Orthogonal Representations of Finite Groups

Dissertation

Oliver Braun

October 9, 2016

Updated version

This is an updated version of my PhD thesis. An error in Remark 6.5.9 is corrected and in Section 6.4 I include a reference to [BN16], which removes the restriction that n be 1 or 2.

Oliver Braun
October 9, 2016

Contents

1 Introduction

In ordinary representation theory of finite groups one studies linear actions of finite groups on finite-dimensional vector spaces over a field K whose characteristic does not divide the group order. Such an action on a vector space V naturally gives rise to an action on $K[V]$, the ring of polynomial functions on V. The study of fixed points of G on $K[V]$ is the subject of algebraic invariant theory, which originated in the nineteenth century and was later extended to include geometric aspects of orbit spaces of linear algebraic groups on algebraic varieties and schemes.

In fact, the idea of examining properties of mathematical objects that stay the same when certain transformations are applied to the object is so universal that it pervades all of mathematics. Examples include elementary geometric properties such as the sum of the angles of a triangle and the ratio of the radius and circumference of a circle, which are constant for triangles of all shapes and sizes and circles of all radii. In linear algebra, the trace and determinant of a linear endomorphism remain unchanged when base change is applied, in discrete mathematics an example is provided by the chromatic number of a graph, which is an invariant under graph isomorphisms and in measure theory, the famous Lebesgue measure of a set is unaffected by translations.

Returning to the subject of representation theory of finite groups, consider a representation $\Delta : G \to \mathrm{GL}(V)$. We pose the question whether there exists a non-degenerate quadratic form q on V such that $\Delta(G)$ is a subgroup of the orthogonal group $\mathrm{O}(V, q)$ – justifying the designation "orthogonal representation" for such a pair (V, q). If that is the case q is necessarily an invariant of the naturally induced action of G on the space of all quadratic forms on V and the task of investigating the properties of q suggests itself. In fact under some mild restrictions the existence of such a quadratic form is guaranteed and the inspection of its properties is the central topic of this thesis.
An alternative formulation of this problem is the following. Given Δ, assume that the space of G-invariant quadratic forms on V is one-dimensional, in which case we call the representation Δ uniform. It is well known that the so-called character χ – which is defined as $\chi(g) = \mathrm{tr}(\Delta(g))$ for all $g \in G$ – completely determines Δ up to a suitable equivalence relation. So it is fair to say that χ determines q up to multiplication by scalars of K. Our research problem, which is precisely formulated on page 46, may now be stated as: How can one read off properties of q from the character χ?

We borrow suitable invariants to determine the isometry class of q from the algebraic

theory of quadratic forms, which was originally a branch of number theory linked to diophantine equations. It grew to become an independent subject of mathematics with deep connections not only to number theory but also geometry, group theory, topology and modular forms.
For the present work the discriminant $\mathrm{d}_{\pm}(q)$ and the Clifford invariant $\mathfrak{c}(q)$, which are introduced in due course, are of tremendous importance.

A remarkably simple answer to the abovementioned question exists in case the character χ has values in an imaginary quadratic number field $\mathbb{Q}(\sqrt{\delta})$. There exists no G-invariant quadratic form on V, however $\chi + \overline{\chi}$ is the character of a uniform representation and the arising quadratic form q has discriminant $\mathrm{d}_{\pm}(q) = \delta^{\chi(1)}$. Under favorable circumstances one may even derive the Clifford invariant from the knowledge of δ and representation-theoretic properties of χ. See Theorem 4.3.9 for details.

The relationship between χ and the isometry type of q was also investigated by Gabriele Nebe in [Neb99] and the subsequent publication [Neb00a], where a character-theoretic method was developed and applied to provide an answer in some cases. Another result of Nebe's is a version of Frobenius reciprocity for orthogonal representations which yields, among other things, a description of the S_n-invariant bilinear forms on some irreducible representations. We give an account of both methods in the body of this thesis, cf. Corollary 4.3.20 and Theorem 4.3.13.

Outline and results

Chapter 3 serves as an introduction to the algebraic theory of bilinear and quadratic forms. We introduce the abovementioned invariants $\mathrm{d}_{\pm}$ and $\mathfrak{c}$ for quadratic forms and discuss quadratic forms over certain kinds of rings. While most of the covered material, which we mainly extracted from Martin Kneser's work [Kne02], is classical and well known to experts, we present a useful periodicity result for the Clifford invariant which we have not found in the literature. It describes a periodicity modulo 8 in the sequence

$$\mathfrak{c}(\varphi),\ \mathfrak{c}(\varphi \ominus \varphi),\ \mathfrak{c}(\varphi \ominus \varphi \ominus \varphi),\ \dots$$

for regular quadratic spaces φ, cf. Theorem 3.6.26.

We begin the fourth chapter by briefly introducing the necessary tools and results from the representation theory of finite groups. We then proceed to define orthogonal representations, give some structure results and precisely formulate the central research task for this thesis. The conclusion of the chapter consists of several general methods to tackle the question of determining the K-isometry class of q for an orthogonal representation (V, q), including the three methods mentioned above and a novel result which is a version of Clifford's theorem for orthogonal representations of normal subgroups, cf. Theorem 4.3.14.

Chapter 5 briefly touches upon the subject of orthogonal representations with Schur index 2. We outline previous work on the matter by Alexandre Turull, [Tur93], and formulate a conjecture for a similar situation.

Those general results are then applied in Chapter 6 which is devoted to orthogonal representations of some infinite families of finite groups. First the work of Gabriele Nebe on cyclic and symmetric groups is reviewed. Then we discuss new findings on semidirect products of cyclic groups and present a nearly complete classification of the orthogonal representations of the finite groups $\mathrm{SL}_2(q)$ for arbitrary prime powers q. The details of this classification are the contents of Theorems 6.4.27 and 6.5.10. Clearly these are interesting results in their own right, but they are also of considerable use when trying to determine the orthogonal representations of the finite simple groups. This is because the groups $\mathrm{PSL}_2(q)$ are not only simple but also frequently appear as (maximal) subgroups of other such groups.

The following chapter is predominantly of independent interest. It is concerned with what we call Clifford orders, which we define as follows. Let L be an integral lattice in a quadratic space (V, q) with Clifford algebra $g : V \to \mathcal{C}(V, q)$. Then

$$\mathcal{C}(L) := \langle g(\ell) \mid \ell \in L \rangle ,$$

the order generated by the image of L in $\mathcal{C}(V, q)$, is called the Clifford order of L. We provide some basic properties of such orders before studying their $\mathfrak{p}$-adic Jacobson radicals and the first step of the radical idealizer process, which is a procedure to obtain a hereditary over-order dating back at least to work of Herbert Benz and Hans Zassenhaus, [BZ85]. Our examination of the radical idealizer process culminates in a characterization of the hereditary Clifford orders in terms of invariants of the quadratic lattice (L, q) for odd and even residue class characteristics.
Finally we discuss idempotents in $\mathfrak{p}$-adic Clifford orders, which concludes the theoretical part of this thesis.

In Chapter 8 we present the algorithms used in our studies. We give pseudo-code for all algorithms so that they may be easily implemented in any suitable computer algebra system.

The last chapter contains a number of examples of classifications of orthogonal representations which were obtained through both the theoretical and algorithmic methods presented in the previous chapters. We focus mainly on finite simple groups discussed in the Atlas of Finite Groups [CCN$^+$85] as they offer a wealth of interesting examples and also provide us with some computational challenges due to their increasing size and complexity.

Acknowledgements

In the first place I wish to thank my advisor Prof. Dr. Gabriele Nebe. Not only did she suggest the interesting research topic of my thesis, she also provided me with valuable advice countless times and always demonstrated great interest in my work. Prof. Nebe also acted as the speaker of the DFG research training group “Experimental and Constructive Algebra” from which I held a scholarship during my work on this thesis. I am indebted to the DFG for providing me with funding and thereby the possibility to pursue this research project.

It has been a privilege to work with many distinguished colleagues at Lehrstuhl D für Mathematik. Above all I should mention my friend and colleague Sebastian Schönnenbeck, to whom I am grateful for numerous fruitful discussions and constant encouragement. Furthermore my thanks go to Dr. Markus Kirschmer for helpful advice concerning the computer algebra system `Magma`.

Finally I would like to thank my friends, my parents and my siblings for supporting me throughout my studies.

2 Symbols, notations and conventions

Sets and combinatorics

1. The disjoint union of sets is denoted by $\sqcup$.
2. The difference of sets is denoted by $-$.
3. In this thesis, the set $\mathbb{N}$ of natural numbers does not contain 0.
   We write $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$.
4. If $n \in \mathbb{N}$ is a natural number, we write $\underline{n} := \{x \in \mathbb{N} \mid x \leq n\}$.
5. For $n \in \mathbb{N}$, we define $\begin{pmatrix} n \\ k \end{pmatrix} := \begin{cases} \frac{n!}{k!(n-k)!} & 0 \leq k \leq n, \\ 0 & k < 0 \text{ or } k < n. \end{cases}$

Rings

1. All rings are associative and unital. Commutativity of multiplication is not assumed.
2. If R is a ring, $R^\times$ denotes its unit group.
3. If R is commutative, $(R^\times)^2 := \{x^2 \mid x \in R^\times\}$ denotes the subgroup of squares of $R^\times$.
4. $Z(R)$ denotes the center of R, i.e. $Z(R) = \{x \in R \mid xy = yx \text{ for all } y \in R\}$.
5. If R is an integral domain, we dnote by $\mathrm{Quot}(R)$ the quotient field, or field of fractions, of R.
6. For $n \times n$-matrices over a ring R, we use the notation $R^{n \times n}$, or, if the expression for n is more complicated, $\mathrm{Mat}_n(R)$.

Modules

1. Unless otherwise stated, all modules considered are left modules.
2. If M is an R-module, M^* denotes the dual R-module $\mathrm{Hom}_R(M, R)$.

Groups

1. If n is a natural number, C_n designates an abstract cyclic group of order n.

3 Bilinear and quadratic forms

3.1 First definitions

In this section let A denote a commutative ring. Although there is classically a strong preference for studying quadratic forms over fields of characteristic distinct from two, we will define as many of the concepts as possible for commutative rings of arbitrary characteristic, mainly following Martin Kneser's "Quadratische Formen" [Kne02], from which we cite most definitions and results.

Definition 3.1.1 (Bilinear modules) Let M be a module over A and b a symmetric bilinear form on M, that is, a map

$$b \ : \ M \times M \to A$$

satisfying $b(x, y) = b(y, x)$ and $b(ax + y, z) = ab(x, z) + b(y, z)$ for all $x, y, z \in M$ and $a \in A$. Then we call (M, b) a bilinear A-module.

Definition 3.1.2 (Isometry of bilinear forms) Let (M, b), (M', b') be two bilinear A-modules. An isometry (sometimes more precisely referred to as an isometric embedding)

$$\varphi \ : \ (M, b) \to (M', b')$$

from (M, b) to (M', b') is an injective A-module homomorphism with the additional property that for all $x, y \in M$ we have $b'(\varphi(x), \varphi(y)) = b(x, y)$.
(M, b) and (M', b') are said to be isometric, written as $(M, b) \cong (M', b')$, if there is a bijective isometry between them, in which case the inverse map φ^{-1} is an isometry as well, thus yielding an equivalence relation on bilinear spaces.

Definition 3.1.3 (Orthogonality) Let (M, b) be a bilinear module over A with elements $x, y \in M$ and a submodule $N \subseteq M$.

1. x and y are called orthogonal (or perpendicular) if $b(x, y) = 0$.

2. $N^\perp := \{x \in M \mid b(x, f) = 0 \text{ for all } f \in F\}$ is called the orthogonal submodule of N (one easily checks that this is indeed a submodule of M and that $(F^\perp)^\perp \supseteq F$).

3. Let $M_1, ..., M_n$ be submodules of M. We say that M is the orthogonal direct sum of the submodules $M_1, ..., M_n$ if
$$M = \bigoplus_{i=1}^{n} M_i$$
and $b(M_i, M_j) = \{0\}$ for $1 \leq i \neq j \leq n$. In this situation, we write
$$M = \bigoplus_{i=1}^{n} M_i.$$

Definition 3.1.4 If V is an A-module, we let $V^* := \mathrm{Hom}_A(V, A)$.
Given a submodule N of a bilinear A-module (M, b), we define the module homomorphism
$$b_N \ : \ M \to N^*, m \mapsto \Big(n \mapsto b(m, n)\Big).$$
Notice that $\ker(b_N) = N^\perp$.

Lemma 3.1.5 ([Kne02, (1.3)]) *Again, let (M, b) be a bilinear module with submodule N. We have $M = N \oplus N^\perp$ if and only if $N \cap N^\perp = \{0\}$ and $b_N(M) = b_N(N)$.*

Definition 3.1.6 A bilinear module (M, b) is called non-degenerate if b_M is injective, i.e. $M^\perp = \{0\}$. The bilinear module is called regular if b_M is injective and M is finitely generated and projective as an A-module.
A submodule $N \leq M$ is called non-degenerate or regular if these properties hold for $(N, b|_{N \times N})$.

Theorem 3.1.7 ([Kne02, Satz (1.6)]) *Any regular submodule of a bilinear module (M, b) is an orthogonal direct summand of M.*

Theorem 3.1.8 ([Kne02, Satz (1.7)]) *An orthogonal direct sum of bilinear modules is non-degenerate or regular, respectively, if and only if this holds for each summand.*

If the bilinear A-module under consideration is free of finite rank as an A-module, there is an important invariant of the isometry class, which we will now define.

Definition 3.1.9 (Gram matrix) Let (M, b) be a free bilinear A-module of finite rank n with ordered basis $B := (m_1, ..., m_n)$. The matrix $(b(m_i, m_j))_{1 \leq i,j, \leq n}$ is called the Gram matrix of (M, b) with respect to the basis B.

Definition 3.1.10 We denote a free bilinear A-module with an $n \times n$-Gram matrix $G = (g_{i,j})_{1 \leq i,j \leq n}$ by
$$\left\langle \begin{matrix} g_{1,1} & \cdots & g_{1,n} \\ \vdots & ... & \vdots \\ g_{n,1} & \cdots & g_{n,n} \end{matrix} \right\rangle.$$
If G is a diagonal matrix with elements $g_1, ..., g_n$ on the diagonal we also write $\langle g_1, ..., g_n \rangle$.

Notice that if we perform a base change on M, using a matrix $T \in \mathrm{GL}_n(A)$, the Gram matrix G changes to $T^{tr}GT$. This motivates the following definition.

Definition 3.1.11 (Determinant and discriminant) Let (M, b) be a free bilinear A-module with Gram matrix G (with respect to some basis). Then we call

$$\det(M, b) := \det(G)(A^\times)^2 \in A/(A^\times)^2$$

the determinant of (M, b). The fact that we have defined the determinant to be an element of the square class group $A/(A^\times)^2$ renders this construction independent of the choice of a basis, thus yielding an isometry invariant.
Putting $m := \mathrm{rank}_A(M)$, we call the invariant

$$\mathrm{d}_\pm(M, b) := (-1)^{m(m-1)/2} \det(M, b) \in A/(A^\times)^2,$$

which sometimes shows a more desirable behavior than $\det(M, b)$, the discriminant of (M, b).

We can now describe non-degeneracy and regularity of bilinear spaces in terms of their determinants.

Theorem 3.1.12 ([Kne02, Satz (1.15)]) *A free bilinear module (M, b) over a ring A is non-degenerate if and only if $\det(M, b)$ is not a zero divisor in A. It is regular if and only if $\det(M, b)$ is invertible.*

If the ring A is a field we obtain some stronger results which we shall briefly discuss now.

Theorem 3.1.13 ([Kne02, Satz (1.19)]) *A finite-dimensional bilinear space over a field is regular if and only if it is non-degenerate.*
For any subspace F of a regular bilinear space (V, b) we have

$$\dim(F) + \dim(F^\perp) = \dim(V)$$

and $(F^\perp)^\perp = F$.

Theorem 3.1.14 ([Kne02, Satz (1.20)]) *Let (V, b) be a finite-dimensional bilinear space over a field A. There is a decomposition*

$$V = \left(\bigoplus_{i=1}^{r} V_i \right) \oplus F$$

where all V_i are regular subspaces of dimension 1 or 2 and $b(F, F) = 0$. V is regular if and only if $F = \{0\}$.
In case the characteristic of A is not two, one may choose the V_i to be one-dimensional. A suitable basis may be found by extending a basis of F to a basis of V by choosing vectors which are pairwise orthogonal.

Example 3.1.15 In this example, we present two infinite series of important bilinear modules over the ring $\mathbb{Z}$.

1. Let $L := \mathbb{Z}^n$ and
$$b \ : \ L \times L \to \mathbb{Z}, \ (x, y) \mapsto \sum_{i=1}^{n} x_i y_i.$$
Then we define $\mathbb{I}_n$ to be the bilinear $\mathbb{Z}$-module (L, b). With respect to the standard basis $\{e_1, ..., e_n\}$ of L the Gram matrix of $\mathbb{I}_n$ is the identity matrix - the determinant is $\det(\mathbb{I}_n) = 1$.
$\mathbb{I}_n$ is decomposable as $\bigoplus_{i=1}^{n} \langle 1 \rangle$.

2. $\mathbb{A}_n := \{(x_1, ..., x_{n+1}) \in \mathbb{I}_{n+1} \mid \sum_{i=1}^{n+1} x_i = 0\} \leq \mathbb{I}_{n+1}$. A $\mathbb{Z}$-basis of $\mathbb{A}_n$ is given by
$$e_1 - e_2, \ e_2 - e_3, \ ..., e_n - e_{n+1}$$
with Gram matrix
$$\begin{pmatrix} 2 & -1 & & & & \\ -1 & 2 & -1 & & & \\ & -1 & 2 & & & \\ & & & \ddots & & \\ & & & & 2 & -1 \\ & & & & -1 & 2 \end{pmatrix}.$$
We obtain $\det(\mathbb{A}_n) = n + 1$.
Notice that $\mathbb{A}_n$ is the orthogonal module of the vector $(1, 1, ..., 1) \in \mathbb{I}_{n+1}$.

Next, we will define quadratic forms.

Definition 3.1.16 (Quadratic forms) Let E be an A-module and consider a map $q \ : \ E \to A$ satisfying
$$q(ax) = a^2 q(x) \text{ for all } a \in A, \ x \in E \text{ and}$$
$$q(x + y) = q(x) + q(x) + b_q(x, y)$$
for some bilinear form b_q on E. (E, q) is called a quadratic A-module.

Definition 3.1.17 (Isometry of quadratic forms) Assume that (E, q) and (E', q') are two quadratic modules. An isometry $f \ : \ (E, q) \to (E', q')$ is a module monomorphism $E \to E'$ such that $q'(f(x)) = q(x)$ for all $x \in E$.
(E, q) and (E', q') are said to be isometric, written $(E, q) \cong (E', q')$, if there is a bijective isometry between them, just as in the case of bilinear modules.

Definition 3.1.18 (Scaling of modules and forms) Let $\varphi := (E, f)$ be a bilinear or quadratic module over a ring A. Then we put $a\varphi := (aE, f)$ and $a \circ \varphi := (E, af)$ for $a \in A$.

Definition 3.1.19 (Extension of scalars) If (E, q) is a quadratic module over A and $S \supseteq A$ is a ring extension, we define $S \otimes_A (E, q)$ to be the quadratic S-module $(S \otimes_A E, q_S)$, where q_S is defined by $q_S(s \otimes e) := s^2 q(e)$ and $b_{q_S}(s \otimes e, s' \otimes e') := ss' b_q(e, e')$. We also define the scalar extension of bilinear spaces in accordance with this definition.

Remark 3.1.20 The class of all quadratic A-modules forms a category with (injective) isometries as morphisms. We denote this category by A-QMod.

Definition 3.1.21 Let (E, q) and (E', q') be quadratic modules over A.

1. The orthogonal direct sum of (E, q) and (E', q'), denoted by $(E, q) \oplus (E', q')$, is defined to be the module $E \oplus E'$ with quadratic form $q \oplus q'$ defined by

$$(q \oplus q')(x, x') := q(x) + q(x').$$

2. The tensor product of (E, q) and (E', q'), $(E, q) \otimes (E', q')$, is the module $E \otimes_A E'$ equipped with the quadratic form $q \otimes q'$ defined by

$$(q \otimes q')(x \otimes x') := 2q(x) \cdot q'(x') \text{ and } b_{q \otimes q'}(x \otimes x', y \otimes y') = b_q(x, y) \cdot b_{q'}(x', y').$$

The introduction of the factor 2 in the definition of the tensor product may seem remarkable. It is, however, necessary, as will be explained in Remark 3.1.23.

Definition 3.1.22 1. A quadratic A-module (E, q) is called regular if (E, b_q) is regular. (E, q) is called non-degenerate if (E, b_q) is non-degenerate.

2. $x \in E$ is called singular if $q(x) = 0$.

3. A submodule $F \leq E$ is called singular if $q(F) = \{0\}$.

4. (E, q) is called anisotropic if $q(x) = 0$ implies $x = 0$.

5. We define the determinant $\det(E, q)$ to be $\det(E, b_q) \in A/(A^\times)^2$ and the discriminant $\mathrm{d}_\pm(E, q) := \mathrm{d}_\pm(E, b_q) \in A/(A^\times)^2$.

From the definition of quadratic forms we obtain the equation

$$4q(x) = q(2x) = q(x + x) = 2q(x) + b_q(x, x), \tag{3.1}$$

implying

$$2q(x) = b_q(x, x)$$

which has important consequences for the theory.

Remark 3.1.23 Equation (3.1) sheds light on the factor 2 occurring in the definition of the tensor product. Namely, we have

$$\begin{aligned}2(q \otimes q')(x \otimes x') &= b_{q\otimes q'}(x \otimes x', x \otimes x')\\ &= b_q(x,x)b_{q'}(x',x')\\ &= 2q(x) \cdot 2q'(x'),\end{aligned}$$

which shows that our definition is appropriate by cancelling the factor 2 (if 2 is not a zero-divisor in A).

Remark 3.1.24 Let (M, b) be a bilinear module over A. Then M is a quadratic A-module with quadratic form q_b given by

$$q_b \ : \ M \to A, \ m \mapsto b(m,m).$$

In light of equation (3.1), notice that we have the equations

$$b_{q_b} = 2b \text{ and } q_{b_q} = 2q.$$

This shows that the notions of bilinear modules and quadratic modules are equivalent if $2 \in A^\times$.
Concretely, if we associate to a bilinear space (E, b) the quadratic space $(E, \frac{1}{2}q_b)$, then we can reconstruct (E, b) via $b_{\frac{1}{2}q_b} = b$. Conversely, we associate to a quadratic space (E, q) the bilinear space $(E, \frac{1}{2}b_q)$ in order to be able to reconstruct (E, q) via $q_{\frac{1}{2}b_q} = q$.

If $2 \notin A^\times$, but 2 is not a zero divisor in A, q is still uniquely determined by b_q.

Most generally, one can always find a (not necessarily symmetric) bilinear form $a \ : \ E \times E \to A$ such that $q(x) = a(x,x)$ if E is a free module of finite rank. In this case, we have $b_q(x,y) = a(x,y) + a(y,x)$.
If $\{e_1, ..., e_n\}$ is a basis of E, we have

$$q\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n q(e_i)x_i^2 + \sum_{1\le i<j\le n} b_q(e_i,e_j)x_i x_j$$

and we can define

$$a\left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j\right) := \sum_{1\le i\le j\le n} a_{i,j} x_i y_j, \tag{3.2}$$

where $a_{i,i} := q(e_i)$ and $a_{i,j} := b_q(e_i, e_j)$ for $i \le j$.

Definition 3.1.25 A free quadratic A-module E defined as in the situation of equation (3.2) of the last remark is denoted by

$$(E,q) = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ & a_{2,2} & & \\ & & \ddots & \\ & & & a_{n,n} \end{bmatrix}$$

or $(E,q) = [a_1, ..., a_n]$ if $q\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n a_i x_i^2$.
If $2 \in A$ is not a zero divisor, we put $b_{i,j} := b_q(e_i, e_j) = b_{j,i}$ and may also write

$$(E,q) = \left\langle \begin{matrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & \ldots & \vdots \\ b_{n,1} & \cdots & b_{n,n} \end{matrix} \right\rangle .$$

For example, letting A be a ring where 2 is not a zero divisor, if $E = A$ is free of rank one with basis vector e_1 and quadratic form q defined by $q(e_1) = 1$, we have $(E,q) = [1] = \langle 2 \rangle$.

Definition 3.1.26 (Hyperbolic modules) The free quadratic A-module (A^2, q) with $q\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) := x_1 x_2$ is called the hyperbolic plane over A. We denote this quadratic module by $\mathbb{H} := \mathbb{H}(A)$ and we have

$$\mathbb{H} = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} = \left\langle \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \right\rangle .$$

Notice that $\det(\mathbb{H}) = -1$, whence $\mathbb{H}$ is always a regular quadratic module over any ring.

Let (E,q) be a quadratic A-module which is finitely generated and projective. We define $\mathbb{H}(E,q)$ to be a quadratic space on $E \oplus E^*$ with quadratic form defined by

$$\overline{q}(x,f) := q(x) + f(x)$$

for all $x \in E$ and $f \in E^*$.
$\mathbb{H}(E,q)$ is regular since as one readily verifies from the concrete description of $b_{\mathbb{H}(E,q)}$ as

$$b_{\mathbb{H}(E,q)} \ : \ \mathbb{H}(E,q) \to \mathbb{H}(E,q)^*, \ (x,f) \mapsto \Big((y,g) \mapsto b_q(x,y) + f(y) + g(x)\Big).$$

In fact, the isometry type of the quadratic module $\mathbb{H}(E,q)$ is independent of q. An isometry $\mathbb{H}(E,q) \cong \mathbb{H}(E,0)$ is easily constructed, cf. [Kne02, (2.20)]. The quadratic space $\mathbb{H}(E) := \mathbb{H}(E,0)$ is called the hyperbolic module associated to E.

In the case $2 \notin A^\times$, or even $\mathrm{char}(A) = 2$, it follows from equation 3.1 that there are no free regular quadratic modules of rank 1. In fact, there are no free regular modules of any odd rank n, as we shall see in the following.

Theorem 3.1.27 ([Kne02, (2.9)-(2.11)]) *Let (E,q) be a free quadratic A-module of odd rank n, with basis $\{e_1, ..., e_n\}$. Then there is a polynomial $P_n \in \mathbb{Z}[X_1, ..., X_{\frac{n(n+1)}{2}}]$ satisfying*

$$\det(E,q) = 2P_n(q(e_i), b_q(e_i, e_j)).$$

Definition 3.1.28 Let (E, q) be free of odd rank n and basis $\{e_1, ..., e_n\}$. Then we call

$$\mathrm{d}_{\frac{1}{2}}(E, q) := P_n(q(e_i), b_q(e_i, e_j))(A^\times)^2 \in A/(A^\times)^2$$

the semi-determinant of (E, q). We call (E, q) semi-regular if any (and thereby all) representatives of the square class of $\mathrm{d}_{\frac{1}{2}}(E, q)$ are invertible in A.
Notice that we have $\det(E, q) = 2\mathrm{d}_{\frac{1}{2}}(E, q)$.

Clearly our definition of the semi-determinant is independent of the choice of a basis since we have defined it to be a square class, like the determinant. If $2 \in A^\times$ then any semi-regular space is also regular. In contrast, if $2 \notin A^\times$ we can consider the quadratic module $[1]$ which is not regular - it has determinant 2 - but semi-regular, as its semi-determinant is 1.

Finally we formulate an analogue of Theorem 3.1.14 for quadratic spaces over fields.

Theorem 3.1.29 ([Kne02, Satz (2.15)]) *Let (E, q) be a finite-dimensional quadratic vector space over a field A. There is a decomposition*

$$(E, q) = \bigoplus_{i=1}^{r} E_i \oplus \bigoplus_{j=1}^{s} F_j \oplus G$$

where the E_i are regular of dimension two, the F_j are semi-regular of dimension one and $q(G) = \{0\}$.

If $\mathrm{char}(A) \neq 2$ we may choose $r = 0$ and all F_j are regular.
If A is of even characteristic $A^2 := \{a^2 \mid a \in A\}$ is a subfield of A and we may choose $s \leq [A : A^2]$.

(E, q) is regular if and only if $s = 0$ and $G = \{0\}$.
(E, q) is semi-regular if and only if $s \leq 1$ and $G = \{0\}$.

3.2 Orthogonal groups and Witt's theorem

Definition 3.2.1 (Orthogonal group) The automorphism group of a quadratic module (E, q) over a ring A is called the orthogonal group of (E, q). It is the group of invertible isometries $E \to E$, in symbols

$$\mathrm{O}(E, q) := \{f \;:\; E \to E \mid f \in \mathrm{Aut}_A(E) \text{ and } q(f(x)) = q(x) \text{ for all } x \in E\}.$$

If A is a field of characteristic distinct from two, we can formulate two equivalent theorems attributed to Witt which have far-reaching consequences.

Theorem 3.2.2 (Witt's cancellation theorem) *Let A be a field of characteristic not two and F, G_1 and G_2 quadratic spaces over A with F regular and $F \oplus G_1 \cong F \oplus G_2$. Then $G_1 \cong G_2$.*

Theorem 3.2.3 (Witt's extension theorem) *Let E be a quadratic space over a field A with $\mathrm{char}(A) \neq 2$. Let F_1, F_2 be regular subspaces and $t : F_1 \to F_2$ a bijective isometry. Then there is an extension of t to E, i.e. an element $u \in \mathrm{O}(E)$ satisfying $u|_{F_1} = t$.*

A proof of the equivalence of the two theorems and a proof of the statement itself may be found in [Kne02, Satz (3.1)].

In order to formulate a generalization of this theorem which drops the hypothesis on the characteristic of A, we first need a definition.

Definition 3.2.4 (Primitivity) Let E be an A-module.

1. A submodule $F \leq E$ is called primitive if F is a direct summand of E.

2. If E carries a bilinear form b and $F \leq E$ is a submodule, then F is called sharply primitive, if it is finitely generated, projective and $b_F(E) = F^*$.

Remark 3.2.5

1. Any regular submodule F is sharply primitive.

2. Any sharply primitive submodule is primitive.

3. If E is regular and $F \leq E$ is primitive, F is sharply primitive.

Given this definition, we can now state the generalized version of Theorem 3.2.3

Theorem 3.2.6 ([Kne02, Satz (3.4)]) *Let E be a quadratic space over a field A, $F_1, F_2 \leq E$ sharply primitive subspaces and $t : F_1 \to F_2$ a bijective isometry. Then t may be extended to an isometric automorphism of E.*

Corollary 3.2.7 (Witt cancellation) *Let F, G_1 and G_2 be quadratic spaces over a field A and let F be regular. Then $F \oplus G_1 \cong F \oplus G_2$ if and only if $G_1 \cong G_2$.*

Definition 3.2.8 (Witt index) If A is a field and (E, q) a finite-dimensional quadratic space over A, the dimension of a maximal singular and sharply primitive subspace is called the Witt index of (E, q), denoted by $\mathrm{ind}(E, q)$.

Corollary 3.2.9 *Let (E, q) be a quadratic space over a field A and put $m := \mathrm{ind}(E, q)$. Then there is a subspace $F \leq E$ such that $\mathrm{ind}(F, q|_F) = 0$ and $(E, q) \cong (F, q|_F) \oplus \mathbb{H}(A^m)$.*

Definition 3.2.10 In the situation of Corollary 3.2.9, we call $(F, q|_F)$ the anisotropic kernel of (E, q).

Definition 3.2.11 (Reflections) Let (E, q) be a quadratic A-module and $e \in E$ such that $q(e) \in A^\times$. Then

$$s_e \ : \ E \to E, \ x \mapsto x - b_q(x, e)q(e)^{-1}e$$

is called the reflection along e.

Remark 3.2.12 Reflections s_e have the following properties.

1. $s_e^2 = \mathrm{id}_E$.

2. $s_e(e) = -e$, $s_e(v) = v$ if $b_q(e, v) = 0$.

3. $s_e \in \mathrm{O}(E, q)$.

4. For any $g \in \mathrm{O}(E, q)$, we have $gs_eg^{-1} = s_{g(e)}$.

The following result is a consequence of Witt's theorems.

Theorem 3.2.13 ([Kne02, Satz (3.5)]) *If the quadratic space (E, q) is regular or semi-regular over a field A, any isometric automorphism $u \in \mathrm{O}(E, q)$ may be written as a product of reflections, unless $A = \mathbb{F}_2$ and $E \cong \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} \oplus \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$.*

3.3 The Witt group

In this section we define the Witt group of a ring. This is an Abelian group consisting of classes of regular quadratic forms under a certain equivalence relation which captures the "essential part" of a quadratic form. The group-theoretic structure of the Witt group then gives insight into the interplay of all regular quadratic forms over A.

Definition 3.3.1 Let φ and ψ be quadratic modules over a ring A. We call φ and ψ Witt equivalent if there are hyperbolic modules $\mathbb{H}_1$ and $\mathbb{H}_2$ such that

$$\varphi \oplus \mathbb{H}_1 \cong \psi \oplus \mathbb{H}_2.$$

Let

$$W(A) := \{[\varphi] \mid \varphi \text{ is a regular quadratic } A\text{-module}\}$$

denote the set of Witt equivalence classes of regular quadratic modules over A.
$W(A)$ is an Abelian group with group law $[\varphi] + [\psi] := [\varphi \oplus \psi]$, $-[\varphi] = [(-1) \circ \varphi]$ and neutral element $0 = [\mathbb{H}]$.

Remark 3.3.2 Clearly, if A is an integral domain, two regular quadratic modules over A are isometric if and only if they are Witt equivalent and of equal rank.

Remark 3.3.3 If A is a field, using Witt's cancellation theorem 3.2.7 and the decomposition from Corollary 3.2.9, one obtains that two regular quadratic forms over A are Witt equivalent if and only if their anisotropic kernels are isometric.
In other words, any Witt equivalence class is represented by an anisotropic space.

Example 3.3.4 If A is an algebraically closed field, we have

$$W(A) \cong \begin{cases} C_2 & \operatorname{char}(A) \neq 2, \\ 0 & \operatorname{char}(A) = 2. \end{cases}$$

If $A = \mathbb{R}$, then any regular quadratic space φ may be written as

$$\varphi \cong \bigoplus_{i=1}^{r} [1] \oplus \bigoplus_{j=1}^{s} [-1]$$

(this result is known as Sylvester's inertia theorem) and the map

$$\operatorname{sgn} \ : \ W(\mathbb{R}) \to \mathbb{Z}, \ [\varphi] \mapsto r - s,$$

the signature, is a group isomorphism.

We will present further examples of Witt groups in the next section.

3.4 Quadratic forms over certain rings

This section is a brief survey of quadratic forms over certain types of rings.

Finite fields

Let $p \in \mathbb{Z}$ be a prime and $A \cong \mathbb{F}_{p^n}$ a finite field.

Definition 3.4.1 (Norm form) Let $E := \mathbb{F}_{p^{2n}}$ and let $q \ : \ E \to \mathbb{F}_{p^n}$ be the norm form, that is, $q(x) = x \cdot x^{p^n}$, which is a quadratic form over $\mathbb{F}_{p^n}$ with $b_q(x, y) = \operatorname{tr}_{\mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n}}(xy^{p^n})$.
(E, q) is anisotropic. We call (E, q) the norm form of A and write $N(A) := (E, q)$.

Remark 3.4.2 (Quadratic spaces of dimension one and two) We have

$$[A^\times : (A^\times)^2] = \begin{cases} 2 & p \neq 2, \\ 1 & p = 2, \end{cases}$$

which shows that there are only one or two (semi-)regular spaces over a finite field, depending on the characteristic.
Any regular quadratic space of dimension two is isometric to either $\mathbb{H}(A)$ or $N(A)$, cf. [Kne02, (12.2)].

The following classification follows from Theorem 3.1.29.

Theorem 3.4.3 *If φ is a regular quadratic A-module of dimension $2m$, we have*

$$\varphi \cong \begin{cases} \bigoplus_{i=1}^m \mathbb{H} \cong \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & \text{or} \\ N(A) \oplus \bigoplus_{i=1}^{m-1} \mathbb{H} \cong \begin{bmatrix} 1 & a \\ & b \end{bmatrix} \oplus \bigoplus_{i=1}^{m-1} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}, \end{cases}$$

where $X^2 + aX + b \in A[X]$ is irreducible. Clearly, these two modules are not isometric.

If φ is semi-regular of dimension $2m+1$, we have

$$\varphi \cong \begin{cases} [1] \oplus \bigoplus_{i=1}^m \mathbb{H} \cong [1] \oplus \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & \text{or} \\ [\varepsilon] \oplus \bigoplus_{i=1}^m \mathbb{H} \cong [\varepsilon] \oplus \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}, \end{cases}$$

where the second case only occurs if $p \neq 2$ (and $\varepsilon \in A^\times - (A^\times)^2$). If that happens these two modules are not isometric.

Corollary 3.4.4 (Witt groups of finite fields) *Put $q := p^n$. Then we have*

$$W(\mathbb{F}_q) \cong \begin{cases} C_2 & q \equiv 0 \pmod 2, \\ C_2 \times C_2 & q \equiv 1 \pmod 4, \\ C_4 & q \equiv 3 \pmod 4. \end{cases}$$

For the reader's convenience, we include the group tables for the odd characteristic cases. Notice that in these cases, the parity of the dimension and the determinant are sufficient in order to determine the isometry class of a regular quadratic $\mathbb{F}_q$-space.

$q \equiv 1 \pmod 4$, $W(\mathbb{F}_q) \cong C_2 \times C_2$, $\varepsilon \in \mathbb{F}_q^\times - (\mathbb{F}_q^\times)^2$.

$+$	$[\mathbb{H}]$	$[[1]]$	$[[\varepsilon]]$	$[N] = [[1,\varepsilon]]$
$[\mathbb{H}]$	$[\mathbb{H}]$	$[[1]]$	$[[\varepsilon]]$	$[N]$
$[[1]]$	$[[1]]$	$[\mathbb{H}]$	$[N]$	$[[\varepsilon]]$
$[[\varepsilon]]$	$[[\varepsilon]]$	$[N]$	$[\mathbb{H}]$	$[[1]]$
$[N]$	$[N]$	$[[\varepsilon]]$	$[[1]]$	$[\mathbb{H}]$
dim (mod 2)	0	1	1	0
det	1	1	ε	ε

$q \equiv 3 \pmod 4$, $W(\mathbb{F}_q) \cong C_4$.

$+$	$[[1]]$	$[N]$	$[[-1]]$	$[\mathbb{H}]$
$[[1]]$	$[N]$	$[[-1]]$	$[\mathbb{H}]$	$[[1]]$
$[N]$	$[[-1]]$	$[\mathbb{H}]$	$[[1]]$	$[N]$
$[[-1]]$	$[\mathbb{H}]$	$[[1]]$	$[N]$	$[[-1]]$
$[\mathbb{H}]$	$[[1]]$	$[N]$	$[[-1]]$	$[\mathbb{H}]$
dim (mod 2)	1	0	1	0
det	1	1	-1	-1

Complete discretely valuated rings and fields

Let R be a complete discrete valuation ring, $K = \mathrm{Quot}(R)$ and $k = R/\pi R$ the residue field. We will assume that k is finite.

The ability to lift isometries, cf. Theorems (15.5) and (15.6) of [Kne02], strongly relates properties of quadratic forms over R with those of forms over k. Concretely, we have the following results.

Theorem 3.4.5 *There is a group isomorphism $W(R) \cong W(k)$.*

Theorem 3.4.6 *Let φ be a regular or semi-regular quadratic module over R. Put $n := \mathrm{rank}_R(\varphi)$.*

1. *If n is at least 3, there exists a regular or semi-regular space ψ satisfying $\varphi \cong \mathbb{H} \oplus \psi$.*

2. *There are exactly two isometry types of regular R-modules of rank two, namely $\mathbb{H}(R)$ and $N(R)$ which is defined by $\overline{N(R)} = N(k)$.*

3. *If $\mathrm{char}(k)$ is odd, then $\varphi \cong \bigoplus_{i=1}^{n} [1]$ or $\varphi \cong [\varepsilon] \oplus \bigoplus_{i=1}^{n-1} [1]$ for some $\varepsilon \in R^\times - (R^\times)^2$.*

4. If $\mathrm{char}(k)$ *is even, we have the possibilities*

$$\varphi \cong \begin{cases} [1] \oplus \bigoplus_{i=1}^{m} \mathbb{H}(R) & n = 2m+1, \\ \bigoplus_{i=1}^{m} \mathbb{H}(R) & n = 2m, \\ N(R) \oplus \bigoplus_{i=1}^{m-1} \mathbb{H}(R) & n = 2m. \end{cases}$$

Definition 3.4.7 We put $\mathcal{U} := \big(K \otimes N(R)\big) \oplus \big(\pi \circ (K \otimes N(R))\big)$. $\mathcal{U}$ is an anisotropic space of dimension 4.

Theorem 3.4.8 ([Kne02, (16.3), (16.4)]) *Let φ be regular or semi-regular over K and* $\mathrm{ind}(\varphi) = 0$*. Then* $\dim(\varphi) \leq 4$ *and if* $\dim(\varphi) = 4$ *we have* $\varphi \cong \mathcal{U}$*.*

We now turn our attention towards the simplest cases, namely $\mathbb{Z}_p$ and $\mathbb{Q}_p$. Since one-dimensional spaces are classified by square classes, we provide the following result.

Remark 3.4.9 Let $\varepsilon \in \mathbb{Z}_p^\times - (\mathbb{Z}_p^\times)^2$.

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \text{ is represented by } \begin{cases} \{1, \varepsilon\} & \text{if } p \neq 2, \\ \{1, 3, 5, 7\} & \text{if } p = 2. \end{cases}$$

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \text{ is represented by } \begin{cases} \{1, \varepsilon, p, p\varepsilon\} & \text{if } p \neq 2, \\ \{1, 3, 5, 7, 2, 6, 10, 14\} & \text{if } p = 2. \end{cases}$$

Theorem 3.4.10 ($W(\mathbb{Q}_p)$, [Kne02, (18.1)], [Sch85, 6.6]) *If p is odd, there is an isomorphism* $W(\mathbb{Q}_p) \cong W(\mathbb{F}_p) \times W(\mathbb{F}_p)$*.*
For $p = 2$ we have $W(\mathbb{Q}_2) \cong C_2 \times C_2 \times C_8$*.*

Quadratic forms over $\mathbb{Q}$

We will follow Section 17 of [Kne02] in order to describe the Witt group of the field of rational numbers.

Definition 3.4.11 Define $s_\infty : W(\mathbb{Q}) \to W(\mathbb{R})$ via $[\varphi] \mapsto [\mathbb{R} \otimes \varphi]$.
Define $s_2 : W(\mathbb{Q}) \to \mathbb{Z}/2\mathbb{Z}$ via $[\varphi] \mapsto v_2(\mathrm{d}_\pm(\varphi)) + 2\mathbb{Z}$.
Both s_∞ and s_2 are well-defined group homomorphisms.

Due to Theorem 3.1.29, $W(\mathbb{Q})$ is generated by $\{[a] \mid a \in \mathbb{Z} \text{ squarefree}\}$.

Definition 3.4.12 For p odd, define $s_p : W(\mathbb{Q}) \to W(\mathbb{F}_p)$ on the abovementioned generators via

$$[a] \mapsto \begin{cases} [a + p\mathbb{Z}] & p \nmid a, \\ [\frac{1}{p}a + p\mathbb{Z}] & p \mid a. \end{cases}$$

s_p is a well-defined group homomorphism.

Theorem 3.4.13 ([Kne02, Satz (17.8)]) *The homomorphisms s_∞, s_2 and s_p define an isomorphism*

$$s \ : \ W(\mathbb{Q}) \to W(\mathbb{R}) \oplus \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_{p \neq 2} W(\mathbb{F}_p).$$

Remark 3.4.14 By [Neb99, Satz 1.3.19], two quadratic spaces φ, ψ over $\mathbb{Q}$ are isometric if and only if they have the same dimension, determinant, signature over $\mathbb{R}$ and equal invariants s_p for all odd primes p.

3.5 Lattices

Let R be a Dedekind domain, $K := \mathrm{Quot}(R)$ its field of fractions and (V, q) a regular quadratic space over K.

Definition 3.5.1 An R-submodule L of V is called a lattice if it is finitely generated and of maximal rank in V. Equivalently one can say that L is an R-submodule of V which is finitely generated and contains a K-basis of V.

Remark 3.5.2 Sometimes a lattice as defined above is referred to as a full lattice. Then the definition of a lattice is relaxed to include R-submodules of smaller rank than $\dim_K(V)$.

Definition 3.5.3 (Integral lattice) An integral lattice L in V is an R-lattice in V such that $q(\ell) \in R$ for all $\ell \in L$, which implies that $b_q(\ell_1, \ell_2) \in R$ for all $\ell_1, \ell_2 \in L$.

Definition 3.5.4 (Dual lattice) Let L be a lattice in V. The dual of L is defined as

$$L^{\#} := \{x \in V \mid b_q(x, \ell) \in R \ \forall \ \ell \in L\}.$$

$L^{\#}$ is again a lattice in V.

Remark 3.5.5 A lattice L in V is integral if and only if $L \subseteq L^{\#}$, in which case $L^{\#}/L$ is a finitely generated Abelian group.

If R is a principal ideal domain, any R-lattice L is a free R-module. Over an arbitrary Dedekind domain this may not be the case. However, one can still say the following.

Remark 3.5.6 (Pseudo-basis) There is a K-basis $\{e_1, ..., e_n\}$ of V and fractional ideals $\mathfrak{a}_1, ..., \mathfrak{a}_n$ of R such that

$$L = \mathfrak{a}_1 e_1 \oplus ... \oplus \mathfrak{a}_n e_n.$$

We call $\{(\mathfrak{a}_i, e_i) \mid 1 \leq i \leq n\}$ a pseudo-basis for L.

Proof. This is the content of Theorem (4.13) of [Rei75]. □

If we specialize K to be a complete discretely valuated field and let R be its valuation ring with maximal ideal πR, we obtain the following statement about the structure of a lattice L in a regular bilinear space (V, b).

Theorem 3.5.7 (Jordan decomposition) *A lattice L in (V, b) may be decomposed as follows.*

$$L \cong \bigoplus_{i=a}^{c} (L_a, \pi^a b_a)$$

where $a \leq c \in \mathbb{Z}$ such that the (L_i, b_i) are (semi-)regular bilinear $\mathcal{O}_\mathfrak{p}$-lattices, which may be zero. The invariants $\operatorname{rank}_{\mathcal{O}_\mathfrak{p}}(L_a)$ and $\det(\overline{b_a}) \in \mathbb{F}_\mathfrak{p}^\times/(\mathbb{F}_\mathfrak{p}^\times)^2$ are uniquely determined. In the case of an integral lattice, we have $a \geq 0$.

Proof. This statement is proved in [O'M73, §91c]. □

3.6 Clifford algebras

This section is devoted to an isometry invariant of tremendous importance, which is functorially associated to a quadratic space, namely an A-algebra called the Clifford algebra. Over fields this algebra gives rise to an element of the Brauer group which will be crucial to our study of quadratic forms and orthogonal representations.

Following [Kne02], we develop as much of the theory of the Clifford algebra as possible for arbitrary commutative rings. For some results however, we will have to work over a field. Therefore we let A be a commutative ring and K a field.

