Rational forms of finite matrix groups

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften
der RWTH Aachen University zur Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Computermathematiker

Jan Jongen

aus Siegburg

Berichter: Universitätsprofessor Dr. Wilhelm Plesken
Universitätsprofessorin Dr. Gabriele Nebe

Tag der mündlichen Prüfung: 17.07.2012

Diese Dissertation ist auf den Internetseiten der Hochschulbibliothek
online verfügbar.

Abstract

Let k be a perfect field, K/k a finite GALOIS extension with GALOIS group Γ and G a finite subgroup of $\mathrm{GL}_n(\overline{k})$. Viewing $\mathrm{GL}_n(\overline{k})$ as an algebraic group turns G into an algebraic group. A first result in this thesis is that G has fundamental invariants whose coefficients lie in k if and only if G is defined over k. Three guiding questions arise naturally.

Existence: If the finite matrix group G is not defined over k, can we transform G into a finite matrix group G' which is defined over k? Reasonably, such a G' will be called a k-form of G, and if additionally G' is a subgroup of $\mathrm{GL}_n(K)$, a (K/k)-form respectively.

Classification: If G is defined over k and a subgroup of $\mathrm{GL}_n(K)$, how many non equivalent, i.e. not conjugate by an element of $\mathrm{GL}_n(k)$, (K/k)-forms of G are there?

Arithmetic: If G is defined over k, what are the arithmetic features of G beside the fact that there exists a set of fundamental invariants whose coefficients lie in k?

It is shown that the classification of K/k-forms can be answered by counting the embeddings $\Gamma \to \mathrm{Aut}(G)$ up to conjugation inside $\mathrm{Aut}(G)$ and some restrictions on the induced Γ-action.

Using BRAUER-CLIFFORD theory necessary and sufficient conditions on the field K to admit a (K/k)-form of G are deduced and those conditions are good enough to answer the case of k being a finite field or the real numbers completely.

Turning to the arithmetic theory of $(K/\mathbb{Q})$-forms, a correspondence between $(K/\mathbb{Q})$-forms of G and modules over some special skew group rings $K * (G \rtimes \Gamma)$ is proved. Introducing complex characters of $K * (G \rtimes \Gamma)$, an explicit correspondence between those and the irreducible complex characters of G is obtained. The SCHUR index is defined and character induction and restriction are developed.

If K admits a central canonical conjugation, we define a canonical involution on $K * (G \rtimes \Gamma)$ and show that this involution is the anti adjoint automorphism of a symmetric positive definite bilinear form.

Zusammenfassung

Sei k ein perfekter Körper, K/k eine endliche GALOIS Erweiterung mit GALOIS Gruppe Γ und G eine endliche Untergruppe von $\mathrm{GL}_n(\overline{k})$. Als endliche Untergruppe der algebraischen Gruppe $\mathrm{GL}_n(\overline{k})$, ist auch G eine algebraische Gruppe. Es zeigt sich, dass der Invariantenring von G genau dann Erzeuger mit rationalen Koeffizienten besitzt, wenn G über k definiert ist. Die Arbeit konzentriert sich nun auf die folgenden drei fundamentalen Fragen:
Existenz: Falls G nicht über k definiert ist, ist es möglich G in eine über k definiert Gruppe G' zu transformieren? Eine solche Gruppe G' wird eine k-Form von G genannt. Falls G' zusätzlich eine Untergruppe von $\mathrm{GL}_n(K)$ ist, so heißt G' eine (K/k)-Form von G.
Klassifikation: Wie viele nicht äquivalente, das heißt über $\mathrm{GL}_n(k)$ nicht konjugierte, (K/k)-formen von G gibt es?
Arithmetik: Welche arithmetischen Eigenschaften besitzt eine über k-definierte endliche Matrixgruppe G?

Die Klassifikation der (K/k)-Formen von G ist im Wesentlichen durch die bis auf Konjugation in $\mathrm{Aut}(G)$ verschiedenen Einbettungen $\Gamma \to \mathrm{Aut}(G)$ beantwortet. Hinzu kommen einige technische Voraussetzungen an die Γ-Operation auf G.

Mithilfe der BRAUER-CLIFFORD Theorie werden für die Existenz einer (K/k)-Form von G hinreichende und notwendige Bedingungen an den Körper K hergeleitet. Diese sind ausreichend, um die Existenzfrage für endliche Körper und die reellen Zahlen vollständig zu entscheiden.

Die arithmetische Theorie der (K/k)-Formen von G basiert auf einer Korrespondenz zwischen ebensolchen Formen und Moduln über speziellen getwisteten Gruppenringen $K * (G \rtimes \Gamma)$. Die Begriffe des (komplexen) Charakters und des SCHUR Index werden auf getwistete Gruppenringe verallgemeinert. Desweiteren werden Induktion und Restriktion für komplexe $K * (G \rtimes \Gamma)$-Charaktere entwickelt. Falls der Körper K eine kanonische komplexe Konjugation besitzt, so existiert eine kanonische Involution auf $K * (G \rtimes \Gamma)$.

Contents

Chapter 1

Introduction

Nineteenth century mathematicians like Klein, Fricke, Maschke and Valentiner constructed representations of finite groups like $\mathrm{PSL}_2(7)$, $\mathrm{SL}_2(5)$ or $3.\mathrm{A}_6$ and calculated fundamental polynomial invariants. A variety of geometric methods was used, most prominently the theory of Riemannian surfaces and Klein's line geometry cf. [Kle99], [Kle72]. It often turned out that these invariants are polynomials with rational coefficients whereas the matrices of the representations have irrational entries.

The objective of this thesis is to study this phenomenon systematically within a modern algebraic and arithmetic framework.

Let k be a perfect field, K/k a finite Galois extension with Galois group Γ and G a finite subgroup of $\mathrm{GL}_n(\overline{k})$. Viewing $\mathrm{GL}_n(\overline{k})$ as an algebraic group turns G into an algebraic group. Theorem (2.1.7) states that G has fundamental invariants whose coefficients lie in k if and only if G is defined over k i.e. that G is given by polynomial equations whose coefficients lie in k. Three guiding questions arise naturally.

1. If the finite matrix group G is not defined over k, can we transform G into a finite matrix group G' which is defined over k? Reasonably, such a G' will be called a k-form of G and if additionally G' is a subgroup of $\mathrm{GL}_n(K)$ a (K/k)-form respectively. (Existence)

2. If G is defined over k and a subgroup of $\mathrm{GL}_n(K)$, how many non equivalent, i.e. not conjugate by an element of $\mathrm{GL}_n(k)$, (K/k)-forms of G are there? (Classification)

3. If G is defined over k, what are the arithmetic features of G beside the fact that there exists a set of fundamental invariants whose coefficients lie in k? (Arithmetic)

Existence and classification of K/k-forms

If G is irreducible, the classification of K/k-forms admits the following rather simple answer.

Theorem 1.0.1 (Preliminary)**.** *Let K/k be a* Galois *extension with group Γ, G a finite irreducible subgroup of $\mathrm{GL}_n(K)$ defined over k. The number of non* *equivalent K/k-forms of G equals the number of homomorphism $\Gamma \to \mathrm{Aut}(G)$ up to conjugation inside $\mathrm{Aut}(G)$ and some restrictions on the induced Γ-action on G.*

The main observation regarding the existence question is that if G is defined over k and lies in $\mathrm{GL}_n(K)$, then Γ acts on G as group automorphisms. This action extends k-linearly to the enveloping algebra $\Delta(kG)$ of the natural representation of G and turns it into a central simple Γ-algebra in the sense of [Tur94a]. TURULL defines a equivalence relation on those algebras, which is very similar to the equivalence relation on central simple algebras leading to the BRAUER-group. He also establishes a group structure on the equivalence classes [Tur94b] and this group is called the BRAUER-CLIFFORD group. Some natural operations on the BRAUER-CLIFFORD group are introduced, most notably a group homomorphism induced by Γ-equivariant scalar extension. The main theorem, as stated in the second chapter, says:

Theorem 1.0.2. *Let K/k be a* GALOIS *extension with group Γ, G a finite subgroup of $\mathrm{GL}_n(K)$ with natural representation Δ. There exists a (K/k)-form of G if and only if the equivalence class of $\Delta(kG)$ in the* BRAUER-CLIFFORD *group lies in the kernel of the scalar extension homomorphism.*

The benefit of this theorem is that the equivalence class depends only on the GALOIS group Γ as an abstract group and can be defined independently of K. Hence, all GALOIS extensions K/k with GALOIS group isomorphic to Γ are considered at once. Necessary and sufficient conditions on the field K to admit a (K/k)-form of G are deduced and those conditions are good enough to answer the case of k being a finite field or the real numbers completely. Those results are a part of the publication [Jon11].

Character theory and arithmetic theory of K/k-forms

Turning to the arithmetic theory of (K/k)-forms, we assume that $k = \mathbb{Q}$. It turned out to be sensible to fix the finite GALOIS extension K together with the embedding $^- : \Gamma \to \mathrm{Aut}(G)$ and to look at K-linear representations $\Delta : G \to \mathrm{GL}_l(K)$ with the property

$$\Delta(\overline{\sigma}(g)) = \sigma(\Delta(g)) \text{ for all } g \in G \text{ and } \sigma \in \Gamma$$

Such a representation will be called a $(K/k, ^-)$-representation of G. By the work of SHODA on semilinear representation theory special skew group rings enter the picture, cf. [Sho38a], [Sho38b], [NS36]. These skew group rings, denoted $K * (G \rtimes \Gamma)$ in the following, are constructed from the Γ-action on G and the natural Γ-action on K. We rediscover the following theorem, which can be easily extracted from the work of SHODA.

Theorem 1.0.3. *Let G be a finite group, K/k be a finite* GALOIS *extension with group Γ and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. There exists a one to one correspondence between $K * (G \rtimes \Gamma)$-modules up to isomorphism and $(K/k, ^-)$-representations of G up to conjugation with matrices in $\mathrm{GL}_n(k)$.*

As a first approximation $A := \mathbb{C} \otimes_{\mathbb{Q}} K * (G \rtimes \Gamma)$-modules respectively their characters are studied. The main result is the following explicit correspondence between the characters of A-modules and the absolutely irreducible complex characters of G.

Theorem 1.0.4. *Let K/k be a finite* GALOIS *extension with group Γ, $^{-} : \Gamma \to \mathrm{Aut}(G)$ an embedding, χ an irreducible complex character of G and choose a complex embedding of K into $\mathbb{C}$. Define $\widehat{\chi} : K * (G \rtimes \Gamma) \to \mathbb{C}$ as the $\mathbb{Q}$-linear extension of*

$$\widehat{\chi}(yg) = \begin{cases} \sum_{\sigma \in \Gamma} \sigma(y)\chi(\overline{\sigma}(g)) & \text{if } g \in G, \\ 0 & \text{if } g \notin G. \end{cases}$$

with $y \in K$ and $g \in G \rtimes \Gamma$. Denote the $\mathbb{C}$-linear extension of $\widehat{\chi}$ by $\widetilde{\chi}$.

Then $\widetilde{\chi}$ is an irreducible character of A and the map $\chi \mapsto \widetilde{\chi}$ defines a one to one correspondence between the irreducible complex characters of G and those of A.

To measure the amount of information loss passing from $K * (G \rtimes \Gamma)$ to A, the SCHUR index of a irreducible character of A is introduced and it is shown that the SCHUR index equals the order of the scalar extension of the equivalence class of the enveloping k-algebra in the BRAUER-CLIFFORD group.

If K has a central canonical complex conjugation σ, that is an element of center of Γ which induces complex conjugation in every embedding of K into $\mathbb{C}$, a canonical involution on ι_σ on $K * (G \rtimes \Gamma)$ is defined. Restricted to $G \rtimes \Gamma$ this involution inverts the elements and restricted to K it is the canonical complex conjugation. For any $\mathbb{Q}$-linear representation $\Delta : K * (G \rtimes \Gamma) \to \mathbb{Q}^{n \times n}$ we show the following theorem.

Theorem 1.0.5. *Let ι_σ be the canonical involution on $K * (G \rtimes \Gamma)$. For every $\mathbb{Q}$-linear representation $\Delta : K * (G \rtimes \Gamma) \to \mathbb{Q}^{n \times n}$ there exists a symmetric positive definite matrix $\Phi \in \mathbb{Q}^{n \times n}$ such that*

$$\Delta(\iota_\sigma(x)) = \Phi^{-1} \Delta(x)^{tr} \Phi$$

for all $x \in K * (G \rtimes \Gamma)$.

For the natural involution invariant $\mathbb{Z}$-order $\mathbb{Z}_K * (G \rtimes \Gamma)$ in $K * (G \rtimes \Gamma)$ this leads to a situation very similar to integral representation theory of finite groups. With the numerous and powerful methods developed by PLESKEN and NEBE [NP95] on lattices and integral representation theory, $\mathbb{Z}_K * (G \rtimes \Gamma)$ structures on various interesting EUCLIDEAN lattices are obtained.

Coming back to where we started, we rediscover the beautiful representations mentioned in the beginning from $\mathbb{Z}_K * (G \rtimes \Gamma)$-structure on various interesting lattices. Most prominently, KLEIN'S 3-dimensional representation of $\mathrm{PSL}_2(7)$ realized over $\mathbb{Q}(\zeta_7)$ comes from a $\mathbb{Z}[\zeta_7] * (\mathrm{PSL}_2(7) \rtimes \Gamma)$ structure on an 18-dimensional 7-modular lattice corresponding to an irreducible maximal finite subgroup of $\mathrm{GL}_{18}(\mathbb{Q})$. Moreover, various other lattices such as the LEECH-lattice, the root lattice E_8 and NEBE'S recently discovered 72-dimensional, extremal even unimodular lattice Λ_{72} [Neb] turn up.

The last part of this thesis is about the following theorem, which was proposed by PLESKEN.

Theorem 1.0.6. *Let K be an algebraically closed field, G a finite subgroup of $\mathrm{GL}_n(K)$ with natural module $V := K^n$, p a point in K^n and assume that the characteristic of K does not divide $|G|$. The rank of the* Jacobian *matrix, evaluated at p, of any system of fundamental polynomial invariants equals the dimension of the subspace of fixed points under the stabilizer G_p of p in G.*

This theorem is then applied to study the orbit stratification of V.

Outline

Chapter 2 provides the necessary formal definitions to study k-forms of finite groups. The existence question is addressed briefly and the work of Shoda on semilinear representation theory is reviewed. Furthermore, the classification theorem is proved.

The chapters 3 and 4 consists mainly of the paper "The Brauer-Clifford group and rational forms of finite groups" [Jon11]. Brauer-Clifford theory is reviewed and the main theorem (1.0.2) is proved. This theorem is applied to the cases of finite fields, the real numbers and number fields with the additional assumption that G is isomorphic to $\mathrm{PSL}_2(q)$ where q is an arbitrary prime power.

Chapter 5 studies the character theory of $\mathbb{C} \otimes_{\mathbb{Q}} K * (G \rtimes \Gamma)$ and introduces a modified character table. The proof of theorem (1.0.4) is given via a detailed study of the central primitive idempotents of $\mathbb{C} \otimes_{\mathbb{Q}} K * (G \rtimes \Gamma)$. The Schur index and its properties are discussed and induction and restriction of $K * (G \rtimes \Gamma)$-modules is introduced.

Chapter 6 defines the canonical involution on $K * (G \rtimes \Gamma)$ and provides the necessary arithmetic theory to study lattices over the natural $\mathbb{Z}$-order $\mathbb{Z}_K * (G \rtimes \Gamma)$ in $K * (G \rtimes \Gamma)$. Putting everything together, a procedure to calculate nice $(K/\mathbb{Q})$-forms of G is given.

In chapter 7 this procedure is applied to a variety of different groups and fields.

Fairly independent of the rest of the thesis, chapter 8 studies the quotient map of finite matrix groups.

General assumptions

If not stated otherwise, k will be a perfect field and K/k a finite Galois extension with Galois Γ.

Acknowledgment

I would like to express my gratitude to several people; first of all I would like to thank Prof. Plesken for teaching me about this topic and for the numerous discussions, secondly my family for without them this thesis would not be possible. Furthermore I would like to thank Wolfgang Krass for proof-reading and my colleagues at Lehrstuhl B for creating a nice working atmosphere. This work was partially supported by the SPP 1388 of the German Science Foundation (DFG).

Chapter 2

Forms of finite groups

Let k be a perfect field and K/k a finite GALOIS extension with group Γ. In [Ser02, Chapter III] SERRE mentions the following general principle underlying the theory of forms: "Let X be an "object defined over k", we shall say that an object Y, defined over k, is a K/k-form of X if Y becomes isomorphic to X when the ground field is extended to K."

Hence, the existence and classification question mentioned in the introduction can be asked for general algebraic objects for which it makes sense to speak of something "defined over k". If X is either a vector space with tensors, that is for example a central simple algebra, or a semisimple algebraic group, we can refer to a good amount of literature on both questions cf. [Sat71], [Ser79], [Ser02]. Little is known when it comes to finite groups and even less for representations.

In the first section some basic definition from the theory of algebraic groups are given and k-forms of finite matrix groups G, respectively representations thereof, are defined. Theorem (2.1.7) shows that the ring of polynomial invariants of those forms is generated by a set of polynomials whose coefficients lie in k.

The existence of (K/k)-forms of G, where K/k is a finite GALOIS extension, is addressed briefly in the second section. Some obvious necessary conditions on the natural character of G are obtained, which imply that the automorphism group of G acts transitively on the GALOIS conjugates on the natural character of G. Considering the REE group ${}^2\mathrm{F}_4(2)'$ in dimension 26 shows that this condition is not sufficient.

An easy, nevertheless important, observation is that if those necessary conditions are fulfilled, the enveloping k-algebra of the natural representation of G is equipped with a Γ-action as k-algebra automorphisms. This will be the starting point for further investigations of the existence question in the third chapter.

Section three basically reviews the work of SHODA, who established a correspondence between k-forms of finite matrix groups, up to conjugation with matrices in $\mathrm{GL}_n(k)$, and modules over certain skew group rings.

The classification question is answered using elementary group theory in the last section.

2.1 Definitions and first properties

We have to recall some basic definitions from algebraic group theory. The book [Sat71] of Satake will be the main source.

Definition 2.1.1. Let $N \in \mathbb{N}$, a subset X of $\overline{k}^N$ is called an (affine) **algebraic set** if there exists a subset $J \subseteq \overline{k}[x_1, ..., x_N]$ such that $X = \{x \in \overline{k}^N \mid f(x) = 0 \text{ for all } f \in J\}$. Denote by $\mathcal{I}(X) := \{f \in \overline{k}[x_1, ..., x_N] \mid f(x) = 0 \text{ for all } x \in X\}$ the ideal corresponding to X. If $\mathcal{I}(X)$ is generated by elements of $k[x_1, ..., x_N]$ we say that X is **defined over** k.

The following basic proposition can be found in the book of Satake.

Proposition 2.1.2. *[Sat71, Prop. 1.1.1] For an algebraic set X, the following conditions are equivalent:*

1. *X is defined over k*

2. *$\sigma X := \{\sigma(x) = \sigma(x_i) \mid x \in X\} = X$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$.*

Definition 2.1.3. Let X be an algebraic set in $\overline{k}^N$. A **polynomial function** (defined over k) on X is the restriction to X of a function defined by a polynomial in $\overline{k}[x_1, ..., x_N]$ (resp., $k[x_1, ..., x_N]$).

For an algebraic set A, denote by $\overline{k}[A]$ (resp., $k[A]$) the ring of polynomial functions on A (defined over k).

Definition 2.1.4. Let A and B be algebraic sets in $\overline{k}^n$ and $\overline{k}^m$ respectively. A **polynomial** map φ from A to B is a mapping given by $\varphi = (\varphi_1, ..., \varphi_m), \varphi_i \in \overline{k}[A]$. We say the φ is **defined over** k if $\varphi_i \in k[A]$.

Now we can define algebraic groups.

Definition 2.1.5. G is called an (affine) **algebraic group** if

1. G is an abstract group

2. G is an algebraic set in $\overline{k}^N$

3. The mapping $G \times G \to G$, $(x, y) \mapsto x^{-1}y$ is a polynomial map.

G is **defined over** k if G as an algebraic set is defined over k, and the mapping in 3. is defined over k.

Let n be an integer and G a finite subgroup of $\mathrm{GL}_n(\overline{k})$. Viewing $\mathrm{GL}_n(\overline{k})$ as an algebraic group, turns G into a (totally disconnected) algebraic group. We say that G is defined over k if it is defined over k as an algebraic group.

To establish a connection with invariant theory we need the following lemma which goes back to Speiser.

Lemma 2.1.6 (Speiser)**.** *Let K/k be a finite* Galois *extension with group Γ, and V a K-vector space equipped with a semi-linear Γ-action i.e. a Γ-action satisfying*

$$\sigma(\lambda v) = \sigma(\lambda)\sigma(v) \text{ for all } \sigma \in \Gamma, v \in V \text{ and } \lambda \in K.$$

Then the natural map $V^\Gamma \otimes_k K \to V$ is an isomorphism.

Proof. [GS06, Lemma 2.3.8] □

We come to the first main theorem.

Theorem 2.1.7. *For a finite subgroup G of $\mathrm{GL}_n(\overline{k})$ the following are equivalent:*

1. *The algebraic group G is defined over k.*
2. *The ring of polynomial invariants of G is generated by elements whose coefficients lie in k.*
3. *The absolute* Galois *group of $\overline{k}$ acts naturally on G and induces a group homomorphism $^-: \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(G)$*

Proof. The equivalence of 1) and 3) is immediate by proposition (2.1.2).

2) $\Rightarrow$ 1) : From invariant theory of finite groups it is clear that a set of generating invariants uniquely determines G as an algebraic group. Since it is possible to choose such fundamental invariants with coefficients in k, the group G is defined over k.

3) $\Rightarrow$ 2) : Without loss of generality we can assume that G lies in $\mathrm{GL}_n(K)$, where K/k is a finite Galois extension with Galois group Γ. Let Γ act on $K[x_1, ..., x_n]$ by applying an element $\sigma \in \Gamma$ to the coefficients. This is a semilinear action and using 3) one checks that this induces a semi-linear action on the invariant ring $K[x_1, ..., x_n]^G$. Using lemma (2.1.6) it follows that for every degree $d \in \mathbb{N}$ we can find a k-basis of $K[x_1, ..., x_n]^G_{\leq d}$. By Noethers bound we only have to look up to degree $|G|$ to find fundamental invariants. Hence there exists a set of fundamental invariants with coefficients in k. □

The following example illustrates the theorem.

Example 2.1.8. Consider the matrix group

$$\mathrm{Q}_8 := \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} , \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

isomorphic to the quaternion group of order 8. The group Q_8 is defined over $\mathbb{Q}$, since the ring of polynomial invariants is generated by $x_1^2x_2^2, x_1^4+x_2^4, x_1x_2^5-x_2x_1^5$. Applying the complex conjugation to the entries of the matrices induces an injective homomorphism $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{Q}_8)$. The image of this homomorphism is the group generated by the inner automorphism given by conjugation with the second generator.

We now define the notion of a k-form of a finite matrix group G.

Definition 2.1.9. Let G be a finite subgroup of $\mathrm{GL}_n(\overline{k})$, then a subgroup $\widetilde{G}$ of $\mathrm{GL}_n(\overline{k})$ is called a k**-form of** G if $\widetilde{G}$ is defined over k and conjugates to G inside $\mathrm{GL}_n(\overline{k})$. It is a (K/k)**-form of** G if additionally $\widetilde{G}$ lies in $\mathrm{GL}_n(K)$. We say that two (K/k)-forms of G are **equivalent** if they are conjugate to each other by an element of $\mathrm{GL}_n(k)$.

Note that those definitions differ slightly from the theory of k-forms of algebraic groups, since we use conjugation rather than polynomial maps.

Examples of finite subgroups of $\mathrm{GL}_n(\overline{k})$ defined over k appear as stabilizers of a single polynomial with coefficients in k.

Example 2.1.10. Let $n, d \in \mathbb{N}$ and $H_{n,d}$ a hypersurface of degree d in $(n+1)$-dimensional projective space $\mathbb{P}^{(n+1)}(\mathbb{C})$, defined by an equation $p(x_0, ..., x_{n+1}) = 0$ of degree d with $p \in \mathbb{Q}[x_0, ..., x_{n+1}]$. The algebraic group $\mathrm{GL}_{n+2}(\mathbb{C})$ acts on $\mathbb{C}[x_0, ..., x_{n+1}]$.

1. If $H_{n,d}$ is non singular and $n \geq 2, d \geq 3$, then by [MM64] the stabilizer of p in $\mathrm{GL}_n(\mathbb{C})$ is finite and defined over $\mathbb{Q}$.
2. Let $p = x_0^3 x_1 + x_1^3 x_2 + x_2^3 x_0$, then its stabilizer in $\mathrm{GL}_3(\mathbb{C})$ is finite and isomorphic to $\mathrm{C}_4 \times \mathrm{PSL}_2(7)$. KLEIN'S famous three dimensional representation of $\mathrm{PSL}_2(7)$ [Kle99] can be constructed this way.

The next remark shows that it is enough to work with finite GALOIS extensions K/k rather than $\overline{k}$.

Remark 2.1.11. If G is defined over k there exists a GALOIS extension K of k with GALOIS group Γ, such that G lies in $\mathrm{GL}_n(K)$ and the map $^-$ of (2.1.7) restricts to an injective homomorphism $^- : \Gamma \to \mathrm{Aut}(G)$.

A more precise definition of a k-form is given by adding the field K and the homomorphism $^- : \Gamma \to \mathrm{Aut}(G)$.

Definition 2.1.12. Let G be a finite subgroup of $\mathrm{GL}_n(\overline{k})$, K/k a GALOIS extension with GALOIS group Γ and $^- : \Gamma \to \mathrm{Aut}(G)$ an injective homomorphism. A representation $\Delta : G \to \mathrm{GL}_n(K)$ is a $(K/k, ^-)$**-representation** of G, if for all $g \in G$ and $\sigma \in \Gamma$ one has $\sigma(\Delta(g)) = \Delta(\overline{\sigma}(g))$.

Remark 2.1.13. Choosing $K = k$ in the last definition one gets back the definition of k-linear representations of G.

2.2 Existence question

A precise version of the existence question for (K/k)-forms of finite groups is given in the next remark.

Remark 2.2.1. Given a finite subgroup G of $\mathrm{GL}_n(\overline{k})$ is it possible to find a GALOIS extension K/k with group Γ and an embedding $^- : \Gamma \to \mathrm{Aut}(G)$, such that there exists a $(K/k, ^-)$-representation of G which is $\mathrm{GL}_n(\overline{k})$ conjugate to the natural representation of G?

Assuming that (2.2.1) has a positive answer for G, one obtains an obvious necessary condition involving the natural character of G.

Remark 2.2.2. For the existence of a $(K/k, ^-)$-representation of G it is necessary that the embedding $^- : \Gamma \to \mathrm{Aut}(G)$ has the property that $\sigma \circ \chi = \chi \circ \overline{\sigma}$ for all $\sigma \in \Gamma$.

One might conjecture, that if $\mathrm{Aut}(G)$ acts transitively on the set of Galois conjugate characters of the natural character χ, then there exists a (K/k)-form of G. The next example shows this is not the case. It was found by an inspection of the ATLAS [CCN+85] and does not provide much structural insight.

Example 2.2.3. Let $k = \mathbb{R}$, $\Gamma = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and G be the Ree group $^2\mathrm{F}_4(2)'$. Use the ATLAS to see that there are two characters χ_1, χ_2 of degree 26 which have values in $\mathbb{C}$ and are Galois conjugates of each other. Check that the automorphism group of G acts transitively on $\{\chi_1, \chi_2\}$. Assume that there exists a subgroup of $\mathrm{GL}_{26}(\mathbb{C})$ which is defined over $\mathbb{R}$, isomorphic to G and has χ_1 or χ_2 as its natural character. Hence there exists an embedding $^- : \Gamma \to \mathrm{Aut}(G)$ with $\chi_1 \circ \overline{\sigma} = \sigma \circ \chi_1 = \chi_2$. Use the ATLAS again to see that such an embedding cannot exist, more precisely that there is no automorphism of order 2 of G interchanging χ_1 and χ_2.

Let Δ be the natural representation G and χ the natural character. Assume that Δ is a $(K/k, ^-)$-representation of G, then this has the following consequence on the enveloping algebra $\Delta(kG)$.

