrm{Stab}_{\Delta(G)}(1)$	$\mathfrak{N}$	$D(\Delta, G)$	C	d	$\lvert \mathfrak{C}/\sim_{\mathfrak{N}} \rvert$	$\lvert \mathfrak{C} \rvert$
$PSL(2,11)$	$\mathrm{Aut}(G)$	$[144, 65, 16]^+$	$[144, 67]$	12^- 16^-	5 4 $\sum = 9$	$\mathbf{4} \cdot 2 + \mathbf{1} \cdot 1 = 9$ $\mathbf{2} \cdot 2 + \mathbf{2} \cdot 1 = 6$ $\sum = 15$
$PSL(2,11)_{\max}$	$\mathrm{Aut}(G)$	$[144, 55, 20]^+$	$[144, 56]$	12^+ 20^- 20^+	1 1 1	$\mathbf{1} \cdot 1 = 1$ $\mathbf{1} \cdot 1 = 1$ $\mathbf{1} \cdot 1 = 1$
S_6	G	$[132, 55, 8]^+$	$[132, 66]$	2 4^- 6 8^-	1 2 2 4	$\mathbf{1} \cdot 1 = 1$ $\mathbf{2} \cdot 1 = 2$ $\mathbf{2} \cdot 1 = 2$ $\mathbf{4} \cdot 1 = 4$
$A_6.C_2$	G	$[132, 65, 4]^+$	$[132, 66]$	2 4^-	1 2	$\mathbf{1} \cdot 1 = 1$ $\mathbf{2} \cdot 1 = 2$
$\mathrm{Aut}(A_6)$	G	$[66, 11, 20]^-$	$[66, 11]$	20^-	1	$\mathbf{1} \cdot 1 = 1$
M_{11}	G	$[12, 1, 12]^+$	$[12, 1]$	12^+	1	$\mathbf{1} \cdot 1 = 1$

Bibliography

[1] A. Bak. K-Theory of forms. *Annals of Mathematics Studies*, 98, 1981.

[2] S. D. Berman. On the theory of group codes. *Kibernetika*, 3:31–39, 1967.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24:235–265, 1997.

[4] C. C. Chevalley. *The algebraic theory of spinors*. Columbia University Press, 1954.

[5] N. Chigira, M. Harada, and M. Kitazume. Permutation groups and binary self-orthogonal codes. *Journal of Algebra*, 309:610–621, 2007.

[6] C. W. Curtis and I. Reiner. *Methods of Representation Theory*, volume 1. John Wiley and Sons, 1990.

[7] J. Dieudonné. Pseudo-discriminant and Dickson invariant. *Pacific Journal of Mathematics*, 5:907–910, 1955.

[8] A. Fröhlich and A. McEvett. Forms over rings with involution. *Journal of Algebra*, 12:79–104, 1969.

[9] A.M. Gleason. Weight polynomials of self-dual codes and the MacWillams identities. In *Actes du Congrès International des Mathèmaticiens*, volume 3, pages 211–215, Nice, 1970. Gauthiers-Villars.

[10] M. J. E. Golay. Notes on digital coding. In *Proceedings of the I.R.E.*, volume 37, page 657, June 1949.

[11] A. Günther. A mass formula for self-dual permutation codes. to appear in Finite Fields and their Applications.

[12] A. Günther and G. Nebe. Automorphisms of doubly-even self-dual binary codes. to appear in Journal of the London Mathematical Society.

[13] A. Günther and G. Nebe. Clifford-Weil groups of quotient representations. *Albanian Journal of Mathematics*, 2:159–169, 2008.

[14] A. Günther, G. Nebe, and E. M. Rains. Clifford-Weil groups for finite group rings, some examples. *Albanian Journal of Mathematics*, 2:185–198, 2008.

[15] R. W. Hamming. Error detecting and error correcting codes. *The Bell System Technical Journal*, 26:147–160, 1950.

[16] C. M. Hernandez and M. R. Sanchez. Relative hermitian Morita theory. I. Morita equivalences of algebras with involution. *Journal of Algebra*, 162:146–167, 1993.

[17] R. Howe. Invariant theory and duality for classical groups over finite fields, with applications to their singular representation theory. Preprint.

[18] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge UK, 2003.

[19] G. Hughes. Structure theorems for group ring codes with an application to self-dual codes. *Designs, Codes and Cryptography*, 24:5–14, 2001.