Definition 3.6.1 Let $\varphi = (E, q)$ be a quadratic A-module. An A-algebra $\mathcal{C} := \mathcal{C}(\varphi)$ together with an A-module homomorphism $g : E \to \mathcal{C}$ is called a Clifford algebra if

1. For all $v \in E$ we have $g(v)^2 = q(v) \cdot 1_\mathcal{C}$ and

2. for any A-algebra B and any A-module homomorphism $f : V \to B$ satisfying $f(x)^2 = q(x) \cdot 1_B$ there exists a unique A-algebra homomorphism $\vartheta : \mathcal{C} \to B$ such that the following diagram commutes.

$$\begin{tikzcd}
& V \arrow[dl, "f"'] \arrow[d, "g"] \\
B & \mathcal{C} \arrow[l, dotted, "\vartheta"]
\end{tikzcd}$$

Theorem 3.6.2 ([Kne02, Satz (5.4)]) *For any quadratic A-module φ there exists a Clifford algebra $\mathcal{C}(\varphi)$ and it is unique up to isomorphism.*

Remark 3.6.3 If A is a field, let $T(E) := \bigoplus_{i=0}^{\infty} \bigotimes_{k=1}^{i} E$ be the tensor algebra of E and let $I(E,q)$ be the two-sided ideal of $T(E)$ which is generated by $v \otimes v - q(v) \cdot 1_{T(E)}$, $v \in E$. Then $\mathcal{C}(E,q) \cong T(E)/I(E,q)$, which proves the existence in a much simpler way than the general proof provided in [Kne02].

Corollary 3.6.4 *The set $\{g(e) \mid e \in E\}$ generates $\mathcal{C}(\varphi)$ as an A-algebra. If $\{e_i \mid i \in S\}$ is an A-module generating set of E and S is ordered,*

$$\bigcup_{\ell=0}^{\infty} \{g(e_{i_1}) \cdot ... \cdot g(e_{i_\ell}) \mid i_1 < ... < i_\ell\}$$

is a generating set of $\mathcal{C}(\varphi)$ as an A-module.

The result of Corollary 3.6.4 can be strengthened in the following way.

Theorem 3.6.5 ([Kne02, Satz (5.12)]) *If E is a free A-module of rank m with basis $\{e_1, ..., e_m\}$, the Clifford algebra $\mathcal{C}(\varphi)$ is a free A-module of rank 2^m with basis*

$$\bigcup_{\ell=0}^{m} \{g(e_{i_1}) \cdot ... \cdot g(e_{i_\ell}) \mid 1 \leq i_1 < ... < i_\ell \leq m\}.$$

Convention 3.6.6 When performing computations in a Clifford algebra, we will often omit the map g. In other words, we assume $E \subseteq \mathcal{C}(E,q)$, provided that no confusion can arise from this.

Remark 3.6.7 In most cases the Clifford algebra is not commutative. Let $x, y \in E$, then in $\mathcal{C}(E,q)$ we have

$$(x+y)^2 = q(x+y) = q(x) + q(y) + b_q(x,y),$$

which is equal to $x^2 + xy + yx + y^2$. We obtain

$$xy = -yx + b_q(x,y).$$

Example 3.6.8

1. Consider the free rank-one quadratic module $(E,q) = [a]$. Then $T(E) \cong K[X]$ and therefore the Clifford algebra is isomorphic to

   $$\mathcal{C}(E,q) \cong K[X]/(X^2 - a).$$

2. If the quadratic form q on E is the zero form $\mathcal{C}(E,q)$ is isomorphic to the exterior algebra $\bigwedge E$.

Remark 3.6.9 Let A-Alg be the category of associative A-algebras with A-algebra homomorphisms as morphisms between the objects.

Now consider $(E_i, q_i) \in A$-QMod, $1 \leq i \leq 3$ and morphisms $E_i \xrightarrow{f_i} E_{i+1}$, $i = 1, 2$, which are isometric embeddings by the definition of the category A-QMod. For $1 \leq i \leq 3$ let $E_i \xrightarrow{g_i} \mathcal{C}(E_i, q_i)$ be the respective Clifford algebras. Then $g_2 \circ f_1$ is a homomorphism of A-modules satisfying

$$(g_2 \circ f_1)(x)^2 = q_2(f_1(x)) \cdot 1_{\mathcal{C}(E_2,q_2)} = q_1(x) \cdot 1_{\mathcal{C}(E_2,q_2)}.$$

Therefore by the universal property of $\mathcal{C}(E_1, q_1)$ there is a unique A-algebra homomorphism $\mathcal{C}(E_1, q_1) \to \mathcal{C}(E_2, q_2)$ which we denote by $\mathcal{C}(f_1)$.

$\mathcal{C}(f_2) \; : \; \mathcal{C}(E_2, q_2) \to \mathcal{C}(E_3, q_3)$ may be constructed analogously.

It is straightforward to see that the uniqueness property of g_i forces $\mathcal{C}(\mathrm{id}_{(E_1,q_1)}) = \mathrm{id}_{\mathcal{C}(E_1,q_1)}$ and $\mathcal{C}(f_2 \circ f_1) = \mathcal{C}(f_2) \circ \mathcal{C}(f_1)$.

Therefore $\mathcal{C}$ is a covariant functor from A-QMod to A-Alg.

Lemma 3.6.10 *If $S \supseteq A$ is a ring extension and $\varphi = (E, q)$ a quadratic A-module, we have*

$$\mathcal{C}(S \otimes_A \varphi) \cong S \otimes_A \mathcal{C}(\varphi)$$

as S-algebras.

Proof. This is an application of the universal property of $\mathcal{C}(S \otimes_A \varphi)$. Let $g \; : \; \varphi \to \mathcal{C}(\varphi)$ be the Clifford algebra of φ and define $g' \; : \; S \otimes_A \varphi \to S \otimes_A \mathcal{C}(\varphi)$ by $s \otimes x \mapsto s \otimes g(x)$. It is then easily checked that $g'(s \otimes x) = q_S(s \otimes x) \cdot 1_{S \otimes_A \mathcal{C}(\varphi)}$.

In order to prove that $S \otimes_A \mathcal{C}(\varphi)$ also fulfills the second part of the universal property of $\mathcal{C}(S \otimes_A \varphi)$ let $\mathfrak{B}$ be an S-algebra and $f \; : \; S \otimes_A E \to \mathfrak{B}$ an S-module homomorphism satisfying $f(s \otimes x)^2 = q_S(s \otimes x) \cdot 1_{\mathfrak{B}}$.

Consider $\iota \; : \; S \to \mathfrak{B}, \; s \mapsto s \cdot 1_{\mathfrak{B}}$ and the A-algebra homomorphism

$$\vartheta_0 \; : \; \mathcal{C}(\varphi) \to \mathfrak{B}|_A,$$

where $\mathfrak{B}|_A$ is the A-algebra obtained from $\mathfrak{B}$ by restriction of scalars which is defined by the universal property of $\mathcal{C}(\varphi)$.

Applying the universal property of the tensor product to the A-bilinear map $S \times \mathcal{C}(\varphi) \to \mathfrak{B}, \; (x, s) \mapsto \iota(s) \cdot \vartheta_0(x)$ yields an A-linear map $\overline{\vartheta} \; : \; S \otimes_A \mathcal{C}(\varphi) \to \mathfrak{B}$, which is also S-linear and multiplicative and fulfills $\overline{\vartheta} \circ g' = f$ by construction. □

Definition 3.6.11 It follows from the proof of Theorem 3.6.2 that $\mathcal{C}(\varphi)$ is $\mathbb{Z}/2\mathbb{Z}$-graded in the following way. Again, let $\{e_i \mid i \in S\}$ be an A-module generating set of E and put

$$\mathcal{C}_0 := \mathcal{C}_0(\varphi) := \langle g(e_{i_1}) \cdot \ldots \cdot g(e_{i_{2\ell}}) \mid \ell \in \mathbb{N}_0, \; i_j \in S \rangle_{A\text{-}\mathsf{Mod}},$$
$$\mathcal{C}_1 := \mathcal{C}_1(\varphi) := \langle g(e_{i_1}) \cdot \ldots \cdot g(e_{i_{2\ell+1}}) \mid \ell \in \mathbb{N}_0, \; i_j \in S \rangle_{A\text{-}\mathsf{Mod}}.$$

Then, as A-modules, $\mathcal{C}(\varphi) = \mathcal{C}_0 \oplus \mathcal{C}_1$ and $\mathcal{C}_i \mathcal{C}_j \subseteq \mathcal{C}_{i+j \mod 2}$. The submodule $\mathcal{C}_0$ is a subalgebra of $\mathcal{C}(\varphi)$ called the even part of the Clifford algebra and $\mathcal{C}_1(\varphi)$ is a $\mathcal{C}_0(\varphi)$-submodule of $\mathcal{C}(\varphi)$.

For $x \in \mathcal{C}_i$, $i \in \{0, 1\}$, we denote the degree of x by $\deg(x)$.

Definition 3.6.12 (Graded tensor product) Let $A = A_0 \oplus A_1$ and $B = B_0 \oplus B_1$ be two $\mathbb{Z}/2\mathbb{Z}$-graded algebras. Then the graded tensor product of A and B, denoted by $A \mathbin{\widehat{\otimes}} B$, is $A \otimes B$ as a module with multiplication defined by

$$(a \otimes b)(a' \otimes b') = (-1)^{\deg(b)\deg(a')}(aa') \otimes (bb')$$

for $a_i \in A_i$, $a'_k \in A_k$, $b_j \in B_j$ and $b'_\ell \in B_\ell$.
$A \mathbin{\widehat{\otimes}} B$ is graded via

$$(A \mathbin{\widehat{\otimes}} B)_0 = (A_0 \otimes B_0) \oplus (A_1 \otimes B_1),\ (A \mathbin{\widehat{\otimes}} B)_1 = (A_0 \otimes B_1) \oplus (A_1 \otimes B_0).$$

Theorem 3.6.13 ([Kne02, (5.10)]) *If φ and ψ are quadratic A-modules, there is an isomorphism*

$$\mathcal{C}(\varphi \perp \psi) \cong \mathcal{C}(\varphi) \mathbin{\widehat{\otimes}} \mathcal{C}(\psi)$$

of A-algebras.

We will now focus our attention on Clifford algebras over fields in order to define the Clifford invariant. Recall the definition of the Brauer group, which is presented, for example, in [Rei75].

Definition 3.6.14 (Brauer group) Two central simple K-algebras $\mathfrak{A}$ and $\mathfrak{B}$ are called Brauer-equivalent if there are $m, n \in \mathbb{N}$ such that $\mathfrak{A}^{n \times n} \cong \mathfrak{B}^{m \times m}$ as K-algebras.
The Brauer group $\mathrm{Br}(K)$ of K is defined to be the set of all Brauer equivalence classes of central simple algebras with

$$[\mathfrak{A}][\mathfrak{B}] := [\mathfrak{A} \otimes_K \mathfrak{B}],\ [\mathfrak{A}]^{-1} = [\mathfrak{A}^{\mathrm{op}}],\ 1_{\mathrm{Br}(K)} = [K].$$

By $\mathrm{Br}_2(K)$ we denote the maximal exponent-two subgroup of $\mathrm{Br}(K)$.

It turns out that, over a field, Clifford algebras of regular quadratic spaces have some advantageous properties.

Theorem 3.6.15 ([Kne02, (11.1)-(11.2)]) *Let φ be a regular quadratic K-space.*

- *If $\dim(\varphi)$ is even, $\mathcal{C}(\varphi)$ is a central simple K-algebra.*
- *If $\dim(\varphi)$ is odd, $\mathcal{C}_0(\varphi)$ is a central simple K-algebra.*
  The center of $\mathcal{C}(\varphi)$ is isomorphic to $L := K[X]/(X^2 - \mathrm{d}_\pm(\varphi))$. If $\mathrm{d}_\pm(\varphi)$ is not a square in K, then L is a degree two field extension of K and $\mathcal{C}(\varphi)$ is a simple K-algebra with center L. Otherwise $\mathcal{C}(\varphi)$ is the direct sum of two isomorphic copies of a central simple K-algebra.

In either case, $\mathcal{C}(\varphi)$ is a semisimple K-algebra.

Definition 3.6.16 (Clifford invariant) We write

$$c(\varphi) := \begin{cases} \mathcal{C}(\varphi) & \dim(\varphi) \text{ is even,} \\ \mathcal{C}_0(\varphi) & \dim(\varphi) \text{ is odd.} \end{cases}$$

This is a central simple K-algebra for regular φ and we can therefore define

$$\mathfrak{c}(\varphi) := [c(\varphi)] \in \mathrm{Br}(K),$$

the Clifford invariant of φ.

Remark 3.6.17 Assume that K is a field of characteristic different from two. Then it follows from [Sch85, Lemmas 9.2.8, 9.2.9] that $c(\varphi)$ is a tensor product of quaternion algebras. Therefore we actually have $\mathfrak{c}(\varphi) \in \mathrm{Br}_2(K)$, the maximal exponent two subgroup of the Brauer group.
If K is a number field or a p-adic field, a tensor product of quaternion algebras is Brauer-equivalent to a quaternion algebra, cf. [Vig80, I Thm. 2.9].
See loc.cit. for the statement that over a number field, a quaternion algebra $\mathcal{Q}$ is determined up to isomorphism by the even (and finite) number of places of K ramified in it, where a place $\mathfrak{p}$ is called ramified in $\mathcal{Q}$ if $[K_\mathfrak{p} \otimes_K \mathcal{Q}] \neq [K_\mathfrak{p}] \in \mathrm{Br}(K_\mathfrak{p})$. Therefore we sometimes use the notation $\mathcal{Q}_{\mathfrak{p}_1,\ldots,\mathfrak{p}_s}$ to denote a Quaternion algebra ramified precisely at the places $\mathfrak{p}_1, ..., \mathfrak{p}_s$.

Theorem 3.6.18 (Product formula, [Kne02, (18.5)]) *Let K be a number field, $\mathfrak{p}$ a finite or real place of K and φ a regular quadratic space. Then $\mathfrak{c}_\mathfrak{p}(\varphi) := \mathfrak{c}(K_\mathfrak{p} \otimes_K \varphi) \in \mathrm{Br}_2(K_\mathfrak{p})$, and $\mathrm{Br}_2(K_\mathfrak{p})$ may be identified with $\{\pm 1\}$. We then have*

$$\prod_{\mathfrak{p}} \mathfrak{c}_\mathfrak{p}(\varphi) = 1,$$

where the product is taken over all finite and real places of K.

Remark 3.6.19 Due to the existence of a local-global principle for Brauer-equivalence of central simple algebras – this is the theorem of Albert, Brauer, Hasse and Noether, cf. [Rei75, Thm. (32.11)] – over a number field K, $\mathfrak{c}(\varphi)$ is completely determined by all local Clifford invariants $\mathfrak{c}_\mathfrak{p}(\varphi)$.

For explicit computations of Clifford invariants in $\mathrm{Br}_2(K)$, it is useful to define quaternion symbols, which generate the group $\mathrm{Br}_2(K)$.

Definition 3.6.20 (Quaternion symbol) Let $\mathrm{char}(K) \neq 2$ and $a, b \in K^\times$. Then $(a, b) \in \mathrm{Br}_2(K)$ is defined as $\mathfrak{c}([a, b])$. It is the Brauer class of the quaternion algebra $\left(\frac{a,b}{K}\right)$ - this notation designates the quotient of the free associative algebra on the symbols $\{i, j\}$ subject to the relations generated by $i^2 = a$, $j^2 = b$ and $ij = -ji$.
Commonly, one puts $k := ij$.

Lemma 3.6.21 ([Sch85, (11.8)]) *Over a field of characteristic not two,* $\left(\frac{a,b}{K}\right)$ *is a skew field if and only if the quadratic form* $[1, -a, -b, ab]$ *is anisotropic.*

Remark 3.6.22 ([Vig80, Cor. II 1.2]) Let $a, b, c, u, v \in K^\times$. The quaternion symbols have the following properties.

1. $(a, b) = (b, a)$,
2. $(au^2, bv^2) = (a, b)$,
3. $(a, -ab) = (a, b)$,
4. $(a, a) = (-1, a) = (a, -1)$,
5. $(a, -a) = [K]$,
6. $(a, bc) = (a, b)(a, c)$,
7. $(1, a) = (a, 1) = [K]$.

Recall that over a field of characteristic not two, any quadratic form may be diagonalized. Using this, one obtains the following result which allows for an explicit computation of the Clifford invariant.

Theorem 3.6.23 ([Kne02, (11.12)]) *Let* $a_1, ..., a_n \in K^\times$*,* $n = 2m$ *even,* $r := m - 1$ *and* $s := \frac{m(m-1)}{2}$*. Then*

1. $$\mathfrak{c}([a_1, ..., a_n]) = \prod_{1 \leq j < i \leq n} (a_j, a_i) \left(-1, \prod_{i=1}^{n} a_i\right)^r (-1, -1)^s,$$

2. $$\mathfrak{c}([a_1, ..., a_{n-1}]) = \prod_{1 \leq j < i \leq n-1} (a_j, a_i) \left(-1, \prod_{i=1}^{n-1} a_i\right)^r (-1, -1)^s.$$

Proposition 3.6.24 *Let* φ *and* ψ *be regular quadratic spaces over* K*,* $\mathrm{char}(K) \neq 2$ *and* $a \in K^\times$*. Then the Clifford invariant adheres to the following rules.*

1. $$\mathfrak{c}(a \circ \varphi) = \begin{cases} \mathfrak{c}(\varphi) \cdot (\mathrm{d}_\pm(\varphi), a) & \dim(\varphi) \text{ even,} \\ \mathfrak{c}(\varphi) & \dim(\varphi) \text{ odd.} \end{cases}$$

2. *If* $\dim(\varphi) \equiv \dim(\psi) \mod 2$*,*
$$\mathfrak{c}(\varphi \oplus \psi) = \mathfrak{c}(\varphi)\mathfrak{c}(\psi)(\mathrm{d}_\pm(\varphi), \mathrm{d}_\pm(\psi)).$$

3. *If* $\dim(\varphi) \equiv 1 \mod 2$ *and* $\dim(\psi) \equiv 0 \mod 2$*,*
$$\mathfrak{c}(\varphi \oplus \psi) = \mathfrak{c}(\varphi)\mathfrak{c}(\psi)(-\mathrm{d}_\pm(\varphi), \mathrm{d}_\pm(\psi)).$$

Proof. The first statement follows from 3.6.23 by explicit computation. The second and third statements are proved in [Lam73, Theorem 3.9]. □

Example 3.6.25 Define $\mathfrak{I}_n$ to be the quadratic $\mathbb{Q}$-space whose associated bilinear form is $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{I}_n$, i.e. the quadratic form on $\mathfrak{I}_n$ is $x \mapsto \frac{1}{2}\sum_{i=1}^n x_i^2$. This means that $\mathfrak{I}_n$ is diagonalized as $[\frac{1}{2}, ..., \frac{1}{2}]$.

The determinant is $\det(\mathfrak{I}_n) = 1$ for all n. Next, we want to compute the Clifford invariant.

Notice that $(\frac{1}{2}, \frac{1}{2}) = (-1, \frac{1}{2}) = 1 \in \mathrm{Br}(\mathbb{Q})$ by Lemma 3.6.21. Write $n = 2m$ or $n = 2m-1$. Then, by Theorem 3.6.23, we have $\mathfrak{c}(\mathfrak{I}_n) = (-1,-1)^s$, where $s = \frac{m(m-1)}{2}$. The value $(-1,-1)^s$ is trivial if and only if s is even, which is equivalent to $m \in 4\mathbb{Z} \cup (1+4\mathbb{Z})$. We therefore obtain

$$\mathfrak{c}(\mathfrak{I}_n) = \begin{cases} (1,1) & n \equiv 0,1,2,7 \pmod 8, \\ (-1,-1) & n \equiv 3,4,5,6 \pmod 8. \end{cases}$$

Next, let $\mathfrak{A}_{n-1}$ be the quadratic $\mathbb{Q}$-space defined as the orthogonal complement of the vector $(1,1,...,1) \in \mathfrak{I}_n$, i.e. $\mathfrak{I}_n = [\frac{1}{2}n] \oplus \mathfrak{A}_{n-1}$. The associated bilinear form of $\mathfrak{A}_{n-1}$ is $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{A}_{n-1}$ and the determinant of $\mathfrak{A}_{n-1}$ is n.

Using Proposition 3.6.24, we can now obtain the Clifford invariant of $\mathfrak{A}_{n-1}$ from that of $\mathfrak{I}_n$. The values again depend on n modulo 8 and are noted in the following table.

$n \mod 8$	$\mathrm{d}_\pm(\mathfrak{A}_{n-1})$	$\mathfrak{c}(\mathfrak{A}_{n-1})$
1	n	1
2	n	$(-1,n)$
3	$-n$	$(-1,n)$
4	$-n$	$(-1,-1)$
5	n	$(-1,-1)$
6	n	$(-1,-n)$
7	$-n$	$(-1,-n)$
8	$-n$	1

The fact that the Clifford invariant of $\mathfrak{I}_n$ depends on the value of n modulo 8 is no mere coincidence. Over the real and complex numbers there is a periodicity of Clifford algebras, which is a manifestation of a theorem from algebraic topology, called Bott periodicity. We will now briefly describe the periodicity of real and complex Clifford algebras, which is proved in Chapter 5, Section 4 of [Lam73].

Let V be a regular quadratic space over $\mathbb{C}$. Then $V \cong \bigoplus_{i=1}^{\dim(V)}[1]$, as $\mathbb{C}$ is algebraically closed. Put $\mathcal{C}_n := \mathcal{C}(\bigoplus_{i=1}^n [1])$. Then we have the relations

$$\mathcal{C}_1 \cong \mathbb{C} \oplus \mathbb{C},\ \mathcal{C}_2 \cong \mathbb{C}^{2\times 2} \text{ and } \mathcal{C}_{n+2} \cong (\mathcal{C}_n)^{2\times 2}.$$

This may be understood as a periodicity modulo 2.

Over the reals we have the following situation. Let V be a regular quadratic $\mathbb{R}$-space. By Sylvester's Theorem $V \cong \bigoplus_{i=1}^{p}[1] \oplus \bigoplus_{j=1}^{q}[-1]$. We put $\mathcal{C}_{p,q} := \mathcal{C}(V)$. Then the isomorphism type of $\mathcal{C}_{p,q}$ will only depend on the signature $p-q$ modulo 8 and the dimension of V, which is $p+q$.

This symbolic "clock" describes the Clifford algebras $\mathcal{C}_{0,0}, ..., \mathcal{C}_{7,0}$, where the arrows indicate a modification of the underlying quadratic space by orthogonal addition of the one-dimensional space [1].

$$\begin{tikzcd}
 & & \begin{matrix}\mathbb{R}\\ p{-}q{\equiv}0\end{matrix} \arrow[dr] & & \\
 & \begin{matrix}\mathbb{C}^{8\times 8}\\ p{-}q{\equiv}7\end{matrix} \arrow[ur] & & \begin{matrix}\mathbb{R}{\oplus}\mathbb{R}\\ p{-}q{\equiv}1\end{matrix} \arrow[dr] & \\
\begin{matrix}\mathbb{H}^{4\times 4}\\ p{-}q{\equiv}6\end{matrix} \arrow[ur] & & & & \begin{matrix}\mathbb{R}^{2\times 2}\\ p{-}q{\equiv}2\end{matrix} \arrow[dl] \\
 & \begin{matrix}(\mathbb{H}{\oplus}\mathbb{H})^{2\times 2}\\ p{-}q{\equiv}5\end{matrix} \arrow[ul] & & \begin{matrix}\mathbb{C}^{2\times 2}\\ p{-}q{\equiv}3\end{matrix} \arrow[dl] & \\
 & & \begin{matrix}\mathbb{H}^{2\times 2}\\ p{-}q{\equiv}4\end{matrix} \arrow[ul] & &
\end{tikzcd}$$

The real Clifford algebras then satisfy the following periodicity law modulo 8.

$$\mathcal{C}_{p+8,q} \cong \mathcal{C}_{p+4,q+4} \cong \mathcal{C}_{p,q+8} \cong \mathcal{C}_{p,q}^{16\times 16}.$$

Together with the calculation rule

$$\mathcal{C}_{p+1,q+1} \cong \mathcal{C}_{p,q}^{2\times 2}$$

one can thus compute all Clifford algebras $\mathcal{C}_{p,q}$ up to isomorphism of $\mathbb{R}$-algebras.

We now present a result about the Clifford invariant, which is in a similar vein.

Theorem 3.6.26 *Let K be a field of characteristic not two and φ a regular quadratic space over K. Abbreviate $\varphi^n := \bigoplus_{i=1}^{n} \varphi$ for $n \in \mathbb{N}$. Then we have*

1. $\mathfrak{c}(\varphi^8) = 1$,

2. $\mathfrak{c}(\varphi^{8r+k}) = \mathfrak{c}(\varphi^k)$ *for all* $r \in \mathbb{N}$.

If $\dim(\varphi)$ *is even, we get a periodicity modulo* 4*:*

3. $\mathfrak{c}(\varphi^4) = 1$,

4. $\mathfrak{c}(\varphi^{4r+k}) = \mathfrak{c}(\varphi^k)$ *for all* $r \in \mathbb{N}$.

Proof. This follows from Proposition 3.6.24.

1. Notice that $\mathrm{d}_\pm(\varphi^4) = (-1)^{\frac{1}{2}\cdot 4\dim(\varphi)(4\dim(\varphi)-1)}\det(\varphi)^4 = 1$. Using this, we obtain

$$\mathfrak{c}(\varphi^8) = \mathfrak{c}(\varphi^4 \ominus \varphi^4) = \mathfrak{c}(\varphi^4)^2(\mathrm{d}_\pm(\varphi^4), \mathrm{d}_\pm(\varphi^4)) = 1.$$

2. By the same argument as before, we obtain $\mathrm{d}_\pm(\varphi^8) = 1$ and

$$\mathfrak{c}\left(\varphi^{8r+k}\right) = \mathfrak{c}\left((\varphi^r)^8 \ominus \varphi^k\right) = \mathfrak{c}((\varphi^r)^8)\mathfrak{c}(\varphi^k)\Big(\mathrm{d}_\pm((\varphi^r)^8), \pm\mathrm{d}_\pm(\varphi^k)\Big) = \mathfrak{c}(\varphi^k).$$

The statement about spaces of even dimension is proved analogously. □

Corollary 3.6.27 *Let* φ *be a regular quadratic space of odd dimension over a field of characteristic disctinct from two. Then we have the identities*

$$\mathfrak{c}(\varphi) = \mathfrak{c}(\varphi^7) \text{ and } \mathfrak{c}(\varphi^3) = \mathfrak{c}(\varphi^5).$$

Remark 3.6.28 As the example of $\mathfrak{I}_n$ shows, there may in general not be a smaller period than 8.

We conclude this section with a fundamental theorem due to Helmut Hasse which on the one hand underlines the importance of the Clifford invariant and on the other hand shows that the invariants we have so far defined for quadratic spaces are exhaustive in a certain sense.

Theorem 3.6.29 ([Has24]) *Two quadratic spaces* φ *and* ψ *over a number field* K *are isometric if and only if*

1. $\dim(\varphi) = \dim(\psi)$,
2. $\mathrm{d}_\pm(\varphi) = \mathrm{d}_\pm(\psi)$,
3. $\mathrm{sgn}(K_\mathfrak{p} \otimes_K \varphi) = \mathrm{sgn}(K_\mathfrak{p} \otimes_K \psi)$ *at all real places* $\mathfrak{p}$ *of* K *and*
4. $\mathfrak{c}(\varphi) = \mathfrak{c}(\psi)$.

4 Orthogonal representations

This chapter serves as an introduction to both classical representation theory and orthogonal representations, the subject which is at the very heart of this thesis. It contains a survey of methods used to give partial answers to the question raised in the introduction.

4.1 Representation theory

In this section, we present the results from representation theory which we will need in this thesis. The subject of representation theory is of course far too vast to be presented in an exhaustive way in this thesis. We refer the reader to the excellent books [CR87a, CR87b], from which we obtain most of the statements and results of this section.

Ordinary representation theory is primarily concerned with representations of finite groups over algebraically closed fields of characteristic zero. This particular branch of representation theory has been extensively studied and is understood extremely well. After all, the publication of the Atlas of finite groups, [CCN$^+$85], containing information on the irreducible representations of a large amount of the finite simple groups, is considered one of the greatest mathematical achievements of the twentieth century.

Throughout this section, we will denote by G a finite group and by K a field of characteristic zero. In some cases where greater generality is appropriate or even required, we will choose a different letter to denote an arbitrary field.

Definition 4.1.1 (Representations) A representation of G is a group homomorphism

$$\Delta \ : \ G \to \mathrm{GL}_n(K)$$

for some $n \in \mathbb{N}$. This endows K^n with a KG-module structure, where KG is the group algebra of G over K, which is defined to be the free K-vector space on the set G with multiplication defined by distributive extension of the group law.
On the other hand, any finite-dimensional KG-module gives rise to a representation of G, which means that these two concepts are equivalent. Sometimes KG-modules are

therefore also referred to as representations of G.
We call a representation irreducible if its associated KG-module is simple.
Two representations are called equivalent if their associated KG-modules are isomorphic.

Definition 4.1.2 (Characters) Let Δ be a representation of G. The map

$$\chi_\Delta \ : \ G \to K, \ g \mapsto \mathrm{tr}(\Delta(g)),$$

which is easily checked to be constant on conjugacy classes of G, is called the character of Δ.
We call χ irreducible if Δ is irreducible and denote by $\mathrm{Irr}(G)$ the set of irreducible characters over the algebraic closure $\overline{K}$ of K.

If k is an arbitrary field of characteristic zero and χ a character of G, we call

$$k[\chi] := k[\{\chi(g) \mid g \in G\}]$$

the character field of χ over k. The extension $k[\chi]/k$ is an Abelian Galois extension.

The importance of characters is underlined by the following statement.

Theorem 4.1.3 *Two representations Δ_1 and Δ_2 of G are equivalent if and only if their characters χ_{Δ_1} and χ_{Δ_2} are equal.*

This is largely based on the Theorem of Maschke.

Theorem 4.1.4 (Maschke, [CR87a, (3.14)]) *KG is a semisimple K-algebra if and only if* $\mathrm{char}(K) \nmid |G|$.

Maschke's result shows why representation theory of finite groups is so heavily dependent on the characteristic of the base field. If the characteristic of K does not divide the group order, when trying to describe the module category KG-mod it is sufficient to describe all the simple modules, i.e., irreducible representations.

Next, we provide some simple constructions of representations, which we will be important in later sections.

Proposition 4.1.5 *1. For any finite group, we always have the one-dimensional KG-module K with G acting trivially, i.e. $gx = x$ for all $g \in G$ and $x \in K$.
We denote both the module and its character by $\mathbb{1}_G$. No confusion should arise from this.*

2. *If V is a KG-module, then so is $V^* = \operatorname{Hom}_K(V, K)$. The action of $g \in G$ on a linear form φ is defined as*

$$(g\varphi)(x) := \varphi(g^{-1}x)$$

for all $x \in V$. The character of V^* is $\chi^* \,:\, g \mapsto \chi(g^{-1})$.

3. *If V and W are KG-modules, we have a KG-module struture on $V \otimes_K W$ by setting*

$$g(v \otimes w) := gv \otimes gw,$$

with $\chi_{V \otimes W} = \chi_V \chi_W$.

4. *Consider the KG-module $V \otimes_K V$ and the K-linear map*

$$s \;:\; V \otimes V \to V \otimes V,\; x \otimes y \mapsto \frac{1}{2}(x \otimes y + y \otimes x).$$

We call the image of s the symmetric square $S^2(V)$ and its kernel the alternating or exterior square $\bigwedge^2(V)$. These two vector spaces are KG-modules with characters

$$\chi_{S^2(V)} = \frac{1}{2}(\chi_V^2 + \chi_V^{(2)})$$

and

$$\chi_{\bigwedge^2(V)} = \frac{1}{2}(\chi_V^2 - \chi_V^{(2)}),$$

where $\chi^{(2)}(g) := \chi(g^2)$.

Definition 4.1.6 (Restriction and induction) Let H be a subgroup of G, V a KG-module and W a KH-module.

1. By restriction of scalars, we can turn V into a KH-module $V|_H$.

2. The construction $KG \otimes_{KH} W$ yields a KG-module $\operatorname{ind}_H^G(W)$ with character

$$\operatorname{ind}_H^G(\chi_W) \;:\; G \to K,\; g \mapsto \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \chi_W(x^{-1}gx).$$

3. Let $G = \bigsqcup_{i=1}^s g_i H$ be a decomposition of G into left H-cosets. Under the induction functor ind_H^G, a KH-homomorphism $f \;:\; W \to W'$ is transformed into a KG-morphism f^G, which is explicitly given by

$$f^G\left(\sum_{i=1}^s g_i \otimes w_i\right) = \sum_{i=1}^s g_i \otimes f(w_i).$$

4. Restriction and induction are functors $KG\text{-}\mathsf{mod} \to KH\text{-}\mathsf{mod}$ and $KH\text{-}\mathsf{mod} \to KG\text{-}\mathsf{mod}$, respectively.

Definition 4.1.7 The space of class functions of G carries the inner product

$$(\varphi, \psi)_G := \frac{1}{|G|} \sum_{g \in G} \varphi(g)\psi(g^{-1}).$$

$\mathrm{Irr}(G)$ is an orthonormal basis of the space of class functions (recall that the definition of $\mathrm{Irr}(G)$ includes the condition that the ground field be algebraically closed).

Theorem 4.1.8 (Frobenius reciprocity, [CR87a, (10.9)]) *Let $H \le G$ be a subgroup. For characters χ of G and ψ of H, we have the equality*

$$(\chi, \mathrm{ind}_H^G(\psi))_G = (\chi|_H, \psi)_H.$$

Now, we will briefly touch upon a subject known as Clifford theory. As a historic remark, it should be noted that this branch of representation theory was initiated by Alfred H. Clifford, an American algebraist (1908-1992), whereas the Clifford algebra in the theory of quadratic forms was introduced by the British geometer William K. Clifford (1845-1879).

Theorem 4.1.9 (Clifford, [CR87a, (11.1)]) *Let k be an arbitrary field and N a normal subgroup of G. Denote by M a simple KG-module and by L a simple KN-constituent of $M|_N$. We then have the following statements.*

1. *$M|_N$ is a semisimple KN-module and it is isomorphic to a direct sum of G-conjugates of L.*
   The conjugate ${}^gL$ of L by $g \in G$ is defined to be the KN-module affording the representation $x \mapsto \Delta_L(g^{-1}xg)$.
   The submodules of the form $\displaystyle\sum_{X \le M|_N,\ X \cong_{KN} {}^gL} X$ are called the KN-homogeneous components of $M|_N$.

2. *The KN-homogeneous components of $M|_N$ are permuted transitively by G.*

3. *Let L^e be the KN-homogeneous component of $M|_N$ containing L and T its stabilizer in G, which is the same as the stabilizer of L, i.e. $T = \{g \in G \mid {}^gL \cong_{KN} L\}$. Decompose G into $\bigsqcup_{i=1}^t g_iT$. Then $\{g_iL \mid 1 \le i \le t\}$ is a complete set of non-isomorphic conjugates of L and each appears with the same multiplicity in $M|_N$, i.e.*

   $$M|_N \cong \left(\bigoplus_{i=1}^t {}^{g_i}L \right)^e.$$

   Clearly, $t = [G : T]$. T is often called the inertia subgroup of L and is also denoted by $I_G(L)$.

4. *L^e is a KT-module and $M \cong \mathrm{ind}_T^G(L^e)$.*

Remark 4.1.10 Clifford's theorem is easily translated into the language of characters, where it is stated as follows. Let χ be an irreducible character of G and ϑ an irreducible character of N such that $(\chi|_N, \vartheta) =: e > 0$. Then $\chi|_N = e \sum_{i=1}^t {}^{g_i}\vartheta$.

Remark 4.1.11 Let G be a finite group with normal subgroup N and $\vartheta \in \mathrm{Irr}(N)$. Abbreviate $T := I_G(\vartheta)$ and put

$$\mathrm{Irr}(G|\vartheta) := \{\chi \in \mathrm{Irr}(G) \mid (\chi|_N, \vartheta)_N > 0\},$$
$$\mathrm{Irr}(T|\vartheta) := \{\chi \in \mathrm{Irr}(T) \mid (\chi|_N, \vartheta)_N > 0\}.$$

Then $\chi \mapsto \mathrm{ind}_T^G(\chi)$ induces a bijection

$$\mathrm{Irr}(T|\vartheta) \to \mathrm{Irr}(G|\vartheta).$$

We now explain how to find the irreducible representations of a group G over a field of characteristic zero which is not necessarily algebraically closed.

Definition 4.1.12 (Splitting field) We call a field L a splitting field for G if every irreducible representation of G over E is absolutely irreducible, which is to say that it remains irreducible over all field extensions of E. Equivalently, $\mathrm{End}_{EG}(V) \cong E$ for all simple EG-modules V.

The existence of a splitting field of finite degree over K is ensured by a theorem attributed to Richard Brauer [CR87a, Theorem (15.16)].

In general, which is to say without the assumption that K be a splitting field, one has the following situation.

Theorem 4.1.13 (Schur's lemma) *Let V be a simple KG-module. Then $\mathrm{End}_{KG}(V)$ is a division algebra over K.*

The central result we need is the following.

Theorem 4.1.14 ([CR87b, (74.5)]) *Let k be an arbitrary field of characteristic zero and E a splitting field for G such that E/k is a finite Galois extension. The following statements hold.*

1. *Let U a simple kG-module and put $D := \mathrm{End}_{kG}(U)$, $L := Z(D)$, m the index of D, which is square root of $\dim_L(D)$, cf. Section 29 of [Rei75], and $t := [L : k]$. Then there is an isomorphism of EG-modules*

$$E \otimes_k U \cong (V_1 \oplus \ldots \oplus V_t)^m,$$

where $\{V_1, \ldots, V_t\}$ are a set of non-isomorphic simple EG-modules permuted transitively by $\mathrm{Gal}(E/k)$.

2. *Let $\chi \in \mathrm{Irr}(G)$, afforded by some absolutely simple EG-module V. There is a simple kG-module U, which is unique up to isomorphism, such that χ occurs in the character η of G afforded by U. Then V is one of the V_i appearing in the first statement, $V = V_1$ say, and we have*

$$\eta = m(\chi_1 + ... + \chi_t),\ L \cong k[\chi_1] \cong ... \cong k[\chi_t],$$

where V_i affords the character χ_i of G.

3. *Suppose that $\chi \in \mathrm{Irr}(G)$ is afforded by a simple FG-module, where F/k is a finite extension. Then $F \supseteq k[\chi]$ and $\dim_{k[\chi]}(F)$ is a multiple of m. Further, there exist such fields F for which $\dim_{k[\chi]}(F) = m$.*

Definition 4.1.15 (Schur index) We call m in the above theorem the Schur index of χ over k and write $m =: m_k(\chi)$

We conclude this section with a few results on the Schur index.

Corollary 4.1.16 ([CR87b, (74.8)]) *Let V be an absolutely simple EG-module affording the character χ. Then the direct sum of m coplies of V is realizable over the field $k[\chi]$ and m is minimal with this property.*
In addition, m divides $\dim_E(V)$.

Over certain fields, we obtain very strong restriction on the Schur index.

Theorem 4.1.17 ([CR87b, (74.9)]) *Over a field of characteristic $p > 0$, all Schur indices are 1 and all absolutely irreducible representations are realizable over their respective character fields.*

Theorem 4.1.18 (Brauer-Speiser, [CR87b, (74.27)]) *Let the character $\chi \in \mathrm{Irr}(G)$ be real-valued. Then the rational Schur-index $m_{\mathbb{Q}}(\chi)$ is 1 or 2. It is 1 if χ is of odd degree.*

The theorem of Benard-Schacher [CR87b, (74.20)] shows that simple components of group algebras have uniformly distributed invariants, which is to say that the local Schur index at a prime place $\mathfrak{p}$ of a number field K only depends on the rational prime p below $\mathfrak{p}$. This justifies the notations $m_p(\chi) := m_{\mathfrak{p}}(\chi) := m_{K_{\mathfrak{p}}}(\chi)$ and $\mathbb{R} \otimes_K V$ for the completion $K_{\mathfrak{q}} \otimes_K V$ at an arbitrary real place $\mathfrak{q}$.

It is also worth noting that a non-trivial Schur index can only occur at primes dividing the group order $|G|$, cf. [CR87b, (74.11)].

4.2 Orthogonal representations

We are now going to introduce objects which are central to this work, namely what we will call orthogonal representations.
Throughout this section, let G be a finite group.

Definition 4.2.1 Let R be an integral domain and V an RG-module of finite rank. Assume that there is a regular quadratic form $q : V \times V \to R$ such that for all $g \in G$ we have $q(gx) = x$ for all $x \in V$. We say that q is G-invariant. In this case we call (V, q) an orthogonal RG-module.
Let $\Delta : G \to \mathrm{GL}(V)$ be the representation associated to V. Then the above hypotheses mean that the image of Δ is contained in the orthogonal group $\mathrm{O}(V, q)$.

Even though we have stated this definition for arbitrary integral domains, the case we are most interested in is the case $R = K$, where K is a field of characteristic not two. When appropriate, we will impose some additional restrictions on K.
Recall that if 2 is invertible, which is clearly the case in our situation, there is a bijective correspondence between quadratic and bilinear forms. We will use the latter, without loss of generality, in order to obtain some structural results.

Remark 4.2.2 Let K be a totally real number field or $K = \mathbb{R}$ and V a finite-dimensional KG-module. Then there exists a regular quadratic form on V that is fixed by G.

This is proved by the following "averaging argument".

Proof. The form $q := \bigoplus_{i=1}^{\dim(V)}[1]$ is totally positive definite. The same holds for the forms

$$q_g : V \to K, \ x \mapsto q(gx)$$

for all $g \in G$. Hence their sum, which is of course G-invariant, is totally positive definite as well. □

The existence of a G-invariant non-degenerate bilinear form on a K-vector space V has the following representation-theoretic interpretation.

Theorem 4.2.3 *We have $V \cong_{KG} V^*$ if and only if there is a G-invariant non-degenerate K-bilinear form $\Phi : V \times V \to K$.*

Proof. Firstly, assume the existence of a G-invariant and non-degenerate Φ as in the statement. Then

$$\psi : V \to V^*, \ v \mapsto \Phi(v, -) = \Big(x \mapsto \Phi(v, x)\Big)$$

is K-linear. Recalling the definition of the action of G on V^*, one checks that ψ is G-equivariant:

$$\psi(gv)(w) = \Phi(gv, w) = \Phi(v, g^{-1}w) = \psi(v)(g^{-1}w) = (g\psi)(v)(w).$$

The non-degeneracy of Φ implies that $\ker(\psi) = \{0\}$, which shows that ψ is an isomorphism.

Secondly, assume that there is an isomorphism $\varphi : V \to V^*$ of KG-modules. Define

$$\Phi : V \times V \to K, \ (v, w) \mapsto \varphi(v)(w).$$

Φ is K-bilinear and, because of the following computation, G-invariant.

$$\Phi(gv, gw) = \varphi(gv)(gw) = (g\varphi)(v)(w) = \varphi(v)(g^{-1}gw) = \Phi(v, w).$$

Finally, we must show that Φ is non-degenerate. Let $v \in V$ such that $\Phi(v, w) = 0$ for all $w \in V$. Then

$$0 = \Phi(v, w) = \varphi(v)(w)$$

for all $w \in V$, which implies $v = 0$ because φ is an isomorphism. □

Definition 4.2.4 Let V be a KG-module. We define the following K-vector spaces.

1. $\mathcal{B}_G(V) := \{\phi : V \times V \to K \mid \phi \text{ is a } G\text{-invariant bilinear form}\}$.

2. $\mathcal{F}_G(V) := \{\phi : V \times V \to K \mid \phi \text{ is a } G\text{-invariant symmetric bilinear form}\}$.

3. $\mathfrak{S}_G(V) := \{\phi : V \times V \to K \mid \phi \text{ is a } G\text{-invariant skew-symmetric bilinear form}\}$.

Often, $\mathcal{F}_G(V)$ is called the form space of V.
An orthogonal KG-module V is called uniform if $\dim_K(\mathcal{F}_G(V)) = 1$.

Remark 4.2.5 Let V be a K-vector space. The space of K-bilinear forms is isomorphic to $V^* \otimes_K V^*$. Under this isomorphism the subspace of symmetric bilinear forms corresponds to $S^2(V^*)$ while the skew-symmetric forms correspond to $\bigwedge^2(V^*)$.

If V additionally admits a KG-module structure, so do V^*, $V^* \otimes_K V^*$, $S^2(V^*)$ and $\bigwedge^2(V^*)$. The spaces of G-invariant forms are then isomorphic to the respective fixed spaces $(V^* \otimes_K V^*)^G$, $S^2(V^*)^G$ and $\bigwedge^2(V^*)^G$.

Using this description of bilinear forms, we obtain the following properties.

Remark 4.2.6 Let V and W be KG-modules and L/K a field extension. Then the following properties hold.

1. $L \otimes_K V^G = (L \otimes_K V)^G$.

2. $(V \oplus W)^G = V^G \oplus W^G$.

3. $L \otimes_K S^2(V) \cong S^2(L \otimes_K V)$.

4. $L \otimes_K \bigwedge^2(V) \cong \bigwedge^2(L \otimes_K V)$.

Corollary 4.2.7 *If L/K is a field extension, we have $L \otimes_K \mathcal{F}_G(V) \cong \mathcal{F}_G(L \otimes_K V)$.*

Corollary 4.2.8 *Let V and W be two KG-modules. Then we have*

$$\mathcal{F}_G(V \oplus W) \cong \mathcal{F}_G(V) \oplus (V^* \otimes W^*)^G \oplus \mathcal{F}_G(W) \cong \mathcal{F}_G(V) \oplus \mathrm{Hom}_{KG}(V, W^*) \oplus \mathcal{F}_G(W),$$

which implies

$$\mathcal{F}_G\left(\bigoplus_{i=1}^{m} V\right) \cong \bigoplus_{i=1}^{\frac{m(m+1)}{2}} \mathcal{F}_G(V) \oplus \bigoplus_{j=1}^{\frac{m(m-1)}{2}} \mathfrak{S}_G(V).$$

Analogously, we have

$$\mathfrak{S}_G(V \oplus W) \cong \mathfrak{S}_G(V) \oplus (V^* \otimes W^*)^G \oplus \mathfrak{S}_G(W) \cong \mathfrak{S}_G(V) \oplus \mathrm{Hom}_{KG}(V, W^*) \oplus \mathfrak{S}_G(W)$$

and

$$\mathfrak{S}_G\left(\bigoplus_{i=1}^{m} V\right) \cong \bigoplus_{i=1}^{\frac{m(m+1)}{2}} \mathfrak{S}_G(V) \oplus \bigoplus_{j=1}^{\frac{m(m-1)}{2}} \mathcal{F}_G(V).$$

From now on we will assume that K is a totally real number field.

Since the dimension of the form space on a KG-module V is of extreme interest, the following formula is quite useful.