Remark 2.2.4. If Δ is a $(K/k, ^-)$-representation of G, then

$$\Gamma \times \Delta(kG) \to \Delta(kG) \ : \ (\sigma, X) \mapsto \sigma(X)$$

is a well defined Γ-action as k-algebra automorphisms. On $\Delta(G)$ it is given by $\sigma(\Delta(g)) = \Delta(\overline{\sigma}(g))$ for all $g \in G$.

For the rest of this section we will restrict ourselves to the case that G is an absolutely irreducible finite matrix group. An important observation is that absolutely irreducible representations, of a given degree, of a finite group are, up to equivalence, uniquely determined by their characters. Most certainly this result was known to Brauer and in the following form is found in [Jam].

Proposition 2.2.5. *Let G be a finite group, K a field and $\Delta, \Theta : G \to \mathrm{GL}_n(K)$ absolutely irreducible representations. Then Δ is equivalent to Θ if and only if $\mathrm{Tr}(\Delta(g)) = \mathrm{Tr}(\Theta(g))$ for all $g \in G$.*

The next lemma shows that the condition on natural character of remark (2.2.2) implies that the Γ-action on G via $(\sigma, g) \mapsto \overline{\sigma}(g)$ extends uniquely to a Γ-action on $\Delta(kG)$ as k-algebra automorphisms.

Lemma 2.2.6. *Let (K/k) be a finite Galois extension with group Γ, G an absolutely irreducible finite subgroup of $\mathrm{GL}_n(K)$, $\Delta : G \to \mathrm{GL}_n(K)$ the natural representation of G and χ the natural character. Assume that $^- : \Gamma \to \mathrm{Aut}(G)$ is an embedding with the property that $\sigma \circ \chi = \chi \circ \overline{\sigma}$ for all $\sigma \in \Gamma$. The Γ-action $\Gamma \times kG \to kG \ : \ (\sigma, \sum_{g \in G} a_g g) \mapsto \sum_{g \in G} a_g \overline{\sigma}(g)$ induces an Γ-action on $\Delta(kG)$ as k-algebra automorphisms.*

Proof. Since Δ is absolutely irreducible it induces an absolutely irreducible representation of the semisimple algebra $kG/\mathrm{rad}(kG)$. The two sided ideal $\mathrm{rad}(kG)$ is Γ invariant under the given Γ-action on kG, hence Γ acts on $kG/\mathrm{rad}(kG)$. This representation is uniquely defined by its character by proposition (2.2.5) and one checks that the condition $\sigma \circ \chi = \chi \circ \overline{\sigma}$ for all $\sigma \in \Gamma$ implies that the central primitive idempotent of $kG/\mathrm{rad}(kG)$ corresponding to Δ is Γ invariant. This proves the lemma. □

The following remark is immediate from the proof of the last lemma.

Remark 2.2.7. If the characteristic of K is coprime to $|G|$, the assumption of G being absolutely irreducible in the last lemma is redundant.

Hence, for a positive answer to the existence question (2.2.1) it is necessary that Γ acts as k-algebra automorphisms on the enveloping algebra $\Delta(kG)$. This will be the starting point of chapter three.

2.3 Skew group rings

In this section we introduce skew group rings into the picture. We assume that the Galois extension K/k with group Γ and the embedding $^- : \Gamma \to \mathrm{Aut}(G)$ are given, hence we take a slightly different point of view from the last section. The objective is to consider all possible $(K/k, ^-)$-representations at once. Most of this section reviews Shoda's work on semilinear representation theory cf. [NS36], [Sho38a] and [Sho38b]. Recall the definition of a skew group ring.

Definition 2.3.1. Let R be a ring, G a finite group and $\Theta : G \to \mathrm{Aut}(R)$ a group homomorphism. The **skew group ring** $R * G = \oplus_{x\in G} Rx$ is defined to be the free R-module with basis $\{x\}_{x\in G}$ and multiplication defined by

$$r_x x r_y y = r_x \Theta(x)(r_y) xy \text{ for all } x, y \in G \text{ and } r_x, r_y \in R$$

Assume the situation of remark (2.1.11) that K/k is a Galois extension and $^- : \Gamma \to \mathrm{Aut}(G)$ an injective homomorphism. Use the Γ-action on G via $(\sigma, g) \mapsto \overline{\sigma}(g)$ to define the semidirect product $G \rtimes \Gamma$ and let $\Theta : G \rtimes \Gamma \to \Gamma$ be the natural epimorphism. Construct the skew group ring $K * (G \rtimes \Gamma)$ and note that it is a k-algebra.

Remark 2.3.2. The natural embeddings induce the following commutative diagram:

$$\begin{tikzcd} k \arrow[r] \arrow[d] & k\Gamma \arrow[r] \arrow[d] & k(G \rtimes \Gamma) \arrow[d] \\ K \arrow[r] & K * \Gamma \arrow[r] & K * (G \rtimes \Gamma) \end{tikzcd}$$

Hence $K * (G \rtimes \Gamma)$ is build from the group ring $k(G \rtimes \Gamma)$, incorporating the group theoretic action of Γ on G and the crossed product algebra $K * \Gamma$, which incorporates the arithmetic action of Γ on K.

The objective is to prove the following main theorem, which could be easily extracted from the work of Shoda.

Theorem 2.3.3. *Let G be a finite group, K/k be a finite* Galois *extension with group Γ and $^{-} : \Gamma \to \mathrm{Aut}(G)$ an embedding. There exists a one to one correspondence between $K * (G \rtimes \Gamma)$-modules up to isomorphism and $(K/k, ^{-})$-representations of G up to conjugation with matrices in $\mathrm{GL}_n(k)$.*

This theorem sheds some light on the connection to invariant theory given in theorem (2.1.7).

Remark 2.3.4. Let M be a $K*(G\rtimes\Gamma)$-module and view $M^* := \mathrm{Hom}(M, k)$ as a K-vectorspace. The group $G\rtimes\Gamma$ acts K-semilinearily on M^* via $g\omega := \omega\circ g^{-1}$ for all $g \in G \rtimes \Gamma$ and $\omega \in M^*$. This extends to a K-semilinear action on the symmetric algebra. Choose a k-basis $x_1, ..., x_n$ of $(M^*)^\Gamma$ and view it as a K-basis of M^*. Hence, the group $G \rtimes \Gamma$ acts on the polynomial ring $K[x_1, ..., x_n]$ by applying Γ to the coefficients and using the natural G-action. This action is K-semilinear, preserves the natural grading and turns $K[x_1, ..., x_n]$ into an infinite dimensional $K * (G \rtimes \Gamma)$-module. Lemma (2.1.6) shows that for every degree $r \in G$ a k-basis of $K[x_1, ..., x_n]^{G\rtimes\Gamma}_{\leq r}$ is a K-basis of $K[x_1, ..., x_n]^{G}_{\leq r}$.

The last remark can be found in the work of Shoda [Sho38b]. Before we prove the main theorem, we revisit example (2.1.8).

Example 2.3.5. Let $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \Gamma$ and $^{-} : \Gamma \to \mathrm{Aut}(\mathrm{Q}_8)$ be the homomorphism mapping the generator σ of Γ to the inner automorphism induced by conjugation with the second generator of Q_8. Consider the skew group ring $\mathbb{Q}(i) * (\mathrm{Q}_8 \rtimes\Gamma)$ and note that a $\mathbb{Q}$-linear representation Δ of $\mathbb{Q}(i) * (\mathrm{Q}_8 \rtimes\Gamma)$ is completely determined by the images of i, σ, a, b, where a, b are the generators of Q_8. Since the natural representation of Q_8 is a $(\mathbb{Q}(i)/\mathbb{Q}, ^{-})$-representation, the last theorem provides a $\mathbb{Q}(i) * (\mathrm{Q}_8 \rtimes\Gamma)$ structure on $\mathbb{Q}(i)^{2\times1}$. The induced $\mathbb{Q}$-linear representation is given by:

$$i \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \sigma \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$b \mapsto \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad a \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

Note that these matrices generate a subgroup of $\mathrm{GL}_4(\mathbb{Q})$ isomorphic to $(\mathrm{C}_4 \curlyvee_{\mathrm{C}_2} \mathrm{Q}_8) \rtimes \mathrm{C}_2$, where $\mathrm{C}_4 \curlyvee_{\mathrm{C}_2} \mathrm{Q}_8$ is the central product amalgamated over C_2. With the methods developed later, one sees that $\mathbb{Q}(i) * (\mathrm{Q}_8 \rtimes\Gamma)$ has the Wedderburn decomposition $\oplus_{i=1}^{4}\mathbb{Q}^{2\times2} \oplus \mathbb{Q}^{4\times4}$. Hence it is not isomorphic to the group ring $\mathbb{Q}(\mathrm{C}_4 \curlyvee_{\mathrm{C}_2} \mathrm{Q}_8) \rtimes \mathrm{C}_2$, which decomposes as $\oplus_{i=1}^{16}\mathbb{Q}^{1\times1} \oplus \mathbb{Q}^{4\times4}$.

We proceed to prove the main theorem.

Lemma 2.3.6. *Let $\Delta : G \to \mathrm{GL}_n(K)$ be a $(K/k, ^-)$-representation. The action of G on $K^{n\times 1}$ via Δ and the componentwise action of Γ turn $K^{n\times 1}$ into an $K * (G \rtimes \Gamma)$ module.*

Proof. Follows from the definition of a $(K/k, ^-)$-representation. □

Let M be a $K * (G \rtimes \Gamma)$-module. Note that M is a K-vectorspace and that Γ acts K-semilinearily on M. Denote by M^Γ the k-space of fixed points of M under Γ. Lemma (2.1.6) implies that a k-basis of M^Γ can be considered as a K-basis of M. Such a basis is used in the next lemma to construct a $(K/k, ^-)$-representation.

Lemma 2.3.7. 1. *Let M be a $K * (G \rtimes \Gamma)$ module of K-dimension n and B a k-basis of M^Γ. The K-linear representation $\Delta_{M,B} : G \to \mathrm{GL}_n(K)$ with respect to the basis B is a $(K/k, ^-)$-representation.*

2. *If M_1, M_2 are two isomorphic $K * (G \rtimes \Gamma)$-modules of K-dimension n, and $B, \widetilde{B}$ be $\mathbb{Q}$-bases of M_1^Γ and M_2^Γ respectively, then there exists a $Y \in \mathrm{GL}_n(k)$ such that*

$$Y^{-1}\Delta_{M_1,B}(g)Y = \Delta_{M_2,\widetilde{B}}(g) \text{ for all } g \in G$$

Proof. Identify G and Γ with subgroups of $G := G \rtimes \Gamma$. Let $B = (B_1, ..., B_n)$, then by definition we have $g(B_j) = \sum_{i=1}^n \Delta(g)_{i,j} B_i$ for all $g \in G$. Hence

$$\begin{aligned} \overline{\sigma}(g)(B_j) &= (\sigma g \sigma^{-1})(B_j) \\ &= \sum_{i=1}^n \sigma(\Delta(g)_{i,j}) B_i \end{aligned}$$

This implies $\sigma(\Delta(g)) = \Delta(\overline{\sigma}(g))$ for all $g \in G$, that is Δ is a $(K/k, ^-)$-representation.

For the second part let $B, \widetilde{B}$ be k-bases of M_1^Γ, M_2^Γ and $\varphi : M_1 \to M_2$ a $K*G$-module isomorphism. It is clear that φ restricts to an isomorphism $M_1^\Gamma \to M_2^\Gamma$, so $Y := {}^B\varphi^{\widetilde{B}}$ lies in $\mathrm{GL}_n(k)$. Obviously Y has the desired properties. □

The second part of the last lemma is a classical result of Shoda [Sho38a]. Summing up, lemma (2.3.6) and (2.3.7) induce mutually inverse maps between $K * (G \rtimes \Gamma)$-modules up to isomorphism and $(K/k, ^-)$-representations of G up to conjugation with matrices in $\mathrm{GL}_n(k)$.

2.4 Classification

From the point of view of invariant theory (K/k)-forms of finite matrix groups are more appropriate than the rather restrictive $(K/k, ^-)$-representations. The objective is to classify the $(K/k, ^-)$-representations leading to the same K/k-form of a finite matrix group. Those are classified using elementary group theory and this answers the classification question raised in the introduction of this chapter.

Note that for any homomorphism $\varphi : \Gamma \to \mathrm{Aut}(G)$ it makes sense to speak of a $(K/k, \varphi)$-representation of G. We will prove the following classification theorem.

Theorem 2.4.1. *Let K/k be a finite* GALOIS *extension with group Γ, G a finite irreducible subgroup of $\mathrm{GL}_n(K)$ defined over k and*

$$\mathcal{G} := \{\varphi : \Gamma \to \mathrm{Aut}(G) \mid \textit{There exists a } (K/k,\varphi)\textit{-representation } \Delta \textit{ of } G \textit{ and the matrix group } \Delta(G) \textit{ is conjugate to } G \textit{ inside } \mathrm{GL}_n(K)\}$$

The group $\mathrm{Aut}(G)$ acts on $\mathcal{G}$ via

$$\mathrm{Aut}(G) \times \mathcal{G} \to \mathcal{G} \ : \ (\psi, \varphi) \mapsto (\Gamma \to \mathrm{Aut}(G) \ : \ \sigma \mapsto \psi \circ \varphi(\sigma) \circ \psi^{-1})$$

and the orbits correspond to the equivalence classes of (K/k)-forms of G.

Proof. Since G is defined over k, the natural representation is obviously a $(K/k, ^-)$ representations, where $^- : \Gamma \to \mathrm{Aut}(G)$ is obtained from the Γ-action on G mentioned in lemma (2.1.7). Hence $\mathcal{G}$ is non empty and one easily checks that the $\mathrm{Aut}(G)$ action on $\mathcal{G}$ is well defined.

Let G' be a (K/k)-form of G. By definition there exists a matrix $X \in \mathrm{GL}_n(K)$ such that $XG'X^{-1} = G$. Define $\varphi_{G'} : \Gamma \to \mathrm{Aut}(G) : \sigma \mapsto (g \mapsto X\sigma(X^{-1}gX)X^{-1})$ and $\Delta_{G'} : G \to \mathrm{GL}_n(K)$, $g \mapsto X^{-1}gX$. From

$$\sigma(\Delta_{G'}(g)) = \sigma(X^{-1}gX) = X^{-1}\varphi(g)X$$

it follows that $\Delta_{G'}$ is a $(K/k, \varphi_{G'})$-representation of G.

One easily checks that this defines a map between (K/k)-forms of G up to conjugation with elements of $\mathrm{GL}_n(k)$ to $\mathcal{G}$. From the definition of $\mathcal{G}$ it is obvious that this map is surjective. It remains to prove the injectivity.

Note that it is enough to show that if $\varphi_{G'} = \varphi_G$, then G' is conjugate to G via an element of $\mathrm{GL}_n(k)$. Assume that $\varphi_{G'} = \varphi_G$ and $XG'X^{-1} = G$ where $X \in \mathrm{GL}_n(K)$, then we can find matrices $\lambda_\sigma \in \mathrm{C}_{\mathrm{GL}_n(K)}(G) := \{Y \in \mathrm{GL}_n(K) \mid YgY^{-1} = g \text{ for all } g \in G\}$ such that

$$X = \lambda_\sigma \sigma(X) \text{ for all } \sigma \in \Gamma$$

View λ_σ as a map $\Gamma \to \mathrm{C}_{\mathrm{GL}_n(K)}(G)$ and check that this defines a 1-cocycle with values in $\mathrm{C}_{\mathrm{GL}_n(K)}(G)$. Using the proof of the HILBERT 90 theorem [Ser79, p. 151] and the irreducibility of G, we find that λ_σ is a coboundary i.e. $\lambda_\sigma = Y^{-1}\sigma(Y)$ for an $Y \in \mathrm{C}_{\mathrm{GL}_n(K)}(G)$. Define $\widetilde{X} := YX$ the $\widetilde{X} \in \mathrm{GL}_n(k)$ and conjugates G' to G. □

Remark 2.4.2. Let G be a finite subgroup of $\mathrm{GL}_n(K)$ where K/k is a GALOIS extension with group Γ.

1. Let $\varphi_1, \varphi_2 : \Gamma \to \mathrm{Aut}(G)$ be two embeddings, such that $\varphi_2(\sigma) = \psi \circ \varphi_1(\sigma) \circ \psi^{-1}$ with $\psi \in \mathrm{Aut}(G)$. The canonical isomorphism between the semi direct products $G \rtimes_{\varphi_1} \Gamma$ and $G \rtimes_{\varphi_2} \Gamma$ induces an isomorphism between the skew group rings $K * (G \rtimes_{\varphi_1} \Gamma)$ and $K * (G \rtimes_{\varphi_2} \Gamma)$.

2. In general the set $\mathcal{G}$ is hard to compute, but if $p \in \{5, 7\}$, $G \cong \mathrm{PSL}_2(p)$ and $K = \mathbb{Q}(\zeta_p)$ then there exists a unique conjugacy class of elements of order $p - 1$ in $\mathrm{Aut}(G)$. Hence there exists only one $\mathrm{Aut}(G)$ orbit on $\mathcal{G}$. So, independently of the (irreducible) representation of G all possible $(K/\mathbb{Q})$-forms of G are equivalent.

Chapter 3

Brauer-Clifford theory

Let k be a perfect field, recall the existence question posed in remark (2.2.1):

Given a finite subgroup G of $\mathrm{GL}_n(\overline{k})$ is it possible to find a Galois extension K/k with group Γ and an embedding $^- : \Gamma \to \mathrm{Aut}(G)$, such that there exists a $(K/k, ^-)$-representation of G which is $\mathrm{GL}_n(\overline{k})$ conjugate to the natural representation Δ of G?

It was shown that for a positive answer to this question, it is necessary that the Γ-action $\Gamma \times kG \to kG \ : \ (\sigma, \sum_{g\in G} a_g g) \mapsto \sum_{g\in G} a_g \overline{\sigma}(g)$ induces an Γ-action on the k-enveloping algebra $\Delta(kG)$ as k-algebra automorphisms.

This turns $\Delta(kG)$ into a central simple Γ-algebra in the sense of [Tur94a]. Turull defines a equivalence relation for those algebras, which is similar to the equivalence relation on central simple algebras leading to the Brauer group. We will recall this relation in the first section. Furthermore, Turull establishes a group structure on the equivalence classes [Tur94b] and this group is called the Brauer-Clifford group. Some natural operations on the Brauer-Clifford group are introduced, most notably, a group homomorphism induced by Γ-equivariant scalar extension.

The main theorem (3.2.1), as stated in the second section, says: There exists a $(K/k, ^-)$-representation of G if and only if the equivalence class of $\Delta(kG)$ viewed as a central simple Γ-algebra lies in the kernel of this homomorphism. The main benefit of this theorem is that this equivalence class depends only on the Galois group Γ as an abstract group and can be defined independently of K. Hence all Galois extensions K/k with Galois group isomorphic to Γ are considered at once.

This leaves two problems. The first one is to recognize elements in the Brauer-Clifford group and the second is to decide if an element of the Brauer-Clifford group lies in the kernel of the homomorphism coming from scalar extension with K. One result is that both problems can be reduced to the case that the Γ is a p-group.

In general it is an open problem to recognize elements in the Brauer-Clifford group or equivalently, to find a convenient description of it. In section three we restrict to a subgroup of the Brauer-Clifford group which is a central product of the Brauer group over k with a second cohomology group $\mathrm{H}^2(\Gamma, L^*)$ where L is a subfield of K and Galois over k. Given an element of this group, it is possible to calculate necessary and sufficient conditions on a field K to admit a $(K/k, ^-)$-representation of G.

3.1 The Brauer-Clifford group

Let U be a finite group, k a perfect field. The following reviews shortly the theory of central simple U-algebras. More details can be found in the work of Turull (cf. [Tur94a]). A **U-algebra** A is a finite dimensional associative k-algebra together with a U-action on A as k-algebra automorphisms. The U-algebra A is a **simple** U-algebra if it has only the trivial two sided U-invariant ideals, and A is called **central** if k is the fixed field of the U-action restricted to the center of A. Two U-algebras are U-isomorphic if there exist a U-equivariant k-algebra isomorphism and this is denoted $A \cong_U B$. A U-algebra A is **trivial** if there exists a kU-module M such that $A \cong_U \mathrm{End}_k(M)$ with U acting on $\mathrm{End}_k(M)$ by conjugation. Two central simple U-algebras A and B are **equivalent** if there exist trivial U-algebras E_1 and E_2 such that $A \otimes_k E_1 \cong_U B \otimes_k E_2$. Let L be a central simple commutative U-algebra, then A is a central simple **U-algebra over** L if the center $\mathrm{C}(A)$ of A is isomorphic to L as a central simple U-algebra. The notion of equivalence of central simple U-algebras defines an equivalence relation on the set of all central simple U-algebras over L. If A is a central simple U-algebra over L, denote by $[A]$ its equivalence class. The Brauer-Clifford group is defined as follows.

Definition 3.1.1. Let L be a commutative central simple U-algebra. As a set, the Brauer-Clifford group $\mathrm{BrCliff}(U, L)$ consists of all equivalence classes of central simple U-algebras over L. The group structure is given by:

$$\mathrm{BrCliff}(U,L) \times \mathrm{BrCliff}(U,L) \to \mathrm{BrCliff}(U,L) \ : \ ([A],[B]) \mapsto [A \otimes_L B]$$

For more details, especially proofs of the statements implicit in the definition, see [Tur09b]. Note that the identity element of the Brauer-Clifford group is the equivalence class $[L]$ where L is viewed as a central simple U-algebra. Furthermore if U is the trivial group one gets the Brauer group.

Now through this chapter, it is assumed that the commutative central simple U-algebra L is a field. Hence there exists an epimorphism $\hat{}: U \to \mathrm{Gal}(L/k)$.

Some natural operations on the Brauer-Clifford group need to be introduced. The first operation is "forgetting the U-action" cf. [Tur09b, Theorem 8.2]

Remark 3.1.2. There exists a natural homomorphism $\kappa : \mathrm{BrCliff}(U, L) \to \mathrm{Br}(L)^{\mathrm{Gal}(L/k)}$. Denote by $\mathrm{FMBrCliff}(U, L)$ the kernel of κ, then there is the following exact sequence:

$$1 \longrightarrow \mathrm{FMBrCliff}(U,L) \longrightarrow \mathrm{BrCliff}(U,L) \longrightarrow \mathrm{Br}(L)^{\mathrm{Gal}(L/k)}$$

Note that $\mathrm{FMBrCliff}(U, L)$ consists of the equivalence classes of those central simple U-algebras which are isomorphic, as central simple L-algebras, to matrix algebras over L.

We introduce the notion of a U-field.

Definition 3.1.3. Let U a finite group, K/L and L/k field extensions and let U-act on L and K as field automorphisms, then L, K are called **U-fields**. If the embedding of $L \to K$ is U-equivariant, then K/L is called a **U-field extension**.

In particular, if A is a central simple U-algebra over L, then L is a U-field. The next operation is scalar extension by a U-field.

Definition 3.1.4. Let A be a central simple U-algebra over the field L and K a U-field extension of L. Then **scalar extension of A by a U-field** K is the U-algebra $A \otimes_L K$ with U acting diagonally.

It is clear that this is a simple U-algebra over K. Since the fixed field of the U-action on K might be a proper extension of k, scalar extension of A by a U-field K might not be central over k. To avoid this problem, one views scalar extension of A by a U-field K as an algebra over the fixed field of K under U.

To carry the concept of scalar extension with a U-field over to the Brauer-Clifford group, one has to look at the trivial U-algebras. The next proposition deals with those U-algebras.

Proposition 3.1.5. *Let F be a U-field extension of k, M a kU-module and consider $M \otimes_k F$ as an FU-module. There exists a natural U-equivariant F-algebra isomorphism between the scalar extension of the trivial U-algebra* $\mathrm{End}_k(M)$ *by F and the U-algebra* $\mathrm{End}_F(M \otimes_k F)$ *where U acts by conjugation.*

Proof. Consider

$$\mathrm{End}_k(M) \otimes_k F \to \mathrm{End}_F(M \otimes_k F) \;:\; \psi \otimes c \mapsto c(\psi \otimes \mathrm{id})$$

with $\psi \in \mathrm{End}_k(M)$ and $c \in F$ □

The next lemma shows that scalar extension is well defined on the Brauer-Clifford group.

Lemma 3.1.6. *Let K be a U-field extension of L. Then scalar extension by K induces a group homomorphism:*

$$\mathrm{ext}_{K/L} : \mathrm{BrCliff}(U, L) \to \mathrm{BrCliff}(U, K) \;:\; [A] \mapsto [A \otimes_L K]$$

Proof. We have to show that this map is well defined. Let F be the fixed field of K under U. Assume that A and B are equivalent central simple U algebras over L and let M_1, M_2 be kU-modules such that $A \otimes_k \mathrm{End}_k(M_1) \cong_U B \otimes_k \mathrm{End}_k(M_2)$. Consider $\mathrm{End}_F(M_i \otimes F)$ for $i = 1, 2$ as trivial U-algebras. Use lemma (3.1.5) to calculate:

$$\begin{aligned}
(A \otimes_L K) \otimes_F \mathrm{End}_F(M_1 \otimes_k F) &\cong_U A \otimes_L K \otimes_F (\mathrm{End}_k(M_1) \otimes_k F) \\
&\cong_U (A \otimes_k \mathrm{End}_k(M_1)) \otimes_L K \\
&\cong_U (B \otimes_k \mathrm{End}_k(M_2)) \otimes_L K \\
&\cong_U (B \otimes_L K) \otimes_F \mathrm{End}_F(M_2 \otimes_k F)
\end{aligned}$$

Hence $A \otimes_L K$ is equivalent to $B \otimes_L K$ as central simple U-algebras over K and $\mathrm{ext}_{K/L}$ is well defined. The homomorphism property is obvious. □

The following remark considers a sequence of U-field extensions.

Remark 3.1.7. Let K be a U-field extension of L and L be a U-field extension of k, then $\mathrm{ext}_{K/k} = \mathrm{ext}_{K/L} \circ \mathrm{ext}_{L/k}$

Another natural map of the Brauer-Clifford group can be obtained via restriction to subgroups of U.

Lemma 3.1.8. *Let N be a subgroup of U, then the map* $\mathrm{res}_N : \mathrm{BrCliff}(U, L) \to \mathrm{BrCliff}(N, L) \ : \ [A] \mapsto [A \otimes_L L]$ *is a group homomorphism*

Proof. Analogous to the proof of (3.1.6) □

Using the operations introduced so far, it is possible to define the notion of an equivariant splitting field of a central simple U-algebra.

Definition 3.1.9. Let A be a central simple U-algebra over L. The U-field extension K of L is an **equivariant splitting field** of A, if $[A]$ is in the kernel of the map $\mathrm{ext}_{K/L} : \mathrm{BrCliff}(U, L) \to \mathrm{BrCliff}(U, K)$.

It is obvious that if K is an equivariant splitting field of a central simple U-algebra A, then $\mathrm{ext}_{K/L}([A])$ lies in $\mathrm{FMBrCliff}(U, K)$. For this reason it is important to find a convenient description of $\mathrm{FMBrCliff}(U, L)$. In [Tur09a] Turull shows that $\mathrm{FMBrCliff}(U, L)$ is isomorphic to the second cohomology group $\mathrm{H}^2(U, L^*)$. The next theorem recalls this isomorphism and is a special case of [Tur09a, Theorem 3.10].

Theorem 3.1.10. *Let A be a central simple U-algebra over L such that $[A] \in \mathrm{FMBrCliff}(U, L)$ and $\iota : A \to k^{l\times l}$ a k-algebra embedding with $\mathrm{C}_{k^{l\times l}}(\iota(A)) = \iota(L)$. Then there exists a map $F : U \to k^{l\times l} \ : \ u \mapsto F(u)$ such that $F(u)\iota(a)F(u)^{-1} = \iota(u(a))$ for all $a \in A$. Fix such maps ι, F, then*

$$h(A) : U \times U \to L \ : \ (s, t) \mapsto F(s)F(t)F(st)^{-1}$$

is a 2-cocycle with values in L^*. This construction induces a group isomorphism $h : \mathrm{FMBrCliff}(U, L) \to \mathrm{H}^2(U, L^*) \ : \ [A] \mapsto h(A)$.

There exists an alternative way to calculate the cocycle $h(A)$. Recall that with a central simple U-algebra L comes an epimorphism $\widehat{\ } : U \to \mathrm{Gal}(L/k)$.