[20] M. Klemm. Über die Reduktion von Permutationsmoduln. *Mathematische Zeitschrift*, 143:113–117, 1975.

[21] M. Kneser. Klassenzahlen definiter quadratischer Formen. *Archiv der Mathematik*, 8:241–250, 1057.

[22] M. Kneser. *Quadratische Formen*. Springer, 2002.

[23] M. Knus, A. Merkurjev, M. Rost, and J. Tignol. *The book of involutions*. Vol. 44 of American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, 1998.

[24] F. J. MacWilliams. *Codes and ideals in group algebras*. Combinatorial Mathematics and its Applications. University of North Carolina Press, Chapel Hill, 1969.

[25] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland Mathematical Library 16. North-Holland Publishing Co., 1977.

[26] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson. Good self-dual codes exist. *Discrete Mathematics*, 3:153–162, 1972.

[27] C. Martinez-Pérez and W. Willems. Self-dual codes and modules for finite groups in characteristic two. *IEEE Trans. Inform. Theory*, 50(8):1798–1803, 2004.

[28] C. Martínez-Pérez and W. Willems. Self-dual extended cyclic codes. *Applicable Algebra in Engineering, Communication and Computing*, 1:1–16, 2006.

[29] J. Morales. Maximal hermitian forms over $\mathbb{Z}G$. *Commentarii mathematici Helvetici*, 63:209–225, 1988.

[30] A. Munemasa. A mass formula for Type II codes over finite fields of characteristic two. In *Codes and designs*, Ohio State Univ. Math. Res. Inst. Publ. 10, pages 207–214, Columbus, OH, 2000.

[31] G. Nebe. On the cokernel of the Witt decomposition map. *Journal de Théorie de Nombres de Bordeaux*, 12:489–501, 2000.

[32] G. Nebe, H.-G. Quebbemann, E. M. Rains, and N. J. A. Sloane. Complete weight enumerators of generalized doubly even self-dual codes. *Finite Fields and their Applications*, 10:540–550, 2004.

[33] G. Nebe, E.M. Rains, and N.J.A. Sloane. *Self-dual codes and invariant theory*. Algorithm and Computation in Mathematics 17. Springer, 2006.

[34] T. Okuyama and Y. Tsushima. On a conjecture of P. Landrock. *Journal of Algebra*, 104:203–208, 1986.

[35] H.-G. Quebbemann. On even codes. *Discrete Mathematics*, 98(1):29–34, 1991.

[36] E. M. Rains. Shadow bounds for self-dual codes. *IEEE Trans. Info. Theory*, 44:134–139, 1998.

[37] W. Scharlau. *Quadratic and Hermitian Forms*. Die Grundlehren der Mathematischen Wissenschaften 270. Springer, 1985.

[38] P. Sin and W. Willems. *G*-invariant quadratic forms. *Journal für die reine und angewandte Mathematik*, 420:45–59, 1991.

[39] N.J.A. Sloane. Gleason's theorem on self-dual codes and its generalizations. Talk given at Conference on Algebraic Combinatorics in honor of Eiichi Bannai, Sendai, Japan, June 2006.

[40] N.J.A. Sloane and J.G. Thompson. Cyclic self-dual codes. *IEEE Trans. Inform. Theory*, 29(3):364–366, 1983.

[41] D. E. Taylor. *The geometry of the classical groups*. Sigma Series in Pure Mathematics 9. Heldermann Verlag, 1992.

[42] W. Willems. A note on self-dual group codes. *IEEE Trans. Inf. Theory*, 48(12):3107–3109, 2002.

[43] W. Willems and A. Zimmermann. On Morita theory for self-dual modules. *Quarterly Journal of Mathematics (Oxford)*, pages 1–14, 2008.

Lebenslauf

Annika Günther

17.08.1983	geboren in Neuss
1990 - 1993	Burgunderschule in Neuss (Grundschule)
1993 - 2001	Cornelius-Burgh-Gymnasium in Erkelenz
Okt. 2001 - Sep. 2003	Grundstudium der Mathematik an der Heinrich-Heine-Universität Düsseldorf
Okt. 2003 - Sep. 2006	Hauptstudium an der RWTH Aachen
Sep. 2006	Diplom in Mathematik von der RWTH Aachen
Okt. 2006 - Sep. 2009	Doktorandin an der RWTH Aachen, gefördert durch die Landesgraduiertenförderung