Theorem 4.2.9 ([Ple81]) *Let V be a KG-module with character χ. Consider a decomposition of χ into complex irreducible characters of G,*

$$\chi = \sum_{i=1}^{r} a_i \chi_i + 2 \sum_{j=1}^{s} b_j \psi_j + \sum_{k=1}^{t} c_k(\nu_k + \overline{\nu_k}),$$

with $a_i, b_j, c_k \in \mathbb{Z}$, χ_i real, ψ_j quaternionic and ν_k complex. This terminology is used to denote characters of $\mathbb{R}$-linear representations whose endomorphism rings are isomorphic to $\mathbb{R}$, the Hamilton quaternions and $\mathbb{C}$, respectively.
Then the dimension of the form space on V is

$$\dim_K(\mathcal{F}_G(V)) = \dim_{\mathbb{R}}(\mathcal{F}_G(\mathbb{R} \otimes_K V)) = \sum_{i=1}^{r} \frac{1}{2}(a_i^2 + a_i) + \sum_{j=1}^{s} (2b_j^2 - b_j) + \sum_{k=1}^{t} c_k^2.$$

Proof. We follow [Ple81]. The character of G on the space of symmetric bilinear forms is $\frac{1}{2}(\chi^2 + \chi^{(2)})$, where $\chi^{(2)}(g) := \chi(g^2)$. Hence, $\dim_K(\mathcal{F}_G(V)) = (\frac{1}{2}(\chi^2 + \chi^{(2)}), \mathbb{1}_G)_G$. We now compute

$$\frac{1}{2}(\chi^2, \mathbb{1}_G)_G = \frac{1}{2}(\chi, \overline{\chi})_G = \frac{1}{2}(\chi, \chi)_G = \frac{1}{2}\left(\sum_{i=1}^{r} a_i^2 + \sum_{j=1}^{s} 4b_j^2 + \sum_{k=1}^{t} 2c_k^2\right).$$

The Frobenius-Schur theorem [CR87b, 73.13] states that $(\chi_i^{(2)}, \mathbb{1}_G)_G = 1$, $(\psi_j, \mathbb{1}_G)_G = -1$ and $(\nu_k^{(2)}, \mathbb{1}_G)_G = (\overline{\nu_k}, \mathbb{1}_G)_G = 0$, whence

$$\frac{1}{2}(\chi^{(2)}, \mathbb{1}_G)_G = \frac{1}{2}\left(\sum_{i=1}^{r} a_i - \sum_{j=1}^{s} 2b_j\right),$$

which completes the proof. □

Corollary 4.2.10 *V is uniform if and only if $\mathbb{R} \otimes_K V$ is irreducible.*

Given that computing decompositions of G-modules into irreducible constituents is usually faster in the case of finite ground fields (cf. the `MeatAxe`-algorithm, see [Hol98] for a brief survey), we now present a method which allows us to perform a computation over a finite field in order to obtain the K-dimension of $\mathcal{F}_G(V)$.

Since representation theory in characteristic zero is in a certain sense equivalent to that over a sufficiently large field of characteristic p not dividing the group order, we can work over such an appropriately chosen finite field. The details of this are explained in Paragraphs 16 and 17 of Chapter 2 of [CR87a].
To describe the theory we will choose a finite field $\mathbb{F}_q$ such that $\mathrm{char}(\mathbb{F}_q) \nmid 2|G|$ and work over its algebraic closure.

Let $V \in \mathbb{F}_q G\text{-}\mathsf{mod}$ be irreducible. Consider the decomposition of $\overline{\mathbb{F}_q} \otimes_{\mathbb{F}_q} V$ into irreducible modules, i.e. the decomposition of V into absolutely irreducible constituents. Since we are now working over an algebraically closed field, on each constituent there will be precisely either one symmetric or one skew-symmetric form up to scalar multiples or the constituent is not self-dual.

In addition to orthogonal representations, we will call a G-module (over an appropriate ground ring) symplectic if there is a non-degenerate skew-symmetric G-invariant bilinear form on V and we will call V unitary if there are both non-zero symmetric and non-zero skew-symmetric G-invariant bilinear forms on V.

Now, if we assume V to be self-dual we have the following decomposition.

$$\overline{\mathbb{F}_q} \otimes_{\mathbb{F}_q} V \cong \bigoplus_{i=1}^{s} V_i^{\alpha_i} \oplus \bigoplus_{j=1}^{t} W_j^{\beta_j} \oplus \bigoplus_{\ell=1}^{r} (X_\ell \oplus X_\ell^*)^{\gamma_\ell}, \tag{4.1}$$

where the V_i are orthogonal, the W_j symplectic and the X_ℓ are not self-dual, which is why their respective duals occur with the same multiplicity in the decomposition. Notice that the $X_\ell \oplus X_\ell^*$ are unitary.

It is our aim to compute the dimension $\dim_{\mathbb{F}_q}(\mathcal{F}_G(V))$ from the decomposition (4.1). This is easily done using the formulas in Corollary 4.2.8.

Lemma 4.2.11 *Given the decomposition* (4.1)*, the dimension* $\dim_{\mathbb{F}_q}(\mathcal{F}_G(V))$ *is*

$$\sum_{i=1}^{s} \frac{\alpha_i(\alpha_i+1)}{2} + \sum_{j=1}^{t} \frac{\beta_j(\beta_j-1)}{2} + \sum_{\ell=1}^{r} \gamma_\ell^2.$$

Now, if $\widetilde{V}$ is a KG-module and we realize it over $\mathbb{F}_q$ (call the resulting module V) as described in [CR87a], we have $\dim_K(\mathcal{F}_G(\widetilde{V})) = \dim_{\mathbb{F}_q}(\mathcal{F}_G(V))$, which makes the above considerations useful in practice. In fact, this method of computing the dimension of the form space is implemented in the method `InvariantForms` of the computer algebra system `Magma`, [BCP97], cf. also Chapter 8. Of course, this method yields the dimension of $\mathfrak{S}_G(V)$ at the same time.

Now, with Hasse's Theorem 3.6.29 in mind, we formulate the central question already presented in the introduction to this thesis:

Let V be a uniform KG-module and ϕ a regular G-invariant quadratic form on it. What are the determinant (or discriminant) and Clifford invariant of ϕ?

Notice however, that for all $a \in K^\times$, $a\phi$ is an invariant and regular form as well, so it really only makes sense to ask for the determinant in even-dimensional cases and the Clifford invariant in odd-dimensional cases. This is due to the multilinearity of the determinant and the formulas in Proposition 3.6.24. However, there are some cases where an even-dimensional representation admits only one Clifford invariant. This happens when the discriminant is a square, see for example the orthogonal representations of $\mathrm{PSL}_2(8)$ or $\mathrm{PSL}_2(9)$ as described in Theorems 6.5.10 and 6.4.27.

The following theorem provides a first restriction on the possible determinants.

Theorem 4.2.12 ([NP95, Theorem II.2]) *Let V be a uniform KG-module and ϕ an invariant form on V. Then a finite prime place $\mathfrak{p}$ of K occurring with odd multiplicity in* $\det(\phi)$ *is a divisor of the group order $|G|$.*

In order to conclude this section, we want to briefly touch upon the subject of certain group actions on the character table, namely that of $\mathrm{Out}(G)$ and that of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Proposition 4.2.13 *It is a standard fact that the group* $\mathrm{Out}(G)$ *of outer automorphisms acts on the character table of* G *by permuting conjugacy classes, i.e. columns of the table. This means that given a character* χ *with* KG*-module* V_χ *and a* G*-invariant form* F *on* V_χ*,* F *is also an invariant form on the module* $V_{\sigma\chi}$ *corresponding to the character* $\sigma\chi$ *for any* $\sigma \in \mathrm{Out}(G)$*, since the invariant forms on* V_χ *and* $V_{\sigma\chi}$ *are defined by the same set of linear equations.*
Hence, if V_χ *is uniform, so is* $V_{\sigma\chi}$ *and the determinants and Clifford invariants of the invariant forms coincide.*

Next, we discuss an action of a Galois group on a finite-dimensional associative algebra over a number field.

Definition 4.2.14 Let E/L be a Galois extension of number fields and A a finite-dimensional associative E-algebra. Then E is a quotient of the free associative algebra over E in variables $x_1, ..., x_n$ by some relations, which are "non-commutative polynomials" with coefficients in E. Every $\sigma \in \mathrm{Gal}(E/L)$ acts on E by its natural action on the coefficients of the relations. We call the resulting algebra ${}^\sigma A$.

Remark 4.2.15 This action of $\mathrm{Gal}(E/L)$ on A may equivalently be described as follows. Let $v_1, ..., v_\ell$ be an E-basis of A. The ℓ^3 elements $a_{i,j,k}$ defined by

$$v_i v_j = \sum_{k=1}^{\ell} a_{i,j,k} v_k$$

are called the structure constants or multiplication table of A. The action of an automorphism $\sigma \in \mathrm{Gal}(E/L)$ on A is given by mapping each $a_{i,j,k}$ to $\sigma(a_{i,j,k})$.
A and ${}^\sigma A$ clearly have the expected properties, e.g. if A is simple, so is ${}^\sigma A$; or if A is ramified at the place $\mathfrak{p}$ of E, then ${}^\sigma A$ is ramified at $\sigma(\mathfrak{p})$.
Clearly, this action on finite-dimensional K-algebras induces an action of $\mathrm{Gal}(E/L)$ on $\mathrm{Br}(E)$.

With this action at hand, we return to our previous setup, where we obtain the following straightforward result.

Proposition 4.2.16 *Let* $\chi \in \mathrm{Irr}(G)$*, with corresponding* G*-module* V_χ *and an invariant form* q *on* V_χ*. Let* $\sigma \in \mathrm{Gal}(\mathbb{Q}[\chi]/\mathbb{Q})$*. Then* ${}^\sigma q$ *is an invariant form on* $V_{{}^\sigma\chi}$*, where* ${}^\sigma q$ *is obtained from* q *by applying* σ *to a Gram matrix of* q*.*
It is evident that $\det({}^\sigma q) = \sigma(\det(q))$ *and that* $\mathcal{C}({}^\sigma q) = {}^\sigma\mathcal{C}(q)$*.*

4.3 Various methods

Throughout this section, unless otherwise stated, we will assume that K is a totally real number field and G is a finite group.

The following methods and construction may help to answer the central question raised in the introduction of this thesis.

4.3.1 Restriction

Let $H \leq G$ be a subgroup and V a uniform KG-module. Assume that $V|_H$ decomposes into uniform KH-modules, $V|_H \cong X_1 \oplus ... \oplus X_r$.

Proposition 4.3.1 *If* $0 \equiv \dim_K(V) \equiv \dim_K(X_1) \equiv ... \equiv \dim_K(X_r) \pmod 2$*, then* $\det(V)$ *is the product of the* $\det(X_i)$*,* $1 \leq i \leq r$*.*
If $\dim_K(V)$ *is odd and* $r = 1$*,* $\mathfrak{c}(V) = \mathfrak{c}(X_1)$*.*

This statement is evident. In the case of an odd-dimensional representation and multiple KH-constituents, i.e. $r \geq 2$, it may often be impossible to read off $\mathfrak{c}(V)$ from the Clifford invariants of the constituents due to the rules in Proposition 3.6.24.

4.3.2 Permutation representations

Proposition 4.3.2 *Let* $\chi \in \mathrm{Irr}(G)$*,* $\chi(1) := n$*. Assume that* $\mathbb{1}_G + \chi$ *is the character of a permutation representation. Then there is an orthogonal* KG*-module* φ_0 *with character* χ *such that*

$$\bigoplus_{i=1}^{n+1} \langle 1 \rangle \cong \langle n+1 \rangle \oplus \varphi_0.$$

This implies $\varphi_0 \cong \mathbb{A}_n$ *and, depending on* n*, the determinant or Clifford invariant of all orthogonal* KG*-modules with character* χ *can be read off from Example 3.6.25.*

4.3.3 Tensor products and exterior and symmetric powers

Let φ be a regular quadratic space over K. Consider the tensor product $\varphi \otimes \varphi$, which is again a quadratic space. It has an orthogonal decomposition into

$$\varphi \otimes \varphi \cong \bigwedge^2(\varphi) \oplus S^2(\varphi),$$

the exterior and symmetric square of φ.

Recall from Definition 3.1.21 that we introduced a factor 2 into the quadratic form on a tensor product. However, as we are working over a field of characteristic zero, we can consider the space $\frac{1}{2} \circ (\varphi \otimes \varphi)$.

Theorem 4.3.3 *Let ψ be another regular quadratic K-space and put $n := \dim(\varphi)$, $m := \dim(\psi)$. Then we have*

$$\begin{aligned} \det\left(\frac{1}{2} \circ (\varphi \otimes \psi)\right) &= \det(\varphi)^m \det(\psi)^n, \\ \mathfrak{c}\left(\frac{1}{2} \circ (\varphi \otimes \psi)\right) &= \mathfrak{c}(\varphi)^m \mathfrak{c}(\psi)^n (\mathrm{d}_{\pm}(\varphi), \mathrm{d}_{\pm}(\psi))^{nm-1}. \end{aligned}$$

Proof. The statement about the determinant is well known. For the Clifford invariant, see [Neb99, Satz 3.1.33]. □

Theorem 4.3.4 *For the exterior square we have $\dim\left(\bigwedge^2 \varphi\right) = \binom{n}{2}$, $\det\left(\bigwedge^2 \varphi\right) = \det(\varphi)^{n-1}$ and*

$$\mathfrak{c}\left(\frac{1}{2} \circ \bigwedge^2 \varphi\right) = (\det(\varphi), \det(\varphi))^{\binom{n-1}{2}} \mathfrak{c}(\varphi)^n \cdot \begin{cases} 1 & n \equiv 1, 2, 12 \pmod{16}, \\ (-1, \det(\varphi)) & n \equiv 3, 6, 15, 16 \pmod{16}, \\ (-1, -1) & n \equiv 4, 5, 9, 10, 13 \pmod{16}, \\ (-1, -\det(\varphi)) & n \equiv 7, 8, 11, 14 \pmod{16}. \end{cases}$$

Proof. This is proved in [Neb99, Satz 3.4.5]. Notice that in that reference, there is only a statement about the so-called "Hasse invariant" of quadratic spaces. However, Satz 3.1.33 of loc.cit. provides a formula that relates the Hasse invariant and the Clifford invariant. □

Remark 4.3.5 The invariants of the symmetric square $S^2(\varphi)$ may now be obtained through the equation $\varphi \otimes \varphi \cong \bigwedge^2 \varphi \obot S^2(\varphi)$.

With the formula for the Clifford invariant of a tensor product of quadratic spaces we can now construct irreducible orthogonal representations with prescribed Clifford invariants.

Remark 4.3.6 Let $G \leq \mathrm{GL}_n(K)$, $H \leq \mathrm{GL}_m(K)$ $(n, m \in \mathbb{N})$ with commuting algebras isomorphic to K. In other words, we have two absolutely irreducible representations of two finite groups over K. Using the Kronecker product we can form the matrix group

$$G \otimes H = \{g \otimes h \mid g \in G,\ h \in H\} \leq \mathrm{GL}_{n \cdot m}(K).$$

Group-theoretically, $G \otimes H$ is isomorphic to some central product $G \curlyvee H$ of G and H. If at least one of G and H has trivial center, this is in fact the direct product of G and H. In either case, the $K[G \curlyvee H]$-module $K^{n \cdot m}$ is also absolutely irreducible.
If n and m are both odd, the Clifford invariants $\mathfrak{c}(K^n)$ and $\mathfrak{c}(K^m)$ (for any regular G- or H-invariant form, respectively) are well-defined, and so is the Clifford invariant on $\mathfrak{c}(K^{n \cdot m})$, which we find to be $\mathfrak{c}(K^n) \cdot \mathfrak{c}(K^m)$.

4.3.4 Trace forms of Hermitian forms

We use the definitions and terminology of Section 3.4.1 of [Neb99].

Definition 4.3.7 Let L/K be a separable extension of degree 2 in characteristic zero and σ the generator of $\mathrm{Gal}(L/K)$. Let V be an L-vector space. $h : V \times V \to L$ is called a Hermitian form if h is linear in the first argument and $h(w,v) = \sigma(h(v,w))$ for all $v, w \in V$.
The trace form t_h of h is $V \times V \to K,\ (x,y) \mapsto \mathrm{tr}_{L/K}(h(x,y))$.
The determinant of h is the determinant of a Gram matrix of h in the norm residue group $K^\times/N_{L/K}(L^\times)$. The discriminant of h is defined as usual.

Theorem 4.3.8 ([Neb99, Satz 3.4.2]) *Write $L = K[\sqrt{\delta}]$ and $n = \dim_L(V)$. We then have $\dim_K(t_h) = 2n$, $\mathrm{d}_\pm(t_h) = \delta^n$ and $\mathfrak{c}(t_h) = (\delta, \mathrm{d}_\pm(h)) \in \mathrm{Br}_2(K)$.*

Theorem 4.3.9 *Let χ be an absolutely irreducible character of G such that $\mathbb{Q}[\chi]$ is totally imaginary. Denote the complex conjugation by $\overline{}$, let K be its fixed field within $\mathbb{Q}[\chi]$ and write $\mathbb{Q}[\chi] = K[\sqrt{\delta}]$ for some $\delta \in K$. Let m denote the Schur index of χ over its character field. Then $m(\chi + \overline{\chi})$ is the character of a KG-module of even dimension which is uniform if and only if $m = 1$.*
The discriminant of any non-zero invariant form on the KG-module whose character contains χ is $\delta^{m\chi(1)}$.
If $m = 1$ and $\delta^{\chi(1)}$ is a square, the Clifford invariant is constant under scalingand may be read off from the discriminant of a G-invariant Hermitian form on a $\mathbb{Q}[\chi]G$-module affording the character $m\chi$.

Proof. The character $\chi + \overline{\chi}$ is irreducible over the reals, so the module affording the character $m(\chi + \overline{\chi})$ is uniform if and only if $m = 1$.
Let V be a $\mathbb{Q}[\chi]G$-module whose character contains χ and let f be a G-invariant symmetric bilinear form on the associated KG-module $V|_K$. Then

$$h : V \times V \to K[\sqrt{\delta}],\ (x,y) \mapsto \frac{1}{2}\left(f(v,w) + \frac{1}{\sqrt{\delta}} f(\sqrt{\delta}v, w)\right)$$

is a G-invariant Hermitian form such that $t_h = f$. Notice that $\dim_{\mathbb{Q}[\chi]}(V) = m\chi(1)$. The statement now follows from the previous theorem. □

Remark 4.3.10 The discriminant of a G-invariant Hermitian form may often be determined by considering the p-modular behaviour of the representation in question. This is illustrated in Chapter 9 of this thesis.

4.3.5 Orthogonal Frobenius Reciprocity

Classical Frobenius reciprocity, which, at the character-theoretic level, establishes the equality

$$(\psi, \chi|_H)_H = (\mathrm{ind}_H^G(\psi), \chi)_G$$

for $H \leq G$, $\chi \in \mathrm{Irr}(G)$ and $\psi \in \mathrm{Irr}(H)$, may also be formulated in the following way. Let R be a ring, $W \in RH\text{-}\mathsf{mod}$ and $V \in RG\text{-}\mathsf{mod}$. Then there is an isomorphism of R-modules

$$\mathrm{Hom}_{RH}(W, V|_H) \to \mathrm{Hom}_{RG}(\mathrm{ind}_H^G(W), V),\ \varphi \mapsto \varphi^G,$$

where φ^G is defined as in Section 4.1. See [CR87a, Theorems 10.8, 10.9] for a more detailed exposition of Frobenius reciprocity.

Assume now that W is equipped with a regular H-invariant symmetric bilinear form F_W and that V is equipped with a regular G-invariant symmetric bilinear form F_V.
Let $G = \bigsqcup_{i=1}^s g_i H$ be a decomposition of G into H-cosets.

Remark 4.3.11 There is a non-degenerate G-invariant symmetric bilinear form F_W^G on $\mathrm{ind}_H^G(W)$ defined by

$$F_W^G(w \otimes g_i, w' \otimes g_j) := \delta_{ij} F_W(w, w')$$

for all $w, w' \in W$ and $1 \leq i, j \leq s$.

Remark 4.3.12 Recall that F_V defines a KG-isomorphism $\widetilde{F_V} : V \to V^*$, $v \mapsto F_V(v, \cdot)$. Define F_V^* to be the symmetric bilinear form on V^* for which $\widetilde{F_V}$ is an isometry. Precisely, for $f \in V^*$ put $v_f := \widetilde{F_V}^{-1}(f) \in V$ and define

$$F_V^*(f, h) := F_V(v_f, v_h)$$

for all $f, h \in V^*$.

We will now consider the KH-isometries

$$\mathrm{Isom}_{KH}\big((W, F_W), (V|_H, F_V)\big) := \left\{ \varphi \in \mathrm{Hom}_{KH}(W, V|_H) \;\middle|\; \substack{\varphi \text{ is injective and} \\ F_W(w,w') = F_V(\varphi(w), \varphi(w')) \\ \text{for all } w, w' \in W} \right\}.$$

Notice that in the question raised in the introduction of this thesis we were only concerned with the K-linear isometry class of a regular symmetric G-invariant form, whereas $\mathrm{Isom}_{KH}\big((W, F_W), (V|_H, F_V)\big)$ contains only H-equivariant isometries.

Orthogonal Frobenius reciprocity, which was first introduced by Gabriele Nebe in [Neb99] (see also [Neb00b]), is concerned with the behavior of these KH-isometries when Frobenius reciprocity is applied. Under the hypothesis that (V, F_V) is a uniform KG-module we obtain the following answer.

Theorem 4.3.13 (Orthogonal Frobenius reciprocity) *Under the abovementioned conditions, there is a bijection*

$$\begin{aligned} &\mathrm{Isom}_{KH}\big((W, F_W), (V|_H, F_V)\big) \\ \to &\mathrm{Isom}_{KG}\left((V^*, F_V^*), \left((\mathrm{ind}_H^G(W))^*, \frac{\dim_K(V)}{\dim_K(W^G)} (F_W^G)^* \right) \right) \end{aligned}$$

defined by

$$\varphi \mapsto (\varphi^G)^*.$$

For the proof of this statement, we refer the reader to the original sources. An application of this method is presented in Section 6.1.

4.3.6 A Clifford theory of orthogonal representations

Let $N \trianglelefteq G$ be a normal subgroup. Clifford theory explains the interplay of irreducible representations of N and G. We want to describe the behavior of invariant forms under this correspondence.

Let K be a totally real number field and (V, F) an irreducible orthogonal KG-module. Let X be an irreducible KN-module occurring as a direct summand of $V|_N$. Let I be the inertia group of X, of index $t := [G : I]$ in G, and let $G = \bigsqcup_{i=1}^t g_i I$ be a decomposition of G into left I-cosets. We then have the following decomposition of $V|_N$ into irreducibles.

$$V|_N \cong \bigoplus_{i=1}^{t} \left({}^{g_i}X\right)^e, \tag{4.2}$$

where e is the multiplicity of X in $V|_N$. In this situation we obtain the following theorem.

Theorem 4.3.14 *1. F restricts to an N-invariant form on $V|_N$ which as a quadratic form over K is isometric to an orthogonal direct sum $F_1 \perp ... \perp F_t$ with regular $F_i \in \mathcal{F}_N\left(\left({}^{g_i}X\right)^e\right)$.*

2. The forms F_i are pairwise K-isometric.

Proof. 1. Clearly, the restriction of F to the submodules ${}^{g_i}X$ is N-invariant.The submodules $\left({}^{g_i}X\right)^e$ are pairwise orthogonal because there are no KN-homomorphisms between them, so that orthogonality follows from Corollary 4.2.8.
But then we have $\det(F) = \prod_{i=1}^t \det(F_i)$ and since F is regular, so is each of the F_i.

2. $X \to {}^{g_i}X,\ x \mapsto g_i x$ is a K-linear map satisfying

$$F|_{X\times X}(x_1, x_2) = F(x_1, x_2) = F(g_i x_1, g_i x_2) = F|_{{}^{g_i}X\times {}^{g_i}X}(g_i x_1, g_i x_2)$$

for all $x_1, x_2 \in X \leq V|_N$. □

Remark 4.3.15 There is a K-linear isomorphism $\mathcal{F}_G(V) \cong \mathcal{F}_I\left(\left({}^{g_i}X\right)^e\right)$.

Proof. As $X' := ({}^{g_i}X)^e$ is a KI-module, X' is a constituent of $V|_I$ and we can write $V|_I \cong X' \oplus Y$ with $\mathrm{Hom}_{KI}(X', Y) = \{0\}$.
We then have

$$(V^* \otimes_K V^*)^G \cong \mathrm{Hom}_{KG}(V, V^*) \cong \mathrm{Hom}_{KG}(V, V) \cong \mathrm{Hom}_{KG}\left(\mathrm{ind}_I^G\left(X'\right), V\right),$$

since V is self-dual. By Frobenius reciprocity this is isomorphic to

$$\mathrm{Hom}_{KI}\left(X', V|_I\right) \cong \mathrm{Hom}_{KI}\left(X', X' \oplus Y\right) \cong \mathrm{Hom}_{KI}\left(X', X'\right).$$

The statement now follows from Remark 4.2.5, which establishes the description of $\mathcal{F}_G(V)$ in terms of the symmetric square $S^2(V^*)^G$. □

Remark 4.3.16 In Section 9.3 we apply this result to group extensions of the form

$$1 \to N \to G \to Q \to 1$$

for normal subgroups N whose orthogonal representations we already know. Theorem 4.3.14 then allows for the computation of Clifford invariants in some such situations. Without this result it may be more subtle to determine Clifford invariants of orthogonal KG-modules from the Clifford invariants of orthogonal KN-modules.

Remark 4.3.17 (Wreath products) Let G be a finite group and $\Delta : G \to \mathrm{GL}(V)$ an irreducible representation of degree d.

$$\Delta_1 : \underbrace{G \times G \times ... \times G}_{k \text{ factors}} \to \mathrm{GL}(V), \ (g_1, g_2, ..., g_k) \mapsto \Delta(g_1)$$

is a uniform (and thereby irreducible) representation of the k-fold direct product of G with itself.
By ordinary Clifford theory $\mathrm{ind}_{G^k}^{G \wr C_k}(\Delta_1)$ is an irreducible representation of the wreath product $G \wr C_k$ of degree $k \cdot d$.
Assume that k and d are both odd, so that the induced representation is of odd degree as well. Applying Theorem 4.3.14 to the chain

$$G \wr C_k \trianglerighteq G \times G \times ... \times G \trianglerighteq G$$

of normal subgroups we obtain the relation

$$\mathfrak{c}(\mathrm{ind}_{G^k}^{G \wr C_k}(\Delta_1)) = \mathfrak{c}(q^k).$$

for $0 \neq q \in \mathcal{F}_G(V)$.

4.3.7 Nebe's character method

In this section, we assume that the finite group G has the property that $|G/G'|$ is odd, where G' is the derived subgroup of G. This property is satisfied, for example, by all perfect groups, so this restriction is not too strict.

The method presented in this section was developed by Gabriele Nebe, cf. [Neb00a] and [Neb99]. It is a character-theoretic method which allows one to read off the discriminant or Clifford invariant from the character table of G under certain favourable conditions.

We briefly present the method and provide proofs for the statements whose proof is not provided in the original sources.

Let $\varphi = (V, q)$ be an orthogonal KG-module of dimension n with character χ. Since the orthogonal group $\mathrm{O}(\varphi)$ acts on $\mathcal{C}(\varphi)$ (and $\mathcal{C}_0(\varphi)$), we also obtain a representation of G on $\mathcal{C}(\varphi)$ and $\mathcal{C}_0(\varphi)$ by restriction, denoted by $\Delta_{\mathcal{C}(\varphi)}$ and $\Delta_{\mathcal{C}_0(\varphi)}$, respectively. Their characters are obtained as follows.

Remark 4.3.18 ([Neb00a, Remark 3.1]) The characters of $\mathcal{C}(\varphi)$ and $\mathcal{C}_0(\varphi)$ as KG-modules with the action described above are given by

$$\widetilde{\chi} := \sum_{i=0}^{n} \bigwedge^{i}(\chi) \text{ and } \widetilde{\chi}_0 := \sum_{\substack{i=0 \\ i\equiv 0 \pmod 2}}^{n} \bigwedge^{i}(\chi),$$

respectively.
Here, $\bigwedge^i(\chi)$ denotes the i-th exterior power of χ.

Proof. Pick a basis $(e_1, ..., e_n)$ of V and let $\Delta : G \to K^{n\times n}$ be the representation matrix associated to the KG-module V with respect to this basis. Then, considering the rule

$$e_i e_j = -e_j e_i + b_q(e_i, e_j) \cdot 1_{\mathcal{C}(\varphi)}$$

for multiplication in $\mathcal{C}(\varphi)$ and equating coefficients, we find that the matrix of $\Delta_{\mathcal{C}(\varphi)}(g)$ with respect to the basis

$$(1, e_1, ..., e_n, e_1e_2, e_1e_3, ..., e_1 \cdot ... \cdot e_n)$$

is

$$\begin{pmatrix} 1 & 0 & * & 0 & ... & * \\ 0 & \Delta(g) & 0 & * & ... & * \\ \vdots & 0 & \bigwedge^2 \Delta(g) & 0 & ... & * \\ \vdots & & 0 & \bigwedge^3 \Delta(g) & ... & * \\ \vdots & & & & \ddots & \vdots \\ 0 & ... & ... & ... & 0 & \bigwedge^n(\Delta(g)) \end{pmatrix}$$

See Proposition 10 of Chapter III, §5 of [Bou89] in order to find a description of the matrix coefficients of $\bigwedge^i(\Delta(g))$. □

Fix a covering group $u : \widetilde{G} \to G$ in the sense of Schur. We let W be the simple $c(\varphi)$-module and m the Schur index of the endomorphism algebra $\mathrm{End}_{c(\varphi)}(W)$.

The Clifford group is defined as

$$\Gamma(\varphi) := \{s \in \mathcal{C}_0(\varphi)^\times \cup (\mathcal{C}(\varphi)^\times \cap \mathcal{C}_1(\varphi)) \mid sVs^{-1} = V\}.$$

We define the maps

$$\gamma : \Gamma(\varphi) \to \{1, -1\},\ s \mapsto \begin{cases} 1 & s \in \mathcal{C}_0(\varphi) \\ -1 & s \in \mathcal{C}_1(\varphi) \end{cases}$$

and

$$\alpha : \Gamma(\varphi) \to \mathrm{O}(\varphi),\ s \mapsto \big(\alpha(s) : V \to V,\ v \mapsto (-1)^{\deg(s)} svs^{-1}\big).$$

Notice that α is surjective, for if $s \in V \subseteq \mathcal{C}_1(\varphi)$ and $q(s) \neq 0$, $\alpha(s)$ is the reflection along s. In the case $\mathrm{char}(K) \neq 2$, reflections generate the orthogonal group, yielding surjectivity. However, the surjectivity of α also holds in characteristic two, as is shown in [Knu91, p. 228].
The kernel of α is $K^\times \subseteq \mathcal{C}_0(\varphi)^\times$, so that we obtain the following exact sequence.

$$1 \to K^\times \to \Gamma(\varphi) \to \mathrm{O}(\varphi) \to 1,$$

from which we can define a projective representation

$$P : \mathrm{O}(\varphi) \to \Gamma(\varphi)$$

which is defined by mapping the reflection along an anisotropic vector $s \in V$ to $s \in \Gamma(\varphi)$.

Lemma 3.2 of [Neb00a] shows that P may be "normalized" in the following way. For all $g \in G$ there exist $a_g \in K^\times$ such that $P_0(g) := a_g P(g)$ has the properties

$$P_0(g) \in \mathcal{C}_0(\varphi),\ P_0(g)\overline{P_0(g)} = 1,$$

where $\overline{}$ is the involution of $\mathcal{C}(\varphi)$ defined by $\overline{v_1 \cdot \ldots \cdot v_s} = v_s \cdot \ldots \cdot v_1$ for $v_i \in V$, and $P_0 \otimes P_0 : G \to \mathrm{GL}(c(\varphi))$ is a linear representation which is equivalent to $\Delta_{c(\varphi)}$. The following theorem makes use of this last fact.

Theorem 4.3.19 ([Neb00a, Theorem 3.5]) *For this theorem, let K be an arbitrary number field. This implies that $c(\varphi)$ is a matrix ring over a quaternion algebra [Vig80, III, §3], as it is a tensor product of quaternion algebras, see [Sch85, Lemma 9.2.8]. Also,*

$\mathcal{C}_0(\varphi) \cong D^{a\times a}$, for some $a \in \mathbb{N}$, where either $D = L := Z(\mathcal{C}_0(\varphi))$ or D is a quaternion division algebra over L.
Let m be the Schur index of D and $m\chi_W$ the character of $\widetilde{G}$ afforded by W over K. Assuming that there is an absolutely irreducible character ψ of $\widetilde{G}$ occurring with odd multiplicity in χ_W, the following two statements hold.

1. *If n is even and L is a field, then L is a subfield of the character field $K[\psi]$.*

2. *Let n be odd. If m is odd, $K(\psi)$ splits D. If m is even, let U be the smallest $K\widetilde{G}$-module whose character contains ψ. Then we have the inclusion $D \subseteq \operatorname{End}_{K\widetilde{G}}(U)$.*

From this theorem we obtain the following corollary, if we once again restrict K to be a totally real number field, in which case the Schur index of a division algebra is 1 or 2 by Theorem 4.1.18 of Brauer and Speiser.

Corollary 4.3.20 ([Neb00a, Corollary 3.6]) *Assume that φ is a positive definite orthogonal representation.*

1. *For n even consider the case where $[K(\psi) : K]$ is odd. Then $\mathrm{d}_\pm(\varphi) = 1$. The same holds if $n \equiv 0 \pmod 4$ and all intermediate fields $K(\psi)/L/K$ of degree $[L : K] = 2$ are totally complex. If $n \equiv 2 \pmod 4$ the extension $K(\psi)/K$ has at least one totally complex intermediate field L satisfying $[L : K] = 2$. One of the intermediate fields with this property is isomorphic to $K[\sqrt{\mathrm{d}_\pm(\varphi)}]$.*

2. *Now let n be odd. If the Schur index of ψ is 1, we have the identity*

   $$[c(\varphi) \otimes_K K(\psi)] = [K(\psi)] \in \mathrm{Br}_2(K(\psi))$$

   for the Clifford invariant $\mathfrak{c}(\varphi)$.
   In case ψ has Schur index 2, we have

   $$[c(\varphi) \otimes_K K(\psi)] = [\operatorname{End}_{K(\psi)\widetilde{G}}(U)] \in \mathrm{Br}_2(K(\psi)),$$

   where U is the irreducible $K(\psi)\widetilde{G}$-module with character 2ψ.

Remark 4.3.21 One favourable case to apply the above method is $H^2(G, \mathbb{C}^\times) = \{1\}$, i.e. $\widetilde{G} \cong G$. For example, all invariants of the irreducible orthogonal representations of the group $\mathrm{PSL}_2(8)$ may be calculated using this method. They are listed in the examples section of this thesis.

The following statement may be useful when applying this method.

Remark 4.3.22 ([Neb99, Bemerkung 3.1.2]) For $g \in \widetilde{G}$, the value of the character $\widetilde{\chi}$ of the G-module $\mathcal{C}(\varphi)$ at the element g may be computed as $\widetilde{\chi}(g) = (-1)^{\dim(\varphi)} p_g(-1)$,

where p_g is the characteristic polynomial of the action of g on V.
Let $\Delta : G \to \mathrm{GL}_n(K)$ denote the representation map of the KG-module V.
If $\dim(\varphi)$ is odd and $\det(\Delta(G)) = \{1\}$, the character $\widetilde{\chi_0}$ of the even part of the Clifford algebra is obtained as $\widetilde{\chi_0} = \frac{1}{2}\widetilde{\chi}$.

Proof. Put $n = \dim(\varphi)$ and write the characteristic polynomial $p_g = p_{\Delta(g)}$ as

$$p_g(X) = \sum_{i=0}^{n} c_i X^{n-i}.$$

It is well known (see, e.g., Chapter III, §11 of [Bou89]) that $c_i = (-1)^i \mathrm{tr}\left(\bigwedge^i \Delta(g)\right)$. Using this fact and Remark 4.3.18, we obtain

$$\begin{aligned}\widetilde{\chi}(g) = \mathrm{tr}(\Delta_{\mathcal{C}(\varphi)}(g)) &= \sum_{i=0}^{n} \mathrm{tr}\left(\bigwedge^i(\Delta(g))\right)\\ &= (-1)^n \sum_{i=0}^{n} (-1)^n \mathrm{tr}\left(\bigwedge^i(\Delta(g))\right)\\ &= (-1)^n \sum_{i=0}^{n} (-1)^i \mathrm{tr}\left(\bigwedge^i(\Delta(g))\right)(-1)^{n-i}\\ &= (-1)^{\dim(\varphi)} p_g(-1),\end{aligned}$$

as claimed.

To prove the second part of the statement, notice that there is an isomorphism

$$\bigwedge^i V \cong \bigwedge^{n-i} V \otimes_K \bigwedge^n V \tag{†}$$

of KG-modules. To see this, notice that the character χ is totally real and that the module affording it is already realized over the totally real field K, implying that all exterior powers are totally real as well. In particular, the characters $\bigwedge^i \chi$ have the same values on g and g^{-1}.

Further assume $\Delta(g)$ to be diagonalized with eigenvalues $\{\zeta_1, ..., \zeta_n\}$. Then

$$\begin{aligned}
\operatorname{tr}\left(\bigwedge^i \Delta(g)\right) &= \sum_{\substack{I\subseteq \underline{n}\\ |I|=i}} \prod_{\ell\in I} \zeta_\ell \\
&= \sum_{\substack{I'\subseteq \underline{n}\\ |I'|=n-i}} \prod_{\ell\in \underline{n}-I'} \zeta_\ell \\
&= \sum_{\substack{I'\subseteq \underline{n}\\ |I'|=n-i}} \det(\Delta(g)) \prod_{\ell\in I'} \zeta_\ell^{-1} \\
&= \det(\Delta(g)) \sum_{\substack{I'\subseteq \underline{n}\\ |I'|=n-i}} \prod_{\ell\in I'} \zeta_\ell \\
&= \det(\Delta(g))\operatorname{tr}\left(\bigwedge^{n-i} \Delta(g^{-1})\right) \\
&= \det(\Delta(g))\operatorname{tr}\left(\bigwedge^{n-i} \Delta(g)\right)
\end{aligned}$$

So the characters of the modules in (†) are identical, which yields a KG-isomorphism. Using this fact, we now obtain

$$\begin{aligned}
\widetilde{\chi_0}(g) &= \sum_{\substack{i=0\\ i\equiv 0 \pmod 2}}^{n} \operatorname{tr}\left(\bigwedge^i \Delta(g)\right) \\
&= \frac{1}{2} \sum_{\substack{i=0\\ i\equiv 0 \pmod 2}}^{n} \left(\operatorname{tr}\left(\bigwedge^i \Delta(g)\right) + \operatorname{tr}\left(\bigwedge^i \Delta(g)\right)\right) \\
&= \frac{1}{2} \sum_{\substack{i=0\\ i\equiv 0 \pmod 2}}^{n} \left(\operatorname{tr}\left(\bigwedge^i \Delta(g)\right) + \operatorname{tr}\left(\bigwedge^{n-i} \Delta(g)\right)\right)
\end{aligned}$$

which is equal to $\frac{1}{2}\widetilde{\chi_0}$ because we assumed that n is odd and $\det(\Delta(g)) = 1$ for all $g \in G$. □

In order to identify the character χ_W one may use this statement about the projective representation $P_0 : G \to \Gamma(\varphi)$.

Remark 4.3.23 ([Neb00a, Corollary 3.3]) Assume that $\operatorname{char}(K) \neq 2$ and consider an element $g \in G$ of order two. Let $e := \dim(\{v \in V \mid gv = -v\})$, the dimension of the (-1)-eigenspace of the action of g on V. Then $P_0(g)^2 = (-1)^{\binom{e}{2}}\mathrm{id}$.

5 Representations of Schur index 2

5.1 Totally real fields

Let G be a finite group and χ an absolutely irreducible character of G with values in a totally real number field K. Assume that the Schur index $m_K(\chi)$ is not 1, in which case $m_K(\chi) = 2$ by the theorem of Brauer and Speiser, cf. Theorem 4.1.18.

In this context the reader should also recall the theorem of Benard-Schacher, which states that for any place $\mathfrak{P}$ of K, be it finite or infinite, the Schur index $m_{\mathfrak{P}}(\chi)$ is equal to the Schur index of χ at the unique place $\mathfrak{p}$ of $\mathbb{Q}$ lying under $\mathfrak{P}$. Therefore we merely write $m_\infty(\chi)$ to denote the Schur index at any real place of K.

Let V be a KG-module with representation $\rho : G \to \mathrm{GL}(V)$ affording the character 2χ. Put $E := \mathrm{End}_{KG}(V)$ – a quaternion skewfield over K.

We present the results of [Tur93] which describe the determinant and Clifford invariant of a G-invariant form on V in that situation.

Under the abovementioned conditions, $\dim_K(\mathcal{F}_G(V)) \in \{1, 3\}$ depending on the Schur index at the infinite places of K. Either way, there is a positive definite G-invariant form $f \in \mathcal{F}_G(V)$, which we fix for the remainder of the section.

Definition 5.1.1 Since f is non-degenerate, it induces an adjoint map ^{ad} on $\mathrm{End}_K(V)$ via

$$f(\tau(v), w) = f(v, \tau^{ad}(w)),$$

where $v, w \in V$ and $\tau \in \mathrm{End}_K(V)$.
The G-invariance of f implies $\rho(g)^{ad} = \rho(g^{-1})$ for all $g \in G$, from which we obtain that ^{ad} preserves both $\rho(G)$ and its centralizer E in $\mathrm{End}_K(V)$.
We can therefore restrict ^{ad} to E and we put $\sigma_f := {}^{ad}|_E$. The map σ_f is an involution on E, that is, an anti-automorphism such that $\sigma_f \circ \sigma_f = \mathrm{id}_E$.

Let $\mathrm{tr}_{\mathrm{red}}$ denote the reduced trace $E \to K$ and note that σ_f has

$$\{e \in E \mid \mathrm{tr}_{\mathrm{red}}(e) = 0\} = \{e \in E \mid e^2 \in K,\ e \notin K\}$$

as an invariant K-linear subspace.
It is shown in the proof of Theorem 2.1 of [Tur93] that we can choose a K-basis

$$\{1, i, j, k := ij = -ji\} \subseteq E$$

for E such that

$$i^2 =: a \in K,\ j^2 =: b \in K,\ \sigma_f(i) = i,\ \sigma_f(j) = j,\ \sigma_f(k) = -k.$$

Considering V as a left E-vector space, we obtain the following lemma from [Tur93].

Lemma 5.1.2 *There is a G-invariant σ_f-Hermitian form h_f on V such that*

$$f(v, w) = \frac{1}{2}\mathrm{tr}_{\mathrm{red}}(h_f(v, w))$$

for all $v, w \in V$.

Proof. h_f is suitably defined in loc.cit. as

$$h_f(v, w) := f(v, w) + i^{-1}f(iv, w) + j^{-1}f(jv, w) + k^{-1}f(kv, w). \qquad \square$$

Given this setup, Turull proceeds to prove his two main theorems, which we summarize below.

Theorem 5.1.3 *Under the above conditions,* $\det(f) = 1 \in K^\times/(K^\times)^2$.
If we additionally assume $m_\infty(\chi) \neq 1$, in which case V is clearly uniform, the G-invariant form f also fulfills

$$\mathfrak{c}(f) = \begin{cases} [E] \in \mathrm{Br}_2(K) & \textit{if } 4 \nmid \chi(1), \\ 1 \in \mathrm{Br}_2(K) & \textit{if } 4 \mid \chi(1), \end{cases}$$

The proof of these results is detailed in Turull's paper. We merely remark on the overall strategy of the proof.
As E is a skewfield and $h_f(v, v) \neq 0$ for all $0 \neq v \in V$, the Hermitian space (V, h_f) admits an orthogonal E-basis $\{e_1, ..., e_n\}$, $n = \frac{1}{2}\chi(1)$, by the usual Gram-Schmidt orthogonalization process. It turns out that then (V, f) is the orthogonal direct sum of the spaces Ee_1, ..., Ee_n - equipped with the respective restrictions of the form f.
The Gram matrix of the restriction of f to each of these spaces is of the form

$$\begin{pmatrix} t & \varepsilon xa & \varepsilon yb & 0 \\ xa & \varepsilon ta & 0 & -yab \\ yb & 0 & \varepsilon tb & xab \\ 0 & -\varepsilon yab & \varepsilon xab & tab \end{pmatrix}$$

for some $t, x, y \in K$, $\varepsilon \in \{\pm 1\}$. The determinant is easily checked to be a square.

In the case $m_\infty(\chi) = 2$, the above matrix specializes to

$$\begin{pmatrix} t & & & \\ & -ta & & \\ & & -tb & \\ & & & tab \end{pmatrix},$$

allowing for the determination of the Hasse invariant. We reformulated Turull's result in terms of the Clifford algebra by means of the conversion formula in [Sch85, Definition 12.7].

5.2 Finite fields

Assume that we are in the same situation as in the last section, with the additional condition that $m_\infty(\chi) = 1$. Choose an odd finite prime $\mathfrak{p}$ of K such that $\mathfrak{p} \nmid |G|$. Let $\mathcal{O}$ be the ring of integers of K and put $\mathbb{F}_\mathfrak{p} := \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$ and $p := \mathrm{char}(\mathbb{F}_\mathfrak{p})$. Then $(K_\mathfrak{p}, \mathcal{O}_\mathfrak{p}, \mathbb{F}_\mathfrak{p})$ is a p-modular system and we can consider the $K_\mathfrak{p}G$-module $K_\mathfrak{p} \otimes_K V$. Notice that $K_\mathfrak{p} \otimes_K E \cong K_\mathfrak{p}^{2\times 2}$, so $K_\mathfrak{p} \otimes_K V$ is reducible. More precisely, there is an absolutely irreducible $K_\mathfrak{p}G$-module X such that $K_\mathfrak{p} \otimes_K V \cong X \oplus X$.

There is a unique absolutely irreducible $\mathbb{F}_\mathfrak{p}G$-module $\overline{X}$ such that the Brauer character of $\overline{X}$ is the ordinary character χ_X of X.

Experimentation with `Magma` [BCP97] suggests the following conjecture, which is quite similar to Turull's result presented in the previous section of this chapter.

Conjecture 5.2.1 *Let $\overline{f}$ be a G-invariant non-degenerate bilinear form on the $\mathbb{F}_\mathfrak{p}G$-module $\overline{X}$. Then* $\det(\overline{f}) = 1 \in \mathbb{F}_\mathfrak{p}^\times/(\mathbb{F}_\mathfrak{p}^\times)^2$.

Using the computer algebra system `Magma` and the Small Groups Library [BEO02], which is implemented in that computer algebra system, one can find hundreds of examples of representations with totally real character with Schur index equalling two while the real Schur index is one. One then proceeds to construct the representation in question over $\mathbb{F}_p$ for a number of primes p not dividing the group order and computes a G-invariant form in order to find evidence of the veracity of the conjecture.