Proposition 3.1.11. *Let A be a central simple U-algebra over L such that $[A] \in \mathrm{FMBrCliff}(U, L)$. Identify A with $L^{n\times n}$, then there exists a collection of matrices $\{X_u\}_{u\in U}$ in $\mathrm{GL}_n(L)$ with the property $u(a) = X_u \widehat{u}(a) X_u^{-1}$ for all $u \in U$ and $a \in L^{n\times n}$. Define the map*

$$\lambda : U \times U \to L : \ (s, t) \mapsto X_s \widehat{s}(X_t) X_{st}^{-1}$$

Then λ is a 2-cocycle with values in L^*. Furthermore λ and $h(A)$ (cf. 3.1.10) define the same cohomology class in $\mathrm{H}^2(U, L^*)$.

Proof. Identify A with $L^{n\times n}$. Because U acts on A as semilinear L-algebra automorphisms, the existence of the matrices $\{X_u\}_{u\in U}$ is clear . We show that it is possible to choose ι, F as in (3.1.10) with the property that the resulting cocycle $h(A)$ is given by $h(A)(s,t) = \lambda(s,t)$ for all $s,t \in U$.

Restriction of scalars provides a k-algebra embedding $\iota : A \to k^{l\times l}$ with $\mathrm{C}_{k^{l\times l}}(\iota(A)) = \iota(L)$. Define $u(a_1, ..., a_n)^t := (\widehat{u}(a_1), ..., \widehat{u}(a_n))^t$, then this turns $L^{n\times 1}$ into a kU-module. Hence there exists a corresponding matrix representation $U \to k^{l\times l} : u \mapsto H_u$. Use this representation to see that $H_u\iota(a)H_u^{-1} = \iota(\widehat{u}(a))$ for all $a \in A$. For $u \in U$ define $F(u) := \iota(X_u)H_u$, then a short calculation shows $F(u)\iota(a)F(u)^{-1} = \iota(u(a))$ for all $a \in A$. So ι and F fulfill the requirements of (3.1.10). Furthermore it is easy to see that $h(A)(s,t) = \lambda(s,t)$ for all $s,t \in U$. Hence λ is a 2-cocycle and it defines the same cohomology class as $h(A)$. □

Corollary 3.1.12. *Let A be a central simple U-algebra over L such that $[A] \in \mathrm{FMBrCliff}(U,L)$ and $\dim_L(A) = n^2$. Then the order of $[A]$, as an element of $\mathrm{BrCliff}(U,L)$, divides n and $|U|$.*

Proof. Since $h : \mathrm{FMBrCliff}(U,L) \to \mathrm{H}^2(U,L^*)$ is an isomorphism, the order of $[A]$ is the same as the order of $h(A)$. Then it is a well known fact in group cohomology, that the order of $h(A)$ divides $|U|$. Consider the equation $\lambda(s,t) = X_s\overline{s}(X_t)X_{st}^{-1}$ of (3.1.11). Taking determinants on both sides shows that λ^n is a coboundary. This implies that the order of λ as an element of $\mathrm{H}^2(U,L^*)$ divides n. Hence the order of $h(A)$ divides n. □

3.2 Main theorem

Recall the existence question of (2.2.1). The main theorem states that this can be decided by considering the enveloping algebra of the natural representation of G as an element of the Brauer-Clifford group.

Theorem 3.2.1. *Let (K/k) be a finite Galois extension with group Γ, $G \leq \mathrm{GL}_n(K)$ a finite and absolutely irreducible matrix group, Δ the natural representation of G, $\Delta(kG)$ the enveloping algebra of the natural representation, L the center of $\Delta(kG)$ and $^- : \Gamma \to \mathrm{Aut}(G)$ an injective homomorphism. Assume the Γ action $\Gamma \times \Delta(G)$, $(\sigma, \Delta(g)) \mapsto \Delta(\overline{\sigma}(g))$ on $\Delta(G)$ extends to a Γ-action on $\Delta(kG)$ as k-algebra automorphisms. This turns $\Delta(kG)$ into a central simple Γ-algebra over L. View K as a Γ-field via the natural action of Γ, then there exists a $(K/k, ^-)$-representation of G, conjugate to the natural representation of G in $\mathrm{GL}_n(\overline{k})$, if and only if K is a Γ-equivariant splitting field of $\Delta(kG)$.*

Proof. Assume that there exists a $(K/k, ^-)$-representation of G. By replacing G with the image of this representation it can be assumed that the natural representation Δ of G is a $(K/k, ^-)$-representation. Scalar extension of $\Delta(kG)$ by the Γ-field K is the central simple Γ-algebra $K^{n\times n}$, where Γ acts by applying its elements entrywise. It is easy to see that this central simple Γ-algebra is equivalent to the central simple Γ-algebra K. Since $[K]$ represents the trivial element of FMBrCliff(Γ, K), it follows that $[\Delta(kG)]$ is in the kernel of the scalar extension map $\mathrm{ext}_{K/L}$. Hence K is an equivariant splitting field of $\Delta(kG)$.

For the "if" part assume that K is an equivariant splitting field of $\Delta(kG)$. Via the natural map $\Delta(kG) \otimes_L K \to K^{n\times n}$ identify the scalar extension of $\Delta(kG)$ by the Γ-field K with $K^{n\times n}$. Note that we are dealing with two Γ-actions on $K^{n\times n}$. To distinguish both actions we write $\widehat{\sigma}$ for an element $\sigma \in \Gamma$ if the entrywise application is meant and σ for the Γ-action coming from the identification of the central simple Γ-algebra $\Delta(kG) \otimes_L K$ with $K^{n\times n}$.

By (3.1.11) there exists a collection of matrices $\{X_s\}_{s\in\Gamma}$ in $\mathrm{GL}_n(K)$ with

$$s(a) = X_s \widehat{s}(a) X_s^{-1} \text{ for all } a \in K^{n\times n} \text{ and } s \in \Gamma \tag{3.1}$$

We prove that it is possible to choose such a collection with the additional property $X_{st} = X_s \widehat{s}(X_t)$ for all $s, t \in \Gamma$.

Let $\{X_s\}_{s\in\Gamma}$ be a collection of matrices in $\mathrm{GL}_n(K)$ such that (3.1) is valid. Define the 2-cocyle $\lambda : \Gamma \times \Gamma \to K^* \; : \; (s,t) \mapsto X_s \widehat{s}(X_t) X_{st}^{-1}$. Proposition (3.1.11) implies that cohomology classes of λ and $h(\mathrm{ext}_{K/L}([\Delta(kG)]))$ are the same in $\mathrm{H}^2(\Gamma, K^*)$. Because K is an equivariant splitting field of $\Delta(kG)$, the latter is trivial. Therefore λ is a coboundary and there exists a map $b : \Gamma \to K^*$ with $\lambda(s,t) = b_s \widehat{s}(b_t) b_{st}^{-1}$ for $s, t \in \Gamma$. For s in Γ define $\tilde{X_s} := \frac{1}{b_s} X_s$, then the collection $\{\tilde{X_s}\}_{s\in\Gamma}$ clearly fulfills (3.1) and an easy calculation shows $\tilde{X_{st}} = \tilde{X_s}\widehat{s}(\tilde{X_t})$ for all $s, t \in \Gamma$.

Given such a collection of matrices the generalized HILBERT 90 theorem [Ser79, p. 151] says there exists a matrix $Y \in \mathrm{GL}_n(K)$ such that $X_s = Y \widehat{s}(Y^{-1})$, for all $s \in \Gamma$. Define the representation $\Theta : G \to \mathrm{GL}_n(K) \; : \; g \mapsto Y^{-1} g Y$ and use (3.1) to calculate:

$$\begin{aligned} \widehat{s}(\Theta(g)) &= \widehat{s}(Y^{-1})\widehat{s}(g)\widehat{s}(Y) \\ &= Y^{-1}(X_s \widehat{s}(g) X_s^{-1})Y \\ &= Y^{-1} s(g) Y \\ &= \Theta(\overline{s}(g)) \end{aligned}$$

Hence, Θ is a $(K/k, {}^{-})$-representation of G. □

Some remarks should be made about the main theorem.

Remark 3.2.2. Let K/k be a GALOIS extension with group Γ, G a finite subgroup of $\mathrm{GL}_n(K)$ and ${}^{-} : \Gamma \to \mathrm{Aut}(G)$ an embedding.

1. The group Γ acts on kG via $\Gamma \times kG$, $(\sigma, \sum_{g\in G} a_g g) \mapsto a_g \overline{\sigma}(g)$ and this induces a Γ-action on $kG/\mathrm{rad}(kG)$ because $\mathrm{rad}(kG)$ is Γ-invariant. If the assumptions of the main theorem are fulfilled, then the the natural representation Δ of G induces a Γ-equivariant k-algebra homomorphism $kG/\mathrm{rad}(kG) \to \Delta(kG)$. Since $kG/\mathrm{rad}(kG)$ is semisimple, it is easy to see that $\Delta(kG)$ is Γ-isomorphic to a simple component of $kG/\mathrm{rad}(kG)$. Therefore, the central simple Γ-algebra $\Delta(kG)$ does not depend on K and on Γ solely as an abstract group.

2. The proof of theorem (3.2.1) is constructive in the sense that it provides an explicit construction of a $(K/k, ^-)$-representation of G. Nevertheless the actual computations are non trivial and involve computations in the second cohomology group and computational class field theory.

3. Lemma (2.2.6) implies that the assumptions of (3.2.1) can be checked using the natural character χ. Specifically they are fulfilled if and only if the natural character fulfills the condition of (2.2.2).

To recognize elements of the Brauer-Clifford group and to decide if a U-field K is an equivariant splitting field come up as natural problems. A first reduction will be a restriction to certain subgroups of U. For this reason it is important to study the interplay of the scalar extension map $\mathrm{ext}_{K/L}$ and the subgroup restriction map of (3.1.8).

Let $\mathrm{BrCliff}(U, L, K)$ be the set of equivalence classes of central simple U-algebras over L for which K is a splitting field (as a central simple L-algebra). Clearly, this is a subgroup of $\mathrm{BrCliff}(U, L)$.

Given a U-field K and a subgroup N of U, the inclusion map $N \to U$ induces a natural map $\mathrm{res} : \mathrm{H}^n(U, K^*) \to \mathrm{H}^n(N, K^*)$ on the cohomology. This map is called the restriction homomorphism. For further details see [Ser79].

Lemma 3.2.3. *Let N be a subgroup of U and K a U-field extensions of L. Denote by $\mathrm{ext}_{K/L}$, res_N and h the maps of (3.1.6), (3.1.8) and (3.1.10). Then the following diagram is commutative.*

$$\begin{tikzcd}
\mathrm{BrCliff}(U, L, K) \arrow[r, "\mathrm{ext}_{K/L}"'] \arrow[d, "\mathrm{res}_N"'] & \mathrm{FMBrCliff}(U, K) \arrow[r, "h"'] \arrow[d, "\mathrm{res}_N"'] & \mathrm{H}^2(U, K^*) \arrow[d, "\mathrm{res}"'] \\
\mathrm{BrCliff}(N, K^N L, K) \arrow[r, "\mathrm{ext}_{K/K^N L}"'] & \mathrm{FMBrCliff}(N, K) \arrow[r, "h"'] & \mathrm{H}^2(N, K^*)
\end{tikzcd}$$

Proof. A verification $\square$

The idea is to use the following fact from group cohomology: An element λ of $\mathrm{H}^2(U, K^*)$ is trivial if and only if λ is in the kernel of $\mathrm{res} : \mathrm{H}^2(U, K^*) \to \mathrm{H}^2(U_p, K^*)$ for all Sylow p-subgroups of U. Combining this fact with lemma (3.2.3) leads to the following theorem, which shows that it is possible to restrict oneself to the case that U is a p-group.

Corollary 3.2.4. *Let K be a U-field extension of L and A be a central simple U-algebra such that $[A]$ is an element of $\mathrm{BrCliff}(U, L, K)$. Then $[A]$ is in the kernel of the map $\mathrm{ext}_{K/L}$ if and only if it is in the kernel of $\mathrm{ext}_{K/K^{U_p}L} \circ \mathrm{res}_{U_p}$ for all* Sylow *p-subgroups of U.*

3.3 A subgroup of the Brauer-Clifford group

In this section we look at a subgroup of the Brauer-Clifford group which admits a convenient description via cohomological methods.

Assume that K and L are GALOIS extensions of k and L is a subfield of K. Let Γ be the GALOIS group of K/k and view K and L as Γ-fields via the natural action of Γ.

Consider a central simple k-algebra as a central simple Γ-algebra over k with trivial action of Γ. This provides an injective homomorphism $\mathrm{Br}(k) \to \mathrm{BrCliff}(\Gamma, k)$. Use this homomorphism to identify the BRAUER group $\mathrm{Br}(k)$ with a subgroup of $\mathrm{BrCliff}(\Gamma, k)$. Then the scalar extensions map $\mathrm{ext}_{L/k}$ (cf. 3.1.6) is a homomorphism $\mathrm{Br}(k) \to \mathrm{BrCliff}(\Gamma, L)$. We will show that this map is injective, hence it is possible to identify the BRAUER group with a subgroup of the BRAUER-CLIFFORD group.

Denote by $\mathrm{Br}(K|k)$ the set of equivalence classes of central simple k-algebras, for which K is a splitting field. This is a subgroup of the BRAUER group $\mathrm{Br}(k)$. In [Ser79, Chapter X] SERRE obtains an isomorphism $\delta : \mathrm{Br}(K|k) \to \mathrm{H}^2(\Gamma, K^*)$ via descent theory.

Let B be a central simple k-algebra of dimension n^2, for which K is a splitting field. View B as a central simple Γ-algebra with trivial action of Γ on B. Since K is a splitting field of B, the scalar extension of B by the Γ-field K can be identified with $K^{n\times n}$. Via this identification view $K^{n\times n}$ as a central simple Γ-algebra over K. Note that we are dealing with two Γ-actions on $K^{n\times n}$. To distinguish both actions we write $\Gamma \times K^{n\times n} \to K^{n\times n} : (\sigma, x) \mapsto \sigma(x)$ if the entrywise application is meant and $\Gamma \times K^{n\times n} \to K^{n\times n} : (\sigma, x) \mapsto \widehat{\sigma}(x)$ for the Γ-action coming from the identification of the central simple Γ-algebra $B \otimes_k K$ with $K^{n\times n}$. Applying proposition (3.1.11) there exists a collection of matrices $\{X_\sigma\}_{\sigma\in\Gamma}$ with the property

$$X_\sigma \sigma(x) X_\sigma^{-1} = \widehat{\sigma}(x) \text{ for all } x \in K^{n\times n} \tag{3.2}$$

Note that B is isomorphic, as k-algebras, to the fixed algebra of $K^{n\times n}$ under Γ. Use (3.2) to see that this fixed algebra is given by $\{x \in K^{n\times n} \mid X_\sigma\sigma(x)X_\sigma^{-1} = x\}$. A 2-cocycle, representing the cohomology class of $\delta(B)$, is $\Gamma \times \Gamma \to K^* : (s,t) \mapsto X_s\overline{s}(X_t)X_{st}^{-1}$ [Ser79, Example 2, p. 159]. This cocycle also represents the cohomology class of $h(\mathrm{ext}_{K/k}([B]))$ by (3.1.11). Going over to the BRAUER-CLIFFORD group yields the following lemma.

Lemma 3.3.1. *The diagram*

$$\begin{tikzcd} \mathrm{Br}(K|k) \arrow[rr, "\delta"] \arrow[dr, "\mathrm{ext}_{K/k}"'] & & \mathrm{H}^2(\Gamma, K^*) \\ & \mathrm{FMBrCliff}(\Gamma, K) \arrow[ur, "h"'] & \end{tikzcd}$$

is commutative.

Note that h and δ in (3.3.1) are isomorphisms. Since the kernel of $\mathrm{ext}_{K/k} : \mathrm{Br}(k) \to \mathrm{BrCliff}(\Gamma, K)$ is contained in $\mathrm{Br}(K|k)$, the map $\mathrm{ext}_{K/k}$ is injective. Furthermore, the factorization $\mathrm{ext}_{K/k} = \mathrm{ext}_{K/L} \circ \mathrm{ext}_{L/k}$ implies that $\mathrm{ext}_{L/k}$ is injective.

Now look at the subgroup of $\mathrm{BrCliff}(\Gamma, L)$ generated by $\mathrm{FMBrCliff}(\Gamma, L)$ and $\mathrm{ext}_{L/k}(\mathrm{Br}(k))$. Denote this group by $\mathrm{ExFMBrCliff}(\Gamma, L)$. It is easy to see that the intersection of $\mathrm{ext}_{L/k}(\mathrm{Br}(k))$ and $\mathrm{FMBrCliff}(\Gamma, L)$ is isomorphic to $\mathrm{Br}(L|k)$. Identify the BRAUER group $\mathrm{Br}(k)$ with $\mathrm{ext}_{L/k}(\mathrm{Br}(k))$, then the next remark describes the structure of $\mathrm{ExFMBrCliff}(\Gamma, L)$.

Remark 3.3.2. The group $\mathrm{ExFMBrCliff}(\Gamma, L)$ is a central product of $\mathrm{Br}(k)$ with $\mathrm{FMBrCliff}(\Gamma, L)$ over $\mathrm{Br}(L|k)$ that is:

$$\mathrm{ExFMBrCliff}(\Gamma, L) = \mathrm{FMBrCliff}(\Gamma, L) \curlyvee_{\mathrm{Br}(L|k)} \mathrm{Br}(k)$$

Note that $\mathrm{FMBrCliff}(\Gamma, L)$ is isomorphic to the second cohomology group $\mathrm{H}^2(\Gamma, L^*)$.

The group $\mathrm{ExFMBrCliff}(\Gamma, L)$ is interesting for two reasons. Firstly, its elements can be recognized via cohomological methods and hence it admits a convenient description via group cohomology. Secondly, in a number of cases it coincides with BRAUER-CLIFFORD group. For example this happens if (L/k) is a cyclic extension.

Theorem 3.3.3. *Let (L/k) a cyclic* GALOIS *extension and Γ a finite group acting on L as field automorphisms. Assume that $L^\Gamma = k$, then* $\mathrm{BrCliff}(\Gamma, L) = \mathrm{ExFMBrCliff}(\Gamma, L)$.

Proof. Let $[A] \in \mathrm{BrCliff}(\Gamma, L)$, $H := \mathrm{Gal}(L/k)$ and $\kappa : \mathrm{BrCliff}(\Gamma, L) \to \mathrm{Br}(L)^H$ as in (3.1.2). Denote by res the map $\mathrm{Br}(k) \to \mathrm{Br}(L) \;:\; C \mapsto C \otimes_k L$. The following exact sequence is due to Teichmüller [Tei40]

$$\mathrm{H}^2(H, L^*) \longrightarrow \mathrm{Br}(k) \xrightarrow[\mathrm{res}]{} \mathrm{Br}(L)^H \longrightarrow \mathrm{H}^3(H, L^*)$$

Cohomology of cyclic groups yields that $\mathrm{H}^3(H, L^*)$ is trivial. Hence there exists an $B \in \mathrm{Br}(k)$ such that $\mathrm{res}(B) = \kappa([A])$. Therefore $\mathrm{ext}_{L/k}(B)^{-1}[A]$ is an element of $\mathrm{FMBrCliff}(\Gamma, L)$. This proves the theorem.

□

Choosing $L = k$ yields [Tur09a, Corollary 3.13].

Corollary 3.3.4. *If $L = k$, then* $\mathrm{BrCliff}(\Gamma, k) \cong \mathrm{Br}(k) \times \mathrm{FMBrCliff}(\Gamma, k)$

Turning back to the general case, assume that K/k is a finite GALOIS extension with group Γ and that L is a subfield of K which is GALOIS over k. View K and L as Γ-fields via the natural Γ action. Let $\mathrm{ExFMBrCliff}(\Gamma, L, K)$ be the group generated by $\mathrm{FMBrCliff}(\Gamma, L)$ and $\mathrm{ext}_{L/k}(\mathrm{Br}(K|k))$. The next problem is to find necessary and sufficient conditions on K to be an equivariant splitting field of a central simple Γ-algebra A over L with $[A] \in \mathrm{ExFMBrCliff}(\Gamma, L)$. In particular if K is an equivariant splitting field of A, then K is a splitting field of A considered as a central simple L-algebra. This provides some necessary conditions on K and we can assume that $[A] \in \mathrm{ExFMBrCliff}(\Gamma, L, K)$.

It is clear that there exists a, not unique, factorization of $[A]$ as:

$$[A] = \mathrm{ext}_{L/k}([B])[C] \text{ with } [B] \in \mathrm{Br}(K|k) \text{ and } [C] \in \mathrm{FMBrCliff}(\Gamma, L)$$

The next step is to calculate $h(\mathrm{ext}_{K/L}([A]))$. Use lemma (3.3.1) to see:

$$\begin{aligned} h(\mathrm{ext}_{K/L}([A])) &= h(\mathrm{ext}_{K/k}([B])h(\mathrm{ext}_{K/L}([C])) \\ &= \delta([B])h(\mathrm{ext}_{K/L}([C])) \end{aligned}$$

The next proposition shows that it is possible to calculate $h(\mathrm{ext}_{K/L}([C]))$ from $h([C])$.

Proposition 3.3.5. *The inclusion $L \to K$ is Γ-equivariant and induces a map $\tau_{L,K} : \mathrm{H}^n(\Gamma, L^*) \to \mathrm{H}^n(\Gamma, K^*)$ on the cohomology. Then $h(\mathrm{ext}_{K/k}([C])) = \tau_{L,K}(h([C]))$ for all $[C] \in \mathrm{FMBrCliff}(\Gamma, L)$*

Proof. Directly from (3.1.11) and the natural embedding $L^{n\times n} \to K^{n\times n}$ □

Summing up gives:

Lemma 3.3.6. *Let $[A] \in \mathrm{ExFMBrCliff}(\Gamma, L, K)$, $[B] \in \mathrm{Br}(K|k)$ and $[C] \in \mathrm{FMBrCliff}(\Gamma, L)$ such that $[A] = [\mathrm{ext}_{L/k}([B])][C]$, then*

$$h(\mathrm{ext}_{K/k}([A])) = \delta([B])\tau_{L,K}(h([C])) \text{ in } \mathrm{H}^2(\Gamma, K^*)$$

Since $[B]$ and $h([C])$ do not depend on K, lemma (3.3.6) can be used to obtain necessary and sufficient conditions on K to be an equivariant splitting field.

If k is a number field, one can be more specific. First of all, recall some constructions from the theory of central simple algebras. Given a 2-cocycle in $\mathrm{Z}^2(\Gamma, K^*)$, it is possible to construct a crossed product algebra. This construction induces an isomorphism between $\mathrm{H}^2(\Gamma, K^*)$ and $\mathrm{Br}(K|k)$.

Let B be a central simple k-algebra B, for which K is a splitting field. The crossed product algebra defined by the 2-cocycle $\delta(B)$ is equivalent to the opposite algebra B^o of B (cf. [Ser79, p159]).

Recall the theorem of Brauer-Hasse-Noether, which says that the sequence

$$1 \longrightarrow \mathrm{Br}(k) \longrightarrow \bigoplus_{\mathfrak{p}} \mathrm{Br}(k_{\mathfrak{p}}) \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z} \tag{3.3}$$

is exact, where $\mathfrak{p}$ runs through all primes of the field k. The map inv is called the Hasse invariant map, computed locally on each component: $\mathrm{inv} = \sum \mathrm{inv}_{k_{\mathfrak{p}}}$. The maps $\mathrm{inv}_{k_{\mathfrak{p}}}$ are called Hasse invariants. For more details on Hasse invariants and central simple algebras see [Rei75].

We saw that there exists a factorization of $[A]$ as

$$[A] = [\mathrm{ext}_{L/k}([B])][C] \text{ with } [B] \in \mathrm{Br}(k) \text{ and } [C] \in \mathrm{FMBrCliff}(\Gamma, L)$$

Let $\tau_{L,K} : \mathrm{H}^2(\Gamma, L^*) \to \mathrm{H}^2(\Gamma, K^*)$ be the map of (3.3.5) and $D_{L,K}$ the crossed product algebra corresponding to the cocycle $\tau_{L,K}(h([C]))$. Lemma (3.3.6) implies that K is an equivariant splitting field of A if and only if the 2-cocycle $\delta([B])\tau_{L,K}(h([C]))$ is a coboundary. This is the case if and only if $[B^o][D_{L,K}]$ is trivial in the Brauer group. Using sequence (3.3), this is equivalent to

$$\mathrm{inv}_{\mathfrak{p}}([B^o]) + \mathrm{inv}_{\mathfrak{p}}([D_{L,K}]) = 0 \in \mathbb{Q}/\mathbb{Z} \text{ for all primes } \mathfrak{p} \text{ of } k$$

Hence K is an equivariant splitting field of A if and only if the crossed product algebra $D_{L,K}$ is equivalent to B. Note that B is independent of K. The next example will illustrate this strategy.

Example 3.3.7. Let $k = \mathbb{Q}$, $G = \mathrm{Q}_8 = \langle a, b \mid a^4, a^2b^2, abab^{-1}\rangle$, then

$$\Delta(a) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \;,\; \Delta(b) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

defines a faithful representation of Q_8. Let u be the inner automorphism of Q_8 induced by conjugation with $\Delta(b)$ and U the subgroup of $\mathrm{Aut}(\mathrm{Q}_8)$ generated by u.

Let K be a quadratic extension of $\mathbb{Q}$, with Galois group Γ and view K as a Γ-field. Let $^- : \Gamma \to U$ sending the generator of Γ to u.

Extend the Γ-action on $\Delta(G)$ via $^-$ to an action on the enveloping algebra $\Delta(\mathbb{Q}G)$ as $\mathbb{Q}$-algebra automorphisms. View $\Delta(\mathbb{Q}G)$ as a central simple Γ-algebra over $\mathbb{Q}$. Since $\mathrm{BrCliff}(\Gamma, \mathbb{Q})$ is a direct product of $\mathrm{FMBrCliff}(\Gamma, \mathbb{Q})$ and $\mathrm{Br}(\mathbb{Q})$ by (3.3.4), there exists a unique factorization

$$[\Delta(\mathbb{Q}G)] = [B][C] \text{ with } [B] \in \mathrm{Br}(k) \text{ and } [C] \in \mathrm{FMBrCliff}(\Gamma, \mathbb{Q})$$

More precisely B is the quaternion algebra $Q(\frac{(-1,-1)}{\mathbb{Q}})$ with trivial Γ-action and C is the matrix algebra $\mathbb{Q}^{2\times 2}$, where the Γ action is given by $\sigma(X) = \Delta(b)X\Delta(b)^{-1}$ for $X \in \mathbb{Q}^{2\times 2}$.

We want to find necessary and sufficient conditions on K to be an equivariant splitting field of $\Delta(\mathbb{Q}G)$.

The $\mathbb{Q}$-algebra B is isomorphic to B^o and the Hasse invariants are

$$\mathrm{inv}_2([B]) = \frac{1}{2},\ \mathrm{inv}_\infty([B]) = \frac{1}{2},\ \mathrm{inv}_\mathfrak{p}([B]) = 0 \text{ other primes } \mathfrak{p} \text{ of } \mathbb{Q}$$

It is well known that K is a splitting field of B if and only if

$$(K_\mathfrak{P} : \mathbb{Q}_2) = 2 \text{ with } \mathfrak{P}_{|\mathbb{Q}} = 2 \text{ and } (K_\infty : \mathbb{R}) = 2 \tag{3.4}$$

Since $\Delta(b)^2 = -1$,

$$h([C]) :\ \Gamma \times \Gamma \to \mathbb{Q} \ :\ (\sigma, \tau) \mapsto \begin{cases} -1, & \text{if } \sigma = \tau = u \\ 1, & \text{otherwise} \end{cases}$$

is a cocycle representing the cohomology class of $h([C])$. Let $D_{\mathbb{Q},K}$ be the crossed product algebra defined by $\tau_{\mathbb{Q},K}(h([C])$. Then the conditions on K to be an equivariant splitting field are (3.4) and

$$\mathrm{inv}_2([D_{\mathbb{Q},K}]) = \frac{1}{2},\ \mathrm{inv}_\infty([D_{\mathbb{Q},K}]) = \frac{1}{2},\ \mathrm{inv}_\mathfrak{p}([D_{\mathbb{Q},K}]) = 0 \text{ other primes } \mathfrak{p} \text{ of } \mathbb{Q}$$

Because $D_{\mathbb{Q},K}$ is a cyclic algebra $(K/\mathbb{Q}, \sigma, -1)$, with σ a generator of $\mathrm{Gal}(K/\mathbb{Q})$, it is possible to give the conditions on K in a more satisfactory way.