With the following code for `Magma` one can gather such evidence for all groups of order up to 200 and all primes up to 17 within about an hour. However, this does not yield a complete list of candidates as we have restricted our program to only search for rational characters for simplicity.

```
N0:=1;
N1:=200;
Primes:=PrimesUpTo(17);
for i in [x : x in [N0..N1] | #Factorization(x) ge 2] do
 for j in [1..NumberOfSmallGroups(i)] do
  G:=SmallGroup(i,j);
  CT:=CharacterTable(G);
  for k in [2..#CT] do
   if Degree(CharacterField(CT[k])) eq 1 then
    SI:=SchurIndices(CT[k]);
    if not (SI eq [] or <0,2> in SI) then
     R:=CharacterRing(G);
     c:=CT[k];
     for p in [x : x in Primes | i mod x ne 0] do
      I:=AbsolutelyIrreducibleModules(G,GF(p));
      V:=[X : X in I | R!BrauerCharacter(X) eq c][1];
      f:=InvariantBilinearForms(MatrixGroup(V))[1];
      if not IsSquare(Determinant(f)) then
       print "Conjecture falsified."; <i,j,k>; break i;
      end if;
     end for;
    end if;
   end if;
  end for;
 end for;
 print "All groups of order " cat IntegerToString(i) cat " checked.";
end for;
```

Examples of finite groups possessing a character with the desired Schur indices include $(48,15)$, $(96,14)$, $(144,16)$, $(160,82)$ and $(192,10)$ in the numbering of the Small Groups Library. In fact, all examples of order less than 200 are of order 48, 96, 144, 160 and 192.

The group-theoretic structure of G seems to have no bearing on our conjecture. All of the small groups considered by means of the above computer program are solvable - their orders have precisely two prime divisors so that solvability is ensured by Burnside's famous $p^a q^b$-theorem, cf. Theorem (3.10) of [Isa76], for example. However, we also verified the conjecture for J_2, the sporadic Hall-Janko group of order 604,800, for some small primes not dividing the group order. In the notation of [CCN$^+$85], χ_{21} is a character satisfying the conditions on the Schur index.

Attempts to apply the methods used in Turull's proof of the results of [Tur93] in order to find a proof of the conjecture stated above have unfortunately not been successful.

However, in the course of these attempts we have found errors in two papers, which we would like to mention here.

Incorrect Theorem 5.2.2 ([YI86, Theorem 1]) *Let $D^{t\times t}$ be a Schur algebra* [1] *over a cyclotomic extension K of $\mathbb{Q}$, where D is a K-central division algebra with index m. Suppose that m is divisible by a prime number q. Let $\{p_1, p_2, ..., p_k\}$ be the set of prime numbers at which D has non-trivial local index divisible by q. Set $h = p_1 p_2 \cdots p_k$ if all the p_i are odd or $h = 2p_1 p_2 \cdots p_k$ if one of the p_i's is 2. Then $[K(\zeta_h) : K]$ divides tm.*

A correct version of this statement may be found in [Pen76], where it is the main theorem. It is obtained by replacing the divisibility relation in the above statement by

$$[K(\zeta_h) : K] \leq tm.$$

The second incorrect statement is the following.

Incorrect Theorem 5.2.3 ([ST79, Theorem 6]) *Let p be an odd prime and K a finite extension of $\mathbb{Q}_p$ with maximal cyclotomic subfield k. Denote by c the tame ramification index of $k/\mathbb{Q}_p$, that is the p-prime part of the ramification index, and abbreviate $m = \frac{p-1}{c}$, $s = \gcd(m, [K : k])$ and $t = \frac{m}{s}$. Furthermore let $\Delta_{z/t}$ denote the skew field with center K and Hasse invariant z/t.*
$\Delta_{z/t}^{d\times d}$ occurs as a direct summand of KH for some finite group H if and only if $\gcd(z, t)\cdot s$ divides d.

A counterexample to both of the above statements is provided by the following example which is due to Walter Feit.

Example 5.2.4 Let ω have the minimal polynomial $X^2 + 2X + 2$ over $\mathbb{F}_3$. Then

$$\begin{pmatrix}
2 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & \omega & \omega & \omega^5 & \omega & \omega^5 & \omega & \omega^5 & \omega^3 \\
0 & \omega^2 & \omega^5 & \omega^2 & 1 & \omega^2 & \omega^5 & \omega & \omega^5 & \omega^6 \\
1 & \omega^2 & 1 & \omega^5 & \omega^6 & \omega^6 & \omega^7 & \omega^6 & \omega^7 & \omega^7 \\
1 & 2 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
0 & \omega^3 & 1 & \omega^5 & 1 & \omega^3 & \omega^3 & \omega & \omega^3 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\omega^6 & \omega^6 & \omega^2 & \omega^5 & \omega^6 & \omega^5 & 2 & \omega & 0 & \omega^7 \\
2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 1 \\
\omega^5 & \omega^3 & \omega & 0 & \omega^2 & 1 & 0 & \omega^2 & 1 & \omega^5 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
\omega^5 & \omega^5 & \omega^5 & 2 & \omega^3 & \omega & 0 & \omega^5 & \omega^3 & \omega^3 \\
\omega^2 & \omega^6 & \omega & 0 & \omega^6 & 2 & 0 & \omega & 0 & \omega^3 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\omega^2 & \omega^2 & 0 & 0 & \omega^6 & \omega & 2 & \omega^5 & \omega^5 & 2 \\
\omega^5 & 0 & \omega^3 & 0 & 2 & \omega^6 & 0 & \omega^6 & \omega^7 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\
\omega^3 & \omega^6 & 0 & 0 & \omega^7 & \omega^5 & 0 & \omega & \omega & 0
\end{pmatrix}$$

[1] A K-central simple algebra B is called a Schur algebra over K if B is isomorphic to a simple component of the group algebra KG for some finite group G.

and

$$\begin{pmatrix} 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 \\ 1 & 2 & 1 & 2 & \omega & \omega^2 & \omega^5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 \\ \omega^3 & \omega^7 & \omega^7 & \omega^3 & \omega^3 & 0 & \omega^7 & 0 & \omega^2 & 0 \\ \omega^2 & \omega^6 & 0 & 0 & \omega^6 & 0 & \omega^2 & 0 & 0 & \omega^2 \end{pmatrix}$$

generate a subgroup G of $\mathrm{GL}_{10}(\mathbb{F}_9)$ isomorphic to a group called $2.M_{22}.2i$ in [Fei96]. This is a group which is isoclinic, but not isomorphic, to the group $2.M_{22}.2$ whose character table is printed in [CCN$^+$85]. The notion of isoclinism is explained in loc.cit. as well.

By [Fei96], Section 6, the group G has a 252-dimensional rational representation which has Schur index 2 at 11 and the infinite place.

By Theorem 1 of [YI86], this would imply that $[\mathbb{Q}(\zeta_{11}) : \mathbb{Q}] = 10$ divides 252, which is clearly false.

With regard to Theorem 6 of [ST79], we find $p = 11$, $K = k = \mathbb{Q}_{11}$, $c = 1$, $m = 10$, $s = 1$, $t = 10$. This yields $z = 5$, which would imply that $\gcd(z, t) \cdot s = 5$ divides 126, but this is incorrect.

To our knowledge, the errors in the cited articles are as follows.

Remark 5.2.5 In [YI86], in the notation of that paper, the authors claim that $K(\zeta_h)$ is a subfield of the matrix algebra $D^{t\times t}$. However, their argument only shows that

$$\left\{ \begin{pmatrix} x & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} \; : \; x \in K(\zeta_h) \right\}$$

is embedded in $D^{t\times t}$, which merely yields an inequality $[K(\zeta_h) : K] \leq tm$ and thereby the statement of [Pen76].

Remark 5.2.6 In [ST79], again in the notation of that paper, in the proof of Theorem 6 the authors construct an element ρ which they claim generates a field extension of K. However, the minimal polynomial of ρ is $X^p - 1$, which is reducible, so that the subalgebra generated by ρ is not a field.

6 Orthogonal representations of certain infinite families of finite groups

In this chapter we describe the orthogonal representations of some infinite families of finite groups. The applied methods are quite varied, encompassing group theory, representation theory and algebraic number theory.
The first two sections are of an expository nature, presenting results from Gabriele Nebe's habilitation thesis [Neb99]. In contrast, the latter sections show the author's own work on semidirect products of cyclic groups and the groups $\mathrm{PSL}_2(q)$ for arbitrary prime powers q.

6.1 Symmetric groups

This section is an application of orthogonal Frobenius reciprocity, cf. Section 4.3.5. It is quoted from [Neb00b], which we will follow quite closely. For the proofs of the statements we refer the reader to that source or [Neb99].
First, we introduce certain Specht modules, which are representations of the symmetric group S_n. A standard reference for the reprentation theory of symmetric groups is [Jam78]. Then we apply Theorem 4.3.13 in order to obtain a recursive formula for the invariant forms of these Specht modules in the Witt Group $W(\mathbb{Q})$.

Let $k, \ell, n \in \mathbb{N}$ with $1 \leq k \leq \ell \leq \frac{n}{2}$ and let $S_\ell \times S_{n-\ell}$ be the so-called Young subgroup of S_n, which is the stabilizer of the subset $\underline{\ell} \subseteq \underline{n}$ in the natural permutation action of S_n on $\underline{n}$.
Let $M^{(n-k,k)}$ denote the $\mathbb{Q}S_n$-permutation module having the k-element subsets of $\underline{n}$ as a basis. We equip the module with an S_n-invariant bilinear form $I_{\binom{n}{k}}$ such that the k-element subsets of $\underline{n}$ are an orthonormal basis. We have $\dim_{\mathbb{Q}}\left(M^{(n-k,k)}\right) = \binom{n}{k}$ and $M^{(n-k,k)} = \mathbb{1}_{S_k \times S_{n-k}}^{S_n}$. Clearly, $\left(M^{(n-k,k)}, I_{\binom{n}{k}}\right) \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{I}_{\binom{n}{k}}$.

Let $T \subseteq \underline{n}$ and define a $\mathbb{Q}$-linear map $\sigma_T \ : \ M^{(n-k,k)} \to \mathbb{Q}$ by

$$\sigma_T(S) := \begin{cases} 0 & \text{if } T \not\subseteq S \\ 1 & \text{if } T \subseteq S \end{cases}$$

for k-elements subsets S of $\underline{n}$. The Specht module $S^{(n-k,k)} \leq M^{(n-k,k)}$ is defined as

$$S^{(n-k,k)} := \bigcap_{T \subseteq \underline{n},\ |T| \leq k} \ker(\sigma_T).$$

$S^{(n-k,k)}$ is an absolutely irreducible $\mathbb{Q}S_n$-submodule of $M^{(n-k,k)}$ and therefore it is uniform. The S_n-invariant symmetric bilinear forms on $S^{(n-k,k)}$ are $\mathbb{Q}$-multiples of the restriction $F_k := I_{\binom{n}{k}}|_{S^{(n-k,k)} \times S^{(n-k,k)}}$.

By Young's rule, [Jam78, 14.4], $M^{(n-\ell,\ell)} \cong \bigoplus_{k=0}^{\ell} S^{(n-k,k)}$ as $\mathbb{Q}S_n$-modules. From this statement, we obtain that $\dim_{\mathbb{Q}}(S^{(n-k,k)}) = \binom{n}{k} - \binom{n}{k-1}$ by induction, and that the trivial module $\mathbb{1}_{S_n}$ is a constituent of multiplicity one of $M^{(n-\ell,\ell)}$. This implies, by classical Frobenius reciprocity, that the fixed space of $S_\ell \times S_{n-\ell}$ on $S^{(n-k,k)}|_{S_\ell \times S_{n-\ell}}$ is one-dimensional. Therefore we may assume it is spanned by some $0 \neq v \in S^{(n-k,k)}$. The following theorem gives us some information about v.

Theorem 6.1.1 ([Neb00b, Theorem 3.1]) *Again, let $1 \leq k \leq \ell \leq \frac{n}{2}$. Then there is $v \in S^{(n-k,k)}$ with $gv = v$ for all $g \in S_\ell \times S_{n-\ell}$, and v satisfies*

$$F_k(v,v) = a(\ell,k) := \binom{n+1-k}{k}\binom{n-\ell}{k}\binom{\ell}{k}^{-1}.$$

We will now apply orthogonal Frobenius reciprocity (Theorem 4.3.13) in order to obtain a recursion formula for $[F_k] \in W(\mathbb{Q})$. Bearing in mind that both $S^{(n-k,k)}$ and $M^{(n-\ell,\ell)}$ are self-dual, we apply orthogonal Frobenius reciprocity to

$$\mathrm{Isom}_{\mathbb{Q}[S_\ell \times S_{n-\ell}]}\big((\mathbb{1}_{S_\ell \times S_{n-\ell}}, \langle a(\ell,k)\rangle), (S^{(n-k,k)}|_{S_\ell \times S_{n-\ell}}, F_k)\big),$$

yielding an isometry in

$$\mathrm{Isom}_{\mathbb{Q}S_n}\left(\left(S^{(n-k,k)}, F_k\right), \left(M^{(n-\ell,\ell)}, a(\ell,k)\frac{\binom{n}{\ell}}{\binom{n}{k} - \binom{n}{k-1}} I_{\binom{n}{\ell}}\right)\right).$$

Since for a in any field K and F a bilinear form over K, aF and $a^{-1}F$ are isometric, we obtain the recursion formula from Corollary 3.4 of [Neb00b]:

$$\left[I_{\binom{n}{\ell}}\right] = \sum_{k=0}^{\ell}\left[\frac{\binom{n}{\ell}}{\binom{n}{k} - \binom{n}{k-1}} a(\ell,k) F_k\right] = \sum_{k=0}^{\ell}\left[\binom{n-2k}{\ell-k} F_k\right].$$

Example 6.1.2 For n sufficiently large, the recursion formula gives us the following relations in $W(\mathbb{Q})$:
$\ell = 0$: $[\mathbb{I}_1] = [F_0]$,
$\ell = 1$: $[\mathbb{I}_n] = [nF_0] + [F_1]$,
$\ell = 2$: $[\mathbb{I}_{\binom{n}{2}}] = [\frac{n(n-1)}{2} F_0] + [(n-2)F_1] + [F_2]$.

Remark 6.1.3 There is no theoretical obstruction to generalizing this method to other Specht modules defined by partitions with more than two parts, however the combinatorics necessary for the explicit computations becomes too involved in order to obtain any useful results – see also Remark 3.5 of [Neb00b].

6.2 Cyclic groups

For cyclic groups, the orthogonal representations over $\mathbb{Q}$ were classified in [Neb99]. We state the results of this classification without proof.

First we will describe the irreducible rational representations of C_n.

Remark 6.2.1 Let Φ_d be the d-th cyclotomic polynomial. Then the group algebra $\mathbb{Q}C_n$ has the following Wedderburn decomposition.

$$\mathbb{Q}C_n \cong \mathbb{Q}[X]/(X^n - 1) \cong \bigoplus_{d|n} \mathbb{Q}[X]/(\Phi_d) \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)$$

For any $d \mid n$, the cyclotomic field $\mathbb{Q}(\zeta_d)$ is an irreducible representation of $C_n = \langle g \rangle$ via

$$\langle g \rangle \times \mathbb{Q}(\zeta_d) \to \mathbb{Q}(\zeta_d),\ (g^i, x) \mapsto \zeta_d^i \cdot x.$$

If $d \neq n$, this representation is not faithful.

Since any irreducible representation occurs in the regular representation $\mathbb{Q}C_n$, these are all of the irreducible representations of C_n.

Remark 6.2.2 Non-faithful representations are faithful representations of quotients of cyclic groups, which are again cyclic, so it will be sufficient to merely consider the faithful representation of C_n.

We will now describe the C_n-invariant forms on the faithful irreducible module $K := \mathbb{Q}(\zeta_n)$. Let $^- \in \mathrm{Gal}(K/\mathbb{Q})$ be the complex conjugation on K, defined by $\zeta_n \mapsto \zeta_n^{-1}$. Put $K^+ := \mathrm{Fix}(^-)$, the maximal totally real subfield of K.

Proposition 6.2.3 *The C_n-invariant symmetric bilinear forms on K are the maps*

$$\phi_\alpha^{(K)} := \phi_\alpha \ :\ (v, w) \mapsto \mathrm{tr}_{K/\mathbb{Q}}(\alpha v \overline{w}),\ \alpha \in K^+,$$

where $\mathrm{tr}_{K/\mathbb{Q}}$ denotes the field trace $K \to \mathbb{Q}$. In particular, $\dim_{\mathbb{Q}}(\mathcal{F}_{C_n}(K)) = \frac{\varphi(n)}{2}$ (here, φ denotes Euler's totient function).

Proof. Since $\mathrm{End}_{\mathbb{Q}C_n}(K) \cong \mathbb{Q}(\zeta_n)$ we know that the space of all C_n-invariant bilinear forms on K is of dimension $\varphi(n)$. So the ϕ_α with $\alpha \in K$ exhaust the space $\mathcal{B}_{C_n}(K)$ for reasons of dimension (it is easily verified that $\phi : K \to \mathcal{B}_{C_n}(K)$, $\alpha \mapsto \phi_\alpha$ is a $\mathbb{Q}$-linear isomorphism because of the non-degeneracy of the trace bilinear form). One easily checks that ϕ_α is symmetric if and only if $\alpha \in K^+$, which proves the statement.□

Definition 6.2.4 We denote the bilinear space (K, ϕ_α) by $\varphi_\alpha = \varphi_\alpha^{(K)}$.

The following theorem, which is Satz 3.3.14 in [Neb99], classifies the orthogonal representations of the cyclic group of order n up to Witt-equivalence.
For the purposes of this citation let h_p denote the p-adic Hasse invariant (cf. [Sch85, Definition 12.4] and see Definition 12.7 of loc.cit. for the relation between the Hasse invariant and the Clifford invariant) and, for odd primes p, denote by $p^{\epsilon n}$ with $\epsilon \in \{\pm\}$ and $n \in \mathbb{N}$ the regular quadratic $\mathbb{F}_p$-space of dimension n and determinant 1 if $\epsilon = +$ and determinant in $\mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2$ if $\epsilon = -$; as in Section 1.3.3 of [Neb99].

Theorem 6.2.5 *Recall the definition of the invariants s_p for odd primes p from Definition 3.4.12. The classifying invariants of φ_α are as follows.*

1. *The determinant of φ_α is*
$$(-1)^{[\mathbb{Q}(\zeta_n):\mathbb{Q}]/2} d_{\mathbb{Q}(\zeta_n)} (\mathbb{Q}^\times)^2 = \begin{cases} q(\mathbb{Q}^\times)^2 & n = q \text{ is an odd prime power} \\ (\mathbb{Q}^\times)^2 & \text{else} \end{cases},$$
where $d_{\mathbb{Q}(\zeta_n)}$ denotes the discriminant of the n-th cyclotomic field.

2. *The signature (cf. Example 3.3.4) of φ_α is $2(a-b)$, where a is the number of embeddings $\iota : K^+ \to \mathbb{R}$ satisfying $\iota(\alpha) > 0$ and b is the number of such embeddings with $\iota(\alpha) < 0$.*

3. *Let $n = p^t$ for an odd prime p, $\alpha \in K^+$ and $K := \mathbb{Q}(\zeta_n)$. Then we can write $\alpha = uy\overline{y}$ with suitable $u \in K^+ \cap (\mathbb{Z}_p \otimes \mathbb{Z}[\zeta_n + \zeta_n^{-1}])^\times$ and $y \in K$. Let $\epsilon \in \{\pm 1\}$ such that $\epsilon N_{K^+/\mathbb{Q}}(u) \equiv (-1)^{(p-1)/2} \pmod{p}$. Then*
$$s_p(\varphi_\alpha) = p^{\epsilon p^{t-1}} \text{ and } h_p(\varphi_\alpha) = \epsilon(-1)^{\frac{p^{t-1}-1}{2}}.$$

4. *Let $n = p^t n'$ for an odd prime p, $t \geq 1$, $\gcd(p, n') = 1$ and put $K := \mathbb{Q}(\zeta_n)$.*
If p splits in K/K^+, we have $h_p(\varphi_\alpha) = 1$.
Otherwise let $(p) = \prod_{i=1}^s \mathfrak{p}_i^e$ and $x := \begin{cases} p^{t-1}(pt-t-1) & t > 0, \\ 0 & t = 0. \end{cases}$
Let $(1-\zeta_n^{n'})^x \alpha(\mathbb{Z}_p \otimes \mathbb{Z}[\zeta_k]) = \prod_{i=1}^s \mathfrak{p}_i^{j_i}$ and put
$$n_p := \sum_{\substack{i=1 \\ j_i \text{ odd}}}^{s} \frac{n}{es} \text{ and } \epsilon := \prod_{i=1}^{s} (-(-1)^{\frac{p-1}{2}\frac{n}{2es}})^{j_i}.$$

Then

$$s_p(\varphi_\alpha) = p^{\epsilon n_p}.$$

Abbreviate $u := \det(\varphi_\alpha)$*. Then*

$$h_p(\varphi_\alpha) = \epsilon(u,p)^{n_p}(-1,p)^{\binom{n_p}{2}} = (u,p)^{n_p}\prod_{i=1}^{s}(-1)^{j_i}.$$

By Remark 3.4.14, the information collected in this statement completely determines the Witt equivalence class of the $\mathbb{Q}$*-bilinear space* φ_α*.*

6.3 Semidirect products of cyclic groups

Let p be an odd prime. This section is devoted to the study of orthogonal representations of $C_p \rtimes C_{\frac{p-1}{2}}$, with faithful action of the latter group on the former, over the field $\mathbb{Q}$. We proceed as in the case of cyclic groups and rely heavily on the results obtained for those groups.

The semidirect product $C_p \rtimes C_{\frac{p-1}{2}}$ is unique up to isomorphism because there is precisely one subgroup of order $\frac{p-1}{2}$ in $\operatorname{Aut}(C_p)$. The semidirect product has a presentation of the form

$$C_p \rtimes C_{\frac{p-1}{2}} \cong \left\langle a, b \mid a^p,\ b^{\frac{p-1}{2}},\ bab^{-1} = a^{i(p)} \right\rangle, \tag{6.1}$$

where $i(p)$ is an integer of multiplicative order $\frac{p-1}{2}$ modulo p.
As a first step, we will classify the irreducible representations over $\mathbb{Q}$.

Proposition 6.3.1 *There is an irreducible and faithful representation of* $G := C_p \rtimes C_{\frac{p-1}{2}}$ *on the* $\mathbb{Q}$*-vector space* $\mathbb{Q}(\zeta_p)$ *via*

$$\begin{aligned} \Phi\ :\ G \times \mathbb{Q}(\zeta_p) &\to \mathbb{Q}(\zeta_p), \\ (a,x) &\mapsto \zeta_p x, \\ (b,x) &\mapsto \sigma(x), \end{aligned}$$

where a, b *are as in* (6.1) *and* σ *is an element of order* $\frac{p-1}{2}$ *in* $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$*.*
The endomorphism ring of this representation is

$$\operatorname{End}_{\mathbb{Q}[C_p \rtimes C_{\frac{p-1}{2}}]}(\mathbb{Q}(\zeta_p)) \cong \begin{cases} \mathbb{Q}(\sqrt{p}) & p \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{-p}) & p \equiv 3 \pmod 4, \end{cases}$$

the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$*.*

Proof. It is easily checked that this an irreducible and fatihful representation of G. Now let f be a $\mathbb{Q}G$-endomorphism of $\mathbb{Q}(\zeta_p)$. Since $f(\zeta_p x) = \zeta_p f(x)$ for all $x \in \mathbb{Q}(\zeta_p)$, f is $\mathbb{Q}(\zeta_p)$-linear and therefore of the form $f(x) = \alpha x$ for some $\alpha \in \mathbb{Q}(\zeta_p)$. Since we also have $f(\sigma(x)) = \sigma(f(x))$ for all $x \in \mathbb{Q}(\zeta_p)$, α must be contained in the fixed field of σ, which is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$. □

Remark 6.3.2 For every divisor d of $\frac{p-1}{2}$ we have an irreducible and non-faithful representation of $C_p \rtimes C_{\frac{p-1}{2}}$ of the form

$$\begin{aligned}\Phi \ : \ G \times \mathbb{Q}(\zeta_d) &\to \mathbb{Q}(\zeta_d),\\ (a, x) &\mapsto x,\\ (b, x) &\mapsto \zeta_d x,\end{aligned}$$

with endomorphism ring isomorphic to $\mathbb{Q}(\zeta_d)$ (see Remark 6.2.1).

Theorem 6.3.3 *The representations of $G := C_p \rtimes C_{\frac{p-1}{2}}$ listed so far are all irreducible representations of this group over $\mathbb{Q}$ up to equivalence.*
Since the non-faithful representations are faithful representations of cyclic groups, we can apply the results of the previous section to study these representations.

Proof. All abovementioned representations have distinct $\mathbb{Q}$-dimensions, so they are pairwise inequivalent. The faithful representation of G contributes a $\frac{p-1}{2} \times \frac{p-1}{2}$ matrix ring over $\mathbb{Q}\left(\sqrt{\pm p}\right)$ to the group algebra as a direct summand. The non-faithful representations each correspond to a direct summand of the form $\mathbb{Q}(\zeta_d)$, where d is a divisor of $\frac{p-1}{2}$. Thus, we have so far found a subspace of the group algebra of dimension

$$2\left(\frac{p-1}{2}\right)^2 + \sum_{d \mid \frac{p-1}{2}} \varphi(d) = \frac{(p-1)^2}{2} + \frac{p-1}{2} = p\frac{p-1}{2},$$

which is the dimension of the entire group algebra, so we have found all irreducible representations.

The second statement of this theorem is obvious since any of the non-faithful representations contain the subgroup generated by a (cf. (6.1)) in their kernel. □

Corollary 6.3.4 *We have an isomorphism*

$$\mathbb{Q}[C_p \rtimes C_{\frac{p-1}{2}}] \cong \mathbb{Q}\left(\sqrt{(-1)^{\alpha(p)}p}\right)^{\alpha(p)\times\alpha(p)} \oplus \bigoplus_{d \mid \alpha(p)} \mathbb{Q}(\zeta_d),$$

where $\alpha(p) := \frac{p-1}{2}$.

Corollary 6.3.5 *The faithful representation constructed in Proposition 6.3.1 is, up to equivalence, independent of the choice of the element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.*

Now we will describe the invariant bilinear forms of $G := C_p \rtimes C_{\frac{p-1}{2}}$ on its faithful representation up to Witt equivalence.

Proposition 6.3.6 *As in Proposition 6.3.1 let b act via $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. The G-invariant symmetric bilinear forms on $K := \mathbb{Q}(\zeta_p)$ are of the form*

$$\phi_\alpha \ : \ K \times K \to \mathbb{Q}, \ (x, y) \mapsto \mathrm{tr}_{K/\mathbb{Q}}(\alpha x \overline{y}),$$

where $^- \in \mathrm{Gal}(K/\mathbb{Q})$ denotes the complex conjugation on K and $\alpha \in \mathrm{Fix}(\langle \sigma, ^- \rangle)$, the fixed field of the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ generated by σ and the complex conjugation.

Proof. This is analogous to the proof of Proposition 6.2.3. □

Corollary 6.3.7 *The faithful representation of G over $\mathbb{Q}$ is uniform if and only if $p \equiv 3 \pmod 4$. More precisely, we have*

$$\mathrm{Fix}(\langle \sigma, ^- \rangle) = \begin{cases} \mathbb{Q}(\sqrt{p}) & p \equiv 1 \pmod 4, \\ \mathbb{Q} & p \equiv 3 \pmod 4. \end{cases}$$

Theorem 6.3.8 *Let p be an odd prime and put $G := C_p \rtimes C_{\frac{p-1}{2}}$, $K := \mathbb{Q}(\zeta_p)$, $K^+ := \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and ϕ_α as in Proposition 6.3.6. The $\mathbb{Q}$-bilinear space $\varphi_\alpha := (K, \phi_\alpha)$ has the following invariants which determine it up to Witt equivalence.*

1. *The determinant of φ_α is $p(\mathbb{Q}^\times)^2$.*

2. *The signature of φ_α is $2(a-b)$, where a is the number of embeddings $\iota \ : \ K^+ \to \mathbb{R}$ satisfying $\iota(\alpha) > 0$ and b is the number of such embeddings with $\iota(\alpha) < 0$.*

3. *The remaining invariants can be read off from Theorem 6.2.5. We will not require them in what follows.*

φ_1 is isometric to $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{A}_{p-1}$.

Proof. This follows from Theorem 6.2.5 by restriction to the unique subgroup of G of order p. □

6.4 $\mathrm{SL}_2(q)$

This section is devoted to the study of the orthogonal representations of $\mathrm{SL}_2(q)$, where $q := p^n$ is an odd prime power.

We begin by providing the character table for $\mathrm{SL}_2(q)$ for all odd prime powers q. These generic character tables were first computed - independently - in [Sch07] and [Jor07]. A modern and comprehensive account of the representation theory of $\mathrm{SL}_2(q)$ is [Bon11], the table is obtained from Theorem 38.1 of [Dor71].

Theorem 6.4.1 ([Dor71, Theorem 38.1]) *Let* $\langle \nu \rangle = \mathbb{F}_q^\times$*. Consider*

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ c = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ d = \begin{pmatrix} 1 & 0 \\ \nu & 1 \end{pmatrix},\ a = \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}$$

$\mathrm{SL}_2(q)$ *contains an element* b *of order* $q+1$*.*
For $x \in \mathrm{SL}_2(q)$*, let* (x) *denote the conjugacy class containing* x*.* $\mathrm{SL}_2(q)$ *has the following* $q+4$ *conjugacy classes of elements, listed together with the size of the classes.*

x	1	z	c	d	zc	zd	a^ℓ	b^m
$\lvert(x)\rvert$	1	1	$\frac{1}{2}(q^2-1)$	$\frac{1}{2}(q^2-1)$	$\frac{1}{2}(q^2-1)$	$\frac{1}{2}(q^2-1)$	$q(q+1)$	$q(q-1)$

where $1 \le \ell \le \frac{q-3}{2}$, $1 \le m \le \frac{q-1}{2}$*.*

Put $\varepsilon := (-1)^{(q-1)/2}$ *and* $\vartheta_r^{(s)} := \zeta_r^s + \zeta_r^{-s}$*. Then the character table of* $\mathrm{SL}_2(q)$ *reads*

	1	z	c	d	a^ℓ	b^m
$\mathbb{1}$	1	1	1	1	1	1
St	q	q	0	0	1	-1
χ_i	$q+1$	$(-1)^i(q+1)$	1	1	$\vartheta_{q-1}^{(i\ell)}$	0
θ_j	$q-1$	$(-1)^j(q-1)$	-1	-1	0	$-\vartheta_{q+1}^{(jm)}$
ξ_1	$\frac{1}{2}(q+1)$	$\frac{1}{2}\varepsilon(q+1)$	$\frac{1}{2}\left(1+\sqrt{\varepsilon q}\right)$	$\frac{1}{2}\left(1-\sqrt{\varepsilon q}\right)$	$(-1)^\ell$	0
ξ_2	$\frac{1}{2}(q+1)$	$\frac{1}{2}\varepsilon(q+1)$	$\frac{1}{2}\left(1-\sqrt{\varepsilon q}\right)$	$\frac{1}{2}\left(1+\sqrt{\varepsilon q}\right)$	$(-1)^\ell$	0
η_1	$\frac{1}{2}(q-1)$	$-\frac{1}{2}\varepsilon(q-1)$	$\frac{1}{2}\left(-1+\sqrt{\varepsilon q}\right)$	$\frac{1}{2}\left(-1-\sqrt{\varepsilon q}\right)$	0	$(-1)^{m+1}$
η_2	$\frac{1}{2}(q-1)$	$-\frac{1}{2}\varepsilon(q-1)$	$\frac{1}{2}\left(-1-\sqrt{\varepsilon q}\right)$	$\frac{1}{2}\left(-1+\sqrt{\varepsilon q}\right)$	0	$(-1)^{m+1}$

where $1 \le i \le \frac{q-3}{2}$, $1 \le j \le \frac{q-1}{2}$, $1 \le \ell \le \frac{q-3}{2}$, $1 \le m \le \frac{q-1}{2}$*.*
The columns for the classes (zc) *and* (zd) *are omitted because for any irreducible character* χ *the relation*

$$\chi(zc) = \frac{\chi(z)}{\chi(1)}\chi(c)$$

holds.

Remark 6.4.2 Consulting the paper [Jan74], we find that all faithful characters of $\mathrm{SL}_2(q)$ have Frobenius-Schur indicator 0 or $-$, so that the orthogonal representations affording those characters are easily described by means of Theorems 4.3.9 and 5.1.3.

Due to the last remark we will focus our attention on $G := \mathrm{PSL}_2(q)$. This is the quotient group of $\mathrm{SL}_2(q)$ by its center, which is why we will denote elements of $\mathrm{PSL}_2(q)$ by 2×2-matrices of determinant 1 over $\mathbb{F}_q$.

From Theorem 6.4.1 we obtain the conjugacy classes and character tables of $\mathrm{PSL}_2(q)$ for $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$.

Lemma 6.4.3 *Let $q \equiv 1 \pmod 4$ and $\langle \nu \rangle = \mathbb{F}_q^\times$. $\mathrm{PSL}_2(q)$ has $\frac{q+5}{4}$ conjugacy classes, represented by*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \nu & 1 \end{pmatrix}, \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}^\ell, \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}^{\frac{q-1}{4}}, b^m,$$

where $1 \leq \ell \leq \frac{q-5}{4}$, $1 \leq m \leq \frac{q-1}{4}$ and b is an element of order $q+1$.

Theorem 6.4.4 *Let $q \equiv 1 \pmod 4$. Then $G = \mathrm{PSL}_2(q)$ has the following character table.*

	1	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ \nu & 1 \end{pmatrix}$	$\begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}^\ell$	$\begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}^{\frac{q-1}{4}}$	b^m
# cl.	1	1	1	$\frac{q-5}{4}$	1	$\frac{q-1}{4}$
$\lvert x^G \rvert$	1	$\frac{q^2-1}{2}$	$\frac{q^2-1}{2}$	$q(q+1)$	$\frac{q(q+1)}{2}$	$q(q-1)$
$\mathbb{1}_G$	1	1	1	1	1	1
St_G	q	0	0	1	1	-1
χ_i	$q+1$	1	1	$\zeta_{q-1}^{i\ell} + \zeta_{q-1}^{-i\ell}$	$\zeta_{q-1}^{i\frac{q-1}{4}} + \zeta_{q-1}^{-i\frac{q-1}{4}}$	0
θ_j	$q-1$	-1	-1	0	0	$-\zeta_{q+1}^{jm} - \zeta_{q+1}^{-jm}$
ξ_1	$\frac{q+1}{2}$	$\frac{1+\sqrt{q}}{2}$	$\frac{1-\sqrt{q}}{2}$	$(-1)^\ell$	$(-1)^{\frac{q-1}{4}}$	0
ξ_2	$\frac{q+1}{2}$	$\frac{1-\sqrt{q}}{2}$	$\frac{1+\sqrt{q}}{2}$	$(-1)^\ell$	$(-1)^{\frac{q-1}{4}}$	0

where $i \in \left\{2, 4, 6, ..., \frac{q-5}{2}\right\}$, $j \in \left\{2, 4, 6, ..., \frac{q-1}{2}\right\}$ and, as before, $1 \leq \ell \leq \frac{q-5}{4}$, $1 \leq m \leq \frac{q-1}{4}$.

Lemma 6.4.5 *Let $q \equiv 3 \pmod 4$ and $\langle \nu \rangle = \mathbb{F}_q^\times$. $\mathrm{PSL}_2(q)$ has $\frac{q+5}{4}$ conjugacy classes, represented by*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \nu & 1 \end{pmatrix}, \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}^\ell, b^m, b^{\frac{q+1}{4}},$$

where $1 \leq \ell \leq \frac{q-3}{4}$, $1 \leq m \leq \frac{q-3}{4}$ and b is an element of order $q+1$.

Theorem 6.4.6 *Let $q \equiv 3 \pmod 4$. Then $G = \mathrm{PSL}_2(q)$ has the following character table.*

	1	$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ \nu & 1\end{pmatrix}$	$\begin{pmatrix}\nu & 0\\ 0 & \nu^{-1}\end{pmatrix}^{\ell}$	b^m	$b^{\frac{q+1}{4}}$
# cl.	1	1	1	$\frac{q-3}{4}$	$\frac{q-3}{4}$	1
$\lvert x^G\rvert$	1	$\frac{q^2-1}{2}$	$\frac{q^2-1}{2}$	$q(q+1)$	$q(q-1)$	$\frac{q(q-1)}{2}$
$\mathbb{1}_G$	1	1	1	1	1	1
St_G	q	0	0	1	-1	-1
χ_i	$q+1$	1	1	$\zeta_{q-1}^{i\ell}+\zeta_{q-1}^{-i\ell}$	0	0
θ_j	$q-1$	-1	-1	0	$-\zeta_{q+1}^{jm}-\zeta_{q+1}^{-jm}$	$-\zeta_{q+1}^{j\frac{q+1}{4}}-\zeta_{q+1}^{-j\frac{q+1}{4}}$
η_1	$\frac{q-1}{2}$	$\frac{-1+\sqrt{-q}}{2}$	$\frac{-1-\sqrt{-q}}{2}$	0	$(-1)^{m+1}$	$(-1)^{\frac{q+1}{4}+1}$
η_2	$\frac{q-1}{2}$	$\frac{-1-\sqrt{-q}}{2}$	$\frac{-1+\sqrt{-q}}{2}$	0	$(-1)^{m+1}$	$(-1)^{\frac{q+1}{4}+1}$

where $i \in \left\{2,4,6,...,\frac{q-3}{2}\right\}$, $j \in \left\{2,4,6,...,\frac{q-3}{2}\right\}$ *and, as before,* $1 \leq \ell \leq \frac{q-3}{4}$, $1 \leq m \leq \frac{q-3}{4}$.

Remark 6.4.7 All representations of $\mathrm{PSL}_2(q)$ have Schur index 1, i.e. they are realizable over their respective character fields. See e.g. [Jan74].

Following [Bon11], we will now briefly explain how some of the representations of $G := \mathrm{PSL}_2(q)$ are obtained. We use the following notations.

$$B := \left\{ \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \in \mathrm{PSL}_2(q) \mid x \in \mathbb{F}_q^{\times}, y \in \mathbb{F}_q \right\},$$

the Borel subgroup of G, which is a semidirect product $U \rtimes T$, where

$$U = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}_2(q) \mid y \in \mathbb{F}_q \right\} \cong \underbrace{C_p \times ... \times C_p}_{n \text{ factors}}$$

and

$$T = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mid x \in \mathbb{F}_q^{\times} \right\} \cong C_{\frac{q-1}{2}}.$$

Remark 6.4.8 (cf. [Bon11, (1.1.3)-(1.1.5)]) Denote by s the element $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{PSL}_2(q)$. Then we have $G = B \sqcup BsB = B \sqcup BsU$, which is called the Bruhat decomposition of G.
Note that we also have the properties $B \cap {}^sB = T$, ${}^st = t^{-1}$ for all $t \in T$ and $BsBsB = G$.

Over an algebraically closed field of characteristic zero, we now have a $\mathbb{Z}$-linear map from the character ring of T to that of G, yielding some of the abovementioned representations of G.

Definition 6.4.9 (Harish-Chandra induction) For $\chi \in \mathrm{Irr}(T)$ let χ_B denote the character of B defined by $b \mapsto \chi \circ \varpi$, where $\varpi : B \to T$ denotes the canonical epimorphism.
We call the $\mathbb{Z}$-linear map

$$\mathsf{R} \ : \ \mathbb{Z}[\mathrm{Irr}(T)] \to \mathbb{Z}[\mathrm{Irr}(G)], \ \chi \mapsto \mathrm{ind}_B^G(\chi_B)$$

the Harish-Chandra induction.

This induction map produces the following representations of G, following Section 3.2.3 of [Bon11].

Theorem 6.4.10 *Let $\alpha \in \mathrm{Irr}(T)$.*

- *If $\alpha^2 \neq 1$, then $\mathsf{R}(\alpha) \in \mathrm{Irr}(G)$. These are the representations χ_i.*
- *If α is the unique linear character of order 2 of T, we have $\mathsf{R}(\alpha) = \mathsf{R}_+(\alpha) + \mathsf{R}_-(\alpha)$ with $\mathsf{R}_\pm(\alpha) \in \mathrm{Irr}(G)$ and $\mathsf{R}_+(\alpha) \neq \mathsf{R}_-(\alpha)$. These are the representations ξ_1 and ξ_2.*
- $\mathsf{R}(\mathbb{1}_T) = \mathbb{1}_G + \mathrm{St}_G$. *$\mathrm{St}_G$ is called the Steinberg character of G.*
- *If $\alpha \notin \{\beta, \beta^{-1}\}$, we have $(\mathsf{R}(\alpha), \mathsf{R}(\beta))_G = 0$.*

The central role played by B in the representation theory of $\mathrm{PSL}_2(p)$ (or $\mathrm{SL}_2(p)$, respectively), is illustrated in [Bon11]. B will also be crucial to our study of orthogonal representations. Therefore we begin by determining the representations of B over a splitting field using Clifford theory with respect to the normal subgroup U.

Remark 6.4.11 T acts freely on $U - \{1\}$, which is to say that every stabilizer is trivial. Hence this action has no fixed points on non-identity elements. This follows from the explicit computation

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 1 & x^2y \\ 0 & 1 \end{pmatrix},$$

bearing in mind that we are working in $\mathrm{PSL}_2(q)$.

We want to determine the inertia subgroups of the irreducible characters of U. As usual, every inertia subgroup contains U and $I_B(\mathbb{1}_U) = B$.

Lemma 6.4.12 *Let $\mathbb{1}_U \neq \chi \in \mathrm{Irr}(U)$. Then $I_B(\chi) = U$.*

Proof. Since $\chi \neq \mathbb{1}_U$, we have $|\ker(\chi)| = p^{n-1}$. So, every fibre of χ has p elements on which a non-identity element $t \in T$ must act without fixed points.
If we assume t satisfies ${}^t\chi = \chi$, then every fibre of χ must be preserved under the action of t. Hence the cardinality of the fibre must be a multiple of the order of t, which is a divisor of $\frac{q-1}{2}$. We obtain a contradiction, as $\gcd\left(p, \frac{q-1}{2}\right) = 1$. □

Remark 6.4.13 There are $\frac{q-1}{2}$ irreducible one-dimensional characters of B which restrict to the trivial character of U. This is because these characters correspond to representations of the quotient group $B/U \cong T \cong C_{\frac{q-1}{2}}$.

For the remaining irreducible characters of B, we use the results of Theorem 4.1.9, which is Clifford's Theorem relating representations of finite groups with representations of their normal subgroups.

Remark 6.4.14 There are two absolutely irreducible characters of B, which are both of degree $\frac{q-1}{2}$. Together with the one-dimensional characters already found, we have exhausted all of $\mathrm{Irr}(B)$.

The next step is to study the two $\frac{q-1}{2}$-dimensional representations in greater detail. We will denote their characters by ψ_1, ψ_2.

Lemma 6.4.15 *The characters ψ_1 and ψ_2 are faithful.*

Proof. The ψ_i are of the form $\mathrm{ind}_U^B(\chi)$ for non-trivial one-dimensional characters of U, i.e. they are characters of monomial representations over $\mathbb{Q}(\zeta_p)$. We therefore have $\ker(\psi_i) \subseteq U$.
Let us assume $g \in \ker(\psi_i) \subseteq U$. Since $U \trianglelefteq B$, the formula for the induced character yields the following equation.

$$\frac{q-1}{2} = \mathrm{ind}_U^B(\chi)(g) = \frac{1}{|U|} \sum_{x \in B} \chi(x^{-1}gx). \tag{6.2}$$

It follows from Remark 6.4.11 that for every $g \in U - \{1\}$ there is a $t \in T \subseteq B$ such that $tgt^{-1} \notin \ker(\chi)$, so that equation (6.2) can only be satisfied if $g = 1$. □

Lemma 6.4.16 *The two absolutely irreducible characters ψ_1 and ψ_2 both have Schur index 1 and may be realized over their character fields, which are*

$$\begin{cases} \mathbb{Q}(\sqrt{q}) & \textit{if } q \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{-q}) & \textit{if } q \equiv 3 \pmod 4. \end{cases}$$

Proof. In the case $q \equiv 3 \pmod 4$ the two characters η_1 and η_2 of $\mathrm{PSL}_2(q)$ (cf. Theorem 6.4.6) restrict to faithful characters of B, as they are themselves faithful characters.

Due to our previous considerations, we find that ψ_1 and ψ_2 are the smallest faithful characters of B. Therefore ψ_1 and ψ_2 are of the form $\eta_1|_B$ and $\eta_2|_B$. Thus we obtain $\mathbb{Q}[\psi_i] = \mathbb{Q}(\sqrt{-q})$.
For the case $q \equiv 1 \pmod 4$, we recall from [Bon11] that for the characters ξ_1 and ξ_2 of $\mathrm{PSL}_2(q)$, cf. Theorem 6.4.4, we have the relation $\xi_1 + \xi_2 = \mathsf{R}(\alpha_0)$. An application of Mackey's formula and Frobenius reciprocity shows

$$\mathsf{R}(\alpha_0)|_B = (\alpha_0)_B + \mathrm{ind}_T^B\big((\alpha_0)_B|_T\big)$$

and

$$\Big((\alpha_0)_B, \mathrm{ind}_T^B\big((\alpha_0)_B|_T\big)\Big)_B = \Big((\alpha_0)_B, \mathrm{ind}_T^B(\alpha_0)\Big)_B = (\alpha_0, \alpha_0)_T = 1,$$

from which we conclude $\big((\alpha_0)_B, (\xi_1 + \xi_2)|_B\big)_B = 2$.
As ξ_1 is an irreducible character of a simple group, it is faithful. Hence, $\xi_1|_B$ is faithful as well, so that either ψ_1 or ψ_2 must be a constituent of this restriction. So, we have $\{\xi_1|_B, \xi_2|_B\} = \{\psi_1 + (\alpha_0)_B, \psi_2 + (\alpha_0)_B\}$.
Since $\mathbb{Q}[(\alpha_0)_B] = \mathbb{Q}$, our claim follows from an inspection of the character values for ξ_1 and ξ_2.
The realizability statement is obtained from Remark 6.4.7. □

Finally, we describe the invariants of the orthogonal representations of B with characters ψ_1, ψ_2 in all arising cases.

Lemma 6.4.17 *If $q \equiv 3 \pmod 4$, in which case q is not a square, $\psi_1 + \psi_2$ is the character of a rational uniform representation of even dimension and the discriminant of a regular B-invariant form on that representation is $(-q)^{\psi_1(1)} = (-q)^{\frac{q-1}{2}}$, which is $-p$ up to rational squares.*
If $q \equiv 1 \pmod 4$, let ψ be one of ψ_1, ψ_2. Then we have

$$\det(\psi) = \begin{cases} 1(\mathbb{Q}^\times)^2 & \text{if } n \equiv 0 \pmod 4 \text{ or } p \equiv 3 \pmod 4, \\ p(\mathbb{Q}^\times)^2 & \text{if } n \equiv 2 \pmod 4 \text{ and } p \equiv 1 \pmod 4, \\ \varepsilon\sqrt{p}(\mathbb{Q}(\sqrt{p})^\times)^2 & \text{if } n \equiv 1 \pmod 2, \end{cases}$$

for some $\varepsilon \in \mathcal{O}_{\mathbb{Q}(\sqrt{p})}^\times$ and in the last case, the determinant of the Galois conjugate of ψ is $\pm\varepsilon^{-1}\sqrt{p}(\mathbb{Q}(\sqrt{p})^\times)^2$.