Let $K = \mathbb{Q}(\sqrt{D})$ where $D \in \mathbb{Z}$ is square-free and denote by $\mathfrak{D}$ the discriminant of K. It is obvious that the condition $\mathrm{inv}_\infty([D_{\mathbb{Q},K}]) = \frac{1}{2}$ implies that

$D < 0$. The other condition $\mathrm{inv}_2([D_{\mathbb{Q},K}]) = \frac{1}{2}$ implies that K is ramified at the prime 2, which is equivalent to the fact that

$$2 \mid \mathfrak{D} = \begin{cases} D, & \text{if and only if } D \equiv 1 \mod 4 \\ 4D, & \text{if and only if } D \equiv 2,3 \mod 4 \end{cases}$$

This shows that $D \equiv 2,3 \mod 4$. Assume that p is a prime with $p \nmid D$ and define $\mathfrak{p} := (p)$. Since $\mathfrak{p}$ is unramified, the condition $\mathrm{inv}_{\mathfrak{p}}([D_{\mathbb{Q},K}]) = 0$ is fulfilled. Now assume that $p \mid D$, then the condition can be written as $\left(\frac{-1,D}{\mathfrak{p}}\right) = 1$ where $\left(\frac{\circ\ ,\ \circ}{\mathfrak{p}}\right)$ is the HILBERT-symbol [Neu99]. Using the explicit formula of the HILBERT symbol in the quadratic case, one concludes that $p \equiv 1 \mod 4$. Hence all quadratic extensions $K/\mathbb{Q}$ with the property that there exist a irreducible and faithful $(K/\mathbb{Q}, ^-)$-representation $\Delta : G \to \mathrm{GL}_2(K)$ of Q_8 are given by: $K = \mathbb{Q}(\sqrt{D})$ where $D = -\prod_i p_i$ or $D = -2\prod_i p_i$ and $p_i \in \mathbb{N}$ are primes with $p_i \equiv 1 \mod 4$.

We look at a example related to NEBE'S recently discovered extremal unimodular 72-dimensional lattice Λ_{72} [Neb].

Example 3.3.8. Let $G = \mathrm{SL}_2(25)$, $K/\mathbb{Q}$ a GALOIS extension of degree 2 with group Γ, $\chi := \chi_{17}$ be the 12-dimensional complex character in ATLAS [CCN+85] notation. This character has SCHUR-index 2 over $\mathbb{Q}$ and the corresponding component of the group algebra B has the HASSE invariants

$$\mathrm{inv}_5([B]) = \frac{1}{2},\ \mathrm{inv}_\infty([B]) = \frac{1}{2},\ \mathrm{inv}_{\mathfrak{p}}([B]) = 0 \text{ other primes } \mathfrak{p} \text{ of } \mathbb{Q}$$

One checks that there exists only one conjugacy class of elements of order 2 in $\mathrm{Aut}(G)$ with the property that its elements fix the character χ and are not inner automorphism. Choose an element φ of this class and define $\Gamma \to \mathrm{Aut}(G)$, $\sigma \mapsto \varphi$. Since φ fixes χ it turns the component B into a central simple Γ-algebra over $\mathbb{Q}$.

By (3.3.4) $\mathrm{BrCliff}(\Gamma, \mathbb{Q})$ is a direct product of $\mathrm{FMBrCliff}(\Gamma, \mathbb{Q})$ and $\mathrm{Br}(\mathbb{Q})$, hence there exists a unique factorization

$$\Delta(\mathbb{Q}G)] = [B][C] \text{ with } [B] \in \mathrm{Br}(\mathbb{Q}) \text{ and } [C] \in \mathrm{FMBrCliff}(\Gamma, \mathbb{Q})$$

More precisely B is the algebra $\Delta(\mathbb{Q}G)$ considered as a Γ-algebra with trivial Γ-action and C is the matrix algebra $\mathbb{Q}^{12\times 12}$ with a non trivial Γ action. Using the ATLAS we see that χ extends to a character of $\mathrm{SL}_2(25) \rtimes \Gamma$ which has values in $\mathbb{Q}(\sqrt{-5})$. From [Tur00, Theorem 3.4] we deduce that

$$h([C]) :\ \Gamma \times \Gamma \to \mathbb{Q}\ :\ (\sigma, \tau) \mapsto \begin{cases} -5, & \text{if } \sigma = \tau \neq 1 \\ 1, & \text{otherwise} \end{cases}$$

is a cocycle representing the cohomology class of $h([C])$. Let $D_{\mathbb{Q},K}$ be the crossed product algebra defined by $\tau_{\mathbb{Q},K}(h([C])$. Then the conditions on K to be an equivariant splitting field are

$$\mathrm{inv}_5([D_{\mathbb{Q},K}]) = \frac{1}{2},\ \mathrm{inv}_\infty([D_{\mathbb{Q},K}]) = \frac{1}{2},\ \mathrm{inv}_{\mathfrak{p}}([D_{\mathbb{Q},K}]) = 0 \text{ other primes } \mathfrak{p} \text{ of } \mathbb{Q}$$

Let $K = \mathbb{Q}(\sqrt{D})$ where $D \in \mathbb{Z}$ is square-free and denote by $\mathfrak{D}$ the discriminant of K. It is obvious that the condition $\mathrm{inv}_\infty([D_{\mathbb{Q},K}]) = \frac{1}{2}$ implies that $D < 0$. We give the various other conditions in an explicit form:

1. Assume that $\mathfrak{p} \nmid \mathfrak{D}$ and $\mathfrak{p} \neq 5$. Since $\mathfrak{p}$ is not ramified in K the condition $\left(\frac{-5,D}{\mathfrak{p}}\right) = 1$ is redundant.

2. Assume that $\mathfrak{p} \mid \mathfrak{D}$ and $\mathfrak{p} \neq 2, 5$. Using the explicit formulas for the HILBERT-symbol, the condition $\left(\frac{-5,D}{\mathfrak{p}}\right) = 1$ is equivalent to $\mathfrak{p} \equiv 1 \mod 4$.

3. The condition $\left(\frac{-5,D}{5}\right) = -1$ we split in two cases. If $5 \nmid \mathfrak{D}$ one easily checks that the condition is equivalent to $D \equiv 2, 3 \mod 5$. If $5 \mid \mathfrak{D}$ it is equvialent to $\left(\frac{D/5}{5}\right) = -1$ where $\left(\frac{\cdot}{5}\right)$ denotes the LEGENDRE-symbol.

4. The last condition to look at is $\left(\frac{-5,D}{2}\right) = 1$. If $2 \mid \mathfrak{D}$ and $2 \nmid D$, this is equivalent to $D \equiv 1 \mod 4$. If $2 \mid D$, then the condition is given by $-3(\frac{D-2}{4}) - 3 \equiv 0 \mod 2$.

With those explicit conditions we see that for example $\mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-7})$ are equivariant splitting fields.

Chapter 4

Applications of the Brauer-Clifford theory

Let K/k finite Galois extension with group Γ and G a finite subgroup of $\mathrm{GL}_n(K)$. In this chapter the Brauer-Clifford theory is applied to study the existence of(K/k)-forms of G for k being a finite field or the real numbers. The existence question of (2.2.1) admits a satisfactory treatment in both cases. For finite fields it turns out that the necessary condition of remark (2.2.2) is also sufficient. Reproving a result of [KM90], a twisted version of the Frobenius-Schur indicator answers the existence question for the real numbers. Hence, in both cases the answer to the existence question depends solely on group theoretic data.

If the finite matrix group can be realized over its character field, general sufficient conditions for the existence of a (K/k)-form are obtained in the third section. Those are used to study the case of G being a subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}})$ and isomorphic to $\mathrm{PSL}_2(q)$, where q is a power of an odd prime. It is shown that G is conjugate to a subgroup of $\mathrm{GL}_n(\mathbb{Q}(\chi))$, where χ is the natural character of G, with a set of fundamental invariants whose coefficients lie in the minimal possible subfield of $\mathbb{Q}(\chi)$.

4.1 Forms over finite fields

Let k be a finite field and K a finite field extension of k with Galois group Γ. Using the well known fact that $\mathrm{H}^2(\Gamma, K^*)$ is trivial, the main theorem (3.2.1) can be simplified.

Corollary 4.1.1. *Let K/k a finite* Galois *extension with group Γ, $G \leq \mathrm{GL}_n(K)$ a finite absolutely irreducible matrix group, Δ the natural representation of G, χ the natural character, and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. Then there exists a $(K/k, ^-)$-representation of G, conjugate in $\mathrm{GL}_n(\overline{k})$ to the natural representation if and only if $\sigma \circ \chi = \chi \circ \overline{\sigma}$ for all $\sigma \in \Gamma$.*

Proof. The only non trivial part is the "if" part. Assume $\sigma \circ \chi = \chi \circ \overline{\sigma}$ for all $\sigma \in \Gamma$. Lemma (2.2.6) implies that the assumptions of the main theorem (3.2.1) are fulfilled. So, consider $\Delta(kG)$ as a central simple Γ-algebra over its center L (cf. 3.2.1). We have to show that K is an equivariant splitting field of $\Delta(kG)$, and to see this we have to calculate $\mathrm{ext}_{K/L}([\Delta(kG)])$. Note that $\mathrm{ext}_{K/L}([\Delta(kG)])$ is an element of $\mathrm{FMBrCliff}(\Gamma, K)$, and by (3.1.10) this group is isomorphic to $\mathrm{H}^2(\Gamma, K^*)$. As mentioned, it is well known from GALOIS cohomology that $\mathrm{H}^2(\Gamma, K^*)$ is trivial. Hence K is an equivariant splitting field of $\Delta(kG)$. □

Remark 4.1.2. In case of finite fields, the condition given in remark (2.2.2) is necessary and sufficient for the existence of a $(K/k, ^-)$-representation of G conjugate in $\mathrm{GL}_n(\overline{k})$ to the natural representation.

4.2 Forms over $\mathbb{R}$

Let k be the real field $\mathbb{R}$, $\Gamma = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, G be a finite and absolutely irreducible subgroup of $\mathrm{GL}_n(\mathbb{C})$ with natural character χ and natural representation $\Delta : G \to \mathrm{GL}_n(\mathbb{C})$. Let u be an element of order 2 in $\mathrm{Aut}(G)$ and let

$$^- : \Gamma \to \mathrm{Aut}(G)$$

be the embedding sending the generator σ of Γ to u.

The sum $\epsilon(\chi) = \frac{1}{|G|}\sum_{g\in G}\chi(g^2)$ is called the FROBENIUS-SCHUR indicator. It has the well known property that:

$$\epsilon(\chi) = \begin{cases} 1, & \text{if and only if } \mathbb{R}(\chi) = \mathbb{R} \text{ and } \mathrm{m}_{\mathbb{R}}(\chi) = 1 \\ -1, & \text{if and only if } \mathbb{R}(\chi) = \mathbb{R} \text{ and } \mathrm{m}_{\mathbb{R}}(\chi) = 2 \\ 0, & \text{if and only if } \mathbb{R}(\chi) = \mathbb{C} \end{cases} \tag{4.1}$$

where $\mathrm{m}_{\mathbb{R}}(\chi)$ is the SCHUR index of the character χ over $\mathbb{R}$ cf. [Isa76, Chapter 10] A twisted version of the FROBENIUS-SCHUR indicator was defined in [KM90] as

$$\epsilon^u(\chi) = \frac{1}{|G|}\sum_{g\in G}\chi(gu(g))$$

The next theorem due to KAWANAKA and MATSUYAMA links the twisted FROBENIUS-SCHUR indicator to the existence of $(\mathbb{C}/\mathbb{R})$-forms of G.

Theorem 4.2.1. *Let $G \leq \mathrm{GL}_n(\mathbb{C})$ be a finite matrix group, u be an element of order 2 in $\mathrm{Aut}(G)$. Then*

$$\epsilon^u(\chi) = \begin{cases} 1, & \text{if and only if } \chi\circ u = \overline{\chi} \text{ and there exists a } (\mathbb{C}/\mathbb{R})\text{-form of } G \\ -1, & \text{if and only if } \chi\circ u = \overline{\chi} \text{ and there is no } (\mathbb{C}/\mathbb{R})\text{-form of } G \\ 0, & \text{otherwise} \end{cases}$$

We will prove this theorem using BRAUER-CLIFFORD theory. Assume that $\chi \circ \overline{\sigma} = \sigma \circ \chi$. Hence the enveloping algebra $\Delta(\mathbb{R}G)$ can be considered as a central simple Γ-algebra over $\mathbb{R}(\chi)$ as in (3.2.1). Distinguish two cases:
Case 1: $\mathbb{R}(\chi) = \mathbb{C}$:

Since $\mathbb{C}$ is algebraically closed, identify $\mathrm{BrCliff}(\Gamma, \mathbb{C})$ and $\mathrm{FMBrCliff}(\Gamma, \mathbb{C})$. View the map h of (3.1.10) as an isomorphism $h : \mathrm{BrCliff}(\Gamma, \mathbb{C}) \to \mathrm{H}^2(\Gamma, \mathbb{C}^*)$. It is well known that $\mathrm{H}^2(\Gamma, \mathbb{C}^*)$ is isomorphic to $\mathrm{Br}(\mathbb{R})$ and the latter group is cyclic of order 2. View h as a map $h : \mathrm{BrCliff}(\Gamma, \mathbb{C}) \to \mathbb{Z}_2$. Then

$$h(\Delta(\mathbb{R}G)) = \begin{cases} 1, & \text{if and only if } \mathrm{m}_{\mathbb{R}}(\chi^{G \rtimes \Gamma}) = 1 \\ -1, & \text{if and only if } \mathrm{m}_{\mathbb{R}}(\chi^{G \rtimes \Gamma}) = 2 \end{cases}$$

Case 2: $\mathbb{R}(\chi) = \mathbb{R}$:

Identify $\mathrm{BrCliff}(\Gamma, \mathbb{R})$ with $\mathrm{Br}(\mathbb{R}) \times \mathrm{FMBrCliff}(\Gamma, \mathbb{R})$ (cf. 3.3.4). Hence the map

$$(\delta, h) : \mathrm{BrCliff}(\Gamma, \mathbb{R}) \to \mathrm{H}^2(\Gamma, \mathbb{C}^*) \times \mathrm{H}^2(\Gamma, \mathbb{R}^*) \ : \ [B][C] \mapsto (\delta(B), h([C]))$$

is an isomorphism. Identify $\mathrm{H}^2(\Gamma, \mathbb{C}^*)$ with $\mathbb{Z}_2$ as in the first case. Because Γ acts trivially on $\mathbb{R}$, the group $\mathrm{H}^2(\Gamma, \mathbb{R}^*)$ is isomorphic to $\mathbb{R}^*/\mathbb{R}^{*2}$ and the latter is a cyclic group of order 2. View (δ, h) as a map $\mathrm{BrCliff}(\Gamma, \mathbb{R}) \to \mathbb{Z}_2 \times \mathbb{Z}_2$. Use Clifford theory to see that there exists an extension $\Theta \in \mathrm{Irr}(G \rtimes \Gamma)$ of the character χ. This extension is unique up to complex conjugation. Then

$$(\delta, h)(\Delta(\mathbb{R}G)) = \begin{cases} (1,1), & \text{if and only if } \mathrm{m}_{\mathbb{R}}(\chi) = 1, \mathbb{R}(\Theta) = \mathbb{R} \text{ and } \mathrm{m}_{\mathbb{R}}(\Theta) = 1 \\ (1,-1), & \text{if and only if } \mathrm{m}_{\mathbb{R}}(\chi) = 1, \mathbb{R}(\Theta) = \mathbb{C} \text{ and } \mathrm{m}_{\mathbb{R}}(\Theta) = 1 \\ (-1,1), & \text{if and only if } \mathrm{m}_{\mathbb{R}}(\chi) = 2, \mathbb{R}(\Theta) = \mathbb{R} \text{ and } \mathrm{m}_{\mathbb{R}}(\Theta) = 2 \\ (-1,-1), & \text{if and only if } \mathrm{m}_{\mathbb{R}}(\chi) = 2, \mathbb{R}(\Theta) = \mathbb{C} \text{ and } \mathrm{m}_{\mathbb{R}}(\Theta) = 1 \end{cases}$$

Observe that all possibilities of the cases 1 and 2 can be distinguished using the Frobenius-Schur indicator of the characters χ and Θ. The next lemma shows that the twisted Frobenius-Schur indicator can be calculated from the Frobenius-Schur indicators of those two characters.

Lemma 4.2.2. *Let u be an element of order 2 in $\mathrm{Aut}(G)$. Assume that θ is an irreducible complex character of $G \rtimes U$ with $\langle \theta_{|G}, \chi \rangle \neq 0$, then:*

$$\epsilon(\theta) = \frac{1}{2} \frac{\theta(1)}{\chi(1)} (\epsilon(\chi) + \epsilon^u(\chi))$$

Proof. Directly from Clifford theory and a calculation □

Assume we are in case 2 of the discussion above. Lemma (3.3.6) implies that the following diagram is commutative

$$\begin{array}{ccc} \mathrm{BrCliff}(\Gamma, \mathbb{R}) & \xrightarrow{\mathrm{ext}_{\mathbb{C}/\mathbb{R}}} & \mathrm{FMBrCliff}(\Gamma, \mathbb{C}) \\ \downarrow{\scriptstyle (\delta,h)} & & \downarrow{\scriptstyle h} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \xrightarrow{(a,b) \to ab} & \mathbb{Z}_2 \end{array}$$

Hence it is easy to decide if $\mathbb{C}$ is an equivariant splitting field.

Use the formula of lemma (4.2.2) and the property (4.1) to see that the twisted Frobenius-Schur is 1 if $\mathbb{C}$ is an equivariant splitting field and -1 if

$\mathbb{C}$ is not. Furthermore, the same result is obtained in case 1. This shows that if $\chi \circ u = \overline{\chi}$, then the twisted FROBENIUS-SCHUR indicator determines whether or not there exists a $(\mathbb{C}/\mathbb{R})$-form of G.

Assume $\chi \circ \overline{\sigma} \neq \sigma \circ \chi$. Use CLIFFORD theory, property (4.1) and lemma (4.2.2) to see that $\epsilon^u(\chi) = 0$. Summing up, one gets the theorem (4.2.1).

4.3 Sufficient conditions for the existence $\mathbb{Q}$-forms

Let k be a number field, K a finite GALOIS extension of k with group Γ, G a finite and absolutely irreducible subgroup of $\mathrm{GL}_n(K)$, χ the corresponding natural character, Δ the natural representation, and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. Assume that the SCHUR index of χ is one and the condition of (2.2.2) is satisfied. In this case it is possible to give sufficient conditions for the existence of a $(K/k, ^-)$-representation of G conjugate in $\mathrm{GL}_n(\overline{k})$ to the natural representation, depending solely on character theoretic data.

The idea is to find conditions which imply that the central simple Γ-algebra $\Delta(kG)$ (cf. 3.2.1) represents the trivial element of the BRAUER-CLIFFORD group. If this is the case, then it is easy to see that K is an equivariant splitting field. Hence there exists a $(K/k, ^-)$-representation of G by (3.2.1). Denote the SCHUR index of χ over k by $\mathrm{m}_k(\chi)$.

Lemma 4.3.1. *Assume the situation of the preceding discussion, specifically that the* SCHUR *index of* χ *is one. If there exists an irreducible complex character* ζ *of the semidirect product* $G \rtimes \Gamma$ *with*

$$k(\zeta) = k,\ \mathrm{m}_k(\zeta) = 1 \text{ and } \zeta_{|G} = \sum_{\sigma \in H} \sigma \circ \chi \text{ where } H = \mathrm{Gal}(k(\chi)/k),$$

Then there exists a $(K/k, ^-)$*-representation of* G *with character* χ.

Proof. The SCHUR index of χ is one, so it can be assumed that G is a subgroup $\mathrm{GL}_n(\mathbb{Q}(\chi))$. Because the condition of (2.2.2) is satisfied, view $\Delta(kG)$ as a central simple Γ-algebra as in (3.2.1). We claim that $[\Delta(kG)]$ represents the trivial element of $\mathrm{BrCliff}(\Gamma, k(\chi))$. It is easy to see that $[\Delta(kG)] \in \mathrm{FMBrCliff}(\Gamma, k(\chi))$, hence it is enough to show that $h(\Delta(kG))$ is a coboundary.

Let $\iota : k(\chi)^{n\times n} \to k^{l\times l}$ be the k-algebra homomorphism induced by restricting scalars. Obviously, there exists a representation $\Theta : G \rtimes \Gamma \to \mathrm{GL}_l(k)$, affording ζ, with the property $\Theta(g) = \iota(\Delta(g))$ for every $g \in G$. Define the map $F : \Gamma \to k^{l\times l} \ :\ \sigma \mapsto \Theta(\sigma)$, then ι and F fulfill the requirements of (3.1.10). Hence $h([\Delta(kG)])(s,t) = \Theta(s)\Theta(t)\Theta(st)^{-1} = 1$ for all $s, t \in \Gamma$, and this shows that $h(\Delta(kG))$ is a coboundary. Therefore K is an equivariant splitting field of $\Delta(kG)$ and the result follows from (3.2.1). □

Using (3.1.12), another sufficient condition can be obtained, cf. [MM, Proposition 8.1].

Corollary 4.3.2. *Let* G *be a finite subgroup of* $\mathrm{GL}_n(K)$ *with natural character* χ*, where* K/k *is a* GALOIS *extension with* GALOIS *group* Γ*. Choose* $^- : \Gamma \to \mathrm{Aut}(G)$ *to be an embedding and assume that the the condition of*

(2.2.2) is fulfilled. If $|\Gamma|$ is prime to the degree of χ, then there exists a $(K/k, ^-)$-representation of G with character χ.

4.4 $\mathbb{Q}$-forms of matrix groups isomorphic to $\mathrm{PSL}_2(p^l)$

Let G be an absolutely irreducible subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}})$ with natural character χ. Assume that G is isomorphic to $\mathrm{PSL}_2(q)$, where q is a power of an odd prime p. Let k be the minimal subfield of $\mathbb{Q}(\chi)$ with the property that a subgroup of $\mathrm{Aut}(G)$ acts transitively on the set of Galois conjugates of χ over k. The aim is to show that there exists a $(\mathbb{Q}(\chi)/k)$-form of G.

To determine k, identify G with $\mathrm{PSL}_2(q)$ and consider an arbitrary faithful and irreducible complex character χ of $\mathrm{PSL}_2(q)$. Note that every automorphism of $\mathrm{PSL}_2(q)$ is induced by a unique automorphism of $\mathrm{SL}_2(q)$ [Die51]. View χ as a character of $\mathrm{SL}_2(q)$, then it is possible to work with $\mathrm{SL}_2(q)$. So let χ be an irreducible complex character of $\mathrm{SL}_2(q)$.

At first, recall some basic facts about $\mathrm{SL}_2(q)$. Let ν be a generator of $\mathbb{F}_q^*$ and define

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, c = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, d = \begin{pmatrix} 1 & 0 \\ \nu & 1 \end{pmatrix}$$
$$a = \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}, b \text{ element of order q+1}$$

Then the conjugacy classes of $\mathrm{SL}_2(q)$ are:

$$(1), (z), (c), (d), (cz), (dz), (a^l), (b^m) \text{ with } 1 \leq l \leq \frac{q-3}{2} \text{ and } 1 \leq m \leq \frac{q-1}{2}$$

Let $\epsilon := (-1)^{\frac{q-1}{2}}$, $\rho \in \mathbb{C}$ a primitive $(q-1)$th root of unity and $\sigma \in \mathbb{C}$ a primitive $(q+1)$th root of unity. Then the complex character table of $\mathrm{SL}_2(q)$ is

	1	z	c	d	a^l	b^m
1_G	1	1	1	1	1	1
ψ	q	q	0	0	1	-1
χ_i	$q+1$	$(-1)^i(q+1)$	1	1	$\rho^{il}+\rho^{-il}$	0
Θ_j	$q-1$	$(-1)^j(q-1)$	-1	-1	0	$-(\sigma^{jm}+\sigma^{-jm})$
ζ_1	$\frac{q+1}{2}$	$\frac{1}{2}\epsilon(q+1)$	$\frac{1}{2}(1+\sqrt{\epsilon q})$	$\frac{1}{2}(1-\sqrt{\epsilon q})$	$(-1)^l$	0
ζ_2	$\frac{q+1}{2}$	$\frac{1}{2}\epsilon(q+1)$	$\frac{1}{2}(1-\sqrt{\epsilon q})$	$\frac{1}{2}(1+\sqrt{\epsilon q})$	$(-1)^l$	0
η_1	$\frac{q-1}{2}$	$-\frac{1}{2}\epsilon(q-1)$	$\frac{1}{2}(-1+\sqrt{\epsilon q})$	$\frac{1}{2}(-1-\sqrt{\epsilon q})$	0	$(-1)^{m+1}$
η_2	$\frac{q-1}{2}$	$-\frac{1}{2}\epsilon(q-1)$	$\frac{1}{2}(-1-\sqrt{\epsilon q})$	$\frac{1}{2}(-1+\sqrt{\epsilon q})$	0	$(-1)^{m+1}$

with $1 \leq i \leq \frac{q-3}{2}$ and $1 \leq j \leq \frac{q-1}{2}$.

It is well known that $\mathrm{Aut}(\mathrm{SL}_2(q))$ is isomorphic to the projective semilinear group $\mathrm{P\Gamma L}_2(q)$ [Die51]. This group is a semidirect product of $\mathrm{PGL}_2(q)$ with $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. The subgroup of $\mathrm{PGL}_2(q)$ generated by the matrix

$$(4.2) \qquad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \text{ if } q \equiv 3 \mod 4 \text{ and } \begin{pmatrix} 0 & \nu \\ -1 & 0 \end{pmatrix} \text{ if } q \equiv 1 \mod 4$$

is a complement of $\mathrm{PSL}_2(q)$ in $\mathrm{PGL}_2(q)$ and cyclic of order 2. Hence $\mathrm{PGL}_2(q)$ is a semidirect product $\mathrm{PSL}_2(q) \rtimes \mathrm{C}_2$.

Let u be the automorphism of $\mathrm{SL}_2(q)$ induced by conjugation with the matrix of (4.2) and F the automorphism induced by the FROBENIUS automorphism of $\mathbb{F}_q$. Note that the images of u and F under the natural epimorphism $\mathrm{Aut}(\mathrm{SL}_2(q)) \to \mathrm{Out}(\mathrm{SL}_2(q))$ generate the outer automorphism group.

To study the action of $\mathrm{Aut}(\mathrm{SL}_2(q))$ on the irreducible complex characters, we have to analyze the action on the conjugacy classes. It is clear that the automorphism group can be replaced by the group of outer automorphisms. So it is enough to consider u and F. Since u and F are given explicitly, the following table can be calculated easily.

C	(1)	(z)	(c)	(d)	(a^l)	(b^m)
${}^uC$	(1)	(z)	(d)	(c)	(a^l)	(b^m)
${}^FC$	(1)	(z)	(c)	(d)	(a^{pl})	(b^{pm})

This table determines the action of $\mathrm{Out}(\mathrm{SL}_2(q))$ on the conjugacy classes completely. A close look at the character table reveals the following fact and determines the field k.

Remark 4.4.1. Assume that the character field of χ is a proper extension of $\mathbb{Q}$. The natural action of $\mathrm{Out}(\mathrm{SL}_2(q))$ on the set of irreducible complex characters induces an action on $\mathbb{Q}(\chi)$ as field automorphisms. Let k be the fixed field of this action or, if χ has values in $\mathbb{Q}$, let $k = \mathbb{Q}$. In all cases k is a minimal subfield of the character field with a subgroup of $\mathrm{Aut}(\mathrm{SL}_2(q))$ acting transitively on the set of GALOIS conjugates of χ over k. Furthermore, $\mathrm{Gal}(\mathbb{Q}(\chi)/k))$ is a cyclic group.

In case that the character field is a proper extension of $\mathbb{Q}$, there exists a natural epimorphism $\pi : \mathrm{Aut}(\mathrm{SL}_2(q)) \to \mathrm{Gal}(\mathbb{Q}(\chi)/k)$ with the property $\pi(\varphi) \circ \chi = \chi \circ \varphi$ for all $\varphi \in \mathrm{Aut}(\mathrm{SL}_2(q))$.

Lemma 4.4.2. *Assume that the character field of χ is a proper extension of $\mathbb{Q}$. Then the natural epimorphism $\pi : \mathrm{Aut}(\mathrm{SL}_2(q)) \to \mathrm{Gal}(\mathbb{Q}(\chi)/k)$ admits a section.*

Proof. Recall that u is the automorphism of $\mathrm{SL}_2(q)$ induced by conjugation with the matrix of (4.2) and F the automorphism induced by the FROBENIUS. It is easy to see that u has order 2 and F has order ν where $q = p^\nu$. Let λ be a generator of the cyclic group $\mathrm{Gal}(\mathbb{Q}(\chi)/k)$. If $\chi \in \{\zeta_{1,2}, \eta_{1,2}\}$, then $k = \mathbb{Q}$ and the map $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{SL}_2(q)) \ : \lambda \mapsto u$ defines a section of π. In case that $\chi \in \{\chi_i, \Theta_j\}$, then it is easy to see that there exists an $l \in \mathbb{N}$ such that $\mathrm{Gal}(\mathbb{Q}(\chi)/k) \to \mathrm{Aut}(\mathrm{SL}_2(q)) \ : \lambda \mapsto F^l$ defines a section. $\square$

Note that remark (4.4.1) and lemma (4.4.2) are, mutatis mutandis, true if χ is a complex character of $\mathrm{PSL}_2(q)$.

Theorem 4.4.3. *Let G be an absolutely irreducible subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}})$ isomorphic to $\mathrm{PSL}_2(q)$ and χ the natural character of G. Then there exists a $(\mathbb{Q}(\chi)/k)$-form of G with k given in (4.4.1).*

Proof. Recall that every character of $\mathrm{PSL}_2(q)$ has SCHUR index one [SS83]. Assume that χ has values in $\mathbb{Q}$, then there exists a subgroup of $\mathrm{GL}_n(\mathbb{Q})$ conjugate to G. This subgroup is clearly a $\mathbb{Q}$-form of G.

Assume that the character field of χ is a proper extension of $\mathbb{Q}$ and identify G with $\mathrm{PSL}_2(q)$. Let $\Gamma := \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ and take a section $^- : \Gamma \to \mathrm{Aut}(G)$ of π cf. 4.4.2. Then $\sigma \circ \chi = \chi \circ \overline{\sigma}$ for all $\sigma \in \Gamma$. This shows that the condition of (2.2.2) is fulfilled.

Assume that $\chi \in \{\eta_1, \eta_2, \zeta_1, \zeta_2\}$. Recall that in those cases $k = \mathbb{Q}$, Γ is cyclic of order 2 and n, the degree of χ, is odd. Then by (4.3.2) there exists a $(\mathbb{Q}(\chi)/\mathbb{Q}, ^-)$-representation of G.

Let $1 \leq i \leq \frac{q-3}{2}$, i even and $\chi = \chi_i$. Choose the section of $^-$ given in the proof of (4.4.2). Note that $\overline{\sigma} = F^l$ for an $l \in \mathbb{N}$. Use CLIFFORD theory to see that $\chi^{G \rtimes \Gamma}$ is an irreducible complex character of $G \rtimes \Gamma$ with the following properties:

$$k(\chi^{G \rtimes \Gamma}) = k \text{ and } (\chi^{G \rtimes \Gamma})_{|G} = \sum_{\sigma \in H} \sigma \circ \chi \text{ where } H = \mathrm{Gal}(k(\chi)/k).$$

To apply (4.3.1), it remains to check that the SCHUR index over k of $\chi^{G \rtimes \Gamma}$ is one. View χ as a character of $\mathcal{G} = \mathrm{SL}_2(q)$, then it is enough to show that the SCHUR index over k of $\chi^{\mathcal{G} \rtimes \Gamma}$ is one.

Let $\mathcal{N} := \langle a, x \rangle$ and $\mathcal{A} := \langle a \rangle$ with

$$x := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} , \; a := \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix}$$

and for $1 \leq \mathbf{k} \leq \frac{(q-3)}{2}$ define the characters $\lambda_{\mathbf{k}} : \mathcal{A} \to \mathbb{C}^* \; : \; a \mapsto \rho^{\mathbf{k}}$. The proof of [SS83, Lemma 2.1] shows that:

$$\langle \chi_{\mathbf{k}}, \lambda_{\mathbf{k}} \rangle_{\mathcal{A}} = 3 \text{ and } \langle \chi_{\mathbf{k}}, \lambda_{\mathbf{l}} \rangle_{\mathcal{A}} = 2 \text{ if } \mathbf{l} \neq \mathbf{k}$$

In particular, $\langle \gamma \circ \chi, \lambda_i \rangle = 2$ for any non trivial GALOIS automorphism $\gamma \in \mathrm{Gal}(\mathbb{Q}(\chi)/k)$. Use this, CLIFFORD theory and FROBENIUS reciprocity to see that $\langle \chi_i^{\mathcal{G} \rtimes \Gamma}, \lambda_i^{\mathcal{G} \rtimes \Gamma} \rangle$ is odd. Assume for the moment that the character $\lambda_i^{\mathcal{G} \rtimes \Gamma}$ is afforded by a representation over k. Since the SCHUR index of $\chi^{\mathcal{G} \rtimes \Gamma}$ over k divides $\langle \chi_i^{\mathcal{G} \rtimes \Gamma}, \lambda_i^{\mathcal{G} \rtimes \Gamma} \rangle$, it has to be odd. Applying the BRAUER-SPEISER theorem one sees that the SCHUR index of $\chi_i^{\mathcal{G} \rtimes \Gamma}$ over k has to be one.

It remains to show that there exists a representation over k affording $\lambda_i^{\mathcal{G} \rtimes \Gamma}$. The group $\mathcal{N}$ is obviously Γ-invariant, hence it is sufficient to show that $\lambda_i^{\mathcal{N} \rtimes \Gamma}$ is afforded by a representation over k. Let $a \in \mathcal{N}$ act on $\mathbb{Q}(\rho_i)$ as left multiplication with ρ^i, $x \in \mathcal{N}$ by applying complex conjugation and F^l by applying the GALOIS-automorphism $\rho^i \mapsto \rho^{ip^l}$. This turns $\mathbb{Q}(\rho^i)$ into an $k(\mathcal{N} \rtimes \Gamma)$-module and it is easy to see that the corresponding representation over k affords $\lambda_i^{\mathcal{N} \rtimes \Gamma}$.

Let $1 \leq j \leq \frac{(q-1)}{2}$, j even and $\chi = \Theta_j$. This case can be treated analogously to the last case. Note that $\mathcal{N}$ has to be replaced by $\mathrm{N}_{\mathcal{G}}(\langle b \rangle)$ and lemma (2.2) of [SS83] by lemma (2.1).

□

Let K/k be a Galois extension with group Γ, G a finite subgroup of $\mathrm{GL}_n(K)$ and assume that G is defined over k. The fixed group G^Γ is a subgroup of $\mathrm{GL}_n(k)$ and is called the **subgroup of k-rational points**.

Remark 4.4.4. Denote by $\mathbb{F}_{p^r} \leq \mathbb{F}_q = \mathbb{F}_{p^f}$ the fixed field of the map F^l used in the proof of (4.4.3). The $(\mathbb{Q}(\chi)/k)$-forms constructed in this proof have the following subgroups of k-rational points:

- $\mathrm{PSL}_2(p^f)$ if χ has values in $\mathbb{Q}$
- $\mathbb{D}_{q-1}$ if $\chi \in \{\eta_1, \eta_2\}$
- $\mathbb{D}_{q+1}$ if $\chi \in \{\zeta_1, \zeta_2\}$
- $\mathrm{PGL}_2(p^r)$ if $2r \mid f$ and χ is χ_i or Θ_j
- $\mathrm{PSL}_2(p^r)$ if $2r \nmid f$ and χ is χ_i or Θ_j

A 3-dimensional representation of $\mathrm{PSL}_2(7)$ over $\mathbb{Q}(\sqrt{-7})$ which has S_3 as the subgroup of $\mathbb{Q}$-rational points can be found in [Elk99].

Proof. Identify G with $\mathrm{PSL}_2(q)$ and obtain $^- : \Gamma \to \mathrm{Aut}(G)$ from the proof of (4.4.3). Then the group of k-rational points is the fixed group of $\mathrm{PSL}_2(q)$ under Γ. Since the subgroups of $\mathrm{PSL}_2(q)$ are well known, cf. [Hup67, Chapter 2, Theorem 8.5] and due to the explicit description of the image of $^-$, the fixed groups can be calculated easily. $\square$

Chapter 5

Skew group rings

Let $k = \mathbb{Q}$, $K/\mathbb{Q}$ a finite GALOIS extension with group Γ, G a finite subgroup of $\mathrm{GL}_n(K)$, Δ the natural representation of G and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. Theorem (2.3.3) establishes a correspondence between $(K/k, ^-)$-representations of G (2.1.12) and modules over the skew group ring $K * E$ where $E = G \rtimes \Gamma$. The objective of this chapter is to study those $K * E$-modules. Actually, slightly more general skew group rings are considered i.e. we do not necessarily assume that E is a split extension of a finite group G with Γ. SHODA and NAKAYAMA [NS36] showed that $K * E$ is a semisimple $\mathbb{Q}$-algebra and noted that, if K is a splitting field of $\mathbb{Q}G$, the number of components of $K * E$ equals the number of components of the group ring KG. In a more recent paper [Kün04] and without restrictions on K, KÜNZER proved FOURIER inversion and a PLANCHEREL-formula for $K * E$. He introduced characters of $K * E$-modules and deduced SCHUR relations for them. However, the character values were not calculated explicitly.

The first section takes a step towards an explicit calculation. As a first approximation $A := \mathbb{C} \otimes_{\mathbb{Q}} K * E$-modules respectively their characters are studied. The main result, given in theorem (5.1.2), is an explicit correspondence between the characters of A-modules and the complex characters of G. Hence, A-modules are uniquely defined by their characters and the scalar product for characters of G can be used to calculate a decomposition into irreducibles. To describe the characters of A a modified character table is defined in (5.1.6) and a convenient notation is introduced.

The proof of theorem (5.1.2) is given in the second section. Its main idea is to compute the central primitive idempotents of A in two different ways, which is a rather technical matter.

Passing over from $K * E$-modules to A-modules some information is lost. More precisely, one has to decide which A-modules actually come from a $K * E$-module. This information is encoded in the SCHUR index which is introduced in section three. It is shown that the SCHUR index equals the order of the equivalence class of the central simple Γ-algebra $\Delta(\mathbb{Q}G)$ in the BRAUER-CLIFFORD group discussed in the third chapter.

In general it is a hard problem to compute the SCHUR index of a given character. A crucial tool is to construct $K * E$-modules from modules over some natural subalgebras of $K * E$. Using Γ-invariant subgroups of G, one can define induction and restriction. Those methods are applied to study the skew group rings $\mathbb{C} \otimes \mathbb{Q}(\zeta_p) * (\mathrm{SL}_2(p) \rtimes \Gamma)$ related to the groups $\mathrm{SL}_2(p)$ where p is a prime. It is shown that the SCHUR index of all of its characters is one. Specifically the $\mathrm{SL}_2(p)$ characters of degree $(p-1)/2$ and $(p+1)/2$ respectively, can be realized as a $(K/\mathbb{Q}, ^-)$-representation.

5.1 Character Theory

Let $K/\mathbb{Q}$ be a GALOIS extension with GALOIS group Γ, E a finite group, $K * E$ a skew group ring and define $G := \mathrm{C}_E(K)$. Throughout we fix an embedding $K \to \mathbb{C}$, hence view K as a subfield of $\mathbb{C}$, and assume that the induced map $E/G \to \Gamma$ is an isomorphism. The main examples are the skew group rings $K * (G \rtimes \Gamma)$ from the third section of the second chapter. Let $A := \mathbb{C} \otimes_{\mathbb{Q}} K * E$ and define a character of A as follows.

Definition 5.1.1. Let V be a finite dimensional A-module of dimension n. Choose a $\mathbb{C}$-basis of V to obtain a linear representation $\Delta_V : A \to \mathbb{C}^{n\times n}$. The character of V is the $\mathbb{C}$-linear map

$$\chi_V : A \to \mathbb{C} \ : \ x \mapsto \mathrm{Tr}(\Delta(x))$$

A character associated to an irreducible A-module V is called an irreducible character. Denote the set of all irreducible characters of A by $\mathrm{Irr}(K * E)$ and since A is semisimple it is enough to know this set.

Identify $K * E$ with $1 \otimes_{\mathbb{Q}} (K * E)$ in A and note that a character of A is uniquely defined by its restriction to this subalgebra. The main theorem gives an explicit correspondence between $\mathrm{Irr}(K*E)$ and the set of irreducible complex characters $\mathrm{Irr}(G)$ of G.

Theorem 5.1.2. *Let K/k be a finite* GALOIS *extension with group Γ, $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding, χ a irreducible complex character of G and choose an embedding of K into $\mathbb{C}$. Define $\widehat{\chi} : K * E \to \mathbb{C}$ as the $\mathbb{Q}$-linear extension of*

$$\widehat{\chi}(yg) = \begin{cases} \sum_{\sigma\in\Gamma} \sigma(y)\chi(\overline{\sigma}(g)) & \text{if } g \in G, \\ 0 & \text{if } g \notin G. \end{cases}$$

with $y \in K$ and $g \in E$. Denote the $\mathbb{C}$-linear extension of $\widehat{\chi}$ by $\widetilde{\chi}$.

Then $\widetilde{\chi}$ is an irreducible character of A and the map $\chi \mapsto \widetilde{\chi}$ defines a one to one correspondence between the irreducible complex characters of G and A.

One important remark on how this correspondence depends on the embedding $K \to \mathbb{C}$ has to be made.

Remark 5.1.3. Using different embeddings $K \to \mathbb{C}$, the image of a complex character may give a different A-character. However, since the set of all irreducible characters of A does not depend on the embedding, this induces a Γ action one the set of irreducible characters of A.

Extending the correspondence of theorem (5.1.2) between the irreducible characters $\mathbb{C}$-linearly, the following corollary is immediate.

Corollary 5.1.4. *The correspondence of theorem (5.1.2) induces an isomorphism between the $\mathbb{C}$-spaces generated by the irreducible character of A and G respectively.*

The proof of (5.1.2) is part of the next section. The main idea is to calculate the central primitive idempotents of A in two ways. It turns out that one way depends on the embedding $K \to \mathbb{C}$ and the other does not. This could be expected from the last remark.

The main theorem has some easy corollaries, which the next remark sums up.

Remark 5.1.5.

1. Every character of A restricts to a class function of E. Let χ, ψ be two irreducible characters of G within the same Γ-orbit, then $\widetilde{\chi}_{|E} = \widetilde{\psi}_{|E}$. This shows that the characters of A are not uniquely determined by their values on E. It emphasizes the fact that $K * E$ is not a K-algebra.

2. It suffices to know the characters of A on a $\mathbb{Q}$-basis of $K * E$. Specifically, the characters are determined by their values on a finite set. Unfortunately there is no canonical choice of a $\mathbb{Q}$-basis of K.

3. The irreducible A-modules are, up to isomorphism, uniquely determined by their character. Hence, every A-module is uniquely determined up to isomorphism by its character.

4. Let M be an A-module with character $\widetilde{\psi}$ where ψ is a character of G. For any irreducible A-module M_i with character $\widetilde{\chi_i}$, the multiplicity of M_i occurring in M is given by $(\psi, \chi_i) = \frac{1}{|G|} \sum_{g \in G} \psi(g)\chi_i(g^{-1})$.

To describe the characters we define a character table for A. Remark (5.1.5) suggests that it should depend canonically on the field K and not on a specific $\mathbb{Q}$-basis.

Definition 5.1.6. Choose a set of representatives $(g_j)_{1 \le j \le h}$ of the conjugacy classes of G and denote by $(\chi_i)_{1 \le i \le h}$ the irreducible characters of G. The character table of A is a map

$$K \to \mathbb{C}^{h \times h} \ , \ y \mapsto (\widetilde{\chi_i}(yg_j))_{1 \le i,j \le h}$$

The next remark introduces a convenient notation for character tables.

Remark 5.1.7.

1. Very often one has $\widetilde{\chi}(yg_j) = |\Gamma| \operatorname{Tr}_{K/\mathbb{Q}}(y)\chi(g_j)$, for example this is the case if the conjugacy class of g_j is fixed by Γ. In this situation we just print the value $|\Gamma|\chi(g_j)$, leaving out the dependence on y. Note that in those cases the value of $\widetilde{\chi}$ does not depend on the embedding of K into $\mathbb{C}$. In the other cases we write down the value of $\widetilde{\chi}$ depending on y and mark the cells gray.

2. The degree of the characters and their restrictions to G can be read off easily. Note that if $\chi, \psi \in \mathrm{Irr}(G)$ are in the same Γ-orbit the gray cells for the characters $\widetilde{\chi}$ and $\widetilde{\psi}$ are interchanged accordingly.

We compute the character tables for two examples.

Example 5.1.8. Consider the skew group ring $\mathbb{Q}(i) * (\mathrm{Q}_8 \rtimes \Gamma)$ of example (2.3.5). Choose $\{1, a^2, a, b, ab\}$ as a set of representatives of the conjugacy classes of G. The character table of A is:

	1	a^2	a	b	ab
$\widetilde{\chi_1}$	2	2	2	2	2
$\widetilde{\chi_2}$	2	2	2	-2	-2
$\widetilde{\chi_3}$	2	2	-2	2	-2
$\widetilde{\chi_4}$	2	2	-2	-2	2
$\widetilde{\chi_5}$	4	-4	0	0	0

Note that no shading was necessary since all conjugacy classes are fixed by Γ. One sees directly that $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}(i) * (\mathrm{Q}_8 \rtimes \Gamma)$ has the Wedderburn decomposition $\oplus_{i=1}^{4} \mathbb{C}^{2\times 2} \oplus \mathbb{C}^{4\times 4}$. In (2.3.5) the character $\overline{\chi_5}$ is realized as a 4-dimensional representation over $\mathbb{Q}$. It is easy to realize the remaining characters over $\mathbb{Q}$, hence $\mathbb{Q}(i) * (\mathrm{Q}_8 \rtimes \Gamma) = \oplus_{i=1}^{4} \mathbb{Q}^{2\times 2} \oplus \mathbb{Q}^{4\times 4}$.

Example 5.1.9. Let $G = \mathrm{A}_5$, then $\mathrm{Aut}(G) = \mathrm{S}_5 = \mathrm{A}_5 \rtimes \mathrm{C}_2$. Choose $K = \mathbb{Q}(\sqrt{5})$ and define $^- : \Gamma \to \mathrm{Aut}(G)$ mapping the generator σ of Γ to the generator of C_2. Note that Γ interchanges the conjugacy classes of elements of order 5. Write $\mathrm{Tr}(y) := y + \sigma(y)$ for $y \in K$ and define $b_5 := \frac{-1+\sqrt{5}}{2}$. The character table for A is:

	1	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,2,3,5,4)$
$\widetilde{\chi_1}$	2	2	2	2	2
$\widetilde{\chi_2}$	6	-2	0	$-\mathrm{Tr}(y \cdot b_5)$	$-\mathrm{Tr}(\sigma(y) \cdot b_5)$
$\widetilde{\chi_3}$	6	-2	0	$-\mathrm{Tr}(\sigma(y) \cdot b_5)$	$-\mathrm{Tr}(y \cdot b_5)$
$\widetilde{\chi_4}$	8	0	2	-2	-2
$\widetilde{\chi_5}$	10	2	-2	0	0

Note that all characters have values in $\mathbb{Q}$. Since χ_2 and χ_3 are in the same Γ-orbit, the corresponding characters $\widetilde{\chi_2}$, $\widetilde{\chi_3}$ agree on G. The Γ action on the characters of A, mentioned in remark (5.1.3), interchanges $\widetilde{\chi_2}$ and $\widetilde{\chi_3}$.

We come back to the special situation of the second chapter. Let $K/\mathbb{Q}$ a finite Galois extension with group Γ, G be a finite subgroup of $\mathrm{GL}_n(K)$ defined over k and $^- : \Gamma \to \mathrm{Aut}(G)$ the induced embedding. In lemma (2.3.6) a $K * (G \rtimes \Gamma)$-module was constructed and its character value is computed in the next corollary.

Corollary 5.1.10. *Let $G \leq \mathrm{GL}_n(K)$ be a defined over k with natural character χ and natural representation Δ. Give $M = K^{n\times 1}$ the $K * (G \rtimes \Gamma)$-module structure of lemma (2.3.6) and view $\mathbb{C} \otimes M$ as an A-module. Denote the corresponding character by χ_M. Under the correspondence (5.1.4) we have $\widetilde{\chi} = \chi_M$.*

Proof. The representation of A associated to $\mathbb{C} \otimes M$ is obtained by restricting the scalars of Δ to $\mathbb{Q}$ and using the componentwise action of Γ on $K^{n\times 1}$. For $y \in K$ and $g \in G$ one computes the corresponding character as:

$$\chi_M(yg) = \sum_{\sigma\in\Gamma} \sigma(\mathrm{Tr}(\Delta(yg)) = \sum_{\sigma\in\Gamma} \sigma(y)\chi(\overline{\sigma}(g)) = \widetilde{\chi}(yg)$$

If $g \notin G$ then $\chi_M(yg) = 0$ follows easily. □

Remark 5.1.11. Specifically, $(K/\mathbb{Q}, {}^{-})$-representations of G that are absolutely irreducible as K-linear representations correspond to the irreducible A-modules coming from $K * (G \rtimes \Gamma)$-modules.

5.2 Central idempotents

In this section we will prove the main theorem (5.1.2). Hence we make the same assumptions as in the beginning of the last section. Let $K/\mathbb{Q}$ be a Galois extension with Galois group Γ, E a finite group, $K * E$ a skew group ring and define $G := \mathrm{C}_E(K)$. Throughout we fix an embedding $K \to \mathbb{C}$, hence view K as a subfield of $\mathbb{C}$, and assume that the induced map $E/G \to \Gamma$ is an isomorphism.

We have to fix some notation. Denote by l the degree of the Galois extension $K/\mathbb{Q}$, let $(y_r)_{1\le r\le l}$ be a $\mathbb{Q}$-basis of K and $(y_r^*)_{1\le r\le l}$ the dual basis with respect to the trace bilinear form. We fix an embedding $K \to \mathbb{C}$ and view K as a subfield of $\mathbb{C}$. Elements of $A = \mathbb{C} \otimes_{\mathbb{Q}} K * E$ will be written as

$$\sum_{g\in E} \sum_{1\le r\le l} a_{g,r} \otimes y_r g$$

with $a_{g,r} \in \mathbb{C}$.

To compute the components of A, it suffices to compute a decomposition of 1_A into central primitive idempotents.

Identify $K * E$ with $1 \otimes K * E$ and K with $1 \otimes K$ in A. View $\mathbb{C}G = \mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}G$ and $\mathbb{C} \otimes K$ as subalgebras of A. It is well known that

$$\mathbb{C} \otimes_{\mathbb{Q}} K \to \oplus_{\sigma\in\Gamma}\mathbb{C} \;:\; a \otimes b \mapsto (a\sigma(b))_\sigma$$

defines a $\mathbb{C}$-algebra isomorphism. Note that $K = 1 \otimes K$ is embedded diagonally into $\oplus_{\sigma\in\Gamma}\mathbb{C}$ but with a twist in each component. Let $(e_\sigma)_{\sigma\in\Gamma}$ be the primitive idempotents of $\mathbb{C}\otimes K$ corresponding to this decomposition. Note that $e_\sigma(1\otimes K)$ corresponds to the embedding $K \to \mathbb{C}$, $y \mapsto \sigma(y)$.

It is clear that Γ acts on the set of those idempotents and permutes them regularly. Let e_{id} be the primitive idempotent of $\mathbb{C} \otimes K$ corresponding to the embedding $K \to \mathbb{C}$ which was fixed in the beginning. Viewing e_{id} as an element of A we have that $\sigma(e_{\mathrm{id}}) = e_{\sigma^{-1}}$ for all $\sigma \in \Gamma$.

The next theorem calculates the central primitive idempotents of A.

Theorem 5.2.1. *Let $K/\mathbb{Q}$ be a* Galois *extension with* Galois *group Γ, $K * E$ a skew group ring, $G := \mathrm{C}_G(K)$ and assume that the induced map $E/G \to \Gamma$ is an isomorphism.*

Let $1_G = \sum_{i=1}^{s} e_i$ be a decomposition of 1 in $\mathbb{C}G$ into central, primitive idempotents and let e_{id} be the primitive idempotent of $\mathbb{C} \otimes K$ constructed in the preceding discussion. View the $(e_i)_{1 \le i \le s}$ and e_{id} as idempotents of A and define

$$\widetilde{e_i} := \sum_{\sigma \in \Gamma} \sigma(e_{\mathrm{id}} e_i)$$

Then $\widetilde{e_i} \in A$ and $1_A = \sum_{i=1}^{s} \widetilde{e_i}$ is a decomposition of 1 in A into central, primitive idempotents of A.

Proof. We show that 1_A decomposes into the $\widetilde{e_i}$ and that those are central, primitive idempotents.

Note that G commutes with $K = 1 \otimes K$ in A and hence in A we have $e_\sigma e_i = e_i e_\sigma$ for all $1 \le i \le s$ and $\sigma \in \Gamma$. It is easy to see that $1_A = \sum_{i=1}^{s} \widetilde{e_i}$ and that the $\widetilde{e_i}$ are central. Let $1 \le i, j \le s$, use the orthogonality of $(e_\sigma)_{\sigma \in \Gamma}$ and $(e_i)_{1 \le i \le s}$ to compute:

$$\begin{aligned} \widetilde{e_i}\widetilde{e_j} = \sum_{\sigma \in \Gamma} \sigma(e_{\mathrm{id}} e_i) \sum_{\sigma \in \Gamma} \sigma(e_{\mathrm{id}} e_j) &= \sum_{\sigma \in \Gamma} \sigma(e_{\mathrm{id}}) \sigma(e_i e_j) \\ &= \delta_{i,j} \widetilde{e_i} \end{aligned}$$

This shows that $1_A = \sum_{i=1}^{s} \widetilde{e_i}$ is a decomposition of 1_A into s distinct central and orthogonal idempotents. The primitivity follows from the fact that A has only s components [Kün04, Corollary, 1.29]. □

Remark 5.2.2. The last theorem depends on the embedding of $K \to \mathbb{C}$. Since those embeddings correspond to Γ, this induces a Γ-action on the set of central primitive idempotents of A. This action is precisely the action mentioned in remark (5.1.3).

We need the following result from number theory cf. [Kün04, Remark 1.23].

Proposition 5.2.3. *Let $K/\mathbb{Q}$ be a* Galois *extension with $\mathbb{Q}$-basis $(y_r)_{1 \le r \le l}$ and dual basis $(y_i^*)_{1 \le r \le l}$. For all $\sigma \in \Gamma$ one has $\sum_{r=1}^{l} y_r \sigma(y_r^*) = \delta_{1,\sigma}$.*

Proof. Use linear algebra to see that the statement is independent of the choice of the basis. Hence it is enough to choose a primitive element $\alpha \in K$ and consider the basis $(1, ..., \alpha^{l-1})$. Let $f(x)$ be the minimal polynomial of α, then

$$\frac{f(x)}{x - \alpha} = b_0 + b_1 x + ... + b_{l-1} x^{l-1}$$

and it is well known [Neu99][p.208] that the dual basis is given by

$$\frac{b_0}{f'(\alpha)}, ..., \frac{b_{l-1}}{f'(\alpha)}$$

The claim follows from an easy calculation. □

Recall that the central, primitive idempotents e_i of $\mathbb{C}G$ can be calculated explicitly [Isa76]. In A they take the form

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1}) \otimes g \in A$$

Combined with the last proposition this leads to explicit description of the $\widetilde{e_i}$.