Proof. In the first case, our claim follows from Theorem 4.3.9.
Consider the subgroup

$$H := \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in \mathrm{PSL}_2(q) \mid a \in \mathbb{F}_p^\times,\ b \in \mathbb{F}_q \right\} \leq B,$$

which is isomorphic to $(C_p \times ... \times C_p) \rtimes C_{\frac{p-1}{2}}$ and of index $[B : H] = \frac{q-1}{p-1}$ in B. H is normal in B. We will therefore use it to apply Theorem 4.3.14, which is our version

of Clifford's theorem for orthogonal representations, in order to study the orthogonal representations with characters ψ_i.
Let ψ be one of ψ_1, ψ_2. Then

$$\psi = \mathrm{ind}_U^B(\chi) = \mathrm{ind}_H^B(\underbrace{\mathrm{ind}_U^H(\chi)}_{=:\kappa})$$

for some one-dimensional $\mathbb{1}_U \neq \chi \in \mathrm{Irr}(U)$. Notice that $U = I_B(\chi) \supseteq I_H(\chi) \supseteq U$, so that κ is irreducible by Clifford's theorem.
An application of Frobenius reciprocity shows $(\psi|_H, \kappa)_H = 1$. Let K be the character field of ψ and denote by V the KB-module affording ψ. We obtain the decompositions

$$V|_H \cong V_1 \oplus ... \oplus V_t, \qquad (\dagger)$$

where we have the following cases, which arise from the two possible character fields of ψ, cf. Lemma 6.4.16.

1. $K = \mathbb{Q}$: In this case, every irreducible constituent is faithful and of dimension $p-1$, hence $t = \frac{1}{2}\frac{q-1}{p-1}$.

2. $K = \mathbb{Q}(\sqrt{p})$: In this case, $t = \frac{q-1}{p-1}$ and every irreducible constituent in $(\dagger)$ is faithful of dimension $\frac{p-1}{2}$.

Since χ is a faithful character of a cyclic group of order p, κ is a faithful character of a group isomorphic to $C_p \rtimes C_{\frac{p-1}{2}}$ by [Isa76, Lemma (5.11)]. Therefore we can apply the results of Section 6.3. If $K = \mathbb{Q}$, we have $\det(V_i) = p$ for all $1 \leq i \leq t$. If $K = \mathbb{Q}(\sqrt{p})$, each of the V_i is an absolutely irreducible constituent of the faithful rational representation of $C_p \rtimes C_{\frac{p-1}{2}}$ and the invariant form on it is a trace bilinear form on $\mathbb{Q}(\zeta_p)$ with base field $\mathbb{Q}(\sqrt{p})$. Therefore $\det(V_i)$ is an element of $\mathbb{Q}(\sqrt{p})$ of norm p. Also, $\det(V_i)$ is contained in the relative discriminant ideal $\Delta_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p})}$, so that $\det(V_i) = \varepsilon\sqrt{p}(\mathbb{Q}(\sqrt{p})^\times)^2$ for some $\varepsilon \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{p})}$, as p is the only ramified prime of the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. □

Now we discuss the orthogonal representations of $G := \mathrm{PSL}_2(q)$.

Lemma 6.4.18 *The Steinberg representation, which is of dimension q, satisfies*

$$\mathfrak{c}(\mathrm{St}_G) = \begin{cases} (-1, q+1) & q \equiv 1 \pmod 8, \\ (-1, -q-1) & q \equiv 5 \pmod 8, \\ (-1,-1) & q \equiv 3 \pmod 8, \\ 1 & q \equiv 7 \pmod 8. \end{cases}$$

Proof. $\mathbb{1}_G + \mathrm{St}_G$ is obtained as $\mathsf{R}(\mathbb{1}_T)$, which means that it is the character of a permutation module, so that the module affording St_G carries an invariant bilinear form isometric to $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{A}_q$. The Clifford invariants of these spaces were determined in Example 3.6.25. □

Lemma 6.4.19 $\det(\theta_j) = q(\mathbb{Q}^\times)^2$.

Proof. Since θ_j is an irreducible character of the simple group G, its restriction $\theta_j|_B$ is faithful as well. Therefore one of ψ_1 and ψ_2 must occur as a constituent of the restriction. None of the one-dimensional irreducible characters of B can occur in $\theta_j|_B$ since, if $\chi \in \mathrm{Irr}(B)$ is such a character,

$$0 \neq (\chi, \theta_j|_B)_B = (\theta_j, \mathrm{ind}_B^G(\chi))_G$$

by Frobenius reciprocity. But this is impossible, since $\mathrm{ind}_B^G(\chi) \in \{\mathbb{1}_G + \mathrm{St}_G, \xi_1 + \xi_2, \chi_i\}$, none of which can contain θ_j as a constituent.
Therefore $\theta_j|_B = \psi_1 + \psi_2$ and the statement immediately follows from Lemma 6.4.17.□

This shows that if q is a square, the discriminant $\mathrm{d}_\pm(\theta_j) = 1$ and we can therefore compute the Clifford invariant, which is well-defined.

Lemma 6.4.20 *If q is a square the Clifford invariant $\mathfrak{c}(\theta_j)$ is trivial for all j.*

Proof. If q is a square we have $q+1 \equiv 2 \pmod 4$ and $-\zeta_{q+1}^2$ is a again a primitive root of unity of order $q+1$. In this situation the characters θ_j, with j even, extend to irreducible characters of $\mathrm{PGL}_2(q)$ with the same character field as is verified by inspection of the character table of $\mathrm{PGL}_2(q)$ (cf. [Ste51, Table III]). Such an extension has Schur index 1 by [Gow76, Theorem 2(a)]. Alternatively, the following argument shows that the extended character has Schur index 1: $\mathrm{PSL}_2(q)$ is a normal subgroup of index 2 of $\mathrm{PGL}_2(q)$. If the extended character could only be realized by a $K\mathrm{PGL}_2(q)$-module V with Schur index 2, we would have $K^{2\times 2} = \mathrm{End}_{K\mathrm{PGL}_2(q)}(V|_N) \supseteq \mathrm{End}_{K\mathrm{PSL}_2(q)}(V) \cong D$ for some division algebra of degree two, which is a contradiction.

Now, as before, we find that the restriction $\theta_j|_B = \psi_1 + \psi_2$. The orthogonal KG-module affording the character θ_j is also a $K[\mathrm{PGL}_2(q)]$-module and while the action of $\mathrm{PGL}_2(q)$ fixes the G-invariant form we are interested in, it interchanges the two KB-submodules so that we have isometric invariant forms f_1 and f_2 on those two submodules.

Applying the formula from Proposition 3.6.24 (2), we find

$$\mathfrak{c}(\psi) = \mathfrak{c}(f_1)\mathfrak{c}(f_2)(\mathrm{d}_\pm(f_1), \mathrm{d}_\pm(f_2)) = 1,$$

as $\mathrm{d}_\pm(f_1)$ and $\mathrm{d}_\pm(f_2)$ either are both square or both p where $p \equiv 1 \pmod 4$, in which case $(p,p) = 1$ as the quadratic form $[1, -p, -p, 1]$ is isotropic. □

Lemma 6.4.21 *For $q \equiv 3 \pmod 4$, $\eta_1 + \eta_2$ is the character of a uniform representation which is irreducible over $\mathbb{Q}$ and of even dimension $q-1$. The discriminant of the invariant form is $-q$.*

Proof. This follows immediately from Theorem 4.3.9. □

Lemma 6.4.22 *The invariant forms on the modules affording the characters χ_i have determinant*

$$(2 - \zeta_{q-1}^{2i} - \zeta_{q-1}^{-2i}) \cdot q.$$

Proof. The characters χ_i are obtained as $\mathsf{R}(\alpha)$ with $\alpha \in \operatorname{Irr}(T)$, $\alpha^2 \neq 1$. We put $\chi_i = \mathsf{R}(\alpha_i)$. Over a splitting field of G we can apply Mackey's theorem [CR87a, (10.13)] to obtain the decomposition

$$\begin{aligned}\mathsf{R}(\alpha_i)|_B &= \operatorname{ind}_B^G((\alpha_i)_B)|_B = \operatorname{ind}_B^B((\alpha_i)_B|_B) + \operatorname{ind}_T^B(((\alpha_i)_B^s)|_{{}^sB\cap B}) \\ &= (\alpha_i)_B + \operatorname{ind}_T^B((\alpha_i)_B^*|_T).\end{aligned}$$

Hence, $(\alpha_i)_B$ is a constituent of $\chi_i|_B$. Since χ_i is real-valued, whereas $(\alpha_i)_B$ is not, we have that $(\alpha_i^*)_B$ is a constituent of $\chi_i|_B$ as well.

Since G is simple and χ_i is a non-trivial irreducible character, it is faithful. Thus, the restriction of χ_i to B is faithful, too. In keeping with the notation from the beginning of this section, we denote the two absolutely irreducible characters of B by ψ_1 and ψ_2. Then the character $\chi_i|_B$ decomposes into

$$\Big((\alpha_i)_B + (\alpha_i^*)_B\Big) + \psi_1 + \psi_2.$$

The determinant of an invariant form on a $\mathbb{Q}[\chi_i]B$-module affording $\psi_1 + \psi_2$ is q by Lemma 6.4.17.

Therefore it remains to find the determinant of an invariant form on a $\mathbb{Q}[\chi_i]B$-module M_i affording the character $(\alpha_i)_B + (\alpha_i^*)_B$. Since $\psi_1 + \psi_2$ has values in $\mathbb{Q}$, we have $\mathbb{Q}[\chi_i] = \mathbb{Q}[(\alpha_i)_B + (\alpha_i^*)_B] = \mathbb{Q}(\zeta_{q-1}^i + \zeta_{q-1}^{-i}) =: K_i$.

The irreducible $\mathbb{Q}$-representation of T containing M_i as a constituent is the representation $\mathbb{Q}(\zeta_{q-1}^i)$, as defined in Remark 6.2.1. Over the field K_i, this rational representation decomposes as the direct sum of Galois conjugates of the relative field extensions $(\mathbb{Q}(\zeta_{q-1}^i)/K_i)$,

$$\mathbb{Q}[\chi_i] \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_{q-1}^i) \cong \bigoplus_{\sigma \in \operatorname{Gal}(K_i/\mathbb{Q})} {}^{\sigma}\big(\mathbb{Q}(\zeta_{q-1}^i)/K_i\big).$$

This decomposition follows from Theorem 4.1.14.

The invariant bilinear forms on $\mathbb{Q}(\zeta_{q-1}^i)$, which are of the form $(x,y) \mapsto \operatorname{tr}_{\mathbb{Q}(\zeta_{q-1}^i)/\mathbb{Q}}(\eta x\overline{y})$ for some $\eta \in K_i$, cf. Proposition 6.2.3, accordingly decompose into the orthogonal direct sum of Galois conjugates

$$(x,y) \mapsto \bigoplus_{\sigma \in \operatorname{Gal}(K_i/\mathbb{Q})}\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\perp \quad {}^{\sigma}\left(\operatorname{tr}_{\mathbb{Q}(\zeta_{q-1}^i)/K_i}(\eta x\overline{y})\right),$$

each of which is easily checked to be of determinant $2 - \zeta_{q-1}^{2i} - \zeta_{q-1}^{-2i}$, which proves our assertion, because M_i is precisely one of the Galois conjugate direct summands. □

The characters ξ_1 and ξ_2

Let $q \equiv 1 \pmod 4$. The absolutely irreducible characters ξ_1 and ξ_2 of $\mathrm{PSL}_2(q)$, which are conjugate under the action of $\mathrm{PGL}_2(q)$, are of odd dimension. Therefore we want to determine the Clifford invariants of the invariant forms on their respective modules. It suffices to determine one of the Clifford invariants by virtue of Proposition 4.2.13.

We aim to apply Nebe's character method presented in Section 4.3.7 in order to solve this problem. The following statement is a first observation.

Lemma 6.4.23 *As in Section 4.3.7, let W denote the simple $c(\varphi)$-module. Then χ_W is a character of* $\mathrm{PSL}_2(q)$ *if and only if* $q \equiv 1,\ -3 \pmod{16}$ *and it is a faithful character of* $\mathrm{SL}_2(q)$ *if and only if* $q \equiv 5,\ 9 \pmod{16}$. *In fact, in the latter case, χ_W only has faithful constituents.*

Proof. We want to apply Remark 4.3.23 to this problem. For odd q, $\mathrm{SL}_2(q)$ is a universal covering group of $\mathrm{PSL}_2(q)$ unless $q = 9$ - it is in fact the unique universal covering group if $q \geq 5$ and $q \neq 9$, cf. [Hup67, V, Satz 25.7]. However, even for $n = 9$ it is sufficient to consider $\mathrm{SL}_2(q)$ due to Lemma 3.1.11 of [Neb99].
Let g be an element of order two in G and denote by e the dimension of the (-1)-eigenspace and by a the dimension of the 1-eigenspace of the action of g on φ. Then by inspection of the character table in Theorem 6.4.4 we find that g is conjugate to $\begin{pmatrix} \nu & \\ & \nu^{-1} \end{pmatrix}^{\frac{q-1}{4}}$ and we obtain the following system of linear equations.

$$a + e = \frac{q+1}{2}, \qquad a - e = (-1)^{\frac{q-1}{4}}.$$

Solving this, we find that

$$e \equiv \begin{cases} 0 \pmod 4 & \text{if } q \equiv 1, -3 \pmod{16}, \\ 2 \pmod 4 & \text{if } q \equiv 5, 9 \pmod{16}, \end{cases}$$

whence

$$(-1)^{\binom{e}{2}} = \begin{cases} 1 & \text{if } q \equiv 1, -3 \pmod{16}, \\ -1 & \text{if } q \equiv 5, 9 \pmod{16}. \end{cases}$$

Now, the extension $\mathrm{SL}_2(q)$ of $\mathrm{PSL}_2(q)$ is of the form $2.G$ with a simple group G, and clearly χ_W is a non-trivial character. Therefore the kernel of χ_W can only be $\{1\}$ or the central order two subgroup of $2.G$. The square of a preimage of g in $2.G$ is contained in said subgroup, which is why the claim follows from Corollary 4.3.23, with which we can check whether or not χ_W is trivial on that subgroup. □

The case $n = 2$

We begin with the case $n = 2$ rather than $n = 1$ because it uses the same idea but is significantly less convoluted, mostly due to the fact that the characters ξ_1 and ξ_2 are rational valued whenever q is a square.

Assume that $q = p^2$, in which case $q \equiv 1, 9 \pmod{16}$. Then ξ_1 and ξ_2 are rational-valued. Let $\xi \in \{\xi_1, \xi_2\}$.

Lemma 6.4.24 *The Clifford invariant $\mathfrak{c}(\xi)$ satisfies*

$$\mathfrak{c}(\xi) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod{16}, \\ [\mathcal{Q}_{p,\infty}] & \text{if } q \equiv 9 \pmod{16} \end{cases}$$

in $\mathrm{Br}(\mathbb{Q})$.

Proof. We focus on the elements of order p in $G = \mathrm{PSL}_2(q)$. From the character table of $\mathrm{PSL}_2(q)$ we obtain that on the two conjugacy classes of elements of order p, ξ has the values $\frac{1+\sqrt{q}}{2} = \frac{1+p}{2}$ and $\frac{1-\sqrt{q}}{2} = \frac{1-p}{2}$, i.e. one of the values is odd and one is even.
Now we determine the value of the character $\widetilde{\chi}$ on the even Clifford algebra $\mathcal{C}_0(\xi)$ on these two conjugacy classes. Since ξ is rational, the characteristic polynomial of an element g of order p is of the form $(X-1)^a\Phi_p^b$, where $\Phi_p \in \mathbb{Q}[X]$ denotes the p-th cyclotomic polynomial. a and b are determined by the systems of linear equations

$$\begin{aligned} &(1) \quad \frac{p^2+1}{2} = a + (p-1)b, \quad \frac{1+p}{2} = a - b, \\ &(2) \quad \frac{p^2+1}{2} = a + (p-1)b, \quad \frac{1-p}{2} = a - b, \end{aligned}$$

which have the solutions

$$\begin{aligned} &(1) \quad a = p, \quad b = \frac{p-1}{2}, \\ &(2) \quad a = 1, \quad b = \frac{p+1}{2}. \end{aligned}$$

Using Remark 4.3.22, we find that the values of $\widetilde{g}$ on the elements of order p are

$$-\frac{1}{2} \cdot (-2)^a = 2^{a-1} = \begin{cases} 2^{p-1} & \text{in the first case,} \\ 1 & \text{in the second case.} \end{cases}$$

This shows that the value of χ_W on one of the elements of order p is odd while it is even on the other one. From the character tables of $\mathrm{PSL}_2(q)$ and $\mathrm{SL}_2(q)$ (cf. Theorems 6.4.1, 6.4.4, 6.4.6) we find: For each irreducible character χ we have $\chi(c) = \chi(d)$ – where c and d represent the two conjugacy classes of elements of order p – with the exception of the characters of degrees $\frac{q\pm1}{2}$.

An inspection of the character values modulo 2 reveals that exactly one of the four characters of degrees $\frac{q\pm1}{2}$ must occur as a constituent of χ_W with odd multiplicity.
Now we can apply Corollary 4.3.20. If $q \equiv 1 \pmod{16}$, this implies that $\mathfrak{c}(\xi) = 1$, otherwise we obtain $\mathfrak{c}(\xi) = [\mathrm{End}_{\mathbb{Q}[\mathrm{SL}_2(q)]}(U)] = [\mathcal{Q}_{p,\infty}]$, where U is an irreducible $\mathbb{Q}[\mathrm{SL}_2(q)]$-module affording the character $2\eta_i$ (using the notation from [Dor71]). The Brauer equivalence class of $\mathrm{End}_{\mathbb{Q}[\mathrm{SL}_2(q)]}(U)$ is obtained from [Jan74]. □

The case $n = 1$

Lemma 6.4.25 *Let $\xi \in \{\xi_1, \xi_2\}$. Then for all $p \equiv 1 \pmod 4$, the character $\widetilde{\xi}_0$ of $\mathcal{C}_0(\xi)$ is*

$$\begin{pmatrix} 1 & z & c & d & a^\ell & b^m \\ 2^{\frac{p-1}{2}} & 2^{\frac{p-1}{2}} & \tau & \overline{\tau} & (-1-(-1)^\ell)\cdot\left((-1)^{\left(\frac{p-1}{2}\right)/\gcd\left(\frac{p-1}{2},\ell\right)}-1\right)^{\gcd\left(\frac{p-1}{2},\ell\right)} & (-2)^{\gcd\left(\frac{p+1}{2},m\right)-1} \end{pmatrix}$$

in the notation of Theorem 6.4.1.
τ denotes an element of $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{p})}$ of norm 1, which is equal to 1 if $p \equiv 1 \pmod 8$, and $\overline{\tau}$ its Galois conjugate.

Proof. The values on $1 \in \mathrm{SL}_2(q)$ and z are clear. For the values on the other conjugacy classes we want to apply Remark 4.3.22.

Let ζ_p be a p-th root of unity. The elements c and d are of order p, so their eigenvalues on the module affording ξ are 1 and the $\frac{p-1}{2}$ primitive p-th roots of unity which are in the same orbit under the Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}[\xi] = \mathbb{Q}(\sqrt{p})$. We denote the non-trivial Galois automorphism of $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ by $\overline{}$. Put

$$Q := \{x \in (\mathbb{Z}/p\mathbb{Z})^\times \mid x \text{ is a square}\},\ N := (\mathbb{Z}/p\mathbb{Z})^\times - Q.$$

Let

$$\mu(X) := \prod_{i\in Q}(X - \zeta_p^i) \in \mathbb{Q}(\sqrt{p})[X]$$

and $\overline{\mu}$ its conjugate under $\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$. Then the characteristic polynomials of c and d are $(X-1)\mu$ and $(X-1)\overline{\mu}$, respectively, for reasons of dimension. Of course, this is merely correct for one of ξ_1 and ξ_2. For the other (Galois conjugate) character the roles of c and d are reversed.
In order to evalute μ at -1, define

$$z := \prod_{i\in Q}(1-\zeta_p^i),\ t := \prod_{n\in N}(1-\zeta_p^n),\ \tau := \prod_{q\in Q}(1+\zeta_p^q) = \prod_{q\in Q}(-1-\zeta_p^q).$$

If $2 \in Q$, which is the case if and only if $p \equiv \pm1 \mod 8$, then $\tau z = z$, which implies $1 = \tau = \mu(-1) = \overline{\mu}(-1)$. Otherwise $\tau z = t = \overline{z}$, implying that τ is a unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ of norm 1, which is not in $\mathbb{Z}$.

Next, consider the element a. Since ξ is a character of $\mathrm{PSL}_2(q)$ and a is of even order $p-1$, a acts like an element of order $\frac{p-1}{2}$. The eigenvalues of a in this action are -1 and all powers $\zeta_{\frac{p-1}{2}}^r$ with $0 \leq r \leq \frac{p-1}{2} - 1$, because $\sum_{r=0}^{\frac{p-1}{2}-1} \zeta_{\frac{p-1}{2}} = 0$, so the eigenvalues add up to the correct character values.
In fact, the restriction of ξ to the subgroup generated by a consists of the regular representation of a cyclic group of order $\frac{p-1}{2}$ and a one-dimensional character defined by $a \mapsto -1$. This shows that the characteristic polynomial of the action of a^ℓ is

$$(X - (-1)^\ell)(X^{\left(\frac{p-1}{2}\right)/\gcd\left(\frac{p-1}{2},\ell\right)} - 1)^{\gcd\left(\frac{p-1}{2},\ell\right)}$$

which we evaluate at -1 in order to obtain the value of $\widetilde{\xi}_0$ on a^ℓ.

Analogously, one finds that on the classes b^m we have the regular representation of a cyclic group of order $\frac{p+1}{2}$. □

Lemma 6.4.26 *We have*

$$\mathfrak{c}(\xi) = \begin{cases} 1 & \text{if } p \equiv 1, -3 \pmod{16}, \\ [\mathcal{Q}_{\infty_1,\infty_2}] & \text{if } p \equiv 5, 9 \pmod{16} \end{cases}$$

in $\mathrm{Br}(\mathbb{Q}(\sqrt{p}))$.

Proof. Throughout this proof, we will use the descriptions of the endomorphism rings of the irreducible representations of $\mathrm{SL}_2(q)$ found in [Jan74]. The main theorem of that paper states that the character fields of the χ_i are $\mathbb{Q}(\zeta_{p-1}^i + \zeta_{p-1}^{-i})$, those of the θ_j are $\mathbb{Q}(\zeta_{p+1}^j + \zeta_{p+1}^{-j})$ and the Hasse invariants of the occurring division algebras are listed. We will not reproduce the Hasse invariants here, but name them in the course of this proof where they occur, without further mentioning of Janusz's paper.

The strategy for this proof is to apply Nebe's theorem, see Corollary 4.3.20. To that end, consider the generic character $\widetilde{\xi}_0$ in Lemma 6.4.25. Let χ_W be the character of the simple $c(\xi)$-module W, satisfying the relation $\chi_W^2 = \widetilde{\xi}_0$.
We want to find an absolutely irreducible character of $\mathrm{PSL}_2(p)$ (if $p \equiv 1, -3 \pmod{16}$) or $\mathrm{SL}_2(p)$ occurring with odd multiplicity in χ_W. Recall that if $p \equiv 1, -3 \pmod{16}$, all constituents of χ_W are characters of $\mathrm{PSL}_2(p)$, whereas if $p \equiv 5, 9 \pmod{16}$, χ_W consists exclusively of faithful characters of $\mathrm{SL}_2(p)$, cf. Lemma 6.4.23.

For convenience, put $K := \mathbb{Q}(\sqrt{p})$.

Let us assume we are in the case $p \equiv 1, -3 \pmod{16}$ and abbreviate $G := \mathrm{PSL}_2(q)$. If one of the characters $\mathbb{1}_G$, St_G, ξ_1 or ξ_2 occurs with odd multiplicity in χ_W, we immediately obtain the desired statement from Nebe's theorem, since the character fields of those characters are subfields of $K = \mathbb{Q}(\sqrt{p})$.
Next, assume that $\mathbb{1}_G$, St_G, ξ_1 and ξ_2 all occur with even multiplicity in χ_W. Consider

the elements c, d and b and the values of the character $\widetilde{\xi_0}$ on them. Since $\widetilde{\xi_0}(b) = 1$, one of the characters θ_j, with j even, must occur in χ_W with odd multiplicity. If one of the θ_j occurring with odd multiplicity in χ_W has the property $[K[\theta_j] : K] \equiv 1 \pmod 2$, the statement of Corollary 4.3.20 reads

$$[c(\xi) \otimes_K K[\theta_j]] = [K[\theta_j]] \in \mathrm{Br}(K[\theta_j]), \tag{$\diamond$}$$

which implies $[c(\xi)] = [K] \in \mathrm{Br}(K)$ by Theorem (28.5) of [Rei75].
If all θ_j occurring with odd multiplicity in χ_W have character fields with even degrees, one of the χ_i with $i \equiv 0 \mod 2$ must occur in χ_W with odd multiplicity and satisfy $[K[\chi_i] : K] \equiv 1 \pmod 2$. To see this, consider the values $\theta_j(b)$. Since $\widetilde{\xi_0}$ has a rational value on b, so must χ_W. But if the degree of the character field is even, an even number of Galois conjugates of θ_j occurs in χ_W in order to produce a rational value on b, which then contributes an even number of -1's on the classes c and d. If none of the χ_i occur with odd multiplicity and none of them has a character field of odd degree, by the same argument we obtain an even number of 1's on the classes c and d, all in all yielding a character value contained in $2\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$, which is a contradiction, since the values of $\widetilde{\xi_0}$ on the classes c and d are units in $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$. Now we can conclude just as before in ($\diamond$).

Now assume that $p \equiv 5, 9 \pmod{16}$ and abbreviate $G := \mathrm{SL}_2(q)$. If one of the characters η_1 or η_2 occurs with odd multiplicity in χ_W and we let U denote the KG-module affording the character $2\eta_i$, we obtain

$$[c(\xi)] = [\mathrm{End}_{KG}(U)] = [\mathcal{Q}_{\infty_1,\infty_2}] \in \mathrm{Br}(K).$$

Let us assume that both η_1 and η_2 have even multiplicity in χ_W. Then one of the θ_j, this time with j odd since all constituents of χ_W must be faithful, occurs in χ_W with odd multiplicity. If for one of those θ_j we have $[K[\theta_j] : K] \equiv 1 \pmod 2$, let U denote the KG-module with character $2\theta_j$. We then have

$$[c(\xi) \otimes_K K[\theta_j]] = [K \otimes_{\mathbb{Q}} \mathrm{End}_{\mathbb{Q}[\theta_j]G}(U)] \in \mathrm{Br}(K[\theta_j]).$$

Notice that the condition $[K[\theta_j] : K] = [K(\zeta_{p+1}^j + \zeta_{p+1}^{-j}) : K] \equiv 1 \pmod 2$ implies that the order $t := \mathrm{ord}(\zeta_{p+1}^j)$ is of the form $2s^m$ for some prime $s \equiv 3 \pmod 4$ and $m \in \mathbb{N}$. In that case, $\mathfrak{E} := \mathrm{End}_{\mathbb{Q}[\theta_j]G}(U)$ is ramified at all infinite places of $L := \mathbb{Q}(\zeta_{p+1}^j + \zeta_{p+1}^{-j})$ and at the unique prime of L dividing s. Hence, $K \otimes_{\mathbb{Q}} \mathfrak{E}$ is ramified at least at the infinite places of KL, of which there is an even number. It is no longer ramified at the primes above s because s is not decomposed in $\mathbb{Q}(\sqrt{p})$ since s divides $p + 1$ and therefore

$$\left(\frac{s}{p}\right) = \left(\frac{p}{s}\right) = \left(\frac{-1}{s}\right) = -1$$

by quadratic reciprocity. So, there is an odd number of primes above s in KL, which can therefore no longer ramify, as the number of ramified places of a quaternion algebra is always even.

Now, as KL/K is an odd degree extension, we conclude that $c(\xi)$ (as a K-algebra) is ramified only at the two infinite places of K, using Theorem (31.9) of [Rei75].
Should all θ_j occurring in χ_W have character fields of even degree, we find that one of the χ_i must occur in χ_W with odd multiplicity and have a character field of odd degree by again considering the classes c and d. However, this situation only arises when $p \not\equiv 1 \pmod 8$, i.e. in our case $p \equiv 5 \pmod{16}$. That is because the order $r := \operatorname{ord}(\zeta_{p-1}^i)$, which is divisible by four, must satisfy $\varphi(r) \equiv 2 \pmod 4$, where φ is Euler's totient function, so that the degree of $\mathbb{Q}[\chi_i]/\mathbb{Q}$, which is $\frac{1}{2}\varphi(r)$, is odd. This immediately implies $r = 4$ (and $\mathbb{Q}[\chi_i] = \mathbb{Q}$), so

$$4 = \frac{p-1}{\gcd(p-1, i)} \Leftrightarrow 4\gcd(p-1, i) = p-1.$$

As i is odd, this implies $8 \nmid p-1$. Now, $\operatorname{End}_{\mathbb{Q}G}(U)$, where U denotes the $\mathbb{Q}G$-module affording $2\chi_i$, is the $\mathbb{Q}$-algebra $\mathcal{Q}_{2,\infty}$. As $\left(\frac{2}{p}\right) = -1$ for $p \equiv 5 \pmod{16}$, 2 is not decomposed in K and therefore $[c(\xi)] = [K \otimes_{\mathbb{Q}} \mathcal{Q}_{2,\infty}] = [\mathcal{Q}_{\infty_1,\infty_2}] \in \operatorname{Br}(K)$. □

This argument cannot be easily extended to the cases $n \geq 3$ because the values of $\widetilde{\xi_0}$ at the elements of order p then both lie in $2\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$.

We summarize our results as a main theorem.

Theorem 6.4.27 (Orthogonal representations of $\mathbf{SL_2}(q)$) *Let χ be a complex irreducible character of $\mathrm{SL}_2(q)$ and K the maximal totally real subfield of its character field. Then the orthogonal representation (V, q) of $\mathrm{SL}_2(q)$ whose character contains χ has the following algebraic invariants.*

χ	K	$\dim_K(V)$	$\mathfrak{c}(\chi)$	$\mathrm{d}_\pm(\chi)$	q
$\mathbb{1}$	$\mathbb{Q}$	1	1	$-$	*all*
St	$\mathbb{Q}$	q	$\mathfrak{c}(\mathbb{A}_q)$	$-$	*all*
χ_i i *even*	$\mathbb{Q}(\vartheta_{q-1}^{(i)})$	$q+1$	$-$	$-\varepsilon(2-\vartheta_{q-1}^{(2i)})q$	*all*
χ_i i *odd*	$\mathbb{Q}(\vartheta_{q-1}^{(i)})$	$2(q+1)$	$[\mathrm{End}_{KG}(W)]$	1	$1 \pmod 4$
			1	1	$3 \pmod 4$
θ_j j *even*	$\mathbb{Q}(\vartheta_{q+1}^{(j)})$	$q-1$	1 *if* $q \in (\mathbb{Q}^\times)^2$	εq	*all*
θ_j j *odd*	$\mathbb{Q}(\vartheta_{q+1}^{(j)})$	$2(q-1)$	1	1	$1 \pmod 4$
			$[\mathrm{End}_{KG}(W)]$	1	$3 \pmod 4$
ξ_1, ξ_2	$\mathbb{Q}(\sqrt{p})$	$\frac{p+1}{2}$	1	$-$	$q = p \equiv 1, -3 \pmod{16}$
			$[\mathcal{Q}_{\infty_1,\infty_2}]$	$-$	$q = p \equiv 5, 9 \pmod{16}$
ξ_1, ξ_2	$\mathbb{Q}$	$\frac{q+1}{2}$	1	$-$	$q = p^2 \equiv 1 \pmod{16}$
			$[\mathcal{Q}_{p,\infty}]$	$-$	$q = p^2 \equiv 9 \pmod{16}$
$\xi_1 + \xi_2$	$\mathbb{Q}$	$q+1$	1	1	$3 \pmod 8$
			$(-1,-1)$	1	$7 \pmod 8$
η_1, η_2	$\mathbb{Q}(\sqrt{q})$	$q-1$	$[\mathcal{Q}_{p,\infty} \otimes K]$	1	$1 \pmod 4$
$\eta_1 + \eta_2$	$\mathbb{Q}$	$q-1$	$-$	$-q$	$3 \pmod 4$

Remark 6.4.28 In [BN16, Theorem 4.2], which appeared after the completion of this thesis, we find that

$$\mathfrak{c}(\xi_1) = \mathfrak{c}(\xi_2) = \begin{cases} 1 \in \mathrm{Br}(\mathbb{Q}(\sqrt{q})) & \text{if } q \equiv 1, -3 \pmod{16}, \\ [\mathcal{Q}_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q})] \in \mathrm{Br}(\mathbb{Q}(\sqrt{q})) & \text{if } q \equiv 5, 9 \pmod{16}, \end{cases}$$

where q is an arbitrary odd prime power. In other words, the restriction $n \in \{1, 2\}$ is removed in loc. cit.

6.5 $\mathrm{SL}_2(2^n)$

We can also apply our methods to the groups $\mathrm{SL}_2(2^n)$ in order to determine the invariants of most of the orthogonal representations of those groups. Let us abbreviate $q := 2^n$ and $G := \mathrm{SL}_2(q)$.

We begin, as before, by presenting the character table for G.

Theorem 6.5.1 ([Dor71, Theorem 38.2]) *Let ν be a generator of $\mathbb{F}_q^\times$ and consider the elements*

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; c := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \; a := \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}$$

of G. The group also contains an element b of order $q+1$. For $x \in G$, let (x) denote the conjugacy class containing x.
G has the following $q+4$ conjugacy classes of elements, listed together with the size of the classes.

x	1	c	a^ℓ	b^m
$\lvert(x)\rvert$	1	q^2-1	$q(q+1)$	$q(q-1)$

for $1 \leq \ell \leq \frac{q-2}{2}$, $1 \leq m \leq \frac{q}{2}$.

The character table of G is

	1_G	c	a^ℓ	b^m
$\mathbb{1}$	1	1	1	1
St	q	0	1	-1
χ_i	$q+1$	1	$\zeta_{q-1}^{i\ell}+\zeta_{q-1}^{-i\ell}$	0
θ_j	$q-1$	-1	0	$-\zeta_{q+1}^{jm}-\zeta_{q+1}^{-jm}$

where $1 \leq i \leq \frac{q-2}{2}$, $1 \leq j \leq \frac{q}{2}$, $1 \leq \ell \leq \frac{q-2}{2}$, $1 \leq m \leq \frac{q}{2}$.

Once again, the Borel subgroup

$$B := \left\{ \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \mid x \in \mathbb{F}_q^\times,\ y \in \mathbb{F}_q \right\}$$

and its subgroups

$$B \trianglerighteq U := \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in \mathbb{F}_q \right\} \cong \underbrace{C_2 \times \ldots \times C_2}_{n \text{ factors}}$$

and

$$T := \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \mid x \in \mathbb{F}_q^\times \right\}$$

will play a central role. Therefore we will first determine the absolutely irreducible representations of B, just as in the case of an odd prime power q, using Clifford theory. As the approach, the results and their proofs are very similar to those of Section 6.4, we will provide the relevant results without detailed proofs.

Lemma 6.5.2 *For all $\mathbb{1}_U \neq \chi \in \operatorname{Irr}(U)$, the inertia groups $I_B(\chi)$ are equal to U.*

Remark 6.5.3 There are $q-1$ irreducible one-dimensional characters of B whose restriction to U is $\mathbb{1}_U$. They are in one-to-one correspondence with the irreducible representations of $B/U \cong T \cong C_{q-1}$.

Lemma 6.5.4 *B has an absolutely irreducible and faithful character of degree $q-1$. We will call this character ψ. It has Schur index 1 and is therefore realizable over its character field, which is $\mathbb{Q}$.*

These are in fact all irreducible characters of B. We will also require knowledge of B-invariant bilinear forms on modules affording the character ψ.

Lemma 6.5.5 *Let φ be an orthogonal $\mathbb{Q}B$-module with character ψ. Then there is some $a \in \mathbb{Q}^\times$ such that $\varphi \cong a \circ (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{I}_{q-1})$.*
Hence, $\mathfrak{c}(\varphi) = 1$ as soon as $n \geq 3$. For $q = 4$ we obtain $\mathfrak{c}(\varphi) = [\mathcal{Q}_{2,\infty}]$.

Proof. By Clifford's theorem, we have $\psi = \operatorname{ind}_U^B(\chi)$ for any $\mathbb{1}_U \neq \chi \in \operatorname{Irr}(U)$. Since χ has all its values in $\{\pm 1\}$, we find that $\mathbb{I}_{q-1}$ is a B-invariant bilinear form on a $\mathbb{Q}B$-module affording the character ψ. □

Now we focus our attention towards the orthogonal representations of G.

Lemma 6.5.6 *A G-invariant form on the Steinberg representation St_G, which is of even dimension q, has the discriminant*

$$\mathrm{d}_\pm(\mathrm{St}_G) = (-1)^{\binom{q}{2}}(q+1) = \begin{cases} -3 & \text{if } q = 2, \\ q+1 & \text{if } q \geq 4. \end{cases}$$

Proof. St_G is obtained via the relation $\mathbb{1}_G + \mathrm{St}_G = \operatorname{ind}_B^G(\mathbb{1}_B)$, as is explained e.g. in the proof of Theorem 38.2 in [Dor71]. Therefore we can apply Proposition 4.3.2. □

Lemma 6.5.7 *A G-invariant form on a module affording one of the characters θ_j has trivial Clifford invariant, unless $q = 4$, in which case the Clifford invariant is $(-1,-1) = [\mathbb{Q}(\sqrt{5}) \otimes_{\mathbb{Q}} \mathcal{Q}_{2,\infty}] = [\mathcal{Q}_{\infty_1,\infty_2}] \in \mathrm{Br}(\mathbb{Q}(\sqrt{5}))$.*

Proof. As an irreducible character of a simple group, θ_j is faithful, and so is its restriction $\theta_j|_B$. Given our knowledge of the representation theory of B, we know $\theta_j|_B = \psi$, so that the statement follows from Lemma 6.5.5. □

For the representations of G affording the characters χ_i, neither the "restriction method", i.e. studying the character $\chi_i|_B$, nor the method used in Lemma 6.4.26 can be applied (at least not in full generality), even though one can easily compute the generic character $\widetilde{(\chi_i)_0}$. For those characters we have to explicitly compute the respective Clifford invariants using a computer algebra system or some other ad-hoc method.

Lemma 6.5.8 *Let $\chi \in \{\chi_i \mid 1 \leq i \leq (q-2)/2\}$. Then the character $\widetilde{\chi_0}$ of the even Clifford algebra is*

$$\begin{pmatrix} 1 & c & a^\ell & b^m \\ 2^q & 0 & (2+\zeta_{q-1}^{i\ell}+\zeta_{q-1}^{-i\ell})\cdot 2^{\gcd(q-1,\ell)-1} & 2^{\gcd(q+1,m)-1} \end{pmatrix}.$$

Proof. The proof is a simple calculation analogous to the proof of Lemma 6.4.25. □

Remark 6.5.9 For $q \in \{4, 8, 16\}$ we obtain the following by explicit computations using `Magma`. [1]

q	i	$\mathfrak{c}(\chi_i)$
4	$i = 1$	$[\mathcal{Q}_{3,\infty}] \in \mathrm{Br}(\mathbb{Q})$
8	$1 \leq i \leq 3$	$1 \in \mathrm{Br}(\mathbb{Q}[\chi_i])$
16	$i \in \{3, 6\}$	$[\mathcal{Q}_{2,\sqrt{5}}] \in \mathrm{Br}(\mathbb{Q}(\sqrt{5}))$
	$i \in \{1, 2, 4, 5, 7\}$	$1 \in \mathrm{Br}(\mathbb{Q}[\chi_i])$

For larger q the computation time significantly increases, so we do not perform the respective computations.

Instead, for $q = 32$, we consider the generic character of $\widetilde{(\chi_i)_0}$. We claim that the Clifford invariant of a G-invariant form on a module affording the character χ_i is trivial.
If one of $\mathbb{1}_G$ or St_G occurs with odd multiplicity in χ_W, the character of the simple $\mathcal{C}_0(\chi_i)$-module, the claim follows. If that is not the case, notice that the value of $\widetilde{(\chi_i)_0}$ on a is $2 + \zeta_{31}^{\ell} + \zeta_{31}^{-\ell}$, which is not divisible by 2 in the ring of integers of the character field. So one of the χ_i must occur in χ_W with odd multiplicity. But then the claim also follows from Nebe's theorem because the degrees of the character fields $\mathbb{Q}[\chi_i]$ are all odd for $q = 32$.

Again, we summarize our results for G as the final theorem of this section.

Theorem 6.5.10 (Orthogonal representations of $\mathbf{SL_2(2^n)}$) *Let $q = 2^n$ and consider $G = \mathrm{SL}_2(q)$. Then the non-trivial irreducible characters of G have G-invariant bilinear forms with the following algebraic invariants.*

[1] This remark is false as stated. Indeed, for $q = 16$ and $i = 5$, the Clifford invariant is $[\mathcal{Q}_{2,3}] \in \mathrm{Br}(\mathbb{Q})$, cf. [BN16, Theorem 6.3].

Character	*Invariant*
St_G	$\mathrm{d}_{\pm}(\varphi) = \begin{cases} -3 & \textit{if } q = 2, \\ q+1 & \textit{if } q \geq 4. \end{cases}$
χ_i, $1 \leq i \leq \frac{q-2}{2}$	*see Remark 6.5.9 for the cases* $q \in \{4, 8, 16, 32\}$.
θ_j, $1 \leq j \leq \frac{q}{2}$	$\mathfrak{c}(\varphi) = \begin{cases} (-1,-1) \in \mathrm{Br}(\mathbb{Q}(\sqrt{5})) & \textit{if } q = 4, \\ 1 \in \mathrm{Br}(\mathbb{Q}[\theta_j]) & \textit{if } q \geq 8. \end{cases}$

7 Clifford orders

This chapter is concerned with the study of so-called “Clifford orders”, which are certain subrings of the Clifford algebra of a quadratic space. These considerations are mostly of independent interest and our main focus lies on arithmetic properties of Clifford orders.

7.1 Basic properties

Throughout this chapter, let K be a totally real number field and $\mathcal{O}$ its ring of integers. (V, q) will denote a regular quadratic K-space of dimension n with Clifford algebra $g : V \hookrightarrow \mathcal{C}(V, q)$.
Let L be an integral $\mathcal{O}$-lattice in V.

Definition 7.1.1 The $\mathcal{O}$-algebra generated by $g(L)$ in $\mathcal{C}(V, q)$ is called the Clifford order of L.
It is an order in the sense of [Rei75], i.e. it is a finitely generated subring which contains a K-basis of $\mathcal{C}(V, q)$.

Convention 7.1.2 As in Section 3.6, we will often tacitly omit the map g when working in a Clifford order, provided that no confusion arises from this omission.

Remark 7.1.3 If L is free as an $\mathcal{O}$-module with basis $\{\ell_1, ..., \ell_n\}$, by Theorem 3.6.5 $\mathcal{C}(L)$ is a free $\mathcal{O}$-module as well. Notice that this is always the case if $\mathcal{O}$ is a principal ideal domain.
Concretely, a basis for $\mathcal{C}(L)$ is then given by

$$\bigsqcup_{r=0}^{n} \{g(\ell_{i_1}) \cdot ... \cdot g(\ell_{i_r}) \mid 1 \leq i_1 < ... < i_r \leq n\}.$$

Remark 7.1.4 Let $\{(\mathfrak{a}_i, e_i) \mid 1 \leq i \leq n\}$ be a pseudo-basis for L, cf. Remark 3.5.6. $\mathcal{C}(L)$ has

$$\bigsqcup_{r=0}^{n} \Big\{ \Big(\mathfrak{a}_{i_1} \cdot ... \cdot \mathfrak{a}_{i_r}, g(e_{i_1}) \cdot ... \cdot g(e_{i_r}) \Big) \mid 1 \leq i_1 < ... < i_r \leq n \Big\}$$

as a pseudo-basis, which is easily verified since on the one hand, the lattice with this pseudo-basis is a sublattice of $\mathcal{C}(L)$ and on the other hand said lattice is multiplicatively closed and contains $g(L)$.

Lemma 7.1.5 *Let $n \in \mathbb{N}$ and $\{a_1, ..., a_n\} \subseteq \mathbb{Z}$. Then for any $1 \leq k \leq n$ we have*

$$\prod_{1 \leq i_1 < ... < i_k \leq n} a_{i_1} \cdot ... \cdot a_{i_k} = (a_1 \cdot ... \cdot a_n)^{\binom{n-1}{k-1}}.$$

Proof. The product under consideration consists of $\binom{n}{k}$ factors of length k since the index set of the product is in bijection with the set of subsets of $\{1, ..., n\}$ of cardinality k. A simple counting argument shows that every one of the a_i appears in $\binom{n-1}{k-1}$ of those factors, which proves the statement. □

Theorem 7.1.6 (Index formula) *Let $L_1 \subseteq L_2$ be two integral $\mathcal{O}$-lattices in V. Then we have $\mathcal{C}(L_1) \subseteq \mathcal{C}(L_2)$ and $[\mathcal{C}(L_2) : \mathcal{C}(L_1)] = [L_2 : L_1]^{(2^{n-1})}$*

Proof. Choose compatible pseudo-bases for L_1 and L_2, see [Rei75, Thm. (4.14)], i.e. a K-basis $\{e_1, ..., e_n\}$ for V, fractional ideals $\mathfrak{a}_1, ..., \mathfrak{a}_n$ of $\mathcal{O}$ and integral ideals $\mathfrak{b}_1, ..., \mathfrak{b}_n$ satisfying $\mathfrak{b}_i \mid \mathfrak{b}_{i+1}$ for all i such that

$$L_2 = \mathfrak{a}_1 e_1 \oplus ... \oplus \mathfrak{a}_n e_n$$

and

$$L_1 = \mathfrak{a}_1 \mathfrak{b}_1 e_1 \oplus ... \oplus \mathfrak{a}_n \mathfrak{b}_n e_n.$$

Then we have $[L_2 : L_1] = N(\mathfrak{b}_1) \cdot ... \cdot N(\mathfrak{b}_n)$ and, using the previous lemma, we compute

$$\begin{aligned}[\mathcal{C}(L_2) : \mathcal{C}(L_1)] &= \prod_{k=1}^{n} \left(\prod_{1 \leq i_1 < ... < i_k \leq n} N(\mathfrak{b}_{i_1}) \cdot ... \cdot N(\mathfrak{b}_{i_k}) \right) \\ &= \prod_{k=1}^{n} [L_2 : L_1]^{\binom{n-1}{k-1}} \\ &= [L_2 : L_1]^{\sum_{k=1}^{n} \binom{n-1}{k-1}} \\ &= [L_2 : L_1]^{(2^{n-1})},\end{aligned}$$

which completes the proof. □

Remark 7.1.7 Within the even Clifford algebra $\mathcal{C}_0(V, q)$, we can consider the even Clifford order $\mathcal{C}_0(L)$. All our previous results carry over in the expected way:

1. If L has $\{(\mathfrak{a}_i, e_i) \mid 1 \leq i \leq n\}$ as a pseudo-basis over a Dedekind domain $\mathcal{O}$,

$$\bigsqcup_{\substack{r=0 \\ r \equiv 0 \mod 2}}^{n} \left\{ \left(\mathfrak{a}_{i_1} \cdot ... \cdot \mathfrak{a}_{i_r}, g(e_{i_1}) \cdot ... \cdot g(e_{i_r}) \right) \mid 1 \leq i_1 < ... < i_r \leq n \right\}$$

   is a pseudo-basis for $\mathcal{C}_0(L)$.
   In particular, if L is a free $\mathcal{O}$-module, so is $\mathcal{C}_0(L)$.