Proposition 5.2.4. *Let $K/\mathbb{Q}$ be* Galois *extension, $(y_r)_{1 \leq r \leq l}$ a $\mathbb{Q}$-basis of K with dual basis $(y_i^*)_{1 \leq r \leq l}$, χ_i the irreducible character of G corresponding to the central, primitive idempotent e_i of $\mathbb{C}G$. The idempotent $\widetilde{e_i}$ is given by:*

$$\widetilde{e_i} = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \sum_{r=1}^{l} \sum_{\sigma \in \Gamma} \sigma(y_r^*) \chi_i(\overline{\sigma}(g^{-1})) \otimes y_r g$$

Proof. From (5.2.3) one concludes that

$$\sigma(e_{\mathrm{id}}) = e_{\sigma^{-1}} = \sum_{r=1}^{l} \sigma^{-1}(y_r^*) \otimes y_r$$

and computes:

$$\begin{aligned}
\widetilde{e_i} = \sum_{\sigma \in \Gamma} \sigma(e_{\mathrm{id}} e_i) &= \frac{\chi_i(1)}{|G|} \sum_{\sigma \in \Gamma} e_{\sigma^{-1}} \sigma(\sum_{g \in G} \chi_i(g^{-1}) \otimes g) \\
&= \frac{\chi_i(1)}{|G|} \sum_{\sigma \in \Gamma} \sum_{g \in G} \sum_{r=1}^{l} \sigma^{-1}(y_r^*) \chi_i(g^{-1}) \otimes y_r \overline{\sigma}(g) \\
&= \frac{\chi_i(1)}{|G|} \sum_{g \in G} \sum_{r=1}^{l} \sum_{\sigma \in \Gamma} \sigma(y_r^*) \chi_i(\overline{\sigma}(g^{-1})) \otimes y_r g
\end{aligned}$$

□

The next step is to calculate the central primitive idempotents of A using the irreducible characters. Note that those characters do not depend on the embedding of K into $\mathbb{C}$.

Lemma 5.2.5. *Let $1_A = \widetilde{e_1} + ... + \widetilde{e_s}$ be the decomposition of 1_A in A into central, primitive idempotents of theorem (5.2.1). Denote by $\widetilde{\chi_i}$ the irreducible character of A corresponding to $\widetilde{e_i}$. For every $1 \leq i \leq s$ we have:*

$$\widetilde{e_i} = \frac{\widetilde{\chi_i}(1)}{|E|} \sum_{g \in E} \sum_{1 \leq r \leq l} \widetilde{\chi_i}(g^{-1} y_r^*) \otimes y_r g$$

Proof. Let ρ denote the regular trace on A and $(M_j)_{1 \leq j \leq s}$ the irreducible A-modules with corresponding characters $\widetilde{\chi_j}$. It is easy to see that the regular trace decomposes as $\rho = \sum_{j=1}^{s} \widetilde{\chi_j}(1)\widetilde{\chi_j}$. Write the idempotent $\widetilde{e_i}$ as

$$\widetilde{e_i} = \sum_{g \in E} \sum_{1 \leq r \leq l} a_{g,r} \otimes y_r g$$

with $a_{g,r} \in \mathbb{C}$. For every $1 \leq \tau \leq l$ and $\widetilde{g} \in E$ one has $\rho(\widetilde{e_i}\widetilde{g}^{-1}y_\tau^*) = a_{\widetilde{g},\tau}|E|$. This implies

$$a_{\widetilde{g},\tau}|E| = \sum_{j=1}^{s} \widetilde{\chi_j}(1)\widetilde{\chi_j}(e_i\widetilde{g}^{-1}y_\tau^*) = \widetilde{\chi}_i(1)\widetilde{\chi}_i(\widetilde{g}^{-1}y_\tau^*)$$

and the claim follows.

□

To prove the main theorem (5.1.2), compare the formulas of proposition (5.2.4) and lemma (5.2.5). Doing so one obtains:

$$\widetilde{\chi}_i(gy_r) = \begin{cases} \frac{\chi_i(1)|\Gamma|}{\widetilde{\chi}_i(1)} \sum_{\sigma\in\Gamma} \sigma(y_r)\chi_i(\overline{\sigma}(g)) & \text{if } g \in G, \\ 0 & \text{if } g \notin G. \end{cases}$$

Substitute $g = 1$ and $y_1 = 1$ to conclude that $\widetilde{\chi}_i(1) = \chi_i(1)|\Gamma|$ and this proves the main theorem.

5.3 The Schur Index

Let $K/\mathbb{Q}$ be a Galois extension with Galois group Γ, E a finite group, $K*E$ a skew group ring and define $G := \mathrm{C}_E(K)$. In this section we study the following question: Given an irreducible character $\widetilde{\chi}$ of A and an algebraic extension field L of $\mathbb{Q}$, is there a L-linear representation of $L \otimes_{\mathbb{Q}} K * E$ affording $\widetilde{\chi}$?

In other words, we want to measure the loss of information passing from $K * E$ to A. This suggests the following definition.

Definition 5.3.1. Let $\widetilde{\chi}$ be an irreducible character of $K * E$. Choose an irreducible $\mathbb{C}$-representation $\widetilde{\Delta}$ of A affording $\widetilde{\chi}$ and an irreducible L-representation Ξ of $L \otimes_{\mathbb{Q}} K * E$ such that $\widetilde{\Delta}$ is a constituent of Ξ. The multiplicity of $\widetilde{\Delta}$ as a constituent of Ξ is called the **Schur index of $\widetilde{\chi}$ over L**. It is denoted by $\mathrm{m}_L(\widetilde{\chi})$.

This definition is the same as in the classical case [Isa76, Chapter 10] and with it we can rephrase remark (5.1.11) using characters only.

Remark 5.3.2. Let G be a finite matrix group and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. The $(K/\mathbb{Q}, ^-)$-representations of G that are absolutely irreducible as K-linear representations correspond to the irreducible $K*(G \rtimes \Gamma)$-characters $\widetilde{\chi}$ with character field $\mathbb{Q}$ and Schur index 1 over $\mathbb{Q}$.

The next remark covers the special case where K is a cyclotomic field.

Remark 5.3.3. Let G be a finite group, $K = \mathbb{Q}(\zeta_q)$ the q-th cyclotomic field with Galois group Γ and assume that Γ acts faithfully on G as group automorphism. Define $E := G \rtimes \Gamma$ and let $K * E$ be the skew group ring constructed using the natural Γ action on K. Note that $\mathrm{C}_q = \langle\zeta_q\rangle$ is a subgroup of K and define $G' := (\mathrm{C}_q \times G) \rtimes \Gamma$. Then every $K * E$-module is a $\mathbb{Q}G'$-module which as a $\mathbb{Q}\,\mathrm{C}_q \rtimes \Gamma$-module is the l-fold copy of the unique faithful and absolutely irreducible $\mathbb{Q}\,\mathrm{C}_q \rtimes \Gamma$-module K for some $l \in \mathbb{N}$. Conversely, every such $\mathbb{Q}G'$-module is a $K * E$-module.

Denote the (absolutely irreducible) character of the $\mathbb{Q}\,\mathrm{C}_q \rtimes \Gamma$-module K by ψ. The irreducible $K * E$ characters correspond to irreducible G' characters which, restricted to $\mathrm{C}_q \rtimes \Gamma$, are $l\psi$ for an $l \in \mathbb{N}$. In this case the Schur index of the irreducible $K * E$-characters agrees with the classical Schur index of the corresponding irreducible G' character.

The Schur index has the following important properties, which can be proved as in the classical case.

Remark 5.3.4.

1. The Schur index of an irreducible $K * E$ character $\widetilde{\chi}$ over a field L is the same as the Schur index of $\widetilde{\chi}$ over the character field $L(\widetilde{\chi})$
2. Let χ be an irreducible character of G and $\widetilde{\chi}$ the corresponding irreducible character of A. If $\widetilde{\psi}$ is the character of any L-representation of $L \otimes_{\mathbb{Q}} K * E$, then $\mathrm{m}_L(\widetilde{\chi})$ divides $(\psi, \chi)_G$.
3. The Schur index is the smallest integer m such that $m\widetilde{\chi}$ is afforded by an $L(\widetilde{\chi})$ representation of $L(\widetilde{\chi}) \otimes_{\mathbb{Q}} K * E$.

Recall the twisted group rings $K * (G \rtimes \Gamma)$ constructed in the first chapter from a finite group G and a Galois extension $K/\mathbb{Q}$ with Galois group Γ. Assume that $\chi \in \mathrm{Irr}(G)$ has the property

$$\sigma(\chi(g)) = \chi(\overline{\sigma}(g) \text{ for all } \sigma \in \Gamma, g \in G$$

Under this assumption the next theorem relates the Schur index of $\widetilde{\chi}$ to the Brauer-Clifford theory of the second chapter.

Theorem 5.3.5. *Let $K/\mathbb{Q}$ be a* Galois *extension with group Γ, G an absolutely irreducible finite subgroup of $\mathrm{GL}_n(K)$ and $^{-} : \Gamma \to \mathrm{Aut}(G)$ an injective homomorphism. Let $\Delta : G \to \mathrm{GL}_n(K)$ be the natural representation, χ the natural character and assume that*

$$\text{(Co)} \qquad \sigma(\chi(g)) = \chi(\overline{\sigma}(g) \textit{ for all } \sigma \in \Gamma, g \in G$$

The Schur *index of the character $\widetilde{\chi}$ of $K * (G \rtimes \Gamma)$ over $\mathbb{Q}$ equals the order of the element $[\Delta(\mathbb{Q}G) \otimes_{\mathbb{Q}(\chi)} K]$ c.f (3.2.1) in the* Brauer-Clifford *group, where $\widetilde{\chi}$ is the character corresponding to χ under (5.1.4).*

Proof. Condition (Co) implies that $\widetilde{\chi}$, the character of A corresponding to χ via (5.1.4), has rational values.

Using theorem (3.2.1) turns $\Delta(\mathbb{Q}G)$ into a central simple Γ-algebra. We will show that in the Brauer-Clifford-group the order of the image of this class under the scalar extension map (3.1.6) equals the Schur-index of $\widetilde{\chi}$ over $\mathbb{Q}$.

Condition (Co) implies that idempotent

$$e_{\widetilde{\chi}} = \frac{\chi(1)}{|G|} \sum_{g \in G} \sum_{r=1}^{l} \sum_{\sigma \in \Gamma} \sigma(y_r^*) \chi(\overline{\sigma}(g^{-1})) \otimes y_r g$$

of A lies in $K * (G \rtimes \Gamma)$ cf. (5.2.4). It is easy to see that the SCHUR index of $\widetilde{\chi}$ is the index of the central simple $\mathbb{Q}$-algebra $B := e_{\widetilde{\chi}}(K * (E \rtimes \Gamma))$. View B as an element of the BRAUER-group, then it is well known that this index equals the order of B [Rei75, Theorem 31.4].

Recall the isomorphism $\delta : \mathrm{Br}(K|\mathbb{Q}) \to \mathrm{H}^2(\Gamma, K^*)$ of the discussion preceding lemma (3.3.1) between the relative BRAUER-group and a second GALOIS cohomology group [Ser79, Chapter X]. The objective is to calculate the image $\delta(B)$.

Define the embedding

$$\Psi : K^{n\times n} \to K^{|\Gamma|n\times|\Gamma|n} \;:\; X \mapsto \mathrm{diag}((\sigma(X))_{\sigma\in\Gamma})$$

where $\mathrm{diag}((\sigma(X))_{\sigma\in\Gamma})$ is a block diagonal matrix with blocks $\sigma(X)$. Denote by

$$\mathrm{P} : \Gamma \to \mathrm{GL}_{|\Gamma|}(\mathbb{Q}) : \;\sigma \mapsto \mathrm{P}(\sigma)$$

the regular representation of Γ. The map

$$\widetilde{\Delta} : K \otimes_{\mathbb{Q}} K * (G \rtimes \Gamma) \to K^{|\Gamma|n\times|\Gamma|n} \;:\; a \otimes yg\sigma \mapsto \mathrm{diag}(a)\Psi(y)\Psi(\Delta(g))(\mathrm{P}(\sigma)\otimes \mathrm{I}_n)$$

with $a, y \in K, g \in G, \sigma \in \Gamma$ is a K-algebra epimorphism and induces a K-algebra isomorphism $K \otimes_{\mathbb{Q}} B \to K^{|\Gamma|n\times|\Gamma|n}$. This shows that K splits B.

Condition (Co) guarantees that for every $\sigma \in \Gamma$ there exists a matrix $X_\tau \in \mathrm{GL}_n(K)$ such that

$$X_\sigma \sigma(\Delta(g)) X_\sigma^{-1} = \Delta(\overline{\sigma}(g)) \text{ for all } g \in G$$

It is clear that for all $\sigma, \tau \in \Gamma$ there exists $\lambda_{\sigma,\tau} \in K$ with $X_{\sigma\tau} = \lambda_{\sigma,\tau} X_\sigma \sigma(X_\tau)$.

Define $Y_\tau := \Psi(\tau)\mathrm{diag}(X_\tau)$ for $\tau \in \Gamma$ and calculate for $\sigma, \tau \in \Gamma$:

$$\begin{aligned} Y_{\sigma\tau} &= \Psi(\sigma\tau)\mathrm{diag}(X_{\sigma\tau}) \\ &= \lambda_{\sigma,\tau}\Psi(\sigma)\Psi(\tau)\mathrm{diag}(X_\sigma)\sigma(\mathrm{diag}(X_\tau)) \\ &= \lambda_{\sigma,\tau}\Psi(\sigma)\mathrm{diag}(X_\sigma)\sigma(\Psi(\tau)\mathrm{diag}(X_\tau)) \\ &= \lambda_{\sigma,\tau} Y_\sigma \sigma(Y_\tau) \end{aligned}$$

Hence the map $\Gamma \to \mathrm{PGL}_n(K) \;:\; \sigma \mapsto Y_\sigma$ is a 1-cocycle. Identify B with $\widetilde{\Delta}(B)$. By construction we have:

$$B = \{x \in K^{n|\Gamma|\times n|\Gamma|} \mid Y_\sigma \sigma(x) Y_\sigma^{-1} = x \text{ for all } \sigma \in \Gamma\}$$

Use the description of δ in [Ser79] to see that the image of B under δ is the 2-cocycle:

$$\delta(B)(\sigma, \tau) = \lambda_{\sigma,\tau} \text{ for all } \sigma, \tau \in \Gamma$$

This cocycle λ uniquely determines the equivalence class of $[\Delta(\mathbb{Q}G) \otimes_{\mathbb{Q}(\chi)} K]$ in the BRAUER-CLIFFORD group by lemma (3.1.11). This proves the theorem. □

We discuss an example similar to (5.1.8).

Example 5.3.6. Denote by ζ_3 a primitive third root of unity. Construct the skew group ring $\mathbb{Q}(\zeta_3) * (\mathrm{Q}_8 \rtimes \Gamma)$ as in (2.3.5) The character table is

	1	a^2	a	b	ab
$\widetilde{\chi_1}$	2	2	2	2	2
$\widetilde{\chi_2}$	2	2	2	-2	-2
$\widetilde{\chi_3}$	2	2	-2	2	-2
$\widetilde{\chi_4}$	2	2	-2	-2	2
$\widetilde{\chi_5}$	4	-4	0	0	0

Hence $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_3) * (\mathrm{Q}_8 \rtimes \Gamma)$ has the WEDDERBURN decomposition $\oplus_{i=1}^{4} \mathbb{C}^{2\times 2} \oplus \mathbb{C}^{4\times 4}$. The character $\widetilde{\chi_5}$ has SCHUR-index 2 over $\mathbb{Q}$ by example (3.3.7). Using remark (5.3.3) this follows also from the fact that the character of degree 4 of $(\mathrm{C}_3 \times \mathrm{Q}_8) \rtimes \Gamma$ has SCHUR-index 2.

Recall the discussion of the case of the real numbers $\mathbb{R}$ in the fourth chapter. Let G be a finite group and u be an element of order 2 in $\mathrm{Aut}(G)$. Define

$$^{-} : \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle \sigma \rangle \to \mathrm{Aut}(G) \ : \ \sigma \mapsto u$$

The skew group algebras under consideration are $\mathbb{C} * (G \rtimes \Gamma)$ and $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} * (G \rtimes \Gamma)$. Using the SCHUR index and the twisted FROBENIUS-SCHUR index, theorem (4.2.1) becomes:

Corollary 5.3.7. *Let χ be an irreducible character of G, then:*

$$\epsilon^u(\chi) = \begin{cases} 1, & \text{if and only if } \mathbb{R}(\widetilde{\chi}) = \mathbb{R} \text{ and } m_{\mathbb{R}}(\widetilde{\chi}) = 1 \\ -1, & \text{if and only if } \mathbb{R}(\widetilde{\chi}) = \mathbb{R} \text{ and } m_{\mathbb{R}}(\widetilde{\chi}) = 2 \\ 0, & \text{otherwise} \end{cases}$$

where $\widetilde{\chi}$ is the character of $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} * (G \rtimes \Gamma)$ corresponding to χ via (5.1.4).

5.4 Induction and Restriction

Let $K/\mathbb{Q}$ be a GALOIS extension with GALOIS group Γ, G a finite subgroup of $\mathrm{GL}_n(K)$ and $^{-} : \Gamma \to \mathrm{Aut}(G)$ an embedding. In this section we restrict ourselves to the special skew group rings $K * E$ where $E := G \rtimes \Gamma$. A convenient way to construct $K * E$ modules is to induce them up from modules over a subalgebra of $K * E$. For this purpose we consider U to be a Γ-stable subgroup of G. View the skew group ring $K * (U \rtimes \Gamma)$ as a subalgebra of $K * E$. For a $K * (U \rtimes \Gamma)$-module M define the induced module $M^E := (K * E) \otimes_{K*(U\rtimes\Gamma)} M$. The following remark describes the induced matrix representation and the character corresponding to an induced module.

Remark 5.4.1. Let M be a $K * (U \rtimes \Gamma)$-module of $\mathbb{Q}$-dimension n, $B = (B_1, ..., B_n)$ a $\mathbb{Q}$-basis of M and Δ the corresponding linear representation. Choose a left transversal s_i of U in G, then $s_i \otimes B_k$ is a $\mathbb{Q}$-basis of M^E. For every $y \in K$ and $g \in E$ the induced representation is the block matrix

$$\Delta^E(yg) = (\dot{\Delta}(yg))_{i,j} \in \mathbb{Q}^{[G:U]n \times [G:U]n}$$

with $n \times n$ blocks

$$\dot{\Delta}(yg) = \begin{cases} 0 & , \text{ if } gs_j \notin s_i U \rtimes \Gamma \\ \Delta(s_i^{-1} y g s_j) & , \text{ if } gs_j \in s_i U \rtimes \Gamma \end{cases}$$

Let χ be the character corresponding to M and χ^E the character corresponding to M^E. Then χ^E is given by:

$$\chi^E(yg) = \sum_{i=1}^{[G:U]} \dot{\chi}(s_i^{-1} y g s_i) \text{ with } \dot{\chi}(yg) = \begin{cases} 0 & ,\text{if } g \notin U \rtimes \Gamma, \\ \chi(yg) & ,\text{if } g \in U \rtimes \Gamma \end{cases}$$

Denote by $C(G), C(U), C(K * E), C(K * (U \rtimes \Gamma)$ the $\mathbb{C}$-space generated by the irreducible characters of G, U, A and $\mathbb{C} \otimes K * (U \rtimes \Gamma)$. Character induction defines maps $\mathrm{Ind} : C(U) \to C(G)$ and $\mathrm{Ind} : C(K * (U \rtimes \Gamma)) \to C(K * E)$.

Theorem 5.4.2. *The following diagram is commutative.*

$$\begin{tikzcd} C(K * (U \rtimes \Gamma)) \arrow[r, "\mathrm{Ind}"'] & C(K * E) \\ C(U) \arrow[u, "\psi \mapsto \widetilde{\psi}"'] \arrow[r, "\mathrm{Ind}"'] & C(G) \arrow[u, "\chi \mapsto \widetilde{\chi}"'] \end{tikzcd}$$

Proof. Reduce to the case of an irreducible character and use the definition of the correspondence (5.1.4). □

Remark 5.4.3. Let U be a Γ-invariant subgroup of G. Character induction from U to G is Γ-equivariant, that is for every character χ of U we have: $(\chi \circ \overline{\sigma})^G = \chi^G \circ \overline{\sigma}$ for all $\sigma \in \Gamma$. Hence, $\widetilde{\chi \circ \overline{\sigma}}^G = \widetilde{\chi^G \circ \overline{\sigma}}$.

Combining the last remark with remark 5.1.5 (4) and classical Frobenius reciprocity, one gets the following corollary.

Corollary 5.4.4. *Given a character $\widetilde{\chi}$ of A and $\widetilde{\psi}$ of $\mathbb{C} \otimes K * (U \rtimes \Gamma)$, the multiplicity of $\widetilde{\chi}$ in $\widetilde{\psi}^E$ is $(\chi, \psi^G) = (\chi_U, \psi)$.*

Let p be a prime, we use character induction to calculate the Schur indices of the characters of a twisted group ring related to the special linear groups $\mathrm{SL}_2(p)$. It turns out that all of those are one over $\mathbb{Q}$.

Example 5.4.5. Let p be a prime, ν a generator of $\mathbb{F}_p^*$, $G = \mathrm{SL}_2(p)$ and $K = \mathbb{Q}(\zeta_p)$ and Γ its Galois group. Conjugation with the matrix

$$x := \begin{pmatrix} \nu^{-1} & 0 \\ 0 & 1 \end{pmatrix}$$

induces an outer automorphism of G, which is of order $p-1$ in $\mathrm{Aut}(G)$. It interchanges the two conjugacy classes of elements of order p and fixes the others.

Let X be the subgroup of $\mathrm{Aut}(G)$ generated by x. Choose the generator σ of Γ as $\sigma(\zeta_p) = \zeta_p^\nu$ and define $^- : \Gamma \to \mathrm{Aut}(\mathrm{SL}_2(p))$ by $\overline{\sigma} \mapsto x \cdot x^{-1}$. Note that the subgroup

$$U := \langle \underbrace{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}}_{:=u} \rangle$$

of G is X-stable and cyclic of order p.

Let $i \in \{1, ..., p-1\}$ and define the representation

$$U \to \mathrm{GL}_1(\mathbb{Q}(\zeta_p)) \;:\; u \mapsto \zeta_p^i$$

Note that this is a $(K/\mathbb{Q}, ^-)$-representation and denote the corresponding irreducible complex character of U by χ_i. Hence the corresponding character $\widetilde{\chi}$ of $K * (U \rtimes \Gamma)$ has SCHUR index 1, i.e. can be realized over $\mathbb{Q}$. Let $\psi \in \mathrm{Irr}(G)$ be any character. Use FROBENIUS reciprocity and the well known character table of G to see that there exists a character $\chi_i \in \mathrm{Irr}(U)$ such that

$$(\psi, \chi_i^G) = (\psi_U, \chi_i)_U = 1$$

Since every irreducible character of $\mathbb{Q}(\zeta_p) * (\mathrm{SL}_2(p) \rtimes \Gamma)$ is of the form $\widetilde{\psi}$ for a unique $\psi \in \mathrm{Irr}(\mathrm{SL}_2(p))$, we see that every irreducible character has SCHUR index one over $\mathbb{Q}$ by remark (5.3.4) and corollary (5.4.4).

Specifically there exist $(\mathbb{Q}(\zeta_p)/\mathbb{Q}, ^-)$-representation of $\mathrm{SL}_2(p)$ affording the characters of degree $(p+1)/2$ and $(p-1)/2$. In the nineteenth century KLEIN constructed such representation for $p = 5, 7, 11$ with geometric methods.

Chapter 6

Arithmetic of skew group rings

Let $K/\mathbb{Q}$ be a finite Galois extension with group Γ, G a finite subgroup of $\mathrm{GL}_n(K)$ and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. Let E be the semidirect product of G with Γ and construct the skew group ring $K * E$ using the natural action of Γ on K. In this chapter we study arithmetic features of the skew group rings $K * E$.

If K admits a central canonical complex conjugation, that is an element of center of Γ which induces complex conjugation in every embedding of K to $\mathbb{C}$, a canonical involution on $K * E$ is defined. Restricted to E this involution inverts the elements and restricted to K it is the canonical complex conjugation. The involution induces an involution on the enveloping $\mathbb{Q}$-algebra $\Delta(K * E)$ of any $\mathbb{Q}$-linear representation $\Delta : K * E \to \mathbb{Q}^{n \times n}$. The main theorem (6.1.2) states that this involution is the adjoint anti-automorphism of a symmetric positive definite bilinear form on the natural $\Delta(K * E)$-module.

Denote by $\mathbb{Z}_K$ the ring of algebraic integers in K. The natural Γ action on $\mathbb{Z}_K$ defines the $\mathbb{Z}$-order $\mathbb{Z}_K * E$ in $K * E$. Let M be a $K * E$-module, the objective of the second and the third section is to introduce theoretical and algorithmic methods to compute the set of all full $\mathbb{Z}_K * E$-lattices in M.

If M is absolutely irreducible, it is shown that this set can be computed from the set of all full $\mathbb{Z}_K G$-lattices in M and all Γ-invariant ideals of $\mathbb{Z}_K$ up to a certain equivalence. In general both sets are hard to obtain theoretically and algorithmic methods are needed. The centering algorithm of Plesken and Nebe provides such a method.

Putting the pieces all together, a procedure to construct numerically nice $(K/\mathbb{Q}, ^-)$-representations of G is proposed in the last section. It is shown that the denominators occurring in those representations divide the discriminant of K.

6.1 Canonical involution

Let G be a finite group and K be either a totally real Galois extension of $\mathbb{Q}$ or a field with a central **canonical complex conjugation**, that is an element of center of the GALOIS group Γ which induces complex conjugation in every complex embedding of K into $\mathbb{C}$. Note that this element is of order 2 and its fixed field is the totally real subfield of K. For cyclotomic fields $\mathbb{Q}(\zeta_n)$ for $n \in \mathbb{N}$, the map $\zeta_n \mapsto \zeta_n^{-1}$ is a central canonical complex conjugation.

Let σ be the identity if K is totally real or the central canonical complex conjugation of K. Define the map

$$\iota_\sigma : K * (G \rtimes \Gamma) \to K * (G \rtimes \Gamma) \ : \ \sum_{g \in G \rtimes \Gamma} a_g g \mapsto \sum_{g \in G \rtimes \Gamma} g^{-1} \sigma(a_g)$$

Proposition 6.1.1. *The map ι_σ is an involution on $K * (G \rtimes \Gamma)$.*

Proof. The map is $\mathbb{Q}$-linear, hence well defined. To see that it is an involution, use that σ is central to compute for all $a, b \in K$ and $g, u \in G \rtimes \Gamma$:

$$\iota_\sigma((ag)(bu)) = \iota_\sigma(a^g bgu) = u^{-1} g^{-1} \sigma(a) \sigma({}^g b)$$

and

$$\iota_\sigma(bu)\iota_\sigma(ag) = u^{-1}\sigma(b) g^{-1} \sigma(a) = u^{-1} g^{-1 g}\sigma(b)\sigma(a) = u^{-1} g^{-1} \sigma(a) \sigma({}^g b)$$

Hence $\iota_\sigma(xy) = \iota_\sigma(y)\iota_\sigma(x)$ for all $x, y \in K * (G \rtimes \Gamma)$. Using the fact that σ is central in Γ and of order 2, one easily checks that $\iota_\sigma^2 = \mathrm{id}_{K*(G \rtimes \Gamma)}$. The claim follows. □

The involution ι_σ is called the **canonical involution** on $K * (G \rtimes \Gamma)$. Let $\Delta : K * (G \rtimes \Gamma) \to \mathbb{Q}^{n \times n}$ be a linear representation, then ι_σ induces an involution on the enveloping $\mathbb{Q}$-algebra $\Delta(K * (G \rtimes \Gamma))$ by $\Delta(x) \mapsto \Delta(\iota_\sigma(x))$. The next theorem shows that this involution is the adjoint anti-automorphism of a symmetric positive definite bilinear form.

Theorem 6.1.2. *Let G be a finite group, K a GALOIS extension of $\mathbb{Q}$ with group Γ and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. Assume that K is either totally real or has a central canonical complex σ and consider the skew group ring $K * (G \rtimes \Gamma)$ with the canonical involution ι_σ. Given a linear representation $\Delta : K * (G \rtimes \Gamma) \to \mathbb{Q}^{n \times n}$, there exists a symmetric, positive definite matrix $\Phi \in \mathbb{Q}^{n \times n}$ with*

$$\Delta(\iota_\sigma(x)) = \Phi^{-1} \Delta(x)^{tr} \Phi$$

for all $x \in K * (G \rtimes \Gamma)$.

Proof. We have to construct a symmetric positive definite matrix $\Phi \in \mathbb{Q}^{n \times n}$ such that

1. $\Delta(\sigma(y))^{-tr} \Phi \Delta(y) = \Phi$ for all $y \in K^*$.
2. $\Delta(g)^{tr} \Phi \Delta(g) = \Phi$ for all $g \in G \rtimes \Gamma$

Assume that $\widetilde{\Phi} \in \mathbb{Q}^{n \times n}$ is a symmetric positive definite matrix satisfying the first condition. One easily checks that the matrix

$$\Phi := \sum_{g \in G \rtimes \Gamma} \Delta(g)^{tr} \widetilde{\Phi} \Delta(g)$$

is symmetric positive definite, and meets both conditions.

It remains to show that a symmetric positive definite matrix $\Phi \in \mathbb{Q}^{n\times n}$ fulfilling the first condition exists. Denote by $\mathrm{P} : K \to \mathbb{Q}^{[K:\mathbb{Q}]\times[K:\mathbb{Q}]}$ the regular representation of K as a $\mathbb{Q}$-algebra with respect to a $\mathbb{Q}$-basis $(y_i)_{1\leq i\leq l}$ of K. By base change one can assume that $\Delta(y) = \mathrm{diag}(\mathrm{P}(y))$ for all $y \in K$, Hence it suffices to show that there exists a s.p.d. matrix $\Phi \in \mathbb{Q}^{[K:\mathbb{Q}]\times[K:\mathbb{Q}]}$ such that $\mathrm{P}(\sigma(y))^{-t}\Phi\mathrm{P}(y) = \Phi$ for all $y \in K^*$.

Choose $\Phi = (\Phi_{i,j})_{1\leq i,j\leq l}$ with $\Phi_{i,j} := \mathrm{Tr}_K(\sigma(y_i)y_j)$ and use linear algebra to check that $\mathrm{P}(\sigma(y))^{-t}\Phi\mathrm{P}(y) = \Phi$ for all $y \in K^*$. By definition Φ lies in $\mathbb{Q}^{[K:\mathbb{Q}]\times[K:\mathbb{Q}]}$. Use that σ is of order 2 to check that

$$\mathrm{Tr}_K(\sigma(y_i)y_j) = \mathrm{Tr}_K(\sigma(y_j)y_i)$$

for all $1 \leq i, j \leq l$, hence Φ is symmetric. It is easy to see (for example use [Neu99, p. 11]) that there exists a matrix $X \in \mathrm{GL}_{[K:\mathbb{Q}]}(K)$ such that $\Phi = \sigma(X^{tr})X$. This implies that Φ is positive definite and proves the theorem. □

Remark 6.1.3.

1. Restricted to the rational group algebra $\mathbb{Q}(G \rtimes \Gamma)$ the involution ι_σ is the canonical involution induced by $g \mapsto g^{-1}$. On the field K it is canonical complex conjugation.

2. Let $\Delta : K * (G \rtimes \Gamma) \to \mathbb{Q}^{n\times n}$ be a linear representation and $\Phi \in \mathbb{Q}^{n\times n}$ the symmetric positive definite matrix of theorem (6.1.2). Then Δ is a $\mathbb{Q}$-linear representation of the group $G \rtimes \Gamma$ and Φ is a positive definite $\Delta(G \rtimes \Gamma)$ invariant form. For cyclotomic fields $K = \mathbb{Q}(\zeta_q)$, the matrix Φ is a $(\mathrm{C}_q \times G) \rtimes \Gamma$-invariant form cf. (5.3.3).

3. If $\Delta : K * (G \rtimes \Gamma) \to \mathbb{Q}^{n\times n}$ is absolutely irreducible, then the symmetric positive definite matrix of theorem (6.1.2) is uniquely determined up multiplication with a positive element of $\mathbb{Q}$.

4. Let χ be an irreducible character of G and $\widetilde{\chi}$ the corresponding character of A cf. (5.1.4). Then $\widetilde{\chi} \circ \iota_\sigma$ is the complex conjugate character of $\widetilde{\chi}$. Specifically, if $\widetilde{\chi}$ has only rational values, the corresponding component of $K * E$ is a central simple $\mathbb{Q}$-algebra with involution. Hence the SCHUR-index of $\widetilde{\chi}$ is at most two. This is a generalization of the BRAUER-SPEISER theorem.

6.2 Canonical order

We turn back to general finite GALOIS extensions $K/\mathbb{Q}$ with group Γ. Let G be a finite subgroup of $\mathrm{GL}_n(K)$ and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. Note that Γ acts naturally on the ring of algebraic integers $\mathbb{Z}_K$ in K. Hence $\mathbb{Z}_K * (G \rtimes \Gamma)$ is a skew group and moreover a $\mathbb{Z}$-order in the skew group ring $K * (G \rtimes \Gamma)$.

Let M be an $K * (G \rtimes \Gamma)$-module, and denote by $\mathcal{Z}(M)$ the set of full $\mathbb{Z}_K * (G \rtimes \Gamma)$ lattices in M. The group $\mathrm{Aut}_{K*(G\rtimes\Gamma)}(M)$ acts on this set and the orbits are the isomorphism classes of full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in M. There are only a finite number of isomorphism classes by the theorem of JORDAN-ZASSENHAUS [Rei75, Theorem 26.4].

Some general remarks can be made on this order.

Remark 6.2.1. 1. The order $\mathbb{Z}_K * (G \rtimes \Gamma)$ contains the $\mathbb{Z}_K$-order $\mathbb{Z}_K G$, the $\mathbb{Z}$-order $\mathbb{Z}_K * \Gamma$ and the integral group ring $\mathbb{Z}G \rtimes \Gamma$.

2. Let $p \in \mathbb{Z}$ be a prime and denote by $\mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ at p and by $\mathfrak{D}$ the discriminant of K. If $p \nmid \mathfrak{D}|G|$, then $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbb{Z}_K * (G \rtimes \Gamma)$ is a maximal $\mathbb{Z}_{(p)}$-order in $K * (G \rtimes \Gamma)$. This result will be proved in the next section and implies the well known group ring case for $K = \mathbb{Q}$ [Rei75, Chapter 9].

3. Let M be a $K * (G \rtimes \Gamma)$-module, then Γ acts on the set $\mathcal{Z}_{\mathbb{Z}_K G}(M)$ of full $\mathbb{Z}_K G$ lattices in M and the fixed points of this action are precisely the elements of $\mathcal{Z}(M)$.

The objective is to calculate $\mathcal{Z}(M)$. Assume that M is an absolutely irreducible $K * (G \rtimes \Gamma)$-module, then it is absolutely irreducible as a KG-module by the character correspondence (5.1.4). Let $L, L' \in \mathcal{Z}(M)$ and view L, L' as $\mathbb{Z}_K G$ lattices. If L' and L are isomorphic, then $L' = aL$ for an $a \in K$. Observe that $L' = aL$ is a $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice if and only if the principal fractional ideal generated by $a \in K$ is Γ-stable under the natural Γ-action.

On the set of Γ-stable principal fractional ideals in K define the equivalence relation:

$$\mathfrak{a}_1 \sim \mathfrak{a}_2 \Leftrightarrow \mathfrak{a}_1 = \lambda \mathfrak{a}_2 \text{ for a } \lambda \in \mathbb{Q}$$

View those ideals as $\mathbb{Z}_K * \Gamma$-lattices of $\mathbb{Z}$-rank $|\Gamma|$, hence there are only finitely many up to isomorphism by Jordan-Zassenhaus. Note that two ideals are isomorphic $\mathbb{Z}_K * \Gamma$-lattices if and only if they are equivalent under the above equivalence relation. Denote by $\mathcal{A}(K)$ a set of representatives of those equivalence classes.

The next proposition shows that $\mathcal{Z}(M)$ can be calculated from the isomorphism classes of full $\mathbb{Z}_K G$-lattice in M and $\mathcal{A}(K)$.

Proposition 6.2.2. *Let M be an absolutely irreducible $K * (G \rtimes \Gamma)$-module. View M as a $\mathbb{Z}_K G$-module and let Υ be a maximal set of pairwise non isomorphic Γ-fixed points of $\mathcal{Z}_{\mathbb{Z}_K G}(M)$. A set of representatives of the isomorphism classes of $\mathcal{Z}(M)$ is given by:*

$$\Omega := \{\mathfrak{a}L \mid \mathfrak{a} \in \mathcal{A}(\mathbb{Z}_K) \textit{and } L \in \Upsilon\}$$

Proof. It is clear that every $L \in \Omega$ is in $\mathcal{Z}(M)$. Furthermore, the elements of Ω are pairwise non isomorphic. Since every $L \in \mathcal{Z}(M)$ is a Γ-stable full $\mathbb{Z}_K N$-lattice in M and it has to appear in the set Ω. $\square$

Remark 6.2.3. Dropping the assumption that M is absolutely irreducible, then M might become reducible as a KG-module. For example this is the case for irreducible $\mathbb{Q}(\zeta_3) * (Q_8 \rtimes \Gamma)$-module affording $2 \cdot \widetilde{\chi_5}$ of example (5.3.6). In those cases it is hard to determine the set of full $\mathbb{Z}_K G$-lattices in M or to compute necessary replacement of $\mathcal{A}(K)$ and the proposition is of not much use.

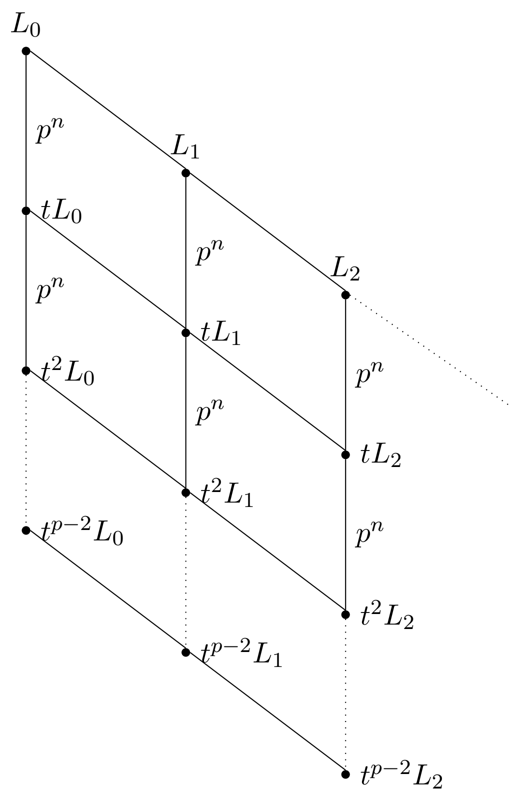
If K is the p-th cyclotomic field then $\mathcal{A}(\mathbb{Q}(\zeta_p))$ is computable.

Example 6.2.4. Let p be a prime and $K = \mathbb{Q}(\zeta_p)$ the p-th cyclotomic field. Then $\mathcal{A}(\mathbb{Z}_K) = \{(1-\zeta_p)^i \mathbb{Z}_K \mid 0 \leq i \leq p-2\}$.

Proof. Multiplying with elements in $\mathbb{Z}$ shows that it suffices to calculate the equivalence classes of Γ-stable principal $\mathbb{Z}_K$-ideals instead of principal fractional ideals. Check that all elements of $T := \{(1-\zeta_p)^i \mathbb{Z}_K \mid 0 \leq i \leq p-2\}$ are Γ-invariant and pairwise non equivalent. Use HILBERT ramification theory to see that every other Γ-stable, principal prime ideal of $\mathbb{Z}_K$ is given by $q\mathbb{Z}_K$ for a prime $q \in \mathbb{Z}$. Hence every Γ-stable ideal of $\mathbb{Z}_K$ is equivalent to an element of T. □

Remark 6.2.5.

1. Let $K = \mathbb{Q}(\zeta_p)$, M be an absolutely irreducible $\mathbb{Q}(\zeta_p) * (G \rtimes \Gamma)$-module of K-dimension n, $\Upsilon = \{L_0, ..., L_k\}$ as in proposition (6.2.2), and assume that L_0 is uniserial $\mathbb{Z}_K G$-lattice. Define $t := (1-\zeta_p)$, then the following HASSE illustrates the situation:



2. Let $G = \mathrm{PSL}_2(p)$ and $K = \mathbb{Q}(\zeta_p)$ with GALOIS group Γ. Assume that $p \equiv -1 \mod 4$ and assume $^- : \Gamma \to \mathrm{Aut}(G)$ as in example (5.4.5). Choose χ to be one of the characters of G of degree $(p-1)/2$ and let M be the $K * (G \rtimes \Gamma)$-module affording $\widetilde{\chi}$, which is of degree $(p-1)^2/2$. It is well known that there exists only one isomorphism class of full $\mathbb{Z}_K G$-lattices in M, hence every full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice in M is uniserial and there are exactly $p-1$ non isomorphic full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in M.

6.3 Centering algorithm

We make the same assumptions mentioned at the beginning of the preceding section. Proposition (6.2.2) relies heavily on the knowledge of $\mathcal{Z}_{\mathbb{Z}_K G}(M)$ and on $\mathcal{A}(K)$. There are theoretical methods to compute $\mathcal{Z}_{\mathbb{Z}_K G}(M)$ [Ple83] but it is a hard problem in general.

As a fallback we need algorithmic methods. Those are provided by the centering algorithm of Plesken and Nebe [PP87]. To apply this algorithm, the following proposition is crucial.

Proposition 6.3.1. *Let $\mathfrak{D}$ be the discriminant of K und Λ a $\mathbb{Z}$-order in $K * (G \rtimes \Gamma)$, which contains $\mathbb{Z}_K * (G \rtimes \Gamma)$. Then we have:*

$$\mathbb{Z}_K * (G \rtimes \Gamma) \subset \Lambda \subset (|G||\Gamma|\mathfrak{D})^{-1}\mathbb{Z}_K * (G \rtimes \Gamma)$$

Proof. Define $E := G \rtimes \Gamma$ and let $\mathrm{Tr}, \mathrm{Tr}_K$ be the regular trace of $K * E$ and the trace of K, respectively. Choose a $\mathbb{Q}$-basis $(y_i)_{1\leq i\leq r}$ of K and let $(y_i^*)_{1\leq i\leq r}$ be the dual basis. Check that

$$\mathrm{Tr}(y_i g) = |E| \,\mathrm{Tr}_K(y_i)\delta_{g,1}$$

for all $1 \leq i \leq r$ and $g \in E$. Let $\gamma = \sum_{i=1}^r \sum_{g\in E} \alpha_{g,i} y_i g \in \Lambda$ and use $\mathfrak{D}y_i^* \in \mathbb{Z}_K$ to see:

$$\mathrm{Tr}(\gamma \underbrace{\mathfrak{D}\widetilde{g}^{-1}y_j^*}_{\in \mathbb{Z}_K * E}) = \sum \alpha_{g,i}\mathfrak{D}\,\mathrm{Tr}(y_i g\widetilde{g}^{-1}y_j^*) = \alpha_{\widetilde{g},j}\mathfrak{D}|E| \in \mathbb{Z}$$

for all $1 \leq j \leq r$ and $\widetilde{g} \in E$. Hence $\alpha_{\widetilde{g},j} \in (\mathfrak{D}|E|)^{-1}\mathbb{Z}$ and the claim follows. □

Note that the second point of remark (6.2.1) follows directly from this proposition.

We will sketch the centering algorithm in the absolutely irreducible case. The key observations, which follow directly from proposition (6.3.1), are given in the next proposition.

Proposition 6.3.2. *Let M be an absolutely irreducible $K*(G\rtimes\Gamma)$-module and L a full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice in M.*

1. *For any prime $p \in \mathbb{Z}$ with $p \nmid \mathfrak{D}|G||\Gamma|$ the $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Z}_K * (G \rtimes \Gamma)$-module L/pL is simple.*

2. *Representatives for the isomorphism classes of $\mathcal{Z}(M)$ are $\mathcal{V}(M) := \{L' \leq L \mid L' \nleq pL$ for all primes $p\}$*

The algorithm can be described as follows.

Algorithm 6.3.3. Let $K/\mathbb{Q}$ a finite Galois extension with group Γ, G a finite subgroup of $\mathrm{GL}_n(K)$ and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. Denote by $\mathfrak{D}$ the discriminant of K. Given an $K * (G \rtimes \Gamma)$ module M and $L \in \mathcal{Z}(M)$. The following steps construct the set $\mathcal{V}(M) := \{L' \leq L \mid L' \nleq pL$ for all primes $p\}$:

1. Compute all primes $p \in \mathbb{Z}$ such that $p \mid \mathfrak{D}|G||\Gamma|$ and L/pL is not a simple $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Z}_K * (G \rtimes \Gamma)$-module.

2. For those primes p compute the irreducible constituents of L/pL.

3. Starting with $N = L$, construct epimorphisms $N \to S$ for all relevant, simple $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Z}_K * (G \rtimes \Gamma)$-modules S.

4. If necessary, add the kernels to $\mathcal{V}(M)$ and start over with those.

This algorithm is in principle not limited to the absolutely irreducible situation. There exists a fast implementation of it in MAGMA [BCP97] due to Kirschmer.

6.4 Forms and fixed lattices

Let $K/\mathbb{Q}$ a finite Galois extension with group Γ and G a finite subgroup of $\mathrm{GL}_n(K)$ which is defined over $\mathbb{Q}$. We want to apply the results of the previous sections to construct nice $\mathbb{Q}$-forms of G, i.e. representations with fundamental invariants having small integer coefficients. Let $^- : \Gamma \to \mathrm{Aut}(G)$ be the embedding from the natural action of Γ on G and recall that $(K/\mathbb{Q}, ^-)$-representations are constructed by taking a $\mathbb{Q}$-basis of the Γ-fixed points of a $K * (G \rtimes \Gamma)$-module M. Hence, it makes sense to use a $\mathbb{Z}$-basis of the Γ-fixed lattice of a $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice in M. Before we describe the exact procedure, we have to fix some notation.

Assume that K is either a totally real field or has a central canonical conjugation and let $\Delta : K * (G \rtimes \Gamma) \to \mathbb{Q}^{n\times n}$ be a $\mathbb{Q}$-linear representation and $M := \mathbb{Q}^{n\times 1}$ the corresponding $K * (G \rtimes \Gamma)$-module. Proposition (6.1.2) implies that

$$\begin{aligned}\mathcal{F}_\Delta(K * (G \rtimes \Gamma)) =\{&\Phi \in \mathbb{Q}^{n\times n} \mid \Phi^{tr} = \Phi,\ \Delta(\iota_\sigma(x)) = \Phi^{-1}\Delta(x)^{tr}\Phi \\ &\text{for all } x \in K * (G \rtimes \Gamma)\}\end{aligned}$$

and

$$\mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma)) = \{\Phi \in \mathcal{F}_\Delta(K * (G \rtimes \Gamma)) \mid \Phi \text{ positive definite}\}$$

are non empty. For a full $\mathbb{Z}_K*(G\rtimes\Gamma)$-lattice L in M and $\Phi \in \mathcal{F}_{\Delta,>0}(K*(G\rtimes\Gamma))$ call

$$L^{\#(\Phi)} := \{x \in \mathbb{Q}^{n\times 1} \mid x^{tr}\Phi y \in \mathbb{Z} \text{ for all } y \in L\} \in \mathcal{Z}(M)$$

the *dual lattice* of L with respect to Φ. The form Φ is *integral* on L if $L \subseteq L^{\#(\Phi)}$ and *primitive* on L, if $L \subseteq L^{\#(\Phi)}$ and $pL \nsubseteq L^{\#(\Phi)}$ for all primes p. If Φ is integral on L, define the determinant $\det(L, \Phi)$ by $|L^{\#(\Phi)}/L|$. Note that if M is absolutely irreducible, then for every $L \in \mathcal{Z}(M)$ there is a unique $\Phi \in \mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$ which is primitive on L.

Remark 6.4.1. The canonical radicalizer-idealizer process [BZ85] guarantees the existence of a lattice $L \in \mathcal{Z}(M)$ and a $\Phi \in \mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$ such that Φ is primitive on L and $L/L^{\#(\Phi)}$ is of square-free exponent. We call such a pair (L, Φ) normalized.

There are numerous arithmetic and geometric invariants attached to a normalized pair (L, Φ). For example one can look for a minimal determinant, a large minimal norm, a high number of vectors of minimal norm and so on, cf. [CS99]. It often turns out that normalized pairs (L, Φ) with nice arithmetic and geometric properties induce nice representations $\mathbb{Z}_K * (G \rtimes \Gamma) \to \mathbb{Z}^{n\times n}$ using a reduced lattice basis. For example one could use LLL [LLL82] reduced bases or various refinements thereof.

It turns out that the result of the following steps often is a numerically nice $(K/\mathbb{Q}, ^-)$-representation of G.

Procedure 6.4.2. Let $K/\mathbb{Q}$ a finite Galois extension with group Γ, G a finite subgroup of $\mathrm{GL}_n(K)$ and $^- : \Gamma \to \mathrm{Aut}(G)$ an embedding. Construct the skew group ring $K * (G \rtimes \Gamma)$ and let M be a $K * (G \rtimes \Gamma)$-module. To construct nice $(K/\mathbb{Q}, ^-)$-representations of G, do the following:

1. Choose pair $(L, \Phi) \in \mathcal{Z}(M) \times \mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$, which is normalized and has nice arithmetic and geometric properties.
2. Define the symmetric positive definite bilinear form
$$\Phi_{L^\Gamma} : L^\Gamma \times L^\Gamma \to \mathbb{Z} \;:\; (v, w) \mapsto v^{tr}\Phi w$$
on L^Γ and after rescaling choose a reduced $\mathbb{Z}$-basis of L^Γ with respect to this form.
3. Construct the $(K/\mathbb{Q}, ^-)$-representation of G using this basis.

Since $L^\Gamma \otimes \mathbb{Z}_K$ is mostly not a $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice, the representation produced by the last procedure often involves certain denominators. Those denominators are described next proposition.

Proposition 6.4.3. *Let $\Delta : G \to \mathrm{GL}_n(K)$ be a $(K/\mathbb{Q}, ^-)$-representation obtained from a $\mathbb{Z}$-basis of the fixed point lattice L^Γ of a full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice in a $K * (G \rtimes \Gamma)$-module M. Then the denominators of the matrix entries of $\Delta(g)$ divide the discriminant of K for every $g \in G$.*

Remark 6.4.4. In the next chapter the famous representations of $\mathrm{PSL}_2(p)$ for $p \in \{5, 7, 11\}$ constructed by Klein in [Kle93], [Kle99], [Kle79] are obtained using the procedure (6.4.2). This explains the denominators of those representations.

To prove the proposition we need to study the fixed lattice L^Γ for a $\mathbb{Z}_K*(G \rtimes \Gamma)$-lattice in M. More generally, we have to understand L as as a $\mathbb{Z}_K*\Gamma$-lattice.

Let R be a Dedekind domain with quotient field $\mathbb{Q}$ and S its integral closure in K. The following general results can be found in [Rei75, Chapter 40].

Theorem 6.4.5 (Auslander-Goldman, Rim)**.** *The order $S * \Gamma$ is a maximal R-order if and only if S/R is unramified.*

Theorem 6.4.6 (Rosen)**.** *The order $S * \Gamma$ is a hereditary R-order if and only if S/R is tamely ramified.*

The next proposition computes the primes p at which $L_{(p)}$ is $(L^\Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_K) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$.

Proposition 6.4.7. *Let $\mathfrak{D}$ be the discriminant of K, M be a $K * (G \rtimes \Gamma)$-module, $L \in \mathcal{Z}(M)$ and $p \in \mathbb{Z}$ a prime such that $p \nmid \mathfrak{D}$. Then $L \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} = (L^\Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_K) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$*

Proof. Since $p \nmid \mathfrak{D}$, the skew group ring $\Lambda := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbb{Z}_K * \Gamma$ is a maximal $\mathbb{Z}_{(p)}$-order by the theorem of AUSLANDER-GOLDMAN, RIM. Two Λ lattices are isomorphic if and only if they have the same $\mathbb{Z}_{(p)}$-rank [Rei75, Theorem 18.7]. This rank equals the $\mathbb{Q}$-dimension of the scalar extension by $\mathbb{Q}$. Use the SPEISER-lemma to see that $L \otimes_{\mathbb{Z}} \mathbb{Q}$ and $(L^\Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_K) \otimes_{\mathbb{Z}} \mathbb{Q}$ have the same $\mathbb{Q}$-dimension. This proves the proposition. □

As a corollary one finds the prime divisors of the index of $L^\Gamma \otimes_Z \mathbb{Z}_K$ in L.

Corollary 6.4.8. *The prime divisors of $[L : (L^\Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_K)]$ divide the discriminant $\mathfrak{D}$ of K.*

From this corollary one easily obtains the proposition on the denominators.

Chapter 7

Examples

In this chapter we apply the arithmetic techniques of the last chapter to construct and study nice $K/\mathbb{Q}$-forms for various finite matrix groups G and fields K with Galois group Γ. This will be done using the procedure (6.4.2).

In the course of this chapter algorithmic methods such as the centering algorithm (6.3.3) or algorithmic group theory are used freely and are often not mentioned separately.

Let $p \equiv -1 \mod 4$ and $K = \mathbb{Q}(\zeta_p)$ the p-th cyclotomic field with Galois group Γ. In the first section a general hermitian construction of $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices, where G is the hermitian automorphism group of a special hermitian $\mathbb{Q}(\sqrt{-p})$-lattice, is developed. Using this construction, one finds $\mathbb{Z}_K * (\mathrm{PSL}_2(p) \rtimes \Gamma)$-lattices of rank $(p-1)^2/2$ which turn out to be modular of level p in the sense of [Que95]. Taking a reduced $\mathbb{Z}$-basis of the fixed lattice under the Galois group Γ, one obtains a representation of $\mathrm{PSL}_2(p)$ in degree $(p-1)/2$, which is absolutely irreducible as a K-linear representation and defined over $\mathbb{Q}$. Klein's famous representations of $\mathrm{PSL}_2(7)$ and $\mathrm{PSL}_2(11)$ in degree 3 and 5 respectively, appear in this arithmetic way.

The group $\mathrm{PSL}_2(7)$ in Klein's representation, which realizes $\mathrm{PSL}_2(7)$ as a subgroup of $\mathrm{GL}_3(\mathbb{Q}(\zeta_7))$, turns out to be particularly interesting. Viewed as a projective curve, the invariant of smallest degree is the famous Klein quartic. The Mordell-Weil-lattice related to this curve [Elk99, 2.3] is the Craig-lattice $\mathbb{A}_6^{(2)}$ which admits a hermitian $\mathbb{Z}[\alpha]$ (where $\alpha^2 + \alpha + 2 = 0$) structure. Computing a $\mathbb{Z}[\zeta_7] * (\mathrm{PSL}_2(7) \rtimes \mathrm{C}_6)$-structure on the hermitian tensor product of this lattice with itself and taking a reduced $\mathbb{Z}$-basis of the fixed lattice under the Galois group C_6 brings back Klein's representation.

Using the hermitian construction of the 72-dimensional extremal unimodular lattice Λ_{72} discovered recently by Nebe [Neb] turns this lattice into a $\mathbb{Z}[\zeta_7] * (\mathrm{SL}_2(25) \rtimes \Gamma)$-lattice, where Γ is the Galois group of $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. After rescaling, the lattices corresponding to fixed points under the subgroups of Γ turn out to be unimodular themselves. Hence unimodular lattices of rank $12, 24$ and 36 are attached to Λ_{72}.

Further examples include the lattice $\mathrm{E}_8 \perp \mathrm{E}_8$, from which Maschke's 4-dimensional representation of the complex reflection group G_{31} can be reconstructed [Mas89], and the Leech lattice, from which it is possible to obtain

KLEIN'S 4-dimensional representation of $2.\mathrm{A}_7$ [Kle87], the double cover of the alternating group.

It often turns out that using cyclotomic fields K to construct $(K/\mathbb{Q},\,^-)$-representations gives the numerically best invariants.

7.1 A hermitian construction

Let $p \equiv -1 \mod 4$, $K = \mathbb{Q}(\zeta_p)$, $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$, F the subfield $\mathbb{Q}(\sqrt{-p})$ of K, σ the canonical complex conjugation of K, and (L,h) a hermitian $\mathbb{Z}_F$-lattice with respect to σ. Denote by G its hermitian automorphism group. In this section we show that under some conditions on G the hermitian tensor product of (L,h) with a CRAIG lattice [CS99, Chapter 8, 7.3] can be turned into a $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice. Specifically, we construct such lattices for $G = \mathrm{PSL}_2(p)$.

We have to introduce some notation. Let V be a F-vectorspace of dimension n endowed with a positive definite hermitian form h with respect to σ. A hermitian lattice is the tuple (P,h) where P is a full $\mathbb{Z}_F$-sublattice in V. The hermitian dual of P defined as

$$P_h^* = \{x \in V \mid h(x,P) \subset \mathbb{Z}_F\}$$

and the hermitian automorphism group is

$$\mathrm{Aut}((P,h)) := \{g \in \mathrm{GL}(V) \mid gP = P \text{ and } h(gx,gy) = h(x,y) \text{ for all } x,y \in P\}$$

From every n-dimensional hermitian $\mathbb{Z}_F$ lattice one obtains a $2n$-dimensional $\mathbb{Z}$-lattice $\mathrm{R}(P,h) := (P, \mathrm{Tr}_{F/\mathbb{Q}} \circ h)$ by restricting scalars. The dual lattice of $\mathrm{R}(P,h)$ is the product of the hermitian dual P_h^* with the different of F i.e. $\mathrm{R}(P,h)^{\#} = 1/(\sqrt{-p})P_h^*$.