2. In the situation of Theorem 7.1.6, we have $\mathcal{C}_0(L_1) \subseteq \mathcal{C}_0(L_2)$ and
$$[\mathcal{C}_0(L_2) : \mathcal{C}_0(L_1)] = \begin{cases} 1, & \text{if } n = 1, \\ [L_2 : L_1]^{2^{n-2}}, & \text{if } n \geq 2. \end{cases}$$

3. As in Section 3.6, we use the notation
$$c(L) := \begin{cases} \mathcal{C}(L) & n \equiv 0 \mod 2, \\ \mathcal{C}_0(L) & n \equiv 1 \mod 2. \end{cases}$$

7.2 The trace bilinear form

Let $\mathrm{tr}_{\mathrm{reg}}$ denote the regular trace of the semisimple K-algebras $\mathcal{C}(V,q)$ or $\mathcal{C}_0(V,q)$. We want to study the bilinear forms
$$T \;:\; \mathcal{C}(L) \times \mathcal{C}(L) \to \mathcal{O},\;\; (x,y) \mapsto \mathrm{tr}_{\mathrm{reg}}(xy)$$
and
$$T \;:\; \mathcal{C}_0(L) \times \mathcal{C}_0(L) \to \mathcal{O},\;\; (x,y) \mapsto \mathrm{tr}_{\mathrm{reg}}(xy)$$
on $\mathcal{C}(L)$ and $\mathcal{C}_0(L)$ in order to obtain some information on the ramified places of the K-algebra $c(V,q)$. It turns out that this bilinear form is strongly related to exterior powers of b_q.

Definition 7.2.1 Let (L,b) be a bilinear space over $\mathcal{O}$. Then, on $\bigwedge^k L$, we have the bilinear form $\bigwedge^k b$ defined as
$$\bigwedge^k L \times \bigwedge^k L \to \mathcal{O},\;\; (x_1 \wedge ... \wedge x_k, y_1 \wedge ... \wedge y_k) \mapsto \det(b(x_i,y_j)_{1 \leq i,j \leq k}).$$

A survey of the properties of such bilinear forms may be found in [McG02].

Theorem 7.2.2 *Let L be an integral $\mathcal{O}$-lattice in a quadratic space (V,q) over K. Assume that L has an orthogonal basis $\{e_1,...,e_n\}$ such that $(L,q) \cong [a_1,...,a_n]$. Then we have*
$$(\mathcal{C}(L),T) \cong \bigoplus_{i=0}^{n} \left(2^{n-i}(-1)^{\binom{i}{2}} \circ \bigwedge^i (L,b_q)\right)$$
via the isometry induced by $e_{i_1} \cdot ... \cdot e_{i_r} \mapsto e_{i_1} \wedge ... \wedge e_{i_r}$.
Analogously, we have an isometry
$$(\mathcal{C}_0(L),T) \cong \bigoplus_{\substack{i=0 \\ i \equiv 0 \mod 2}}^{n} \left(2^{n-1-i}(-1)^{\binom{i}{2}} \circ \bigwedge^i (L,b_q)\right).$$

Proof. We prove the statement for $\mathcal{C}(L)$. The proof for the even Clifford order is completely analogous.
Since $b_q(e_i, e_j) = 0$ for $i \neq j$, we have $e_i e_j = -e_j e_i$ in $\mathcal{C}(L)$ and it is therefore easily verified that

$$\bigcup_{r=0}^{n} \{e_{i_1} \cdot ... \cdot e_{i_r} \mid 1 \leq i_1 < ... < i_r \leq n\}$$

is an orthogonal basis of $\mathcal{C}(L)$ with respect to the regular trace bilinear form. Notice that by [McG02, Proposition 4.1], the set

$$\bigcup_{r=0}^{n} \{e_{i_1} \wedge ... \wedge e_{i_r} \mid 1 \leq i_1 < ... < i_r \leq n\}$$

is an orthogonal basis for $\bigoplus_{r=0}^{n} \bigwedge^r b_q$ and

$$\bigwedge^r b_q(e_{j_1} \wedge ... \wedge e_{j_r}, e_{j_1} \wedge ... \wedge e_{j_r}) = 2^r a_{j_1} \cdot ... \cdot a_{j_r}.$$

Furthermore we have

$$\begin{aligned}
&T(e_{i_1} \cdot ... \cdot e_{i_r}, e_{i_1} \cdot ... \cdot e_{i_r}) \\
=&\mathrm{tr}_{\mathrm{reg}}(e_{i_1} \cdot ... \cdot e_{i_r} \cdot e_{i_1} \cdot ... \cdot e_{i_r}) \\
=&\mathrm{tr}_{\mathrm{reg}}\left((-1)^{\binom{r}{2}} e_{i_1} \cdot ... \cdot e_{i_r} \cdot e_{i_r} \cdot ... \cdot e_{i_1}\right) \\
=&\mathrm{tr}_{\mathrm{reg}}\left((-1)^{\binom{r}{2}} a_{i_1} \cdot ... \cdot a_{i_r}\right) \\
=&2^n (-1)^{\binom{r}{2}} a_{i_1} \cdot ... \cdot a_{i_r} \\
=&2^{n-r} (-1)^{\binom{r}{2}} 2^r a_{i_1} \cdot ... \cdot a_{i_r}
\end{aligned}$$

which completes the proof of the theorem. □

As stated before, L may not be a free $\mathcal{O}$-module, so it may not have an $\mathcal{O}$-basis, let alone an orthogonal basis.
However, passing to the completion $\mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} L$ rectifies this, since $\mathcal{O}_\mathfrak{p}$ is always a principal ideal domain for any finite place $\mathfrak{p}$ of K, and any quadratic module over a complete discrete valuation ring with finite residue field of odd characteristic admits an orthogonal basis due to Theorem 3.4.6, 3.
As we will be mainly interested in the local structure of $\mathcal{C}(L)$ in the remainder of this chapter, the passage from L to $\mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} L$ imposes no real restrictions - in this context recall also the result of Lemma 3.6.10:

$$\mathcal{C}(\mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} L) \cong \mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} \mathcal{C}(L)$$

as $\mathcal{O}_\mathfrak{p}$-algebras.

Even though the proof of our description of the regular trace bilinear form strongly relies on the existence of an orthogonal $\mathcal{O}$-basis of the lattice L, after some brief computations it seems conceivable that the following conjecture holds.

Conjecture 7.2.3 *The statement of Theorem 7.2.2 holds for integral lattices without the assumption that there be an orthogonal basis.*

From our description of the trace bilinear form we also obtain a statement about the discriminant $\operatorname{disc}(\mathcal{C}(L))$ of $\mathcal{C}(L)$, which is defined to be the determinant of the reduced trace bilinear form. This yields some insight into the ramified places of the $K_{\mathfrak{p}}$-algebra $\mathcal{C}(V,q)$.

Corollary 7.2.4 *Let $\mathfrak{p} \nmid (2)$ be a finite prime of K. Consider $\det(L,q)$, which is a class in $\mathcal{O}/(\mathcal{O}^{\times})^2$. Clearly, the $\mathfrak{p}$-valuations of all representatives of the class $\det(L,q)$ are equal. If $v_{\mathfrak{p}}(\det(L,q)) = 0$, then $v_{\mathfrak{p}}(\operatorname{disc}(c(L))) = 0$.*

Proof. Since $\mathfrak{p}$ is an odd prime, $\mathcal{O}_{\mathfrak{p}} \otimes_{\mathcal{O}} L$ has an orthogonal basis and we can apply Theorem 7.2.2 in order to compute $\operatorname{disc}(c(L))$. Excluding the trivial case of $n = 1$, this yields

$$\operatorname{disc}(c(L)) = \begin{cases} \det(L,q)^{(2^{n-1})} & n \equiv 0 \mod 2, \\ 2^{2^{n-2}} \cdot \det(L,q)^{(2^{n-2})} & n \equiv 1 \mod 2, \end{cases}$$

as $\det\left(\bigwedge^i(L,b_q)\right) = \det(L,b_q)^{\binom{n-1}{i-1}}$ for all $1 \leq i \leq n$ by [McG02, Proposition 5.1]. Thus an odd prime can only occur in the discriminant if it occurs in the determinant of the lattice L. □

Corollary 7.2.5 *The odd finite places of K at which $\mathcal{C}(V,q)$ ramifies are contained in the set of odd finite primes occurring in the determinant of an integral lattice L in (V,q). If (V,q) is an orthogonal representation of a finite group G and L is G-invariant, the ramified primes of $\mathcal{C}(V,q)$ are therefore found among the divisors of $2\cdot|G|$ and the infinite places of K (cf. Theorem 4.2.12).*

7.3 The Jacobson radical and the idealizer

This section is devoted to the study of the Jacobson radical of a Clifford order $\mathcal{C}(L)$. As the ground ring, we will use completions $\mathcal{O}_{\mathfrak{p}}$ at finite primes $\mathfrak{p}$ of a number field K with ring of integers $\mathcal{O}$.
We will provide a description of the Jacobson radical and its idealizer, describing in part the so-called radical idealizer process, which produces a hereditary over-order of $\mathcal{C}(L)$. The concept of hereditariness will be introduced in this section.

We choose a uniformizer π for $\mathcal{O}_{\mathfrak{p}}$, i.e. $\pi \in \mathcal{O}_{\mathfrak{p}}$ such that the unique maximal ideal of the local ring $\mathcal{O}_{\mathfrak{p}}$ is $\pi\mathcal{O}_{\mathfrak{p}}$. We denote the residue field by $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_{\mathfrak{p}}/\pi\mathcal{O}_{\mathfrak{p}}$.

In order to ease the notation, we will assume from now on that V is a $K_{\mathfrak{p}}$-space and that L is an integral $\mathcal{O}_{\mathfrak{p}}$-lattice in V rather than merely an $\mathcal{O}$-lattice.

In our investigation we will distinguish two cases, depending on whether or not the characteristic of the residue field $\mathbb{F}_{\mathfrak{p}}$ is even. However, we first state some general results which are independent of the characteristic of the residue class field.

The Jacobson radical of an arbitrary ring R, which is defined to be the intersection of all its maximal left ideals - equivalently, the intersection of all maximal right ideals or the intersection of all the annihilators of the simple modules of the ring - is particularly well understood when R is Artinian. In that case it is the smallest two-sided ideal with semisimple quotient ring and at the same time it is a nilpotent ideal.
Also, even without the hypothesis that R be Artinian, any ideal containing only nilpotent elements is contained in $J(R)$.

Although the orders we consider are certainly not Artinian rings, we can salvage the essence of the above properties in our situation, as the following result shows.

Theorem 7.3.1 ([Rei75, Theorem (6.15)]) *Let Λ be an $\mathcal{O}_{\mathfrak{p}}$-order in some semisimple $K_{\mathfrak{p}}$-algebra and let $\varphi : \Lambda \to \overline{\Lambda} := \Lambda/\pi\Lambda$ be the canonical epimorphism. Then the following statements hold.*

1. $\pi\Lambda \subseteq \varphi^{-1}(J(\overline{\Lambda})) = J(\Lambda)$.

2. $J(\Lambda)^t \subseteq \pi\Lambda$ *for some* $t \in \mathbb{N}$.

3. φ *induces a ring isomorphism* $\Lambda/J(\Lambda) \cong \overline{\Lambda}/J(\overline{\Lambda})$.

4. $J(\Lambda)$ *is the smallest two-sided ideal in* Λ *with semisimple quotient ring.*

The following remark about Clifford algebras of quadratic spaces over finite fields will be of use later on.

Remark 7.3.2 Let $\varphi = (V, q)$ be a regular quadratic space over a finite field k. If $n := \dim(V)$ is even, $\mathcal{C}(\varphi)$ is central simple, cf. Theorem 3.6.15. Therefore it is isomorphic to a matrix ring over a k-central division algebra, which implies $\mathcal{C}(\varphi) \cong \mathrm{Mat}_{2^{n/2}}(k)$ as any finite division algebra is a field by Wedderburn's theorem.
If n is odd, using the same argument, we have

$$\mathcal{C}(\varphi) \cong \begin{cases} \mathrm{Mat}_{2^{(n-1)/2}}(k) \oplus \mathrm{Mat}_{2^{(n-1)/2}}(k), & \text{if } \mathrm{d}_{\pm}(\varphi) \in (k^\times)^2, \\ \mathrm{Mat}_{2^{(n-1)/2}}(\mathfrak{K}), & \text{if } \mathrm{d}_{\pm}(\varphi) \notin (k^\times)^2, \end{cases}$$

where $\mathfrak{K}/k$ is a field extension of degree two.

7.3.1 Hereditary orders and the radical idealizer process

Let Λ be an $\mathcal{O}_{\mathfrak{p}}$-order in a semisimple $K_{\mathfrak{p}}$-algebra A. We follow [Neb05] for a brief introduction to the theory of hereditary orders and the radical idealizer process.

Definition 7.3.3 Λ is called hereditary if every left ideal of Λ is a projective Λ-module.

Hereditary orders admit the following characterization which is closely linked to the Jacobson radical.

Definition 7.3.4 Let L be an $\mathcal{O}_{\mathfrak{p}}$-lattice in A. The left order of L is

$$O_l(L) := \{a \in A \mid aL \subseteq L\}.$$

Analogously one defines the right order $O_r(L)$.
$\mathcal{I}(L) := O_l(L) \cap O_r(L)$ is called the idealizer of L.

Theorem 7.3.5 ([Rei75, Theorem 39.11], [Neb05, Theorem 2.6]) *The following are equivalent.*

1. *Λ is hereditary.*

2. *$\Lambda = \mathcal{I}(J(\Lambda))$.*

3. *$\Lambda = O_l(J(\Lambda))$.*

Remark 7.3.6 (Radical idealizer process) Putting $\Lambda_0 := \Lambda$ and $\Lambda_{n+1} := \mathcal{I}(J(\Lambda_n))$, $n = 0, 1, 2, ...$, defines the so-called radical idealizer process which constructs an ascending chain of $\mathcal{O}_{\mathfrak{p}}$-orders starting in Λ, the radical idealizer chain

$$\Lambda = \Lambda_0 \subseteq \Lambda_1 \subseteq ... \subseteq \Lambda_N = \Lambda_{N+1}.$$

This is a finite process, i.e. $N \in \mathbb{N}$. The order Λ_N is hereditary and called the head order of Λ. If N is minimal with the property $\Lambda_N = \Lambda_{N+1}$ then we call N the radical idealizer length $\ell_{\mathrm{rad}}(\Lambda)$ of Λ.

The next remark gives a lower bound on the length of the radical idealizer chain and is also useful for the explicit calculation of $\mathcal{I}(J(\Lambda))$, since one may calculate modulo the maximal ideal $\pi\mathcal{O}_{\mathfrak{p}}$.

Remark 7.3.7 Put $\Gamma := \mathcal{I}(J(\Lambda))$. Then $J(Z(\Lambda))\Gamma \subseteq \Lambda$, in particular $\pi\Gamma \subseteq \Lambda$.

An algorithmic way of computing the Jacobson radical and its idealizer are explained in more detail in [NS09].

There is also a global version of the radical idealizer proccess.

Remark 7.3.8 If R is a commutative ring with infinitely many prime ideals, then $J(R) = \{0\}$ and the same holds for any R-order Λ, regardless of whether it is hereditary or not. The radical idealizer process as we just defined it would not work in this case. However, one may define the arithmetic radical $J_a(\Lambda)$ to be the intersection of all maximal left ideals of Λ which contain the discriminant ideal, cf. Definition (5.46) in [PZ89]. Using this modified radical, one can then define a radical idealizer process just as in the local case.

7.3.2 Odd residue class field characteristic

In this section we determine both $J(\mathcal{C}(L))$ and its idealizer $\mathcal{I}(J(\mathcal{C}(L)))$ in the case that $2 \notin \mathfrak{p}$. In order to do that we assemble some general results first, which hold in a much wider context than the one set up in this chapter, i.e. integral lattices in quadratic spaces over complete discretely valued fields.

Remark 7.3.9 Let R be an integral domain of characteristic not two and (E, q) a quadratic module over it. If $v \in E$ is contained in $E^{\perp} := (E, b_q)^{\perp}$, then we have $q(v) = 0$ because of the equation $0 = b_q(v, v) = 2q(v)$. Over a ring of characteristic two this statement is clearly false.
In this situation, the module $E/E^{\perp}$ carries a natural quadratic form $\overline{q}$ given by

$$\overline{q} \ : \ E/E^{\perp} \to R, \ v + E^{\perp} \mapsto q(v).$$

Lemma 7.3.10 *Let R be an integral domain,* $\mathrm{char}(R) \neq 2$, *and let $\varphi = (E, q)$ be a quadratic module over R which may be degenerate. Denote by $g \ : \ E \to \mathcal{C}(\varphi)$ the Clifford algebra. Then the Jacobson radical of $\mathcal{C}(\varphi)$ contains the set*

$$X := \{g(x) \ : \ x \in (E, b_q)^{\perp}\}.$$

X has the property that the left and right ideals $\mathcal{C}(\varphi)X$ and $X\mathcal{C}(\varphi)$ are two-sided.

Proof. Letting $x \in (E, b_q)^{\perp}$ and $y \in E$, we have

$$g(x)g(y) + g(y)g(x) = b_q(x, y) = 0$$

and $g(x)^2 = q(x) = 0$, which shows that the set X consists of nilpotent elements which have the property that they commute or anti-commute (i.e. $ab = -ba$ for elements a, b) with any element of fixed degree in $\mathcal{C}(\varphi)$. This shows that the two-sided ideal generated by X consists of nilpotent elements and coincides with $\mathcal{C}(\varphi)X$ and $X\mathcal{C}(\varphi)$. □

Lemma 7.3.11 *Let k be a field of characteristic not two. Let $\varphi = (E, q)$ be a quadratic k-space, $g \ : \ E \to \mathcal{C}(\varphi)$ the Clifford algebra and $E^{\perp} := (E, b_q)^{\perp}$. Then the Jacobson radical $J(\mathcal{C}(\varphi))$ is generated by the set $X := \{g(x) \ : \ x \in E^{\perp}\}$ and the quotient ring $\mathcal{C}(\varphi)/J(\mathcal{C}(\varphi))$ is isomorphic to $\mathcal{C}(E/E^{\perp}, \overline{q})$.*

Proof. We already know from Lemma 7.3.10 that X is contained in $J(\mathcal{C}(\varphi))$.
Next, consider the map

$$f \;:\; E \to \mathcal{C}(E/E^{\perp}, \overline{q}),\; v \mapsto \overline{g}(v + E^{\perp}),$$

where $\overline{g} \;:\; E/E^{\perp} \to \mathcal{C}(E/E^{\perp}, \overline{q})$ is the Clifford algebra of $(E/E^{\perp}, \overline{q})$. This map satisfies $f(v)^2 = q(v) \cdot 1_{\mathcal{C}(E/E^{\perp}, \overline{q})}$, whence, by the universal property of the Clifford algebra, it extends to a k-algebra homomorphism $\overline{f} \;:\; \mathcal{C}(\varphi) \to \mathcal{C}(E/E^{\perp}, \overline{q})$, which is clearly surjective and whose image a semisimple k-algebra, because $E/E^{\perp}$ is a regular quadratic k-space.
We obtain $\dim_k(\ker(\overline{f})) = 2^{\dim(E)} - 2^{\dim(E/E^{\perp})}$ and $X \subseteq \ker(\overline{f}))$. Multiplying the elements in X with basis vectors of $\mathcal{C}(\varphi)$ and counting dimensions, we see that the k-dimension of the ideal generated by X is

$$\sum_{i=1}^{\dim(E^{\perp})} 2^{\dim(E/E^{\perp})} \binom{\dim(E^{\perp})}{i} = 2^{\dim(E)} - 2^{\dim(E/E^{\perp})}.$$

Hence we can conclude that $\ker(\overline{f})$ is precisely the ideal generated by X, which is therefore equal to the Jacobson radical. □

Recall the situation and notation of this section: K is a totally real number field, $\mathfrak{p}$ an odd finite prime, $K_{\mathfrak{p}}$ the completion of K at $\mathfrak{p}$ and $\mathcal{O}_{\mathfrak{p}}$ the valuation ring with uniformizer π. (V, q) is a regular quadratic space over $K_{\mathfrak{p}}$ and $n := \dim_{K_{\mathfrak{p}}}(V)$.

Lemma 7.3.12 *There is a natural quadratic form $\overline{q}$ on the $\mathbb{F}_{\mathfrak{p}}$-vector space $L/\pi L$ given by*

$$\overline{q} \;:\; L/\pi L \to \mathbb{F}_{\mathfrak{p}},\; \ell + \pi L \mapsto q(\ell) + \pi\mathcal{O}_{\mathfrak{p}}$$

and $\mathcal{C}(L)/\pi\mathcal{C}(L) \cong \mathcal{C}(L/\pi L, \overline{q})$.

Proof. Let $\overline{g} \;:\; L/\pi L \to \mathcal{C}(L/\pi L, \overline{q})$ denote the Clifford algebra of $(L/\pi L, \overline{q})$. The map

$$f \;:\; L \to \mathcal{C}(L/\pi L, \overline{q}),\; \ell \mapsto \overline{g}(\ell + \pi L)$$

is surjective, $\mathcal{O}_{\mathfrak{p}}$-linear and satisfies $f(\ell)^2 = q(\ell)1_{\mathcal{C}(L/\pi L, \overline{q})}$, so we obtain an induced epimorphism of $\mathcal{O}_{\mathfrak{p}}$-algebras $\overline{f} \;:\; \mathcal{C}(L) \to \mathcal{C}(L/\pi L, \overline{q})$.
$\pi\mathcal{C}(L)$ is contained in the kernel of $\overline{f}$, yielding a surjective homomorphism $\mathcal{C}(L)/\pi\mathcal{C}(L) \to \mathcal{C}(L/\pi L, \overline{q})$ between $\mathbb{F}_{\mathfrak{p}}$-algebras of equal dimensions, which proves the statement. □

In light of this lemma and in addition to the notation already in place, we put $r := \dim_{\mathbb{F}_{\mathfrak{p}}}\left((L/\pi L, b_{\overline{q}})^{\perp}\right)$. Since $\mathcal{O}_{\mathfrak{p}}$ is complete and $\mathrm{char}(\mathbb{F}_{\mathfrak{p}}) \neq 2$, there is an orthogonal basis

$$\{x_1, ..., x_r, x_{r+1}, ..., x_n\} \subseteq L$$

for the quadratic module $(L, q|_L)$ which we choose in such a way that the first r basis vectors are mapped to a basis of the radical $(L/\pi L, b_{\overline{q}})^{\perp}$ under the natural epimorphism $L \to L/\pi L$.

Theorem 7.3.13 *The Jacobson radical $J(\mathcal{C}(L))$ of the Clifford order is generated by*

$$X := \{\pi,\ x_i \mid 1 \leq i \leq r\}$$

as an ideal.
We have $J(\mathcal{C}(L))^{r+1} \subseteq \pi\mathcal{C}(L)$ and r is minimal with this property.

Proof. The two-sided ideal (X) contains the two-sided ideal (π) and the quotient ring $\mathcal{C}(L)/(X)$ is isomorphic to

$$\Big(\mathcal{C}(L)/(\pi)\Big)/\Big((X)/(\pi)\Big)$$

which is isomorphic to the Clifford algebra of the quadratic space

$$\Big(L/\pi L, \overline{q}\Big)/\Big(L/\pi L, b_{\overline{q}}\Big)^{\perp}$$

equipped with the quadratic form naturally induced by q as in Remark 7.3.9 and Lemma 7.3.12. As in Lemma 7.3.11 we find that $\mathcal{C}(L)/(X)$ is semisimple. Hence, $J(\mathcal{C}(L)) \subseteq (X)$.

The vectors $x \in (L/\pi L, b_{\overline{q}})^{\perp}$ have the property that they commute or anti-commute with all homogeneous elements of $\mathcal{C}(L/\pi L, \overline{q})$. Furthermore, since $\mathrm{char}(\mathbb{F}_{\mathfrak{p}}) \neq 2$, they are all nilpotent in $\mathcal{C}(L/\pi L, \overline{q})$ and therefore generate a two-sided nilpotent ideal.
Any choice of r basis vectors $x_1, ..., x_r$ of $(L/\pi L, b_{\overline{q}})^{\perp}$ constitutes a generating set of this ideal and any product of length $r+1$ of these generators is clearly zero. However, $x_1 \cdot ... \cdot x_r \neq 0$, so the nilpotence degree of the ideal under consideration is precisely $r+1$. From this we obtain that $J(\mathcal{C}(L))^{r+1} \subseteq \pi\mathcal{C}(L)$, that $r+1$ is minimal with this property and that $(x_1, ..., x_r) \subseteq J(\mathcal{C}(L/\pi L, \overline{q}))$.

We can therefore use Theorem 7.3.1 in order to conclude that $(X) \subseteq J(\mathcal{C}(L))$. □

Corollary 7.3.14 *The ℓ^{th} power of the Jacobson radical of $\mathcal{C}(L)$ is generated by products of length ℓ of the generators $\{\pi,\ x_i \mid 1 \leq i \leq r\}$.*

Proof. This follows from the fact that $\{x_i \mid 1 \leq i \leq n\}$ is an orthogonal basis for L which implies that $J(\mathcal{C}(L))$ is generated by commuting and anti-commuting elements. □

Corollary 7.3.15 *The set*

$$\bigcup_{\ell=0}^{n} \Big(\big\{\pi x_{i_1} \cdot ... \cdot x_{i_\ell} \mid 1 \leq i_1 < ... < i_\ell \leq n,\ \{i_1, ..., i_\ell\} \cap \underline{r} = \emptyset\big\}$$
$$\cup \big\{x_{i_1} \cdot ... \cdot x_{i_\ell} \mid 1 \leq i_1 < ... < i_\ell \leq n,\ \{i_1, ..., i_\ell\} \cap \underline{r} \neq \emptyset\big\}\Big)$$

is an $\mathcal{O}_{\mathfrak{p}}$-basis of $J(\mathcal{C}(L))$.
The index of the Jacobson radical in $\mathcal{C}(L)$ is

$$[\mathcal{C}(L) : J(\mathcal{C}(L))] = |\mathbb{F}_{\mathfrak{p}}|^{2^{n-r}}$$

and the quotient ring is isomorphic to the Clifford algebra of an $(n-r)$-dimensional regular quadratic space over $\mathbb{F}_\mathfrak{p}$ whose isomorphism type as an $\mathbb{F}_\mathfrak{p}$-algebra can be read off from Remark 7.3.2.

Theorem 7.3.16 (Structure of the radical idealizer) *This theorem describes the first step of the radical idealizer process for the Clifford order $\mathcal{C}(L)$.*

1. *If $v_\mathfrak{p}(\det(L,q)) \in \{0,1\}$, then $\mathcal{I}(J(\mathcal{C}(L))) = \mathcal{C}(L)$. In particular, $\mathcal{C}(L)$ is a hereditary order.*

2. *If $v_\mathfrak{p}(\det(L,q)) \geq 2$, the idealizer of $J(\mathcal{C}(L))$ is the order of $\mathcal{C}(V,q)$ generated by $\mathcal{C}(L)$ and $\frac{1}{\pi}J(\mathcal{C}(L))^r$, which is not a subset of $\mathcal{C}(L)$, whence we obtain a proper over-order of $\mathcal{C}(L)$ as the radical idealizer.*

Proof. For simplicity, for $I \subseteq \underline{n}$ we define the shorthand notation

$$x_I := x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_{|I|}},$$

where $I = \{i_1, ..., i_{|I|}\}$ and $i_1 < i_2 < ... < i_{|I|}$.

1. Recall the description of the Jacobson radical from Theorem 7.3.13.
If $v_\mathfrak{p}(\det(L,q)) = 0$ then $r = 0$, so the Jacobson radical is simply $\pi\mathcal{C}(L)$. Therefore, if $x \in \mathcal{I}(J(\mathcal{C}(L)))$ then $\pi x \in \pi\mathcal{C}(L)$, which implies $x \in \mathcal{C}(L)$, so this case is trivial.
The condition $v_\mathfrak{p}(\det(L,q)) = 1$ can only be fulfilled if $r = 1$ and $x_1^2 = u\pi$ with $u \in \mathcal{O}_\mathfrak{p}^\times$.
Now, consider an element $x \in \mathcal{C}(V) = K_\mathfrak{p} \otimes_{\mathcal{O}_\mathfrak{p}} \mathcal{C}(L)$. Using the usual basis for $\mathcal{C}(V)$, we can write
$$x = \sum_{I \subseteq \underline{n}} a_I x_I,$$
with $a_I \in K_\mathfrak{p}$. Then we have
$$x_1 x = \sum_{1 \notin I \subseteq \underline{n}} a_I x_{I \cup \{1\}} + \sum_{1 \in I \subseteq \underline{n}} a_I u \pi x_{I - \{1\}}.$$
If x is to lie in the idealizer of the Jacobson radical, we must have $x_1 x \in J(\mathcal{C}(L))$. Using the $\mathcal{O}_\mathfrak{p}$-basis from Corollary 7.3.15, we find that this is the case precisely when $a_I \in \mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$, which implies that $\mathcal{I}(J(\mathcal{C}(L)))$ is a sub-order of $\mathcal{C}(L)$. As the inclusion $\mathcal{C}(L) \subseteq \mathcal{I}(J(\mathcal{C}(L)))$ is clear, the two orders coincide.

2. Let $x \in \mathcal{I}(J(\mathcal{C}(L)))$ and write
$$x = \sum_{I \subseteq \underline{n}} a_I x_I$$
with suitable $a_I \in K_\mathfrak{p}$.
The condition $\pi x \in J(\mathcal{C}(L))$ implies $a_I \in \mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$ with $I \cap \underline{r} = \emptyset$ and $a_I \in \frac{1}{\pi}\mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$ satisfying $I \cap \underline{r} \neq \emptyset$.

Now let $1 \leq j \leq r$. Then there is $u_j \in \mathcal{O}_{\mathfrak{p}}^{\times}$ and a suitable power of π, denoted $\pi^{(j)}$, such that $x_j^2 = u_j \pi^{(j)}$. Let us consider the product $x_j x$, which is equal to

$$\sum_{\substack{I \subseteq \underline{n} \\ I \cap \underline{r} = \emptyset}} a_I x_{I \cup \{j\}} + \sum_{\substack{I \subseteq \underline{n} \\ I \cap \underline{r} \neq \emptyset \\ j \notin I}} \pm a_I x_{I \cup \{j\}} + \sum_{\substack{I \subseteq \underline{n} \\ j \in I}} \pm a_I u_j \pi^{(j)} x_{I - \{j\}}. \tag{†}$$

From the condition $x_j x \in J(\mathcal{C}(L))$, which has to hold for all $1 \leq j \leq r$, we obtain the condition $a_I \in \mathcal{O}_{\mathfrak{p}}$ for all $I \subseteq \underline{n}$ satisfying $I \cap \underline{r} \neq \emptyset$ and $j \notin I$ - this may be read off from the second sum in (†).
In conclusion, this means that a_I must be integral for any $I \subseteq \underline{n}$ such that $I \cap \underline{r} \subsetneq \underline{r}$. For the remaining $I \subseteq \underline{n}$ we obtain $a_I \in \frac{1}{\pi}\mathcal{O}_{\mathfrak{p}}$. Therefore $\mathcal{I}(J(\mathcal{C}(L)))$ is indeed contained in the order generated by $\mathcal{C}(L)$ and $\frac{1}{\pi}J(\mathcal{C}(L))^r$.

Conversely, we will now show that $J(\mathcal{C}(L))^{r+1} \subseteq \pi J(\mathcal{C}(L))$, which will imply the inclusion $\frac{1}{\pi}J(\mathcal{C}(L))^r \subseteq \mathcal{I}(J(\mathcal{C}(L)))$. By Corollary 7.3.14, $J(\mathcal{C}(L))^{r+1}$ is generated by products of length $r+1$ of $\{\pi, x_i \mid 1 \leq i \leq r\}$. Consider such a product and denote it by η.
If π is one of the $r+1$ factors, then η is contained in $\pi J(\mathcal{C}(L))$. If not, then by the pigeonhole principle, one of the x_i must occur more often than once in η, x_d say. Then we obtain $\eta = \pm x_d^2 \widehat{x}$, where $\widehat{x}$ denotes a product of the remaining $r-1$ facors of η. Notice that $x_d^2 \in \pi\mathcal{C}(L)$.
If $r \geq 2$, then there is some other x_j, $1 \leq j \leq r$, which is a factor of $\widehat{x}$, so that η is contained in $\pi J(\mathcal{C}(L))$.
If $r = 1$, we must be in the case where $d = 1$ and $x_1^2 = u\pi^{\beta}$ with $u \in \mathcal{O}_{\mathfrak{p}}^{\times}$ and $\beta \geq 2$. Then $\eta = \pi \cdot u\pi^{\beta-1} \in \pi J(\mathcal{C}(L))$.

By Theorem 7.3.13, r is minimal with the property $J(\mathcal{C}(L))^{r+1} \subseteq \pi\mathcal{C}(L)$, so that $\frac{1}{\pi}J(\mathcal{C}(L))^r$ is indeed not a subset of $\mathcal{C}(L)$. □

7.3.3 Even residue class field characteristic

We now turn our attention towards the case of (residue) characteristic two, i.e. $2 \in \mathfrak{p}$. In the last section, we saw a strong connection between regularity of a quadratic form over a field of odd characteristic and the Jacobson radical of its Clifford algebra.
Recall that in characteristic two there are no regular one-dimensional quadratic spaces. Nonetheless, those small examples already exhibit some interesting properties.

Example 7.3.17 Let k be a finite extension of $\mathbb{F}_2$, $\omega \in k$ and consider the quadratic space $E = [\omega]$. The Clifford algebra of E is the two-dimensional commutative k-algebra $\mathcal{C}(E) \cong k[X]/(X^2 - \omega)$. Notice that there is some $\tau \in k$ such that $\tau^2 = \omega$, so that $\mathcal{C}(E)$ contains a non-trivial nilpotent element and is therefore not semisimple.

On the other hand, let $k = \mathbb{F}_2(T)$ be the rational function field in one indeterminate over $\mathbb{F}_2$ and consider the quadratic space $E = [T]$. The Clifford algebra is isomorphic to $k[X]/(X^2 - T) \cong k[\sqrt{T}]$, which is semisimple as it is a field extension of k.

In light of this example, we will restrict ourselves to the consideration of quadratically closed fields in what follows.

Recall that given a quadratic space (E, q) over a field of odd characteristic, in the previous section we constructed a natural quadratic form $\overline{q}$ on the space $E/E^\perp$, where $E^\perp := (E, b_q)^\perp$, cf. Remark 7.3.9. This was due to the fact that $v \in (E, b_q)^\perp$ implies $q(v) = 0$, which is not true in characteristic two, as the example of the quadratic space [1] shows.
However, there is a suitable substitute method that we can use. We choose a vector space complement E' for $E^\perp$ within E. Clearly, E' is a regular subspace and $E = E^\perp \oplus E'$. Notice that E' is not unique up to isometry, as the example

$$\begin{bmatrix} 0 & 1 & \\ & 0 & \\ & & 1 \end{bmatrix} \cong \begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{bmatrix}$$

over $\mathbb{F}_2$ shows. However, our results will be independent of the choice of E'.

Theorem 7.3.18 *Let k be a quadratically closed field of characteristic two and (E, q) a quadratic k-space with Clifford algebra $g : E \to \mathcal{C}(E, q)$. The Jacobson radical $J(\mathcal{C}(E, q))$ is generated by*

$$X := \left\{ \sqrt{q(x)} + g(x) \mid x \in (E, b_q)^\perp \right\}.$$

Here the symbol $\sqrt{}$ denotes the unique square root of an element in k.

Proof. Clearly $\mathcal{C}(E, q)$ is an Artinian k-algebra and since all elements in X are nilpotent and central, they are contained in the Jacobson radical.

Now decompose (E, q) as $E^\perp \oplus E'$, where $E^\perp := (E, b_q)^\perp$, E' is regular and both subspaces are equipped with the respective restrictions of q. Let $g' : E' \to \mathcal{C}(E')$ be the Clifford algebra of $\mathcal{C}(E')$ and define a linear map $f : E \to \mathcal{C}(E')$ via

$$v \mapsto \begin{cases} \sqrt{q(v)} \cdot 1_{\mathcal{C}(E')} & v \in E^\perp, \\ g'(v) & v \in E'. \end{cases}$$

By construction, f satisfies $f(v)^2 = q(v)$ for all $v \in E$ so that we obtain a k-algebra homomorphism $\overline{f} : \mathcal{C}(E) \to \mathcal{C}(E')$ by the universal property of $\mathcal{C}(E)$. Clearly, $\overline{f}$ is surjective, from which it follows that the dimension of its kernel is $2^{\dim(E)} - 2^{\dim(E')}$. Obviously we have $X \subseteq \ker(\overline{f})$. In order to show that equality holds, we multiply basis elements of $\mathcal{C}(E,q)$ with the elements in X and see that the k-dimension of the ideal generated by X is

$$\sum_{i=1}^{\dim(E')} 2^{\dim(E')}\binom{\dim(E^{\perp})}{i} = 2^{\dim(E)} - 2^{\dim(E')}.$$

Therefore we have $(X) = \ker(\overline{f})$ and since the image of $\overline{f}$ is semisimple by 3.6.15, we have $J(\mathcal{C}(E,q)) \subseteq (X)$. □

Corollary 7.3.19 *$\mathcal{C}(E,q)/J(\mathcal{C}(E,q))$ is isomorphic to the Clifford algebra of a regular quadratic space over k.*

Once again, recall the notation which is in force throughout this section: K denotes a totally real number field with ring of integers $\mathcal{O}$. We denote by $\mathfrak{p}$ a finite prime of K, assumed to be even, i.e. $2 \in \mathfrak{p}$.
We choose a uniformizer π for $\mathcal{O}_{\mathfrak{p}}$ and consider a regular quadratic space (V,q) over the completion $K_{\mathfrak{p}}$. Let L be an integral $\mathcal{O}_{\mathfrak{p}}$-lattice in V.

Remark 7.3.20 Lemma 7.3.12 carries over to the case $\mathrm{char}(\mathbb{F}_{\mathfrak{p}}) = 2$ with identical statement and proof.

Theorem 7.3.21 *Let $\rho : \mathcal{C}(L) \to \mathcal{C}(L)/\pi\mathcal{C}(L)$ be the canonical epimorphism. The Jacobson radical of $\mathcal{C}(L)$ is generated by*

$$\left\{\pi, \rho^{-1}\left(\sqrt{\overline{q}(x)} + \overline{g}(x)\right) \mid x \in (L/\pi L, b_{\overline{q}})^{\perp}\right\}.$$

Of course ρ is no invertible map, so this is to be understood, in a suggestive way, as the choice of a pre-image. This is well-defined in the sense that two pre-images of an element $x \in (L/\pi L, b_{\overline{q}})^{\perp}$ under ρ differ by a multiple of π, so that for every choice of a pre-image, the above set generates the same ideal of $\mathcal{C}(L)$.

We have $J(\mathcal{C}(L))^{r+1} \subseteq \pi\mathcal{C}(L)$ and $r := \dim_{\mathbb{F}_{\mathfrak{p}}}\left((L/\pi L, b_{\overline{q}})^{\perp}\right)$ is minimal with this property.

Proof. Using Theorem 7.3.1, the first part of the statement follows from Theorem 7.3.18.

Let $\{x_1, ..., x_r\}$ be an $\mathbb{F}_{\mathfrak{p}}$-basis of $(L/\pi L, b_{\overline{q}})^{\perp}$. Then a product of length $r+1$ of the (central) generators $\sqrt{q(x_i)} + x_i$ in $\mathcal{C}(L/\pi L, \overline{q})$ involves two identical factors, so that it is zero because

$$(\sqrt{q(x)} + x)^2 = q(x) + x^2 = 0.$$

On the other hand, the product

$$\prod_{i=1}^{r}\left(\sqrt{q(x_i)} + x_i\right)$$

is non-zero, as it is of the form

$$x_1 \cdot ... \cdot x_r + \sum_{\ell=0}^{r-1} \left(\prod_{1 \leq i_1 < ... < i_\ell \leq r} a_{i_1,...,i_\ell} x_{i_1} \cdot ... \cdot x_{i_\ell} \right),$$

which is non-zero in $\mathcal{C}(L/\pi L, \overline{q})$, so that the nilpotence degree of $J(\mathcal{C}(L/\pi L, \overline{q}))$ is precisely $r+1$, which proves the assertion. □

Definition 7.3.22 Given the statement of Theorem 7.3.21, we will choose an $\mathcal{O}_\mathfrak{p}$-basis

$$\{x_1, ..., x_r\} \sqcup \{x_{r+1}, ..., x_n\}$$

for L such that the images of $\{x_1, ..., x_r\}$ under the canonical epimorphism $L \twoheadrightarrow L/\pi L$ form a basis of $(L/\pi L, b_{\overline{q}})^\perp$ and such that $\langle x_1, ..., x_r \rangle_{\mathcal{O}_\mathfrak{p}}$ and $\langle x_{r+1}, ..., x_n \rangle_{\mathcal{O}_\mathfrak{p}}$ are perpendicular sublattices of L. Such a choice is possible by a simple reformulation of Theorem 3.1.14 for local rings.
We then proceed to choose $w_i \in \mathcal{O}_\mathfrak{p}$ for $1 \leq i \leq r$ such that $q(x_i) \equiv w_i^2 \mod \pi\mathcal{O}_\mathfrak{p}$ and put $y_i := w_i + x_i$.

Remark 7.3.23 Notice that if $q(x_i)$ is a square modulo $\pi^2\mathcal{O}_\mathfrak{p}$, then we even have $w_i^2 \equiv q(x_i) \mod \pi^2\mathcal{O}_\mathfrak{p}$.

Proof. Let $a \in \mathcal{O}_\mathfrak{p}$ such that $q(x_i) \equiv a^2 \mod \pi^2\mathcal{O}_\mathfrak{p}$. Then we have $w_i^2 \equiv a^2 \mod \pi\mathcal{O}_\mathfrak{p}$, i.e. we can write $w_i = \pm a + \pi x$ for some $x \in \mathcal{O}_\mathfrak{p}$. But then $w_i^2 = a^2 + \pi^2 x^2 \pm 2\pi a x \equiv a^2 \mod \pi^2\mathcal{O}_\mathfrak{p}$. □

Corollary 7.3.24 *The set*

$$\{\pi x_I \mid I \subseteq \underline{n},\ I \cap \underline{r} = \emptyset\} \cup \{y_{I \cap \underline{r}} \cdot x_{I - \underline{r}} \mid I \subseteq \underline{n},\ I \cap \underline{r} \neq \emptyset\}$$

is an $\mathcal{O}_\mathfrak{p}$-basis of $J(\mathcal{C}(L))$, where for $J \subseteq \underline{r}$, $J = \{j_1, ..., j_{|J|}\}$ and $j_1 < j_2 < ... < j_{|J|}$ we put

$$y_J := y_{j_1} \cdot ... y_{j_{|J|}}.$$

We obtain

$$[\mathcal{C}(L) : J(\mathcal{C}(L))] = |\mathbb{F}_\mathfrak{p}|^{2^{n-r}}.$$

The quotient ring $\mathcal{C}(L)/J(\mathcal{C}(L))$ is isomorphic to $\mathrm{Mat}_{2^{(n-r)/2}}(\mathbb{F}_\mathfrak{p})$.

In order to conclude this section, we determine the radical idealizer of $\mathcal{C}(L)$. This turns out to be more subtle than in the previously considered case of $\mathrm{char}(\mathbb{F}_\mathfrak{p}) \neq 2$, where $v_\mathfrak{p}(\det(L))$ controlled the behavior of the radical idealizer and therefore determined whether or not $\mathcal{C}(L)$ was hereditary.

Example 7.3.25 Consider the two quadratic $\mathbb{Q}_2$-spaces [1] and [3] and the unique maximal $\mathbb{Z}_2$-lattices $L_{[1]}$ and $L_{[3]}$ within each of them. A simple calculation shows that $\mathcal{C}(L_{[3]})$ is hereditary, while $\mathcal{C}(L_{[1]})$ is not, even though $v_2(\det(L_{[1]})) = v_2(\det(L_{[3]})) = 1$.

An explicit analysis of the above examples yields an additional condition we have to impose in order to obtain a hereditary Clifford order. To prove the full characterization, we need some technical statements first.

Lemma 7.3.26 *Let $1 \leq s < t \leq r$. Then the y_s adhere to the following rules, which may be proved by simple calculations.*

1. $y_t y_s = y_s y_t + \underbrace{x_t x_s - x_s x_t}_{=:\sigma_{s,t}}$.

2. $y_t y_s = -y_s y_t + 2w_t y_s + 2w_s y_t - 2w_s w_t + b_q(x_s, x_t)$. *Using this relation, we may express $y_t y_s$ in the "standardized" basis, where $y_s y_t$ may occur, but $y_t y_s$ may not.*

3. $\sigma_{s,t} = x_t x_s - x_s x_t = -2x_s x_t + b_q(x_t, x_s) \in \pi\mathcal{C}(L)$.

4. $y_s^2 = q(x_s) - w_s^2 + 2w_s y_s$

5. $x_\ell y_s = -y_s x_\ell + \underbrace{2w_s x_\ell}_{=:\tau_{s,\ell} \in \pi\mathcal{C}(L)}$ *for all $r < \ell \leq n$.*

Remark 7.3.27 The ℓ-th power of $J := J(\mathcal{C}(L))$ is generated as an $\mathcal{O}_\mathfrak{p}$-lattice by products of length ℓ of the elements of an $\mathcal{O}_\mathfrak{p}$-basis of J.

Lemma 7.3.28 *We have $J^{r+1} \subseteq \pi J$ if $r \geq 2$ or $r = 1$ and $q(x_1)$ is a square in $\mathcal{O}_\mathfrak{p}/\pi^2\mathcal{O}_\mathfrak{p}$.*

Proof. Use the $\mathcal{O}_\mathfrak{p}$-basis

$$\mathfrak{B} = \underbrace{\{y_{I\cap\underline{r}} x_{I-\underline{r}} \mid I \subseteq \underline{n},\ I \cap \underline{r} \neq \emptyset\}}_{=:\mathfrak{B}_1} \sqcup \underbrace{\{\pi x_I \mid I \subseteq \underline{n},\ I \cap \underline{r} = \emptyset\}}_{=:\mathfrak{B}_2}$$

for J and first assume $r \geq 2$. Let η be a product of length $r+1$ of these basis elements. If at least one of the factors is contained in $\mathfrak{B}_2$, then clearly $\eta \in \pi J$.
Otherwise η is a product of $r+1$ elements of $\mathfrak{B}_1$, which means that each factor involves at least one of $y_1, ..., y_r$. So, by the pigeonhole principle, there is some $i \in \underline{j}$ such that y_i occurs at least twice in η. Using the calculation rules in Lemma 7.3.26, we can rearrange η to be in the following form.

$$\eta \equiv y_{<i} \cdot y_i^2 \cdot y_{\geq i} \cdot x_M \pmod{\pi J}$$

where $y_{<i}$ denotes a suitable product of some of the $y_1, ..., y_{i-1}$, $y_{\geq i}$ involves only factors $y_i, ..., y_r$ and M is a subset of $\{r+1, ..., n\}$. This relies on the two facts that $r+1$ is at least three and that the "correcting terms" $\sigma_{s,t}$ and $\tau_{s,\ell}$ are in $\pi\mathcal{C}(L)$ - so when two of the y_k are exchanged there is another $y_{\tilde{k}}$ in the product, guaranteeing that the "correcting term" σ multiplied by $y_{\tilde{k}}$ is contained in πJ.
Now,

$$\eta \equiv y_{<i}(q(x_i) - w_i^2)y_{\geq i} + y_{<i} \cdot 2w_i y_i \cdot y_{\geq i} \equiv 0 \pmod{\pi J}.$$

Let us now consider the case $r = 1$ and let η be a product of $r + 1 = 2$ elements of $\mathfrak{B}$. If one of the factors is contained in $\mathfrak{B}_2$, the statement is evident. So let $y_1x_{I-\{1\}}$ and $y_1x_{J-\{1\}}$ be two elements of $\mathfrak{B}_1$. Again relying on Lemma 7.3.26 we find

$$\begin{aligned}\eta &= y_1x_{I-\{1\}}y_1x_{J-\{1\}}\\ &\equiv y_1^2x_{I-\{1\}}x_{J-\{1\}}\\ &= (q(x_1) - w_1^2)x_{I-\{1\}}x_{J-\{1\}} + 2w_1y_1x_{I-\{1\}}x_{J-\{1\}} \pmod{\pi J},\end{aligned}$$

where the second summand is obviously contained in πJ. The first summand is contained in πJ because of Remark 7.3.23. □

Now we can formulate and prove our main theorem describing the first step of the radical idealizer process.

Theorem 7.3.29 *1. If $r = 0$ or $r = 1$ and $q(x_1)$ is not a square in $\mathcal{O}_\mathfrak{p}/\pi^2\mathcal{O}_\mathfrak{p}$, we have $\mathcal{I}(J(\mathcal{C}(L))) = \mathcal{C}(L)$, i.e. $\mathcal{C}(L)$ is hereditary.*

2. If $r \geq 2$ or $r = 1$ and $q(x_1)$ is a square in $\mathcal{O}_\mathfrak{p}/\pi^2\mathcal{O}_\mathfrak{p}$, $\mathcal{I}(J(\mathcal{C}(L)))$ is the order generated by $\mathcal{C}(L)$ and $\frac{1}{\pi}J(\mathcal{C}(L))^r$. This is a proper over-order of $\mathcal{C}(L)$, so that in this case $\mathcal{C}(L)$ is not hereditary.

Proof. We prove the two statements separately.

1. In the case $r = 0$, there is nothing to show, so assume $r = 1$ and choose the $\mathcal{O}_\mathfrak{p}$-basis
$$\{x_I \mid I \subseteq \{2, ..., n\}\} \cup \{y_1x_I \mid I \subseteq \{2, ..., n\}\}$$
for $\mathcal{C}(L)$, cf. Corollary 7.3.24. Notice that, by the conditions of the theorem, $w_1^2 \not\equiv q(x_1) \mod \pi^2\mathcal{O}_\mathfrak{p}$.
Now let $x \in \mathcal{I}(J(\mathcal{C}(L)))$ and write
$$x = \sum_{I\subseteq\{2,\ldots,n\}} a_Ix_I + \sum_{I\subseteq\{2,\ldots,n\}} a_Iy_1x_I$$
with suitable $a_I \in K_\mathfrak{p}$. Then x satisfies $\pi x \in J(\mathcal{C}(L))$, so let us consider
$$\pi x = \sum_{I\subseteq\{2,\ldots,n\}} \pi a_Ix_I + \sum_{I\subseteq\{2,\ldots,n\}} \pi a_Iy_1x_I.$$
This implies $a_I \in \mathcal{O}_p$ for all $I \subseteq \underline{n}$ such that $1 \notin I$, and $a_I \in \frac{1}{\pi}\mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$ containing 1.
Next, we also have the condition $y_1x \in J(\mathcal{C}(L))$, so let us take a closer look at the product y_1x, which equals
$$\sum_{1\notin I\subseteq\underline{n}} a_Iy_1x_I + \sum_{1\in I\subseteq\underline{n}} 2w_1a_Iy_1x_{I-\{1\}} + \sum_{1\in I\subseteq\underline{n}} (q(x_1) - w_1^2)a_Ix_{I-\{1\}}.$$

An inspection of the last sum reveals the condition $(q(x_1) - w_1^2)a_I \in \pi\mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$ containing 1. This is equivalent to $a_I \in \frac{\pi}{q(x_n)-w^2}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$.

2. For convenience, put $J := J(\mathcal{C}(L))$ and $\mathcal{I} := \mathcal{I}(J)$. Under the conditions of the theorem, we have $J^{r+1} \subseteq \pi J$, i.e. $\frac{1}{\pi}J^r \subseteq \mathcal{I}$. Notice that $\frac{1}{\pi}J^r \not\subseteq \mathcal{C}(L)$, so that $\mathcal{I}$ is a proper over-order of $\mathcal{C}(L)$ and $\mathcal{C}(L)$ is not hereditary.
Now we have to show that $\mathcal{I}$ is contained in the order generated by $\mathcal{C}(L)$ and $\frac{1}{\pi}J^r$. To that end choose the $\mathcal{O}_\mathfrak{p}$-basis
$$\{y_{I\cap\underline{r}} \cdot x_{I-\underline{r}} \mid I \subseteq \underline{n}\}$$
for $\mathcal{C}(L)$. Let $x \in \mathcal{I}$ and write
$$x = \sum_{I\subseteq\underline{n}} a_I y_{I\cap\underline{r}} x_{I-\underline{r}}$$
with suitable $a_I \in K_\mathfrak{p}$.
$\pi x \in J(\mathcal{C}(L))$ implies $a_I \in \mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$, $I \cap \underline{r} = \emptyset$ and $a_I \in \frac{1}{\pi}\mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$, $I \cap \underline{r} \neq \emptyset$.
Next, we aim to show that $a_I \in \mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$ such that $j \notin I$ for all $j \in \underline{r}$. We will show this by induction on j, beginning with the case $j = 1$. We consider the product $y_1 x$ modulo J in order to derive conditions on the coefficients a_I where $1 \notin I$ from the condition $y_1 x \in J$. $y_1 x$ equals
$$\begin{aligned}
&\sum_{1\notin I\subseteq\underline{n}} a_I y_{(I\cap\underline{r})\cup\{1\}} x_{I-\underline{r}} + \sum_{1\in I\subseteq\underline{n}} a_I y_1^2 y_{(I\cap\underline{r})-\{1\}} x_{I-\underline{r}}\\
\equiv &\sum_{\substack{1\notin I\subseteq\underline{n}\\ I\cap\underline{r}\neq\emptyset}} a_I y_{(I\cap\underline{r})\cup\{1\}} x_{I-\underline{r}} + \sum_{1\in I\subseteq\underline{n}} a_I (q(x_1) - w_1^2) y_{(I\cap\underline{r})-\{1\}} x_{I-\underline{r}}\\
+ &\sum_{1\in I\subseteq\underline{n}} a_I 2w_1 y_1 y_{(I\cap\underline{r})-\{1\}} x_{I-\underline{r}}\\
\equiv &\sum_{\substack{1\notin I\subseteq\underline{n}\\ I\cap\underline{r}\neq\emptyset}} a_I y_{(I\cap\underline{r})\cup\{1\}} x_{I-\underline{r}} + \sum_{1\in I\subseteq\underline{n}} a_I (q(x_1) - w_1^2) y_{(I\cap\underline{r})-\{1\}} x_{I-\underline{r}} \pmod{J}.
\end{aligned}$$
For all $I \subseteq \underline{n}$ such that $1 \notin I$, we read off the condition $a_I \in \mathcal{O}_\mathfrak{p}$, as desired.

Relying on this, we consider y_2x modulo J:

$$\begin{aligned}
y_2x &= \sum_{I\subseteq\underline{n}} a_I y_2 y_{I\cap\underline{r}} x_{I-\underline{r}} \\
&\equiv \sum_{1\in I\subseteq\underline{n}} a_I y_2 y_1 y_{(I\cap\underline{r})-\{1\}} x_{I-\underline{r}} \\
&= \sum_{1\in I\subseteq\underline{n}} a_I y_1 y_2 y_{(I\cap\underline{r})-\{1\}} x_{I-\underline{r}} + \sum_{1\in I\subseteq\underline{n}} a_I \sigma_{1,2} y_{(I\cap\underline{r})-\{1\}} x_{I-\underline{r}} \\
&\equiv \sum_{\substack{1\in I\subseteq\underline{n}\\ 2\notin I}} a_I y_{(I\cap\underline{r})\cup\{2\}} x_{I-\underline{r}} + \sum_{\substack{1\in I\subseteq\underline{n}\\ I\cap\underline{r}=\{1\}}} a_I \sigma_{1,2} x_{I-\underline{r}} \\
&\equiv \sum_{\substack{1\in I\subseteq\underline{n}\\ 2\notin I}} a_I y_{(I\cap\underline{r})\cup\{2\}} x_{I-\underline{r}} + \sum_{\substack{I\subseteq\underline{n}\\ I\cap\underline{r}=\{1\}}} a_I(-2w_1w_2 + b_q(x_1,x_2))x_{I-\underline{r}}
\end{aligned}$$

The left and right hand sums are $\mathcal{O}_\mathfrak{p}$-linearly independent, so it is sufficient to consider the left hand sum in order to obtain the condition $a_I \in \mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$ such that $2 \notin I$.

For the induction step, we may now assume that $j \geq 3$, which allows us to make use of the following fact:
Modulo J, a product of (at least) three factors y_a, y_b, y_c satisfies

$$y_a y_b y_c = (y_b y_a + \sigma_{b,a}) y_c \equiv y_b y_a y_c \pmod{J}. \tag{7.1}$$

Now, consider the product y_jx and assume that $a_I \in \mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$ such that at least one of $1, ..., j-1$ is not contained in I. Then

$$\begin{aligned}
y_jx &\equiv \sum_{\underline{j-1}\subseteq I\subseteq\underline{n}} a_I y_j y_{I\cap\underline{r}} x_{I-\underline{r}} \\
&\equiv \sum_{\underline{j}\subseteq I\subseteq\underline{n}} a_I y_{I\cap\underline{j-1}} y_j^2 y_{I\cap\underline{j}} x_{I-\underline{r}} + \sum_{\substack{\underline{j-1}\subseteq I\subseteq\underline{n}\\ j\notin I}} a_I y_{(I\cap\underline{r})\cup\{j\}} x_{I-\underline{r}} \quad (\diamond) \\
&\equiv \sum_{\substack{\underline{j-1}\subseteq I\subseteq\underline{n}\\ j\notin I}} a_I y_{(I\cap\underline{r})\cup\{j\}} x_{I-\underline{r}} \pmod{J},
\end{aligned}$$

where in $(\diamond)$, we apply property (7.1).
From this we can now read off $a_I \in \mathcal{O}_\mathfrak{p}$ for all $I \subseteq \underline{n}$ such that $j \notin I$.

We conclude that a_I is integral for all I which have the property that $I \cap \underline{r}$ is a proper subset of $\underline{r}$.
All in all, we obtain that $\mathcal{I}$ is indeed contained in the order generated by $\mathcal{C}(L)$ and $\frac{1}{\pi}J^r$. □

Remark 7.3.30 Recall that in the case $2 \notin \mathfrak{p}$, we formulated a characterization of the cases in which $\mathcal{C}(L)$ is hereditary in terms of $v_{\mathfrak{p}}(\det(L))$. For $2 \in \mathfrak{p}$ this is possible as well, using the Jordan decomposition. However, the description is much more complicated and therefore less useful.
Let

$$L \cong \bigoplus_{r=0}^{\ell} \pi^r \circ L_r$$

be a Jordan decomposition of L in the bilinear space (V, b_q) associated to (V, q). Then $\mathcal{C}(L)$ is hereditary if and only if $v_{\mathfrak{p}}(\det(L)) = 0$ or $v_{\mathfrak{p}}(\det(L)) \in \{1, 2\}$ and

$$(-1)^{\binom{m}{2}} \mathrm{d}_{\frac{1}{2}}(L_0)$$

is not a square in $\mathcal{O}_{\mathfrak{p}}/\pi^2\mathcal{O}_{\mathfrak{p}}$, where $m := \operatorname{rank}_{\mathcal{O}_{\mathfrak{p}}}(L_0)$.

7.4 Idempotents

In this section we deal with idempotents in Clifford orders. Let us first remain in the local situation, which means that we consider an integral $\mathcal{O}_{\mathfrak{p}}$-lattice L in a regular quadratic $K_{\mathfrak{p}}$-space (V, q).

Theorem 7.4.1 *Let $\rho : \mathcal{C}(L) \to \mathcal{C}(L)/J(\mathcal{C}(L))$ be the natural epimorphism. We can lift idempotents from $\mathcal{C}(L)/J(\mathcal{C}(L))$, which is to say that*

1. *For every idempotent $\varepsilon \in \mathcal{C}(L)/J(\mathcal{C}(L))$ there is an idempotent $\mathfrak{e} \in \mathcal{C}(L)$ such that $\rho(\mathfrak{e}) = \varepsilon$ and*

2. *An idempotent $\mathfrak{e} \in \mathcal{C}(L)$ is primitive in $\mathcal{C}(L)$ if and only if $\rho(\mathfrak{e})$ is primitive in the quotient $\mathcal{C}(L)/J(\mathcal{C}(L))$.*

Moreover, if $\mathfrak{e}$ and $\mathfrak{f}$ are idempotents in $\mathcal{C}(L)$, the left $\mathcal{C}(L)$-modules $\mathcal{C}(L)\mathfrak{e}$ and $\mathcal{C}(L)\mathfrak{f}$ are isomorphic if and only if the left $\rho(\mathcal{C}(L))$-modules $\rho(\mathcal{C}(L)) \cdot \rho(\mathfrak{e})$ and $\rho(\mathcal{C}(L)) \cdot \rho(\mathfrak{f})$ are isomorphic.

Proof. This is the content of the theorems 6.7 and 6.8 of [CR87a]. □

With the help of this theorem we can now deduce a quantitative statement about the number of idempotents in $\mathcal{C}(L)$ from our previous results.

Theorem 7.4.2 *Consider a Jordan decomposition*

$$L \cong L_0 \oplus \pi \circ L_1 \oplus \pi^2 \circ L_2 \oplus ...$$

of the integral lattice L in the associated $K_{\mathfrak{p}}$-bilinear space (V, b_q).

If $2 \notin \mathfrak{p}$, the number of pairwise orthogonal primitive idempotents in a decomposition of 1 in $\mathcal{C}(L)$ is as follows.

$$\begin{array}{ll} 2^{(n-r)}/2 & \textit{if } \operatorname{rank}_{\mathcal{O}_{\mathfrak{p}}}(L_0) \textit{ is even,} \\ 2^{(n-r+1)/2} & \textit{if } \operatorname{rank}_{\mathcal{O}_{\mathfrak{p}}}(L_0) \textit{ is odd and } \mathrm{d}_{\pm}(L_0/\pi L_0) \in (\mathbb{F}_{\mathfrak{p}}^{\times})^2, \\ 2^{(n-r-1)/2} & \textit{if } \operatorname{rank}_{\mathcal{O}_{\mathfrak{p}}}(L_0) \textit{ is odd and } \mathrm{d}_{\pm}(L_0/\pi L_0) \notin (\mathbb{F}_{\mathfrak{p}}^{\times})^2. \end{array}$$

For the case where $2 \in \mathfrak{p}$, the quotient ring $\mathcal{C}(L)/J(\mathcal{C}(L))$ is always isomorphic to the matrix ring $\mathrm{Mat}_{2^{(n-r)/2}}(\mathbb{F}_{\mathfrak{p}})$, so that the number of idempotents is $2^{(n-r)/2}$.

We conclude this section by providing a constructive method to obtain a set of primitive orthogonal idempotents in the Clifford order of an integral lattice L over any integral domain R.

Proposition 7.4.3 *Let R be any commutative ring with unity and P a finitely generated free quadratic R-module. As usual, denote by $\mathbb{H}(P)$ the hyperbolic module on P. Putting $r := \operatorname{rank}_R(P)$, we have*

$$\mathcal{C}(\mathbb{H}(P)) \cong R^{2^r \times 2^r}.$$

Proof. See [Knu91, Proposition (2.1.1)], where a slightly more general result is proved. For $r = 1$, this statement may also be proved by elementary means. □

Lemma 7.4.4 *Let R be an integral domain and $\mathbb{H}$ the hyperbolic plane over R. There is a constructive method to obtain a decomposition of $1 \in \mathcal{C}\left(\bigoplus_{i=1}^{r} \mathbb{H}\right)$ into 2^r pairwise orthogonal primitive idempotents. All of these idempotents are of even degree.*

Proof. We prove this statement by induction on r. For $r = 1$, choose a basis $\{e, f\}$ for $\mathbb{H}$ satisfying $q(e) = q(f) = 0$ and $b_q(e, f) = 1$. Then, in $\mathcal{C}(\mathbb{H})$, we have

$$(ef)^2 = efef = e(-ef + 1)f = -e^2f^2 + ef = ef$$

and, analogously, $(fe)^2 = fe$. In addition, $ef + fe = 1$ and since $\mathcal{C}(\mathbb{H}) \cong R^{2\times 2}$, the idempotents ef and fe are primitive.

Now, let $r \geq 2$. By Theorem 3.6.13,

$$\mathcal{C}\left(\bigoplus_{i=1}^{r} \mathbb{H}\right) = \mathcal{C}\left(\bigoplus_{i=1}^{r-1} \mathbb{H} \oplus \mathbb{H}\right) \cong \mathcal{C}\left(\bigoplus_{i=1}^{r-1} \mathbb{H}\right) \mathbin{\widehat{\otimes}} \mathcal{C}(\mathbb{H}),$$

where, as before, the symbol $\widehat{\otimes}$ denotes the graded tensor product as defined in Definition 3.6.12.

By our induction hypothesis, in the tensor factor $\mathcal{C}(\bigoplus_{i=1}^{r-1} \mathbb{H})$, we find a set $\{\mathfrak{e}_1, ..., \mathfrak{e}_{2^{r-1}}\}$ of primitive orthogonal idempotents of even degree, whose sum is 1. For the hyperbolic

plane associated with the second tensor factor we choose a basis $\{e, f\}$ as in the case $r = 1$.
We claim that

$$\{\mathfrak{e}_i \otimes ef, \mathfrak{e}_i \otimes fe \mid 1 \leq i \leq 2^{r-1}\} \subseteq \mathcal{C}\left(\bigoplus_{i=1}^{r-1} \mathbb{H}\right) \mathbin{\widehat{\otimes}} \mathcal{C}(\mathbb{H})$$

is a set of idempotents with the desired properties.
All properties except for the primitivity are routine calculations using the definition of the grading and multiplication in a graded tensor product. Primitivity follows from the isomorphism $\mathcal{C}(\bigoplus_{i=1}^{r} \mathbb{H}) \cong R^{2^r \times 2^r}$ of Proposition 7.4.3. □

This method yields idempotents in $\mathcal{C}(L)$ in a constructive manner as soon as we have an algorithmic way of finding hyperbolic planes as orthogonal direct summands.

8 Algorithms and methods

In this chapter we describe some of the algorithms we used in our study of orthogonal representations. The descriptions are provided in pseudo-code so that all algorithms may be easily implemented in a suitable computer algebra system.

8.1 Invariant forms

G-invariant bilinear (and quadratic) forms are solutions of a system of linear equations, so in theory they can simply be computed by solving the respective system. However, with increasing group order and dimension of the representation, this approach is no longer feasible.
A more refined method is available in `Magma` via the command `InvariantForms()` for rational representations V. Roughly, this method works in the two following steps:

1. Compute the dimension of $\mathcal{F}_G(V)$ over an appropriate finite field, as explained on pages 45ff.

2. Pick a generating system E for the matrix group G on V. Apply the operator

$$\rho_E \ : \ \mathbb{Q}_{sym}^{\dim(V)\times\dim(V)} \to \mathbb{Q}_{sym}^{\dim(V)\times\dim(V)}, \ X \mapsto \frac{1}{|E|}\sum_{e\in E} eXe^{tr}$$

   until a G-invariant form is obtained. Since we already determined $\dim_{\mathbb{Q}}(\mathcal{F}_G(V))$ we know when we have computed the whole space of G-invariant bilinear forms. This iterative process is explained in greater detail in [PS96].

We apply this method together with `Magma`'s relatively fast handling of rational representations of finite groups in order to determine G-invariant forms on representations over number fields in the following algorithm.

Algorithm 8.1.1 `Invariant Form(`χ`)`
Input: The character χ of a uniform representation V over a totally real number field K.
Output: A G-invariant form on V as a matrix with entries in K.

```
$F \leftarrow \mathbb{Q}[\chi]$.
$V \leftarrow$ the irred. $\mathbb{Q}G$-module whose character contains $\chi$.
$M \leftarrow$ an invertible element of $\mathcal{F}_G(V)$.
$E \leftarrow \mathrm{End}_{\mathbb{Q}G}(V)$.
$e \leftarrow$ an element of $E$ with minimal polynomial $\mu$ of degree $[F : \mathbb{Q}]$.
Factorize $\mu = \mu_1 \cdot \overline{\mu}$ over $F$, $\deg(\mu_1) = 1$.
Compute $r, s \in F[X]$ such that $r\mu_1 + s\overline{\mu} = \gcd(\mu_1, \overline{\mu}) = 1$.
$q \leftarrow r\mu_1(e)$, $p \leftarrow 1 - q$.
$T \leftarrow$ a basis matrix of the images of $p$ and $q$ as linear maps.
$M_0 \leftarrow T \cdot M \cdot T^{tr}$.
return The top left $[F : \mathbb{Q}] \times [F : \mathbb{Q}]$-submatrix of $M_0$.
```

8.2 Clifford invariants

The following algorithm is based on the following three facts and results.

1. The Clifford invariant may be computed locally for each prime $\mathfrak{p}$ of K, as mentioned in Remark 3.6.19.

2. There are only finitely many places where the local Clifford invariant is not trivial, cf. Corollary 7.2.5.

3. At each of the remaining places where the local Clifford invariant may be non-trivial, we apply the formula from Theorem 3.6.23.

The only prerequisite for this algorithm is a procedure `QuaternionSymbol`$(a, b, \mathfrak{p})$ which determines the local quaternion symbol (a, b) in $\mathrm{Br}(K_\mathfrak{p})$ as a value in $\{\pm 1\}$.

Algorithm 8.2.1 `CliffordInvariant`(A, d)

Input: A symmetric matrix A and a parameter $d \in K$ so that $\mathfrak{p} \mid d$ for all ramified places $\mathfrak{p}$ of the Clifford algebra.

Output: The ramified places of the Clifford algebra.

```
$\mathcal{D} \leftarrow$ a diagonalization of $A$.
$D \leftarrow$ the diagonal of $\mathcal{D}$.
$n \leftarrow$ the number of rows of $A$.
if $n$ is even then
    $m \leftarrow \frac{n}{2}$
else
    $m \leftarrow \frac{n+1}{2}$
end if
$r \leftarrow m - 1$, $s \leftarrow \frac{m(m-1)}{2}$
$d \leftarrow \prod_{x \in D} x$
```

```
PLACES ← [ ]
$f$ ← the prime ideals dividing $2 \cdot d$ and the infinite places of $K$.
for $\mathfrak{p} \in f$ do
    $c \leftarrow 1$
    for $1 \leq i \leq n-1$ do
        for $i+1 \leq j \leq n$ do
            $c \leftarrow c \cdot$QuaternionSymbol($D_i, D_j, \mathfrak{p}$)
        end for
    end for
    if $r \equiv 1 \pmod 2$ then
        $c \leftarrow c \cdot$QuaternionSymbol($-1, d, \mathfrak{p}$)
    end if
    if $s \equiv 1 \pmod 2$ then
        $c \leftarrow c \cdot$QuaternionSymbol($-1, -1, \mathfrak{p}$)
    end if
    if $c = -1$ then
        Append $\mathfrak{p}$ to PLACES.
    end if
end for
return PLACES.
```

8.3 Characters on Clifford algebras and square roots of characters

The relation between the coefficients of the characteristic polynomial and the traces of exterior powers mentioned in the proof of Remark 4.3.22 allows one to derive the recursion formula

$$\mathrm{tr}\left(\bigwedge^{k}\Delta(g)\right) = \frac{1}{k}\sum_{m=1}^{k}(-1)^{m-1}\mathrm{tr}(\Delta(g^m))\mathrm{tr}\left(\bigwedge^{k-m}\Delta(g)\right)$$

for a representation Δ.

With this formula in mind, one easily writes a procedure `ExteriorPowers`(χ) to obtain all i-th exterior powers of χ for $0 \leq i \leq \chi(1)$.

A procedure `CliffordCharacter`(χ) for the character of the G-module $c(\chi)$ on the (full or even) Clifford algebra associated to χ is then readily obtained from the formulas in Remark 4.3.18.

In order to apply Nebe's character method it is necessary to find the square roots of the character on $c(\chi)$. This may be done with the following program. Notice that the input of the program includes both the character whose square roots we seek and the group of which it is a character. That is because for Nebe's method to function one often has to pass from G to the covering group $2.G$.

In the formulation of this algorithm assume a character χ to be a list with as many entries as G has conjugacy classes, the first entry being the value of the character on the neutral element of G.

Algorithm 8.3.1 `Roots`(χ, G)

Input: A character χ of a group G.

Output: All possible square roots of χ in the character ring of G.

```
RESULT $\leftarrow$ [ ], VALUES $\leftarrow$ [ ].
$r \leftarrow$ the number of conjugacy classes of $G$.
Append the list $[\sqrt{\chi(1)}]$ to VALUES.
for $2 \leq i \leq r$ do
    if $\chi_i = 0$ then
        Append the list [0] to VALUES.
    else
        Append the list $[\sqrt{\chi_i}, -\sqrt{\chi_i}]$ to VALUES.
    end if
end for
for $s \in \{1, -1\}^{r-1}$ do
    $c \leftarrow [\sqrt{\chi(1)}]$.
    for $2 \leq i \leq r$ do
        Append $s_i \cdot \mathrm{VALUES}_i$ to $c$.
    end for
    if $c$ is a character of $G$ then
        Append $c$ to RESULT.
    end if
end for
return RESULT.
```

Remark 8.3.2 In order to improve the readability of our pseudo-code, we have omitted a very simple, and yet important, optimization. One should not have s iterate over $\{\pm 1\}^{r-1}$ but merely over the cartesian product with as many factors as χ has non-zero values.

Further optimization may be achieved by programming the conditions of Remark 4.3.23 into this procedure.

This is not a particularly fast algorithm and in some cases – depending on the degree of χ and the number of conjugacy classes of G – it may be advantageous to attempt another method to find the square roots, which we briefly explain now.

Algorithm 8.3.3 `RootsAlternative`(χ, C)

Input: A character χ and the respective character table C.

Output: All possible square roots of χ in the character ring of G.

```
RESULT ← [ ].
$L \leftarrow$ the list of the degrees of the irreducible characters in $C$.
Find all $(a_1, ..., a_{|C|}) \in \mathbb{N}^{|C|}$ such that $\sum_{i=1}^{|C|} a_i L_i = \sqrt{\chi(1)}$.        (†)
for all $(a_1, ..., a_{|C|})$ satisfying (†) do
    if $\left(\sum_{i=1}^{|C|} a_i C_i\right)^2 = \chi$ then
        Append $\sum_{i=1}^{|C|} a_i C_i$ to RESULT.
    end if
end for
return RESULT.
```

Remark 8.3.4 Again, we have simplified the algorithm for the sake of readability. Possible improvements include the inclusion of Remark 4.3.23, taking zero values of χ and rationality conditions into account and restricting the multiplicity of the trivial character in the possible roots by $\left\lfloor \sqrt{(\chi, \mathbb{1})_G} \right\rfloor$. All of this leads to more constrained equations and thereby restricts the possible candidates which are to be tested.

8.4 Radical idealizers

For our studies of radicals and idealizers of Clifford orders, we conducted experiments with the following algorithms described in [NS09].

Algorithm 8.4.1 `p-radical`(Λ, p), [NS09, Algorithm (1)]

Input: An order Λ in a finite-dimensional semisimple $\mathbb{Q}$-algebra $\mathfrak{A}$, given in its right regular representation and a prime p. The order Λ should be entered in the form of as many as $d := \dim_{\mathbb{Q}}(\mathfrak{A})$ integer matrices $B^{(1)}, ..., B^{(d)}$.

Output: The p-local Jacobson radical of Λ, i.e., the intersection of all maximal right ideals of Λ which contain $p\Lambda$.

```
$E \leftarrow \langle B^{(i)} + p\mathbb{Z}^{d \times d} \mid 1 \leq i \leq d \rangle_{\mathbb{F}_p}$.
Determine all maximal submodules of the natural module of the $\mathbb{F}_p$-algebra $E$.
$\overline{J} \leftarrow$ the intersection of these maximal submodules.
Compute the preimage $J$ of $\overline{J}$ under $\Lambda \twoheadrightarrow \Lambda/p\Lambda$.
return A basis matrix of $J$.
```

With the next algorithm one can then determine the idealizer of the p-radical of Λ, providing as input the basis matrix we just computed, together with the prime number p.

Algorithm 8.4.2 `idealizer`(Λ, T, p), [NS09, Algorithm (1)]

Input: An order Λ in a finite-dimensional semisimple $\mathbb{Q}$-algebra $\mathfrak{A}$, given in its right regular representation and a basis matrix T of $J_p(\Lambda)$.

Output: A basis matrix of the idealizer of $J_p(\Lambda)$ in $\mathfrak{A}$.

```
Compute $C^{(1)}, ..., C^{(d)} \in \mathbb{Z}^{d \times d}$ s.t. $C^{(i)}_{j,k} = B^{(j)}_{i,k}$ for all $1 \leq i, j, k \leq d$.
$X \leftarrow$ a matrix with $d^2$ columns and 0 rows.
$Y \leftarrow$ a matrix with $d^2$ columns and 0 rows.
**for** $1 \leq i \leq d$ **do**
    Compute $TB^{(i)}T^{-1}$ and obtain a coordinate row vector for this matrix.
    Add this row vector as a new row to $X$.
    Do the same with $C^{(i)}$ and the matrix $Y$.
**end for**
$Z \leftarrow$ the matrix $(X|Y)$.
$K \leftarrow$ a basis matrix of the nullspace of $Z$.
Vertically append a $d \times d$-unit matrix multiplied by $p$ to $K$.
$M \leftarrow$ a basis matrix of the $\mathbb{Z}$-row space of $K$.
**return** $\frac{1}{p} \cdot M$.
```

Remark 8.4.3 1. The algorithm `idealizer` is formulated assuming that the user does linear algebra with rows.

2. In the first step one computes the left regular representation of Λ.

3. The following steps are a concrete moethod to determine

$$O_l(J) \cap O_r(J) = \left\langle \frac{1}{p} T B^{(i)} T^{-1} \mid 1 \leq i \leq d \right\rangle_{\mathbb{Z}} \cap \left\langle \frac{1}{p} T C^{(j)} T^{-1} \mid 1 \leq j \leq d \right\rangle_{\mathbb{Z}} \cap \mathbb{Z}^{d \times d}.$$

9 Computational results and examples

In this last chapter we present an application of the known techniques and results by computing the discriminants and Clifford invariants of a number of uniform representations over their respective character fields. We use the Atlas [CCN+85] in order to have a suitably large number of examples at hand.

9.1 How to read the tables

Layout of the tables

The results for the Atlas-groups are contained in tables. Each row corresponds to one (or several) characters. A typical row of a table may look like this:

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_5	21	$+$	$\mathbb{Q}$	a	$(-1,-1)$	$\chi_5 = \bigwedge^2 \chi_2$

This is the row for the fifth character of the Alternating Group A_8 (the numbering of characters is adapted from [CCN+85]).
From left to right, the columns contain the designation of the character (χ_5), its degree (21), its Frobenius-Schur indicator (+), its character field ($\mathbb{Q}$), the discriminant of a regular G-invariant form (in this case the character is of odd degree, so we write down a parameter a as its discriminant because by scaling any discriminant can be attained), the Clifford invariant of a regular G-invariant form ($(-1,-1)$) and the method which we have used to obtain this information.

Special characters

Given our various results, we designate characters with relevant features in the tables according to the following rules.

$\{\!\{\chi_r, \chi_s\}\!\}$ indicates that the two characters χ_r and χ_s are Galois conjugate, so the same holds for their invariants by Proposition 4.2.16. Therefore we include only one row in the table.

$\llbracket \chi_r, \chi_s \rrbracket$ is the notation we use for the situation where the two characters χ_r and χ_s are in the same orbit under the action of $\mathrm{Out}(G)$. By Proposition 4.2.13 these two characters have identical invariants, so we summarize the relevant information in a single row.

Recall the results of Section 4.3.4: if the character χ is not real-valued, $\chi + \overline{\chi}$ is the character of a uniform representation and in many cases all invariants can be read off from the character field alone. A typical table entry for such a situation may look like this:

$\chi_3 + \chi_4$	$10 + 10$	0	$\mathbb{Q}(\sqrt{-7})$	1	$(-7, -1)$

This means that the group in question has a character of degree 10 with values in $\mathbb{Q}(\sqrt{-7})$ giving rise to a 20-dimensional uniform representation with discriminant 1 and Clifford invariant $(-7, -1)$.

If χ is a real-valued character with Schur index not equal to 1 – in which case it is equal to 2 – we can consider the representation of G with character 2χ. That representation is uniform if the real Schur index is 2, i.e., the Frobenius-Schur indicator is $-$. In our tables we have denoted such a situation as follows.

$2 \cdot \chi_2$	$2 \cdot 6$	$-$	$\mathbb{Q}$	1	$(-1, -3)$

The meaning of this is that the group G has a character χ of degree 6 with Frobenius-Schur indicator $-$. On the 12-dimensional representation over its character field, which is $\mathbb{Q}$, there is a G-invariant form with discriminant 1 and Clifford invariant $(-1, -3)$.

An entry of the form - means that the method we applied did not yield any result. This may happen when we apply some technique to find the determinant, which does not provide any insight to what the Clifford invariant might be. In contrast, in most cases where we apply a brute-force computation to find the Gram matrix of a G-invariant form, we indicate findings on both invariants.

It may happen that we combine some of these notations, cf. the group $U_3(4)$, for example.

Covering groups

We also discuss the covering groups of the Atlas-groups, which is to say groups of the form $m.G$ for a natural number m and a finite simple group G. This designates a group $\widetilde{G}$ containing a cyclic normal subgroup U of order m such that the quotient $\widetilde{G}/U$ is isomorphic to G.

In keeping with the notation of [CCN+85] we designate complex characters of such extensions with the symbol $0n$ in the indicator column. In this situation n is the value of Euler's totient function at m and the meaning of this notation is that a single row describes n Galois-conjugate characters.

The methods

We abbreviate the methods we apply with the following symbols.

$-$: We use this symbol for the trivial character only, where the results are always the same and there is no method to be applied.

r. U: We obtain the relevant information by restricting the character to the specified subgroup U. This is in reference to Section 4.3.1.

p. $\chi_1 + \chi_r$: This indicates that $\chi_1 + \chi_r$ is the character of a permutation representation of G and we apply Proposition 4.3.2.

$\chi_t = \chi_r \chi_s$, $\chi_t = \bigwedge^2 \chi_i$: An equation of such a type is meant to indicate that the character χ_t may be obtained as a tensor product or exterior square of some other character whose invariants we already know. We apply the results of Section 4.3.3.

4.3.9: The character in question has totally complex values and Theorem 4.3.9 is applied to it.

N. χ_i: This symbol is used for a successful application of Nebe's character method, where we have found the character χ_i to be a constituent of odd multiplicity in the character of the simple $\mathcal{C}(\varphi)$-module.

5.1.3: We apply Theorem 5.1.3 to a character with Schur index 2.

`Magma`: We use a brute-force computation to obtain the Gram matrix of a G-invariant form and have `Magma` [BCP97] determine the discriminant and/or Clifford invariant.

9.2 Atlas groups

Here we catalog the invariants, i.e. the discriminant and Clifford invariant, of the G-invariant forms on uniform modules for the finite simple groups in the Atlas [CCN+85], up to order $200,000$. In addition we include the covering groups of these groups.
We omit all groups of the form $L_2(q)$ (in Atlas-notation), as we have already treated them in Section 6.4 and Section 6.5.

Concretely, up to order $200,000$, we have omitted the following groups:

$L_2(5)$, $L_2(7)$, $L_2(9)$, $L_2(8)$, $L_2(11)$, $L_2(13)$, $L_2(17)$, $L_2(19)$, $L_2(16)$, $L_2(23)$, $L_2(25)$, $L_2(27)$, $L_2(29)$, $L_2(31)$ and $L_2(32)$.

The orthogonal representations of the groups M_{11} and $U_4(2)$ were already classified in [Neb99]. We reproduce Nebe's results here.

Although we endeavored to use as few brute-force computations as possible, we have not always been able to avoid them. The groups $L_3(4)$, $Sz(8)$, M_{12} and J_1 were especially problematic in this regard.
Nonetheless, we underline the usefulness of our methods by providing some examples of orthogonal representations of groups of order greater than $200,000$, namely $O_8^+(2)$, M_{24}, M^cL, $R(27)$, $S_8(2)$ and Co_3.

We consulted [ABL+] to obtain representations of some of the groups for explicit computations with characters.

For the first three groups we give detailed proofs. After that we use the abovementioned abbreviations to indicate which methods we applied.

9.2.1 A_7

$|G| = 2,520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$, $H^2(G, \mathbb{C}^\times) \cong C_6$, $\mathrm{Out}(G) \cong C_2$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$
χ_1	1	+	$\mathbb{Q}$	a	$(1,1)$
χ_2	6	+	$\mathbb{Q}$	-7	$(-7,a)$
$\chi_3+\chi_4$	$10+10$	0	$\mathbb{Q}(\sqrt{-7})$	1	$(-7,-1)=[\mathcal{Q}_{7,\infty}]$
χ_5	14	+	$\mathbb{Q}$	-3	-
χ_6	14	+	$\mathbb{Q}$	-15	-
χ_7	15	+	$\mathbb{Q}$	a	$(-1,7)=[\mathcal{Q}_{2,7}]$
χ_8	21	+	$\mathbb{Q}$	a	$(-1,-3)=[\mathcal{Q}_{3,\infty}]$
χ_9	35	+	$\mathbb{Q}$	a	$(-1,-1)=[\mathcal{Q}_{2,\infty}]$

$a \in \mathbb{Q}^\times$.

Proof. There is nothing to show for the trivial character.

$\mathbb{1}_G + \chi_2$ is the character of a permutation module (given by the action on the cosets A_7/A_6) and therefore we obtain $\mathrm{d}_\pm(\chi_2) = -7$ and $\mathfrak{c}(\chi_2) = (-7, a)$ for some $a \in \mathbb{Q}^\times$.

The discriminant and Clifford invariant of an invariant form on a $\mathbb{Q}A_7$-module with character $\chi_3 + \chi_4$ is obtained using Theorem 4.3.9.

A_7 has two conjugacy classes of maximal subgroups isomorphic to $\mathrm{PSL}_2(7)$. The permutation modules on the respective coset spaces both have the character $\mathbb{1}_G + \chi_6$, giving us the fifth row of the table.

The restriction of χ_5 to either one of the conjugacy classes of maximal subgroups isomorphic to $\mathrm{PSL}_2(7)$ is the sum of two unique irreducible characters of degrees 6 and 8, which yields $\mathrm{d}_\pm(\chi_5) = -3$.

The character χ_7 is the exterior square of χ_2, so $\mathfrak{c}(\chi_7) = (-1, 7)$ by Theorem 4.3.4.

Now let φ be an orthogonal $\mathbb{Q}G$-module with character χ_8. The group A_7 has a maximal subgroup isomorphic to $\mathrm{PSL}_2(9)$. The restriction of χ_8 to that subgroup is $\xi + \theta_2 + \theta_4$, where $\xi \in \{\xi_1, \xi_2\}$, in the notation of Section 6.4. Since 9 is a square, we have $\mathfrak{c}(\theta_2) = \mathfrak{c}(\theta_4) = 1$ and $\mathrm{d}_\pm(\theta_2) = \mathrm{d}_\pm(\theta_4) = 1$. Therefore

$$\mathfrak{c}(\chi_8) = \mathfrak{c}(\xi)\mathfrak{c}(\theta_2)\mathfrak{c}(\theta_4) = \mathfrak{c}(\xi) = [\mathcal{Q}_{3,\infty}] = (-1, -3).$$

For the character χ_9 none of our methods are applicable, so we perform a calculation with `Magma` in order to explicitly construct an invariant form and obtain the last row of the table. □

$2.A_7$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$\chi_{10}+\chi_{11}$	$4+4$	0	$\mathbb{Q}(\sqrt{-7})$	1	$(1,1)$	4.3.9
$[\![2\cdot\chi_{12}, 2\cdot\chi_{13}]\!]$	$2\cdot 14$	$-$	$\mathbb{Q}(\sqrt{2})$	1	$[\mathcal{Q}_{\infty_1,\infty_2}]$	5.1.3
$2\cdot\chi_{14}$	$2\cdot 20$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3
$2\cdot\chi_{15}$	$2\cdot 20$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3
$2\cdot\chi_{16}$	$2\cdot 36$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3

$3.A_7$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_{17}	$6+6$	02	$\mathbb{Q}(\sqrt{-3})$	1	$(-1,-3)$	4.3.9
χ_{18}	$15+15$	02	$\mathbb{Q}(\sqrt{-3})$	-3	-	4.3.9
χ_{19}	$15+15$	02	$\mathbb{Q}(\sqrt{-3})$	-3	-	4.3.9
χ_{20}	$21+21$	02	$\mathbb{Q}(\sqrt{-3})$	-3	-	4.3.9
χ_{21}	$21+21$	02	$\mathbb{Q}(\sqrt{-3})$	-3	-	4.3.9
$\{\!\{\chi_{22}, \chi_{23}\}\!\}$	$24+24$	02	$\mathbb{Q}(\sqrt{21})(\sqrt{-7})$	1	-	4.3.9

$6.A_7$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$\{\!\{\chi_{24}, \chi_{25}\}\!\}$	$6+6$	02	$\mathbb{Q}(\sqrt{2})(\sqrt{-3})$	1	$[\mathcal{Q}_{\infty_1,\infty_2}]$	4.3.9
$\{\!\{\chi_{26}, \chi_{27}\}\!\}$	$24+24$	02	$\mathbb{Q}(\sqrt{21})(\sqrt{-7})$	1	-	4.3.9
χ_{28}	$36+36$	02	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$	4.3.9

Remark 9.2.1 The Clifford invariant of χ_{28} was computed with `Magma`.

9.2.2 $L_3(3)$

$|G| = 5,616 = 2^4 \cdot 3^3 \cdot 13$, $H^2(G, \mathbb{C}^\times) \cong \{1\}$, $\mathrm{Out}(G) \cong C_2$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$
χ_1	1	+	$\mathbb{Q}$	a	$(1,1)$
χ_2	12	+	$\mathbb{Q}$	13	$(13,a)(-1,-1)$
χ_3	13	+	$\mathbb{Q}$	a	$(-1,-1) = [\mathcal{Q}_{2,\infty}]$
$\chi_4+\chi_5$	$16+16$	0	$\mathbb{Q}(\sqrt{13})(\sqrt{\delta})$	1	$(1,1)$
$\chi_6+\chi_7$	$16+16$	0	$\mathbb{Q}(\sqrt{13})(\sqrt{\delta})$	1	$(1,1)$
χ_8	26	+	$\mathbb{Q}$	-3	-
$\chi_9+\chi_{10}$	$26+26$	+	$\mathbb{Q}(\sqrt{-2})$	1	$(-1,-1) = [\mathcal{Q}_{2,\infty}]$
χ_{11}	27	+	$\mathbb{Q}$	a	$(-1,-1) = [\mathcal{Q}_{2,\infty}]$
χ_{12}	39	+	$\mathbb{Q}$	a	$(1,1)$

$a \in \mathbb{Q}^\times$, $\delta = -\frac{3}{2}\sqrt{13} - \frac{13}{2}$.

Proof. $\mathbb{1}_G + \chi_2$ is the character of a 13-dimensional permutation module, so there is an orthogonal $\mathbb{Q}G$-module φ with character χ_2, isometric to $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{A}_{12}$. Since $\mathrm{d}_{\pm}(\varphi) = 13$ and $\mathfrak{c}(\varphi) = (-1,-1)$, we obtain the second row of the table by consulting Example 3.6.25 and combining it with the formula of Proposition 3.6.24, 1.

The character field $\mathbb{Q}[\chi_4]$ is easily determined. As $\chi_4(1) = 16$, the discriminant of an orthogonal $\mathbb{Q}(\sqrt{13})G$-module with character $\chi_4 + \chi_5$ is a square by Theorem 4.3.9. As χ_4 is absolutely irreducible modulo 2 and modulo 13 and 3 is a norm of the extension $\mathbb{Q}(\sqrt{13}, \sqrt{\delta})/\mathbb{Q}(\sqrt{13})$, the discriminant of a G-invariant Hermitian form on a $\mathbb{Q}(\sqrt{13})(\sqrt{\delta})G$-module is 1, so we also obtain a trivial Clifford invariant. The row for $\chi_6 + \chi_7$ exhibits identical behavior by the same argument.

Extend the character χ_8 to $G.2$, which has a maximal subgroup isomorphic to $C_{13} \rtimes C_6$, which is of the kind of groups studied in Section 6.3 of this thesis. The restriction of χ_8 to that maximal subgroup is isomorphic to $\mathbb{Q}(\zeta_{13}) \oplus \mathbb{Q}(\zeta_{13}) \oplus \mathbb{Q}(\zeta_\ell)$, with $\ell \in \{3, 6\}$. Either case yields the result that the determinant of a G-invariant bilinear form is 3.
For the Clifford invariants of χ_3, χ_{11} and χ_{12} we explicitly constructed the G-invariant forms with Magma and computed the respective Clifford invariants. □

9.2.3 $U_3(3) \cong G_2(2)'$

$|G| = 6,048 = 2^5 \cdot 3^3 \cdot 7$, $H^2(G, \mathbb{C}^\times) \cong \{1\}$, $\mathrm{Out}(G) \cong C_2$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$
χ_1	1	$+$	$\mathbb{Q}$	a	$(1,1)$
$2 \cdot \chi_2$	$2 \cdot 6$	$-$	$\mathbb{Q}$	1	$(-1,-3) = [\mathcal{Q}_{3,\infty}]$
χ_3	7	$+$	$\mathbb{Q}$	a	$(1,1)$
$\chi_4 + \chi_5$	$7+7$	0	$\mathbb{Q}(\sqrt{-1})$	-1	$(-1,a)$
χ_6	14	$+$	$\mathbb{Q}$	-3	-
χ_7	21	$+$	$\mathbb{Q}$	a	$(-1,-1) = [\mathcal{Q}_{2,\infty}]$
$\chi_8 + \chi_9$	$21+21$	0	$\mathbb{Q}(\sqrt{-1})$	-1	$(-1,a)$
χ_{10}	27	$+$	$\mathbb{Q}$	a	$(-1,-1) = [\mathcal{Q}_{2,\infty}]$
$\chi_{11} + \chi_{12}$	$28+28$	0	$\mathbb{Q}(\sqrt{-1})$	1	$(1,1)$
$\chi_{13} + \chi_{14}$	$32+32$	0	$\mathbb{Q}(\sqrt{-7})$	1	$(1,1)$

$a \in \mathbb{Q}^\times$.

Proof. The 12-dimensional $\mathbb{Q}$-linear representation U with character $2\chi_2$ has discriminant 1 and Clifford invariant $[\mathrm{End}_{\mathbb{Q}G}(U)] = (-1,-3)$ by Theorem 5.1.3.
G has a maximal subgroup isomorphic to $\mathrm{PSL}_2(7)$ and the restriction of χ_3 to that subgroup is the irreducible character $\mathrm{St}_{\mathrm{PSL}_2(7)}$, so $\mathfrak{c}(\chi_7) = 1$.
As the characters χ_4 and χ_5 are totally complex with character fields $\mathbb{Q}(\sqrt{-1})$, we obtain the discriminant and Clifford invariant in row 4 from Theorem 4.3.9. The same holds for the seventh row of the table.
χ_6 restricts to the maximal subgroup $\mathrm{PSL}_2(7)$ as $\eta_1 + \eta_2 + \chi_2$, so $\mathrm{d}_\pm(\chi_6) = -3$. This provides us with no usable information on the Clifford invariant, which is not invariant under scaling in this case, so we leave the respective portion of the table empty.
$\mathbb{1}_G + \chi_{10}$ is the character of a permutation module, so $\mathfrak{c}(\chi_{10}) = (-1,-1)$.
The last two rows are once again obtained from Theorem 4.3.9.
For χ_7 we perform a computation with Magma and find $\mathfrak{c}(\chi_7) = (-1,-1)$. □

9.2.4 M_{11}

$|G| = 7,920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$, $H^2(G, \mathbb{C}^\times) \cong \{1\}$, $\mathrm{Out}(G) \cong \{1\}$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$
χ_1	1	+	$\mathbb{Q}$	a	$(1,1)$
χ_2	10	+	$\mathbb{Q}$	-10	$(11,11)(-11,a)$
$\chi_3+\chi_4$	$10+10$	0	$\mathbb{Q}(\sqrt{-2})$	1	$(-1,-1)$
χ_5	11	+	$\mathbb{Q}$	a	$(-1,-1)$
$\chi_6+\chi_7$	$16+16$	0	$\mathbb{Q}(\sqrt{-11})$	1	$(1,1)$
χ_8	44	+	$\mathbb{Q}$	5	$(-1,-1)(5,a)$
χ_9	45	+	$\mathbb{Q}$	a	$(-1,-1)$
χ_{10}	55	+	$\mathbb{Q}$	a	$(1,1)$

$a \in \mathbb{Q}^\times$.

This table is quoted from [Neb99, Beispiel 3.5.2].

9.2.5 $A_8 \cong L_4(2)$

Other descriptions: $\mathrm{GL}_4(2) \cong \mathrm{PGL}_4(2) \cong \mathrm{PSL}_4(2)$.
$|G| = 20,160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$, $H^2(G, \mathbb{C}^\times) \cong C_2$, $\mathrm{Out}(G) \cong C_2$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_1	1	+	$\mathbb{Q}$	a	$(1,1)$	-
χ_2	7	+	$\mathbb{Q}$	a	$(1,1)$	p. $\chi_1+\chi_2$
χ_3	14	+	$\mathbb{Q}$	-15	$(-15,a)$	p. $\chi_1+\chi_3$
χ_4	20	+	$\mathbb{Q}$	21	-	r. A_7
χ_5	21	+	$\mathbb{Q}$	a	$(-1,-1)$	$\chi_5 = \bigwedge^2 \chi_2$
$\chi_6+\chi_7$	$21+21$	0	$\mathbb{Q}(\sqrt{-15})$	-15	$(-15,a)$	4.3.9
χ_8	28	+	$\mathbb{Q}$	5	-	r. A_7
χ_9	35	+	$\mathbb{Q}$	a	$(-1,-1)$	r. A_7
$\chi_{10}+\chi_{11}$	$45+45$	0	$\mathbb{Q}(\sqrt{-7})$	-7	$(-7,a)$	4.3.9
χ_{12}	56	+	$\mathbb{Q}$	5	$(-1,-3)(5,a)$	`Magma`
χ_{13}	64	+	$\mathbb{Q}$	105	$(3,5)(105,a)$	`Magma`
χ_{14}	70	+	$\mathbb{Q}$	-3	-	$\chi_2\chi_3 = \chi_8+\chi_{14}$

$a \in \mathbb{Q}^\times$.

$2.A_8$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_{15}	8	$+$	$\mathbb{Q}$	1	$(1,1)$	r. $2.A_7$
$\chi_{16}+\chi_{17}$	$24+24$	0	$\mathbb{Q}(\sqrt{-7})$	1	$(1,1)$	4.3.9
$2\cdot\chi_{18}$	$2\cdot 48$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3
$\chi_{19}+\chi_{20}$	$56+56$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$	4.3.9
$\chi_{21}+\chi_{22}$	$56+56$	0	$\mathbb{Q}(\sqrt{-15})$	1	$(1,1)$	4.3.9
$2\cdot\chi_{23}$	$2\cdot 64$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3

9.2.6 $L_3(4)$

Non-ATLAS-description: $\mathrm{PSL}_3(4)$.
$|G| = 20,160 = 2^6\cdot 3^2\cdot 5\cdot 7$, $H^2(G,\mathbb{C}^\times)\cong C_3\times C_4\times C_4$, $\mathrm{Out}(G)\cong D_{12}$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_1	1	$+$	$\mathbb{Q}$	a	$(1,1)$	-
χ_2	20	$+$	$\mathbb{Q}$	21	$(-1,-1)(21,a)$	p. $\chi_1+\chi_2$
$[\![\chi_3,\chi_4,\chi_5]\!]$	35	$+$	$\mathbb{Q}$	a	$(-1,-3)$	`Magma`
$\chi_6+\chi_7$	$45+45$	0	$\mathbb{Q}(\sqrt{-7})$	-7	$(-7,a)$	4.3.9
$[\![\chi_8,\chi_9]\!]$	63	$+$	$\mathbb{Q}(\sqrt{5})$	b	$(1,1)$	`Magma`
χ_{10}	64	$+$	$\mathbb{Q}$	105	$(105,a)$	`Magma`

$a\in\mathbb{Q}^\times$, $b\in\mathbb{Q}(\sqrt{5})^\times$.

$2.L_3(4)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$\chi_{11}+\chi_{12}$	$10+10$	0	$\mathbb{Q}(\sqrt{-7})$	1	$(-2,-7)$	4.3.9
$[\![\chi_{13},\chi_{14}]\!]$	28	$+$	$\mathbb{Q}(\sqrt{5})$	1	$[\mathcal{Q}_{\infty_1,\infty_2}]$	`Magma`
χ_{15}	36	$+$	$\mathbb{Q}$	1	$(-2,-7)$	`Magma`
χ_{16}	64	$+$	$\mathbb{Q}$	1	$(1,1)$	`Magma`
χ_{17}	70	$+$	$\mathbb{Q}$	-1	$(-1,a)$	`Magma`
χ_{18}	90	$+$	$\mathbb{Q}$	-1	$(-1,a)$	`Magma`

$a\in\mathbb{Q}^\times$.

$4_1.L_3(4)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$[\![\chi_{19},\chi_{20}]\!]$	$8+8$	02	$\mathbb{Q}(\sqrt{5})(\sqrt{-1})$	1	-	4.3.9
χ_{21}	$56+56$	02	$\mathbb{Q}(\sqrt{-1})$	1	$(1,1)$	4.3.9
χ_{22}	$64+64$	02	$\mathbb{Q}(\sqrt{-1})$	1	$(1,1)$	4.3.9
$[\![\chi_{23},\chi_{24}]\!]$	$80+80$	02	$\mathbb{Q}(\sqrt{7})(\sqrt{-1})$	1	-	4.3.9

$4_2.L_3(4)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_{25}	$20+20$	02	$\mathbb{Q}(\sqrt{-1})$	1	$(1,1)$	4.3.9
$\llbracket\chi_{26},\chi_{27}\rrbracket$	$28+28$	02	$\mathbb{Q}(\sqrt{5})(\sqrt{-1})$	1	-	4.3.9
χ_{28}	$36+36$	02	$\mathbb{Q}(\sqrt{-1})$	1	$(1,1)$	4.3.9
χ_{29}	$64+64$	02	$\mathbb{Q}(\sqrt{-1})$	1	$(1,1)$	4.3.9
$\llbracket\chi_{30},\chi_{31}\rrbracket$	$80+80$	02	$\mathbb{Q}(\sqrt{7})(\sqrt{-1})$	1	-	4.3.9

$3.L_3(4)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$\llbracket\chi_{32},\chi_{33},\chi_{34}\rrbracket$	$15+15$	02	$\mathbb{Q}(\sqrt{-3})$	-3	-	4.3.9
χ_{35}	$21+21$	02	$\mathbb{Q}(\sqrt{-3})$	-3	-	4.3.9
$\llbracket\chi_{36},\chi_{37}\rrbracket$	$45+45$	02	$\mathbb{Q}(\sqrt{21})(\sqrt{-3})$	-3	-	4.3.9
$\llbracket\chi_{38},\chi_{39}\rrbracket$	$63+63$	02	$\mathbb{Q}(\sqrt{5})(\sqrt{-3})$	-3	-	4.3.9
χ_{40}	$84+84$	02	$\mathbb{Q}(\sqrt{-3})$	1	$(3,5)$	4.3.9

$6.L_3(4)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_{41}	$6+6$	02	$\mathbb{Q}(\sqrt{-3})$	1	$(-1,-3)$	4.3.9
χ_{42}	$36+36$	02	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$	4.3.9
$\llbracket\chi_{43},\chi_{44}\rrbracket$	$42+42$	02	$\mathbb{Q}(\sqrt{5})(\sqrt{-3})$	1	-	4.3.9
$\llbracket\chi_{45},\chi_{46}\rrbracket$	$60+60$	02	$\mathbb{Q}(\sqrt{21})(\sqrt{-3})$	1	-	4.3.9
χ_{47}	$90+90$	02	$\mathbb{Q}(\sqrt{-3})$	1	$(-1,-3)$	4.3.9

$12_1.L_3(4)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$\llbracket\chi_{48},\chi_{49}\rrbracket$	$24+24$	04	$\mathbb{Q}(\sqrt{3},\sqrt{7})(\zeta_{12})$	1	-	4.3.9
$\llbracket\chi_{50},\chi_{51}\rrbracket$	$48+48$	04	$\mathbb{Q}(\sqrt{3},\sqrt{5})(\zeta_{12})$	1	-	4.3.9
χ_{52}	$120+120$	04	$\mathbb{Q}(\sqrt{3})(\zeta_{12})$	1	-	4.3.9

$12_2.L_3(4)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_{53}	$36+36$	04	$\mathbb{Q}(\sqrt{3})(\zeta_{12})$	1	-	4.3.9
$\llbracket\chi_{54},\chi_{55}\rrbracket$	$48+48$	04	$\mathbb{Q}(\sqrt{3},\sqrt{5})(\zeta_{12})$	1	-	4.3.9
$\llbracket\chi_{56},\chi_{57}\rrbracket$	$60+60$	04	$\mathbb{Q}(\sqrt{3},\sqrt{7})(\zeta_{12})$	1	-	4.3.9
χ_{58}	$84+84$	04	$\mathbb{Q}(\sqrt{3})(\zeta_{12})$	1	-	4.3.9

9.2.7 $U_4(2) \cong S_4(3)$

Non-ATLAS-description: $\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$.
$|G| = 25,920 = 2^6 \cdot 3^4 \cdot 5$, $H^2(G, \mathbb{C}^\times) \cong C_2$, $\mathrm{Out}(G) \cong C_2$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$
χ_1	1	$+$	$\mathbb{Q}$	a	$(1,1)$
$\chi_2+\chi_3$	$5+5$	0	$\mathbb{Q}(\sqrt{-3})$	-3	$(-3,a)$
χ_4	6	$+$	$\mathbb{Q}$	-3	$(-3,a)$
$\chi_5+\chi_6$	$10+10$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(-1,-3)$
χ_7	15	$+$	$\mathbb{Q}$	a	$(2,3)$
χ_8	15	$+$	$\mathbb{Q}$	a	$(1,1)$
χ_9	20	$+$	$\mathbb{Q}$	1	$(-1,-1)$
χ_{10}	24	$+$	$\mathbb{Q}$	5	$(5,a)$
χ_{11}	30	$+$	$\mathbb{Q}$	-3	$(-3,a)$
$\chi_{12}+\chi_{13}$	$30+30$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(-1,-3)$
$\chi_{14}+\chi_{15}$	$40+40$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$
$\chi_{16}+\chi_{17}$	$45+45$	0	$\mathbb{Q}(\sqrt{-3})$	-3	$(-3,a)$
χ_{18}	60	$+$	$\mathbb{Q}$	1	$(-1,-1)$
χ_{19}	64	$+$	$\mathbb{Q}$	1	$(3,5)$
χ_{20}	81	$+$	$\mathbb{Q}$	a	$(2,5)$

$a \in \mathbb{Q}^\times$.

This table is quoted from [Neb99, Beispiel 3.5.3].

$2.U_4(2) \cong 2.S_4(3)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$\chi_{21}+\chi_{22}$	$4+4$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$	4.3.9
$2\cdot\chi_{23}$	$2\cdot 20$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3
$\chi_{24}+\chi_{25}$	$20+20$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$	4.3.9
$\chi_{26}+\chi_{27}$	$20+20$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$	4.3.9
$\chi_{28}+\chi_{29}$	$36+36$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$	4.3.9
$2\cdot\chi_{30}$	$2\cdot 60$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3
$\chi_{31}+\chi_{32}$	$60+60$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$	4.3.9
$2\cdot\chi_{33}$	$2\cdot 64$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3
$2\cdot\chi_{34}$	$2\cdot 80$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3

9.2.8 $Sz(8)$

$|G| = 29,120 = 2^6 \cdot 5 \cdot 7 \cdot 13$, $H^2(G,\mathbb{C}^\times) \cong C_2 \times C_2$, $\mathrm{Out}(G) \cong C_3$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_1	1	$+$	$\mathbb{Q}$	a	$(1,1)$	-
$\chi_2+\chi_3$	$14+14$	0	$\mathbb{Q}(\sqrt{-1})$	1	$(-1,-1)$	4.3.9
$\llbracket\chi_4,\chi_5,\chi_6\rrbracket$	35	$+$	$\mathbb{Q}(c_{13})$	b	$[\mathcal{Q}_{2,\infty_1,\infty_2,\infty_3}]$	Magma
χ_7	64	$+$	$\mathbb{Q}$	65	$(65,a)$	p. $\chi_1+\chi_7$
$\llbracket\chi_8,\chi_9,\chi_{10}\rrbracket$	65	$+$	$\mathbb{Q}(\zeta_7+\zeta_7^{-1})$	c	$(1,1)$	Magma
χ_{11}	91	$+$	$\mathbb{Q}$	a	$(-1,-1)$	Magma

$a \in \mathbb{Q}^\times$, $b \in \mathbb{Q}(c_{13})^\times$, $c_{13} = \frac{1}{3}\sum_{i=1}^{12}\zeta_{13}^{i^3}$, $c \in \mathbb{Q}(\zeta_7+\zeta_7^{-1})^\times$.

$2.Sz(8)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$\{\!\!\{\chi_{12},\chi_{13},\chi_{14}\}\!\!\}$	40	$+$	$\mathbb{Q}(\zeta_7+\zeta_7^{-1})$	1	$(1,1)$	Magma
$\{\!\!\{\chi_{15},\chi_{16},\chi_{17}\}\!\!\}$	56	$+$	$\mathbb{Q}(c_{13})$	1	$(1,1)$	Magma
χ_{18}	64	$+$	$\mathbb{Q}$	1	$(1,1)$	Magma
χ_{19}	104	$+$	$\mathbb{Q}$	1	$(1,1)$	Magma

$c_{13} = \frac{1}{3}\sum_{i=1}^{12}\zeta_{13}^{i^3}$

9.2.9 $U_3(4)$

$|G| = 62,400 = 2^6 \cdot 3 \cdot 5^2 \cdot 13$, $H^2(G,\mathbb{C}^\times) \cong \{1\}$, $\mathrm{Out}(G) \cong C_4$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_{\pm}(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_1	1	$+$	$\mathbb{Q}$	a	$(1,1)$	-
$2\cdot\chi_2$	$2\cdot 12$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3
$\llbracket\chi_3+\chi_4,\chi_5+\chi_6\rrbracket$	$13+13$	0	$\mathbb{Q}(\sqrt{5})(\sqrt{\delta})$	δ	-	4.3.9
$\{\!\!\{\chi_7,\chi_8\}\!\!\}$	39	$+$	$\mathbb{Q}(\sqrt{5})$	b	$(1,1)$	Magma
$\llbracket\chi_9+\chi_{10},\chi_{11}+\chi_{12}\rrbracket$	$52+52$	0	$\mathbb{Q}(\sqrt{5})(\sqrt{\delta})$	1	-	4.3.9
χ_{13}	64	$+$	$\mathbb{Q}$	65	$(65,a)$	p. $\chi_1+\chi_{13}$
χ_{14}	65	$+$	$\mathbb{Q}$	a	$(2,3)$	Magma
$\llbracket\chi_{15}+\chi_{16},\chi_{17}+\chi_{18}\rrbracket$	$65+65$	0	$\mathbb{Q}(\sqrt{5})(\sqrt{\delta})$	δ	-	4.3.9
$\llbracket\chi_{19}+\chi_{20},\chi_{21}+\chi_{22}\rrbracket$	$75+75$	0	$\mathbb{Q}(\sqrt{13})(\sqrt{\rho})$	ρ	-	4.3.9

$a \in \mathbb{Q}^\times$, $\delta = \frac{1}{2}\sqrt{5} - \frac{5}{2}$, $\rho = -\frac{3}{2}\sqrt{13} - \frac{13}{2}$.

9.2.10 M_{12}

$|G| = 95,040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$, $H^2(G, \mathbb{C}^\times) \cong C_2$, $\mathrm{Out}(G) \cong C_2$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_1	1	$+$	$\mathbb{Q}$	a	$(1,1)$	-
$\llbracket \chi_2, \chi_3 \rrbracket$	11	$+$	$\mathbb{Q}$	a	$(-1,-1)$	p. $\chi_1 + \chi_2$
$\chi_4 + \chi_5$	$16 + 16$	0	$\mathbb{Q}(\sqrt{-11})$	1	$(1,1)$	4.3.9
χ_6	45	$+$	$\mathbb{Q}$	a	$(-1,-1)$	r. M_{11}
χ_7	54	$+$	$\mathbb{Q}$	-55	-	r. M_{11}
χ_8	55	$+$	$\mathbb{Q}$	a	$(2,3)$	Magma
$\llbracket \chi_9, \chi_{10} \rrbracket$	55	$+$	$\mathbb{Q}$	a	$(1,1)$	$\bigwedge^2 \chi_2 = \chi_9$
χ_{11}	66	$+$	$\mathbb{Q}$	-1	$(-1,a)$	$\diamond$
χ_{12}	99	$+$	$\mathbb{Q}$	a	$(-2,-5)$	Magma
χ_{13}	120	$+$	$\mathbb{Q}$	33	$(33,a)$	Magma
χ_{14}	144	$+$	$\mathbb{Q}$	33	$(33,a)$	Magma
χ_{15}	176	$+$	$\mathbb{Q}$	1	$(3,5)$	Magma

$a \in \mathbb{Q}^\times$.

$\diamond$: Consider χ_{11} as a character of the extension $2.G$. We then have $\chi_{11} = \bigwedge^2 \chi_{18}$. By Nebe's method we find that $\mathrm{d}_\pm(\chi_{18}) = 1$. Then we obtain the invariants of χ_{11} from the formulas in Theorem 4.3.4.

$2.M_{12}$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$\chi_{16} + \chi_{17}$	$10 + 10$	0	$\mathbb{Q}(\sqrt{-2})$	1	$(-1,-1)$	4.3.9
χ_{18}	12	$+$	$\mathbb{Q}$	1	$(-1,-1)$	N. χ_{19}, †
$2 \cdot \chi_{19}$	$2 \cdot 32$	$-$	$\mathbb{Q}$	1	$(1,1)$	5.1.3
$\chi_{20} + \chi_{21}$	$44 + 44$	0	$\mathbb{Q}(\sqrt{-5})$	1	$(1,1)$	4.3.9
$\chi_{22} + \chi_{23}$	$110 + 110$	0	$\mathbb{Q}(\sqrt{-2})$	1	$(-1,-1)$	4.3.9
χ_{24}	120	$+$	$\mathbb{Q}$	1	$(1,1)$	Magma
$\chi_{25} + \chi_{26}$	$160 + 160$	0	$\mathbb{Q}(\sqrt{-11})$	1	$(1,1)$	4.3.9

†: Nebe's method yields the discriminant but does not give us any information about the Clifford invariant, which we computed using Magma.

9.2.11 $U_3(5)$

Other descriptions: $\mathrm{PSU}_3(5)$.
$|G| = 126,000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7$, $H^2(G, \mathbb{C}^\times) \cong C_3$, $\mathrm{Out}(G) \cong S_3$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_1	1	+	$\mathbb{Q}$	a	$(1,1)$	-
$2 \cdot \chi_2$	$2 \cdot 20$	−	$\mathbb{Q}$	1	1	5.1.3
χ_3	21	+	$\mathbb{Q}$	a	$(-2,-5)$	N. χ_2
$[\![\chi_4, \chi_5, \chi_6]\!]$	28	+	$\mathbb{Q}$	5	-	r. A_7
χ_7	84	+	$\mathbb{Q}$	5	-	`Magma`
χ_8	105	+	$\mathbb{Q}$	a	$(3,5)$	`Magma`
χ_9	125	+	$\mathbb{Q}$	a	$(-1,-7)$	p. $\chi_1 + \chi_9$
χ_{10}	126	+	$\mathbb{Q}$	-5	-	$\bigwedge^2 \chi_3 = \chi_7 + \chi_{10}$
$\chi_{11} + \chi_{12}$	$126 + 126$	0	$\mathbb{Q}(\sqrt{-2})$	1	-	4.3.9
$\chi_{13} + \chi_{14}$	$144 + 144$	0	$\mathbb{Q}(\sqrt{-7})$	1	-	4.3.9

$a \in \mathbb{Q}^\times$.

$3.U_3(5)$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_{15}	$21 + 21$	02	$\mathbb{Q}(\sqrt{-3})$	-3	$(-3, a)$	4.3.9
χ_{16}	$21 + 21$	02	$\mathbb{Q}(\sqrt{-3})$	-3	$(-3, a)$	4.3.9
$[\![\chi_{17}, \chi_{18}, \chi_{19}]\!]$	$48 + 48$	02	$\mathbb{Q}(\sqrt{-3})$	1	$(-3, 5)$	4.3.9
χ_{20}	$84 + 84$	02	$\mathbb{Q}(\sqrt{-3})$	1	$(-3, 5)$	4.3.9
χ_{21}	$105 + 105$	02	$\mathbb{Q}(\sqrt{-3})$	-3	$(-3, a)$	4.3.9
χ_{22}	$105 + 105$	02	$\mathbb{Q}(\sqrt{-3})$	-3	$(-3, a)$	4.3.9
χ_{23}	$126 + 126$	02	$\mathbb{Q}(\sqrt{-3})$	1	$(-2, -5)$	4.3.9
$\{\!\{\chi_{24}, \chi_{25}\}\!\}$	$126 + 126$	02	$\mathbb{Q}(\sqrt{6})(\sqrt{-2})$	1	-	4.3.9
$\{\!\{\chi_{26}, \chi_{27}\}\!\}$	$144 + 144$	02	$\mathbb{Q}(\sqrt{21})(\sqrt{-7})$	1	-	4.3.9

Remark 9.2.2 Some of the Clifford invariants in this table were computed with `Magma` and not the method from Theorem 4.3.9.

9.2.12 J_1

$|G| = 175,560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$, $H^2(G, \mathbb{C}^\times) \cong \{1\}$, $\mathrm{Out}(G) \cong \{1\}$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_1	1	$+$	$\mathbb{Q}$	a	$(1,1)$	-
$\{\!\{\chi_2, \chi_3\}\!\}$	56	$+$	$\mathbb{Q}(\sqrt{5})$	$\frac{31}{2} - \frac{5}{2}\sqrt{5}$	-	`Magma`
χ_4	76	$+$	$\mathbb{Q}$	77	$(77, a)(-1,-1)$	`Magma`
χ_5	76	$+$	$\mathbb{Q}$	77	$(77, a)(-1,-1)$	`Magma`
χ_6	77	$+$	$\mathbb{Q}$	a	$(-1,-3)$	`Magma`
$\{\!\{\chi_7, \chi_8\}\!\}$	77	$+$	$\mathbb{Q}(\sqrt{5})$	b	$[\mathcal{Q}_{\sqrt{5},\mathfrak{p}_{19},\infty_1,\infty_2}]$	`Magma`, †
$\{\!\{\chi_9, \chi_{10}, \chi_{11}\}\!\}$	120	$+$	$\mathbb{Q}[\omega]$	see below	-	◇
χ_{12}	133	$+$	$\mathbb{Q}$	a	$(-2,-5)$	`Magma`
$\{\!\{\chi_{13}, \chi_{14}\}\!\}$	133	$+$	$\mathbb{Q}(\sqrt{5})$	b	$[\mathcal{Q}_{3,\mathfrak{p}_{11},\infty_1,\infty_2}]$	`Magma`, $*$
χ_{15}	209	$+$	$\mathbb{Q}$	a	$(3,5)$	`Magma`

$a \in \mathbb{Q}^\times$, $b \in \mathbb{Q}(\sqrt{5})$, $\omega^3 - 2\omega^2 - 5\omega = 1$.

†: $\mathfrak{p}_{19}$ denotes one of the two primes of $\mathbb{Q}(\sqrt{5})$ above 19, which are exchanged by the non-trivial Galois automorphism of $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$.

◇: The dimension of the rational representation associated with the characters χ_9, χ_{10}, χ_{11} is 360, which is too large to be handled within suitable time by `Magma`'s algorithms. We therefore resort to the following method:
First we find that the representation affording the character $\chi \in \{\chi_9, \chi_{10}, \chi_{11}\}$ is absolutely irreducible modulo 2, 3 and 5. Therefore the only primes appearing in the determinant of a G-invariant form on a module with character χ are the primes lying above 7, 11 and 19. The primes 7 and 11 decompose in the extension $\mathbb{Q}[\omega]/\mathbb{Q}$, so that there are integers $a_1, a_2, a_3 \in \mathcal{O}_{\mathbb{Q}[\omega]}$ satisfying $7 = a_1 a_2 a_3$. Analogously we find $b_1, b_2, b_3 \in \mathcal{O}_{\mathbb{Q}[\omega]}$ such that $11 = b_1 b_2 b_3$. The prime 19 is ramified in $\mathbb{Q}[\omega]/\mathbb{Q}$ so that there is some $c \in \mathcal{O}_{\mathbb{Q}[\omega]}$ with the property $19 = c^3$.
We know from Dirichlet's Unit Theorem that there are two fundamental units ϵ_1 and ϵ_2, which generate the unit group together with the torsion unit -1.
Now, for each

$$x \in \{a_1, a_2, a_3, b_1, b_2, b_3, c, \epsilon_1, \epsilon_2, \epsilon_3, -1\}$$

we find a $q \in \mathcal{O}_{\mathbb{Q}[\omega]}$ such that all elements of the above set except for x are squares modulo q.

Next, we construct a $\mathbb{Q}[\omega]$-basis of a 120-dimensional representation with character χ and realize this module over the each of the finite fields $\mathbb{F}_q := \mathcal{O}_{\mathbb{Q}[\omega]}/(q)$. We proceed to compute the G-invariant forms over $\mathbb{F}_q$, which is considerably faster than the analogous computation over $\mathbb{Q}[\omega]$, and find its determinant d. If d is not a square, we now that x occurs in the determinant of an invariant form over $\mathbb{Q}[\omega]$ (modulo squares, of course). Otherwise, x does not occur. In this manner, we find that the determinant of a G-invariant form on a $\mathbb{Q}[\omega]J_1$-module affording the character χ is, up to multiplication by a unit of $\mathcal{O}_{\mathbb{Q}[\omega]}$, an element of norm

$$7^2 \cdot 11 \cdot 19.$$

$*$: $\mathfrak{p}_{11}$ denotes one of the two primes of $\mathbb{Q}(\sqrt{5})$ above 11, which are exchanged by the non-trivial Galois automorphism of $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$.

9.2.13 A_9

$|G| = 181,440 = 2^6 \cdot 3^4 \cdot 5 \cdot 7$, $H^2(G, \mathbb{C}^\times) \cong C_2$, $\mathrm{Out}(G) \cong C_2$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_1	1	+	$\mathbb{Q}$	a	$(1,1)$	-
χ_2	8	+	$\mathbb{Q}$	1	$(1,1)$	p. $\chi_1+\chi_2$
$\chi_3+\chi_4$	$21+21$	0	$\mathbb{Q}(\sqrt{-15})$	-15	-	4.3.9
χ_5	27	+	$\mathbb{Q}$	a	$(-1,-1)$	p. $\chi_1+\chi_2+\chi_5$
χ_6	28	+	$\mathbb{Q}$	1	$(-1,-1)$	$\bigwedge^2 \chi_2 = \chi_6$
$[\![\chi_7,\chi_8]\!]$	35	+	$\mathbb{Q}$	a	$(-1,-1)$	r. A_8
χ_9	42	+	$\mathbb{Q}$	-3	-	r. A_8
χ_{10}	48	+	$\mathbb{Q}$	105	-	r. A_8
χ_{11}	56	+	$\mathbb{Q}$	1	$(1,1)$	$\diamond$
χ_{12}	84	+	$\mathbb{Q}$	5	-	r. A_8
χ_{13}	105	+	$\mathbb{Q}$	a	$(1,1)$	Magma
χ_{14}	120	+	$\mathbb{Q}$	21	-	r. A_8
χ_{15}	162	+	$\mathbb{Q}$	-7	-	r. A_8
χ_{16}	168	+	$\mathbb{Q}$	1	$(3,5)$	r. A_8, $\star$
χ_{17}	189	+	$\mathbb{Q}$	a	$(-1,-1)$	Magma
χ_{18}	216	+	$\mathbb{Q}$	105	-	r. A_8

$a \in \mathbb{Q}^\times$.

$\diamond$: Consider χ_{11} as a character of $2.G$. Then $\chi_{19} \cdot \chi_{20} = \chi_2 + \chi_{11}$. The group $2.G$ has two subgroups isomorphic to $\mathrm{SL}_2(8)$ and each of χ_{19}, χ_{20} restricts irreducibly to one of them. Hence $\mathrm{d}_\pm(\chi_i) = 1$ and $\mathfrak{c}(\chi_i) = (1,1)$ for $i \in \{19, 20\}$. Now we easily obtain the row for χ_{11} from the formulas for orthogonal direct sums and tensor products of orthogonal representations.

$\star$: For $\mathfrak{c}(\chi_{16})$ we used `Magma` to compute an invariant form.

$2.A_9$

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
$[\![\chi_{19}, \chi_{20}]\!]$	8	$+$	$\mathbb{Q}$	1	$(1,1)$	r. $2.A_8$
$\chi_{21} + \chi_{22}$	$48 + 48$	0	$\mathbb{Q}(\sqrt{-6})$	1	$(1,1)$	4.3.9
χ_{23}	56	$+$	$\mathbb{Q}$	1	$(1,1)$	4.3.9
χ_{24}	112	$+$	$\mathbb{Q}$	1	$(1,1)$	`Magma`
$\chi_{25} + \chi_{26}$	$120 + 120$	0	$\mathbb{Q}(\sqrt{-3})$	1	$(1,1)$	4.3.9
χ_{27}	160	$+$	$\mathbb{Q}$	1	$(1,1)$	`Magma`
$\chi_{28} + \chi_{29}$	$168 + 168$	0	$\mathbb{Q}(\sqrt{-15})$	1	$(1,1)$	4.3.9
χ_{30}	224	$+$	$\mathbb{Q}$	1	$(1,1)$	`Magma`

9.2.14 $\mathrm{O}_8^+(2)$

$|G| = 174,182,400 = 2^{12} \cdot 3^5 \cdot 5^2 \cdot 7$, $H^2(G, \mathbb{C}^\times) \cong C_2 \times C_2$, $\mathrm{Out}(G) \cong S_3$.

χ	$\chi(1)$	ind	$\mathbb{Q}[\chi]$	$\mathrm{d}_\pm(\varphi)$	$\mathfrak{c}(\varphi)$	Method
χ_1	1	$+$	$\mathbb{Q}$	a	$(1,1)$	-
χ_2	28	$+$	$\mathbb{Q}$	1	$(-1,-1)$	r. A_9
$[\![\chi_3, \chi_4, \chi_5]\!]$	35	$+$	$\mathbb{Q}$	a	$(-1,-1)$	r. A_9
χ_6	50	$+$	$\mathbb{Q}$	-3	-	r. A_9
$[\![\chi_7, \chi_8, \chi_9]\!]$	84	$+$	$\mathbb{Q}$	5	-	r. A_9
$[\![\chi_{11}, \chi_{12}, \chi_{13}]\!]$	210	$+$	$\mathbb{Q}$	-3	-	r. A_9
χ_{15}	350	$+$	$\mathbb{Q}$	-1	-	$\chi_2 + \chi_{15} = \bigwedge^2 \chi_2$
$[\![\chi_{17}, \chi_{18}, \chi_{19}]\!]$	567	$+$	$\mathbb{Q}$	a	$(-1,-1)$	$\diamond$

$a \in \mathbb{Q}^\times$.

$\diamond$: There are $\theta \in \{\chi_{17}, \chi_{18}, \chi_{19}\}$ and $\chi \in \{\chi_3, \chi_4, \chi_5\}$ such that

$$\chi_2 + \theta = \bigwedge^2 \chi.$$

9.2.15 M_{24}

Let G be the sporadic Mathieu group M_{24} of order $244,823,040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$. There is a permutation representation of G with character $\chi_1 + \chi_2$, so $\mathfrak{c}(\chi_2) = 1$. The character χ_8 is obtained as the exterior square of χ_2, so that $\mathfrak{c}(\chi_8) = (-1,-1)$ by Theorem 4.3.4.

9.2.16 M^cL

Let G be the sporadic McLaughlin group M^cL. Nebe's character method may be applied to the character χ_2. This was already done in [Neb99, Beispiel 3.1.17], where it was shown that $\mathrm{d}_{\pm}(\chi_2) = -15$.
The character χ_3 of degree 231 is obtained as the exterior sqaure of χ_2 so that we find $\mathfrak{c}(\chi_3) = [\mathcal{Q}_{2,3}]$ using Theorem 4.3.4.

9.2.17 $R(27)$

Let $G \cong R(27)$ be the Ree group of order $10,073,444,472 = 2^3 \cdot 3^9 \cdot 7 \cdot 13 \cdot 19 \cdot 37$. There is a permutation representation of G with character $\chi_1 + \chi_{20}$, the latter of which is of degree $19,683$. Therefore $\mathfrak{c}(\chi_{20}) = (-1,-1)$.

9.2.18 $S_8(2)$

Let G be the simple group $S_8(2)$ associated to the symplectic group of degree 8 over $\mathbb{F}_2$. The characters χ_5 and χ_6, which are of degrees 119 and 135, respectively, both have the property that $\chi_1 + \chi_i$, $i \in \{5,6\}$, is the character of a permutation module of G. Therefore we find

$$\mathfrak{c}(\chi_5) = \mathfrak{c}(\chi_6) = 1.$$

9.2.19 Co_3

Let G be the sporadic Conway group Co_3. We can apply Nebe's character method to an irreducible orthogonal $\mathbb{Q}G$-module of dimension 23 with character χ_2. A computation with `Magma` shows that the character χ_W of the simple $\mathcal{C}_0(\varphi)$-module has the trivial character as a constituent with multiplicity 1. The conclusion $\mathfrak{c}(\chi_2) = 1$ is immediate from Nebe's results.
The character χ_3 of degree 253 is obtained as the exterior square of χ_2, so $\mathfrak{c}(\chi_3) = (-1,-1)$.
Finally, $\chi_1 + \chi_5$ is the character of a 276-dimensional permutation representation of G, from which we obtain $\mathfrak{c}(\chi_5) = (-1,-1)$.

9.3 Extensions of finite groups by finite simple groups

9.3.1 $\mathrm{P\Gamma L}_2(8) \cong \mathrm{P\Sigma L}_2(8)$

The projective general semilinear group $\mathrm{P\Gamma L}_2(8) =: G$ is an extension of C_3 by $\mathrm{PSL}_2(8)$. Its character table, which is contained in [CCN$^+$85] as the extension $\mathrm{PSL}_2(8).3$, is obtained from `Magma` as

```
 -------------------------------------------------------
Class |    1  2  3      4      5   6   7   8   9  10  11
Size  |    1 63 56     84     84 252 252 216 168 168 168
Order |    1  2  3      3      3   6   6   7   9   9   9
-------------------------------------------------------
p  =  2    1  1  3      5      4   4   5   8   9  11  10
p  =  3    1  2  1      1      1   2   2   8   3   3   3
p  =  7    1  2  3      4      5   6   7   1   9  10  11
-------------------------------------------------------
X.1   +    1  1  1      1      1   1   1   1   1   1   1
X.2   0    1  1  1      J   -1-J-1-J   J   1   1-1-J   J
X.3   0    1  1  1   -1-J      J   J-1-J   1   1   J-1-J
X.4   +    7 -1 -2      1      1  -1  -1   0   1   1   1
X.5   0    7 -1 -2   -1-J      J  -J 1+J   0   1   J-1-J
X.6   0    7 -1 -2      J   -1-J 1+J  -J   0   1-1-J   J
X.7   +    8  0 -1      2      2   0   0   1  -1  -1  -1
X.8   0    8  0 -1 -2-2*J    2*J   0   0   1  -1  -J 1+J
X.9   0    8  0 -1    2*J -2-2*J   0   0   1  -1 1+J  -J
X.10  +   21 -3  3      0      0   0   0   0   0   0   0
X.11  +   27  3  0      0      0   0   0  -1   0   0   0


Explanation of Character Value Symbols
--------------------------------------


J = RootOfUnity(3)
```

In order to avoid confusion with the characters of $\mathrm{PSL}_2(8)$, we will denote the characters of G by $\widetilde{\chi_i}$, $1 \leq i \leq 11$, according to the numbering of this printed character table.

Consider the restrictions of $\widetilde{\chi_{10}}$ and $\widetilde{\chi_{11}}$ to the normal subgroup $N := \mathrm{PSL}_2(8)$ of G. We obtain

$$\widetilde{\chi_{10}}|_N = \theta_1 + \theta_2 + \theta_4, \ \widetilde{\chi_{11}}|_N = \chi_1 + \chi_2 + \chi_3$$

in the notation of Theorem 6.5.10.

We know $\mathfrak{c}(\theta_j)$ and $\mathfrak{c}(\chi_i)$ to be trivial by Theorem 6.5.10. Let f be a G-invariant regular quadratic form on one of the modules affording χ_{10} or χ_{11}. By scaling with an element $a \in \mathbb{Q}^\times$ we may assume that the determinant of the restriction of f to one of the three submodules is a square. But then, by the orthogonal Clifford theorem, see 4.3.14, the determinants are squares on all submodules. Hence we obtain $\mathfrak{c}(\widetilde{\chi_{10}}) = (-1,-1)$ as well as $\mathfrak{c}(\widetilde{\chi_{11}}) = (-1,-1)$, by applying the formula for the Clifford invariant of orthogonal direct sums in Proposition 3.6.24.

The characters $\widetilde{\chi_1}$, $\widetilde{\chi_4}$ and $\widetilde{\chi_8}$ restrict irreducibly to N and for the remaining characters of G Theorem 4.3.9 may be applied, so that all in all, we have determined all algebraic invariants of the orthogonal representations of G.

9.3.2 $\mathrm{P\Gamma L}_2(32) \cong \mathrm{P\Sigma L}_2(32)$

$G = \mathrm{P\Gamma L}_2(32)$ has three absolutely irreducible representations of degrees 155 and three absolutely irreducible representations of degrees 165.

Let χ be the character of one of the 155-dimensional representations. The restriction of χ to the normal subgroup $\mathrm{PSL}_2(32)$ decomposes into five copies of a 31-dimensional character. Let φ be a $\mathrm{PSL}_2(32)$-invariant quadratic form on one of those representations. Then, by Theorem 3.6.26, we find

$$\mathfrak{c}(\chi) = \mathfrak{c}(\varphi^5) = \mathfrak{c}(\varphi^3) = (-1,-1).$$

Analogously, if θ denotes the character of one of the abovementioned 165-dimensional representations, we obtain

$$\mathfrak{c}(\theta) = \mathfrak{c}(\varphi^5) = \mathfrak{c}(\varphi^3) = (-1,-1).$$

Bibliography

[ABL$^+$] Rachel Abbott, John Bray, Steve Linton, Simon Nickerson, Simon Norton, Richard Parker, Ibrahim Suleiman, Jonathan Tripp, Peter Walsh, and Robert Wilson, *Atlas of Finite Group Representations – Version 3*, published online at `http://brauer.maths.qmul.ac.uk/Atlas/v3/`.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput. (1997), no. 24, 235–265.

[BEO02] Hans Ulrich Besche, Bettina Eick, and Eamonn A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. **12** (2002), no. 5, 623–644.

[BN16] Oliver Braun and Gabriele Nebe, *The Orthogonal Character Table of* $\mathrm{SL}_2(q)$, Preprint available at `arXiv:1609.08852[math.NT]`, 2016.

[Bon11] Cédric Bonnafé, *Representations of* $\mathrm{SL}_2(\mathbb{F}_q)$, Algebra and applications, vol. 13, Springer-Verlag, Berlin-New York, 2011.

[Bou89] Nicolas Bourbaki, *Algebra I, Chapters 1-3*, 2^{nd} ed., Springer-Verlag, Berlin-New York, 1989.

[BZ85] Herbert Benz and Hans Julius Zassenhaus, *Über verschränkte Produktordnungen*, J. Number Theory **20** (1985), no. 3, 282–298.

[CCN$^+$85] John H. Conway, Robert T. Curtis, Simon P. Norton, Richard A. Parker, and Robert A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

[CR87a] Charles W. Curtis and Irving Reiner, *Methods of Representation Theory*, vol. 1, John Wiley and Sons, Inc., New York, 1987.

[CR87b] ______, *Methods of Representation Theory*, vol. 2, John Wiley and Sons, Inc., New York, 1987.

[Dor71] Larry Dornhoff, *Group representation theory. Part A: Ordinary representation theory*, Marcel Dekker, Inc., New York, 1971, Pure and Applied Mathematics, 7.

[Fei96] Walter Feit, *Schur indices of characters of groups related to finite sporadic simple groups*, Israel J. Math. **93** (1996), 229–251.

[Gow76] Roderick Gow, *Schur indices of some groups of Lie type*, J. Algebra **42** (1976), no. 1, 102–120.

[Has24] Helmut Hasse, *Äquivalenz quadratischer Formen in einem beliebigen Zahlkörper*, J. reine u. angew. Mathematik **153** (1924), 158–162.

[Hol98] Derek F. Holt, *The Meataxe as a tool in computational group theory*, London Mathematical Society Lecture Note Series (1998), 74–81.

[Hup67] Bertram Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967.

[Isa76] I. Martin Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[Jam78] Gordon D. James, *The representation theory of the symmetric groups*, Lecture Notes in Mathematics, vol. 682, Springer-Verlag, Berlin-New York, 1978.

[Jan74] Gerald J. Janusz, *Simple components of Q[SL(2, q)]*, Comm. Algebra **1** (1974), 1–22.

[Jor07] Herbert E. Jordan, *Group-Characters of Various Types of Linear Groups*, Amer. J. Math. **29** (1907), no. 4, 387–405.

[Kne02] Martin Kneser, *Quadratische Formen*, Springer-Verlag, Berlin-New York, 2002.

[Knu91] Max-Albert Knus, *Quadratic and Hermitian forms over rings*, Grundlehren der Mathematischen Wissenschaften, vol. 294, Springer-Verlag, Berlin-New York, 1991.

[Lam73] Tsit-Yuen Lam, *The algebraic theory of quadratic forms*, WA Benjamin, 1973.

[McG02] Seán McGarraghy, *Exterior powers of symmetric bilinear forms*, Algebra Colloquium **9** (2002), no. 2, 197–218.

[Neb99] Gabriele Nebe, *Orthogonale Darstellungen endlicher Gruppen und Gruppenringe*, Aachener Beiträge zur Mathematik, no. 26, Wissenschaftsverlag Mainz, Aachen, 1999.

[Neb00a] ———, *Invariants of orthogonal G-modules from the character table*, Experimental Mathematics **9** (2000), no. 4, 623–629.

[Neb00b] ———, *Orthogonal Frobenius reciprocity*, Journal of Algebra **225** (2000), no. 1, 250–260.

[Neb05] ———, *On the radical idealizer chain of symmetric orders*, Journal of Algebra **283** (2005), no. 2, 622–638.

[NP95] Gabriele Nebe and Wilhelm Plesken, *Finite Rational Matrix Groups of Degree 16*, no. 556, 74–144.

[NS09] Gabriele Nebe and Allan Steel, *Recognition of Division Algebras*, Journal of Algebra (2009), no. 322, 903–909.

[O'M73] O.Timothy O'Meara, *Introduction to Quadratic Forms*, Grundlehren der mathematischen Wissenschaften, no. 117, Springer-Verlag, Berlin-New York, 1973.

[Pen76] J. William Pendergrass, *The Size of a Simple Component of a Group Algebra*, Communications in Algebra **4** (1976), no. 11, 1071–1076.

[Ple81] Wilhelm Plesken, *Bravais groups in low dimensions*, Comm. Math. Chem. (1981), no. 10, 97–119.

[PS96] Wilhelm Plesken and Bernd Souvignier, *Constructing rational representations of finite groups*, Experiment. Math. **5** (1996), no. 1, 39–47.

[PZ89] Michael E. Pohst and Hans J. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1989.

[Rei75] Irving Reiner, *Maximal Orders*, vol. 38, Academic Press London, 1975.

[Sch07] Issai Schur, *Untersuchungen über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **132** (1907), 85–137.

[Sch85] Winfried Scharlau, *Quadratic and Hermitian forms*, Springer-Verlag, Berlin-New York, 1985.

[ST79] Eugene Spiegel and Allan Trojan, *The Schur subgroup of a p-adic field*, Canad. J. Math. **31** (1979), no. 2, 300–303.

[Ste51] Robert Steinberg, *The representations of* $\mathrm{GL}(3,q), \mathrm{GL}(4,q), \mathrm{PGL}(3,q)$*, and* $\mathrm{PGL}(4,q)$, Canadian J. Math. **3** (1951), 225–235.

[Tur93] Alexandre Turull, *Schur index two and bilinear forms*, Journal of Algebra **157** (1993), no. 2, 562–572.

[Vig80] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer-Verlag, Berlin-New York, 1980.

[YI86] Toshihiko Yamada and Seiichi Ito, *The degree of a Schur algebra*, TRU Math. **22** (1986), no. 1, 53–61.

Index