Remark 7.1.1. Choose $i \in \{0,...,p-2\}$ and let (P_1,h_1) be the hermitian $\mathbb{Z}_F$-lattice

$$((1-\zeta_p)^i\mathbb{Z}_K, (x,y) \mapsto \mathrm{Tr}_{K/F}(\overline{x}y))$$

for $0 \le i \le p-2$. This is a CRAIG lattice viewed as a hermitian $\mathbb{Z}_F$-lattice. The hermitian automorphism group contains $\mathrm{C}_p \rtimes \mathrm{C}_{(p-1)/2}$, which can be identified with $\langle\zeta_p\rangle \rtimes \mathrm{Gal}(K/F)$.

Let (P_2,h_2) be a hermitian $\mathbb{Z}_F$-lattice and G its hermitian automorphism group. Assume that (P_2,h_2) has the following properties:

1. It is isometric to its GALOIS conjugate lattice.
2. Using the isometry of (1) turns $\mathrm{Gal}(F/\mathbb{Q})$ into a subgroup of the $\mathbb{Z}$-automorphism group of the scalar restriction $\mathrm{R}(P_2,h_2)$. Inside this group the extension of G with $\mathrm{Gal}(F/\mathbb{Q})$ is split.
3. The group $G \rtimes \mathrm{Gal}(F/\mathbb{Q}) - G$ contains an element of order $p-1$.

Define $(\mathcal{L},h) := (P_1 \otimes_{\mathbb{Z}_F} P_2, h_1 \otimes h_2)$ and note that its hermitian automorphism group contains $\mathrm{C}_p \rtimes \mathrm{C}_{(p-1)/2} \times G$. It is easy to see that the CRAIG lattice (P_1,h_1) is isometric to its GALOIS conjugate. Use this fact and the property

(2) of (P_2, h_2) to see that the $\mathbb{Z}$-automorphism group of $\mathrm{R}(\mathcal{L}, h)$ contains the absolutely irreducible matrix group $(\mathrm{C}_p \rtimes \mathrm{C}_{(p-1)/2} \times G) \rtimes \mathrm{C}_2$. Since $p \equiv -1 \mod 4$, we can write this group as $(\mathrm{C}_p \times G) \rtimes \mathrm{C}_{p-1}$, and using an element with property (3), we can assume that $\mathrm{C}_{p-1} \to \mathrm{Aut}(G)$ is injective.

Identifying C_p with $\langle \zeta_p \rangle$ and C_{p-1} with Γ turns $\mathrm{R}(\mathcal{L}, h)$ into a normalized $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice.

Note that choosing a different element with property (3) may result in a different $\mathbb{Z}_K * (G \rtimes \Gamma)$ structure with respect to the classification theorem (2.4.1).

To illustrate this remark, we use it to construct nice $\mathbb{Z}[\zeta_p] * (\mathrm{PSL}_2(p) \rtimes \Gamma)$-lattices.

Example 7.1.2. Let $p \equiv -1 \mod 4$ and $F = \mathbb{Q}(\sqrt{-p})$ and $\Gamma = \mathrm{Gal}(F/\mathbb{Q})$. By [NP95, Theorem V.8] there exists a hermitian unimodular $\mathbb{Z}_F$-lattice (P, h) of rank $(p-1)/2$ with hermitian automorphism group $\mathrm{PSL}_2(p)$. This lattice is in fact a Craig lattice viewed as a hermitian $\mathbb{Z}_F$-lattice as in remark (7.1.1). The automorphism group of the scalar restricted lattice $\mathrm{R}(P, h)$ is $\mathrm{PGL}_2(p)$. Use the ATLAS [CCN$^+$85] to see that the construction of remark (7.1.1) is applicable for $(P_1, h_1) = (P_2, h_2) = (P, h)$.

This turns the scalar restricted lattice $\mathrm{R}((P \otimes P, h \otimes h))$ into a $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice. Since $(P \otimes P, h \otimes h)$ is hermitian unimodular and it follows from algebraic number theory, that $\mathrm{R}((P \otimes P, h \otimes h))$ is modular of level p in the sense of [Que95].

Specifically this construction applies for $p \in \{7, 11\}$ and we will see that Klein's famous representations of the groups $\mathrm{PSL}_2(p)$ are obtained from a reduced $\mathbb{Z}$-basis of the fixed lattice under the Γ-action.

7.2 $\mathrm{PSL}_2(p)$

We start with a general remark on the groups $\mathrm{PSL}_2(p)$ and the irreducible characters of degree $(p+1)/2$ and $(p-1)/2$.

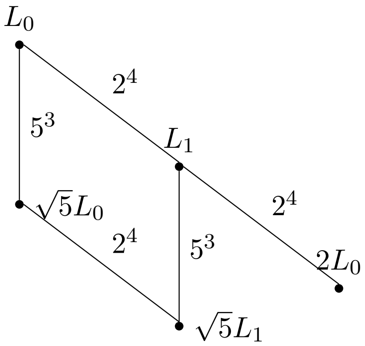
Remark 7.2.1. Let p be an odd prime, $G = \mathrm{PSL}_2(p)$, χ be an irreducible character of degree $(p+1)/2$ or $(p-1)/2$ respectively, K the character field of χ and $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$ with generator σ. The automorphism group of G is $\mathrm{PGL}_2(p)$, which is a split extension of $\mathrm{PSL}_2(p)$ by $\mathrm{C}_2 = \langle \varphi \rangle$. Let $^- : \Gamma \to \mathrm{Aut}(G)$ given by $\sigma \to \varphi$ and note that σ exchanges the conjugacy classes of elements of order p in G. Since χ has irrationalities on those classes, Γ acts on the character field as Galois automorphisms. The character $\widetilde{\chi}$ of $K * (G \rtimes \Gamma)$ is of degree $p-1$ respectively $p+1$, has rational values and Schur index 1 by (4.4.3). Let M be the corresponding $K * (G \rtimes \Gamma)$-module and view M as a KG-module.

It is well known that if $p \equiv -1 \mod 4$, there exists, up to isomorphism, a unique full $\mathbb{Z}_K G$-lattice L in M [NP95, Chapter V]. It follows from proposition (6.2.2) that L and $\sqrt{-p}L$ are representatives of the isomorphism classes of full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in M.

7.2.1 $\mathrm{PSL}_2(5)$

Let $p = 5$, $G = \mathrm{PSL}_2(5)$, K, Γ and $^- : \Gamma \to \mathrm{Aut}(G)$ as in remark (7.2.1). There are four non isomorphic $\mathbb{Z}_K * (\mathrm{PSL}_2(5) \rtimes \Gamma)$-lattices in the 6-dimensional $K * (\mathrm{PSL}_2(5) \rtimes \Gamma)$-module M. It should be noted the the $\mathbb{Z}\,\mathrm{PGL}_2(5)$-lattice $M_{6,2}$ of [NP95] is not a $\mathbb{Z}_K * (\mathrm{PSL}_2(5) \rtimes \Gamma)$-lattice.

Let L_0 be a full $\mathbb{Z}_K * (\mathrm{PSL}_2(5) \rtimes \Gamma)$-lattice in M. The following Hasse diagram illustrates the situation:



One obtains following table.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	$2^2 5^3$	4	$2 \cdot 5$	2
$\sqrt{5}L_0$	$2^2 5^3$	4	$2 \cdot 5^2$	4
L_1	$2^4 5^3$	5	$2^2 5$	3
$\sqrt{5}L_1$	$2^4 5^3$	5	$2^2 5^2$	3

The fixed lattice $(L_0^\Gamma, \Phi_{L_0^\Gamma})$ is a 3-dimensional Bravais-lattice (rhombohedral of even type). Choosing a reduced basis of the fixed lattice, we can realize G as a finite matrix group defined over $\mathbb{Q}$. The group is generated by:

$$\left\langle \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix}, \frac{1}{\sqrt{5}} \begin{pmatrix} 1+2\alpha & -\alpha & -2 \\ 1+2\alpha & -2-\alpha & 1 \\ 0 & -1 & -1 \end{pmatrix} \right\rangle$$

with $\alpha = (-1+\sqrt{5})/2$. Those matrices are of order 2 and 5, respectively. The Gram matrix of $(L_0^\Gamma, \Phi_{L_0^\Gamma})$ is

$$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 4 \end{pmatrix}$$

and represents the invariant of lowest degree of G. It has determinant 10. The subgroup of $\mathbb{Q}$-rational points is isomorphic to S_3 and lies in $\mathrm{GL}_3(\mathbb{Z})$.

7.2.2 Klein's representation

Let $G = \mathrm{SL}_2(5)$, $K = \mathbb{Q}(\zeta_5)$ and use the notation of example (5.4.5) and the ATLAS. Let $\chi := \chi_2$ be one of the irreducible G characters of degree 3. The character $\widetilde{\chi}$ of $K * (G \rtimes \Gamma)$ has degree 12 and Schur index 1 over $\mathbb{Q}$. Let M be a $K * (G \rtimes \Gamma)$-module affording this character. There are two non isomorphic full $\mathbb{Z}_K G$-lattices in M and the HASSE diagram looks like (6.2.5).

One computes the following table of normalized $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices (L_i, Φ_i) in M.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	$2^4 \cdot 5^3$	4	2	1
$(1-\zeta_5)L_0$	$2^4 \cdot 5^9$	8	$2 \cdot 5^2$	2
$(1-\zeta_5)^2 L_0$	$2^4 \cdot 5^3$	4	$2 \cdot 5$	2
$(1-\zeta_5)^3 L_0$	$2^4 \cdot 5^9$	8	2	1
L_1	$2^8 \cdot 5^9$	10	$2^2 \cdot 5^2$	4
$(1-\zeta_5)L_1$	$2^8 \cdot 5^3$	4	$2^2 \cdot 5$	1
$(1-\zeta_5)^2 L_1$	$2^8 \cdot 5^9$	10	2^2	1
$(1-\zeta_5)^3 L_2$	$2^8 \cdot 5^3$	4	2^2	1

The lattice (L_0, Φ_0) corresponds to an irreducible maximal finite subgroup of $\mathrm{GL}_{12}(\mathbb{Q})$ isomorphic to $(\mathrm{C}_2 \times \mathrm{D}_{10} \times \mathrm{A}_5) \rtimes \mathrm{C}_2$ [NP95].

One can choose a reduced $\mathbb{Z}$-basis of L_0^Γ such that the GRAM matrix of $(L_0^\Gamma, \Phi_{L_0^\Gamma})$ is $\mathrm{diag}(1,1,2)$. This provides a $(K/\mathbb{Q}, ^-)$-representation

$$\Delta_{\mathbb{Q}} : \mathrm{PSL}_2(5) \to \mathrm{GL}_3(K),$$

which differs from KLEIN'S representation [Kle93] by an element $\mathrm{O}_3(\Phi_{L_7^\Gamma}, \mathbb{Z})$.

In KLEIN'S representation the group G is generated by

$$\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_5 & 0 \\ 0 & 0 & \zeta_5^{-1} \end{pmatrix}, \frac{1}{\sqrt{5}} \begin{pmatrix} -1 & 1+\zeta_5+\zeta_5^2+\zeta_5^3 & -\zeta_5 \\ -2 & -\zeta_5-\zeta_5^2 & -1-\zeta_5^2 \\ -2 & -1-\zeta_5^3 & 1+\zeta_5+\zeta_5^2 \end{pmatrix} \rangle$$

and the subgroup of $\mathbb{Q}$-rational points is C_2. The invariant of smallest degree is:

$$i_2 := x_1^2 + x_2 x_3$$

This invariant, although it has a very simple structure, corresponds to an indefinite quadratic form over $\mathbb{Q}$, whereas the representation of the last section over fixes a positive definite form.

7.2.3 $\mathrm{PSL}_2(7)$

Let $p = 7$, $K = \mathbb{Q}(\sqrt{-7})$, use the notation of remark (7.2.1) and recall that M is an 18-dimensional absolutely irreducible $K * (\mathrm{PSL}_2(7) \rtimes \Gamma)$-module. Viewing M as a 3-dimensional $K\,\mathrm{PSL}_2(7)$-module every $\mathbb{Z}_K\,\mathrm{PSL}_2(p)$-lattice in M is isomorphic to the BARNES lattice. Let $\alpha := (-1+\sqrt{-7})/2$ and $\beta := (-1-\sqrt{-7})/2$, then as a sublattice of $\mathbb{Z}_K^3$ it is spanned by

$$\langle (1,1,\alpha), (0,\beta,\beta), (0,0,2) \rangle$$

with the hermitian form h:

$$h((a_1,a_2,a_3),(b_1,b_2,b_3)) := \frac{1}{2}\sum_{i=1}^{3} a_i \sigma(b_i)$$

cf. [Neb]. The scalar restriction of this lattice is the CRAIG lattice $\mathbb{A}_6^{(2)}$. Hence, representatives of the isomorphism classes of $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices are $\mathbb{A}_6^{(2)}$ and its dual. One computes the following table.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	7^3	4	7	2
L_1	7^3	4	7^2	4

To construct a $(K/\mathbb{Q}, ^-)$-representation $\Delta : \mathrm{PSL}_2(7) \to \mathrm{GL}_3(K)$ one should use a reduced $\mathbb{Z}$-basis of $(L_0^\Gamma, \Phi_{L_0^\Gamma})$. Let $\alpha = (-1+\sqrt{-7})/2$, the following matrix group is defined over $\mathbb{Q}$, isomorphic to $\mathrm{PSL}_2(7)$ and constructed using a reduced basis of the fixed lattice L_0^Γ.

$$\langle \frac{1}{\sqrt{-7}} \begin{pmatrix} -1+2\alpha & 1 & -1-\alpha \\ 0 & \alpha & -3+\alpha \\ 0 & 1+\alpha & -\alpha \end{pmatrix}, \frac{1}{\sqrt{-7}} \begin{pmatrix} -1+\alpha & 2-\alpha & -3+\alpha \\ 1+\alpha & -1 & -3 \\ 1 & 1-\alpha & -2 \end{pmatrix} \rangle$$

These matrices are of order 2 and 7, respectively. The GRAM matrix of (L_0^Γ, Φ) is

$$\begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & 0 \\ -1 & 0 & 3 \end{pmatrix}$$

and the subgroup of $\mathbb{Q}$-rational points is isomorphic to S_3 and lies in $\mathrm{GL}_3(\mathbb{Z})$. The natural character decomposes into the irreducible character of degree 2 and the sign character, but the natural S_3-lattice $\mathbb{Z}^{3\times 1}$ does not decompose accordingly.

The invariant of smallest degree is:

$$\begin{aligned} i_4 := & x_1^4 - 2x_1^3x_2 - 2x_1^3x_3 + 3x_1^2x_2^2 + 9x_1^2x_2x_3 - 3x_1^2x_3^2 - 2x_1x_2^3 \\ & - 9x_1x_2^2x_3 - 3x_1x_2x_3^2 + 4x_1x_3^3 + x_2^4 + 3x_2^2x_3^2 - 3x_3^4 \end{aligned}$$

The representation and the invariant should be compared to the representation obtained by ELKIES in [Elk99, 1.3]. His representation is also defined over $\mathbb{Q}$ and realized over $\mathbb{Q}(\sqrt{-7})$. Although the invariant seems to have a simpler structure, the generating matrices involve 7 as denominators.

7.2.4 KLEIN'S representation

We construct another representation of $G = \mathrm{PSL}_2(7)$ in degree 3. Let $K = \mathbb{Q}(\zeta_7)$, $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$ and let (L, h) be the 7-modular 18-dimensional $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice of example (7.1.2). More precisely, this lattice is the scalar restriction of the hermitian tensor product of the BARNES lattice with itself.

Note that there is only one conjugacy class of elements of order 6 in $\mathrm{Aut}(G) - G$, hence all the possible $\mathbb{Z}_K*(G\rtimes\Gamma)$-structures lead to equivalent matrix groups defined over $\mathbb{Q}$ in the sense of (2.4.1).

It is easy to see that the $K*(G\rtimes\Gamma)$-module $\mathbb{Q}\otimes M$ is absolutely irreducible and of dimension 18. Denote by Δ the corresponding $\mathbb{Q}$-linear representation of $K * G$ and $\widetilde{\chi}$ its character, then χ is one of the GALOIS conjugate characters of degree 3 of G.

It is well known that all $\mathbb{Z}_K G$-sublattices of L are isomorphic. Use example (6.2.4) and proposition (6.2.2) to see that the isomorphism classes of $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in L are:

$$L > (\zeta_7 - 1)L > (\zeta_7 - 1)^2 L > (\zeta_7 - 1)^3 L > (\zeta_7 - 1)^4 L > (\zeta_7 - 1)^5 L$$

Define $L_i = (\zeta_7 - 1)^i L$ for $0 \le i \le 5$. Since L is absolutely irreducible there exists a unique primitive form $\Phi_{L_i} \in \mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$ for every lattice L_i.

Note that one can view every L_i as a $\mathbb{Z}G'$-lattice for the group $G' := (\mathrm{C}_7 \times \mathrm{SL}_2(7)) \rtimes \mathrm{C}_6$. The primitive forms Φ_{L_i} correspond to G' invariant symmetric positive definite bilinear forms.

One computes the following table.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	7^9	6	1	1
L_1	7^{15}	12	1	1
L_2	7^3	4	1	1
L_3	7^9	6	1	1
L_4	7^{15}	12	7^2	3
L_5	7^3	4	7	2

The automorphism group of (L_0, h_0) is an irreducible maximal finite subgroup of $\mathrm{GL}_{18}(\mathbb{Q})$ isomorphic to $(\mathrm{C}_2 \times \mathrm{PSL}_2(7) \times \mathrm{PSL}_2(7)) \rtimes \mathrm{C}_2 \times \mathrm{C}_2$ [NP95].

Let

$$\Phi_{L_0^\Gamma} : L_0^\Gamma \times L_0^\Gamma \to \mathbb{Z} \ : \ (v, w) \mapsto v^{tr} \Phi w$$

be the positive definite bilinear form on L^Γ induced by Φ_0. Choose a reduced $\mathbb{Z}$-basis of L^Γ such that after rescaling the GRAM matrix of $\Phi_{L_0^\Gamma}$ is the identity matrix in $\mathrm{GL}_3(\mathbb{Z})$. This basis provides a $(K/\mathbb{Q}, ^-)$-representation

$$\Delta_{\mathbb{Q}} : \mathrm{SL}_2(7) \to \mathrm{GL}_3(K),$$

which differs from KLEIN'S representation [Kle99] by an element of the orthogonal group $\mathrm{O}(3, \mathbb{Z}) \cong \mathrm{C}_2 \times \mathrm{S}_4$.

In KLEIN'S representation the group G is generated by

$$\langle \begin{pmatrix} \zeta_7 & 0 & 0 \\ 0 & \zeta_7^2 & 0 \\ 0 & 0 & \zeta_7^4 \end{pmatrix}, \frac{1}{\sqrt{-7}} \begin{pmatrix} \zeta_7^5 - \zeta_7^2 & \zeta_7^6 - \zeta_7 & \zeta_7^3 - \zeta_7^4 \\ \zeta_7^6 - \zeta_7 & \zeta_7^3 - \zeta_7^4 & \zeta_7^5 - \zeta_7^2 \\ \zeta_7^3 - \zeta_7^4 & \zeta_7^5 - \zeta_7^2 & \zeta_7^6 - \zeta_7 \end{pmatrix} \rangle$$

and the subgroup of $\mathbb{Q}$-rational points is C_2 and the invariant of smallest degree is:

$$i_4 := x_1 x_2^3 + x_2 x_3^3 + x_3 x_1^3$$

Viewed as a projective curve in $\mathbb{P}^2$ this is the famous KLEIN quartic. In comparison to the representation constructed in the previous chapter, the invariant of degree 4 has a pretty trinomial structure. It is an interesting fact that the MORDELL-WEIL-lattice related to KLEIN'S quartic [Elk99, 2.3] turns out to be $\mathbb{A}_6^{(2)}$, the lattice from which the representation of the previous section was constructed and from whose hermitian square KLEIN'S representation was obtained.

7.2.5 $\mathrm{PSL}_2(8)$

Let $G = \mathrm{PSL}_2(8)$ and K the totally real subfield of $\mathbb{Q}(\zeta_9)$. The automorphism group of G is a split extension of G by C_3 and there is a unique conjugacy class of elements of order 3 in $\mathrm{Aut}(G) - G$. Choose an isomorphism $^- : \Gamma \to \mathrm{C}_3 \leq \mathrm{Aut}(G)$ and let χ be an absolutely irreducible character of G of degree 7 with K as its character field. There are 3 such characters, all of which are GALOIS conjugate. The character $\widetilde{\chi}$ of $K*(G \rtimes \Gamma)$ has degree 21, character field $\mathbb{Q}$ and SCHUR index 1 over $\mathbb{Q}$. Let M be a $K*(G \rtimes \Gamma)$-module affording this character and Δ the corresponding representation. There are 24 non isomorphic full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in M and each has a unique primitive form $\Phi_L \in \mathcal{F}_{\Delta,>0}(K*(G \rtimes \Gamma))$. Restricting to the normalized lattices corresponding to maximal subgroups of $\mathrm{GL}_{21}(\mathbb{Q})$ one has the following table.

Lattice L	Name	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	$\mathrm{C}_2 \times \mathrm{Sp}_2(6)$	$2^6 3^7$	4	$2^2 3^8$	4
L_1	$\Lambda^2\mathrm{E}_7$	2^6	3	2^2	1

To construct a $(K/\mathbb{Q}, ^-)$-representation $\Delta : G \to \mathrm{GL}_3(K)$, one should use a reduced basis of $(L_1^\Gamma, \Phi_{L_1^\Gamma})$. Doing so gives a matrix group defined over $\mathbb{Q}$ and isomorphic to G. Due to the size, we do not print generating matrices. The denominators of the matrix entries all lie in the fractional ideal generated by $(3(\beta+1))^{-1}$ where β is a zero of $x^3 - 3x + 1$. Note that K is the splitting field of this polynomial.

The invariant of smallest degree is the symmetric positive definite quadratic form $(L_1^\Gamma, \Phi_{L_1^\Gamma})$ with GRAM matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 1 & -1 \\ 0 & 0 & 0 & 1 & 2 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 2 & -1 \\ 0 & 0 & 0 & -1 & -1 & -1 & 2 \end{pmatrix}$$

As in the previous examples one could extend K to $\mathbb{Q}(\zeta_9)$ and find a $(K/\mathbb{Q}, ^-)$-representation. One would expect the invariants to become simpler, but one would loose positive definiteness of the invariant of degree 2.

7.2.6 $\mathrm{PSL}_2(11)$

Let $G = \mathrm{PSL}_2(11)$ and $K = \mathbb{Q}(\zeta_{11})$ and note that there are two conjugacy classes of elements of order 10 in $\mathrm{Aut}(G) - G$. Composition with an inner automorphism of order 5 interchanges both classes. Hence, there are two different $\mathbb{Z}_K * (G \rtimes \Gamma)$-structures on the 50-dimensional 11-modular lattice (L, h) constructed in remark (7.1.2). Fix one such structure on (L, h) and denote by $M := L \otimes \mathbb{Q}$ the corresponding $K * (G \rtimes \Gamma)$-module. The set $\{(\zeta_{11} - 1)^i \mathbb{Z}_k \mid 1 \leq i \leq 9\}$ is a set of representatives of the equivalence classes of Γ-stable principal $\mathbb{Z}_K$-ideals by example (6.2.4). By proposition (6.2.2) the isomorphism classes in $\mathcal{Z}(M)$ are $\{(1 - \zeta_{11})^i L \mid 0 \leq i \leq 9\}$

Define $L_i = (\zeta_{11} - 1)^i L$ for $0 \leq i \leq 9$. There exists a unique, primitive form $\Phi_{L_i} \in \mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$ for every lattice L_i. One computes the following table, in which both structures are considered.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	11^{25}	10	$1, 11^4$	$1, 5$
L_1	11^{35}	22	$1, 11^4$	$1, 5$
L_2	11^{45}	30	$1, 11^4$	$1, 2$
L_3	11^5	6	$1, 11$	$1, 2$
L_4	11^{15}	10	$1, 11$	$1, 2$
L_5	11^{25}	10	$1, 11$	$1, 5$
L_6	11^{35}	22	$11^2, 11^3$	$3, 1$
L_7	11^{45}	30	$11^4, 1$	$5, 1$
L_8	11^5	6	$11, 1$	$2, 3$
L_9	11^{15}	10	$11^3, 11^2$	$5, 5$

Note that the two $\mathbb{Z}_K * (G \rtimes \Gamma)$-structures only differ with respect to the Γ-fixed lattices. For $i \in \{0, 5\}$ one can choose a reduced $\mathbb{Z}$-basis of L^Γ such that, after rescaling, the Gram matrix of $\Phi_{L_i^\Gamma}$ is the identity matrix in $\mathrm{GL}_4(\mathbb{Z})$. This basis provides a $(K/\mathbb{Q}, {}^-)$-representation

$$\Delta_\mathbb{Q} : \mathrm{PSL}_2(11) \to \mathrm{GL}_5(K)$$

and one of those differs from Klein's representation [Kle79] by an element of the orthogonal group $\mathrm{O}(5, \mathbb{Z})$.

In Klein's representation the group G is generated by

$$\langle \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \frac{1}{\sqrt{-11}} \begin{pmatrix} \zeta_{11}^{10} - \zeta_{11}^3 & \zeta_{11}^6 - \zeta_{11}^7 & 1 - \zeta_{11}^2 & -\zeta_{11}^8 + \zeta_{11}^5 & -\zeta_{11}^9 + \zeta_{11}^4 \\ \zeta_{11}^3 - \zeta_{11}^4 & -\zeta_{11}^5 + \zeta_{11}^2 & -\zeta_{11} + \zeta_{11}^6 & \zeta_{11}^{10} - \zeta_{11}^8 & -1 + \zeta_{11}^7 \\ \zeta_{11}^2 - \zeta_{11}^4 & 1 - \zeta_{11}^6 & \zeta_{11}^8 - \zeta_{11}^9 & \zeta_{11}^5 - \zeta_{11} & \zeta_{11}^{10} - \zeta_{11}^7 \\ -1 + \zeta_{11}^8 & \zeta_{11}^5 - \zeta_{11}^3 & \zeta_{11}^6 - \zeta_{11}^2 & \zeta_{11}^7 - \zeta_{11} & \zeta_{11}^9 - \zeta_{11}^{10} \\ -\zeta_{11}^2 + \zeta_{11}^8 & -\zeta_{11}^7 + \zeta_{11}^3 & -\zeta_{11}^9 + \zeta_{11} & \zeta_{11}^{10} - 1 & \zeta_{11}^6 - \zeta_{11}^4 \end{pmatrix} \rangle$$

where the first matrix has order 5 and the second order 3. The subgroup of $\mathbb{Q}$-rational points is C_5 and the invariant of smallest degree is:

$$i_3 := x_4^2 x_3 - x_5^2 x_1 - x_2^2 x_4 - x_3^2 x_5 - x_1^2 x_2,$$

which has a pretty trinomial structure.

Using the second structure one can choose a reduced $\mathbb{Z}$-basis of L_7^Γ such that, after rescaling, the Gram matrix of $\Phi_{L_7^\Gamma}$ is the identity matrix in $\mathrm{GL}_4(\mathbb{Z})$. This basis provides a $(K/\mathbb{Q}, {}^-)$-representation

$$\Delta_\mathbb{Q} : \mathrm{PSL}_2(11) \to \mathrm{GL}_5(K)$$

Due to the size of the entries we do not print the generating matrices. The appearing denominator is 11, which is worse than in Klein's representation. The invariant of smallest degree is

$$\begin{aligned} i_3 = {} & 10x_2x_3x_5 - 6x_2x_4x_5 + 2x_2x_5^2 - 6x_1^2x_2 - x_1^2x_3 + 2x_1^2x_4 + 2x_1x_2^2 - 2x_1^3 - 2x_2^3 - 2x_3^3 - \\ & 2x_4^3 + 2x_5^3 + 6x_2^2x_5 + 6x_2x_3x_4 - x_2x_3^2 - 6x_3^2x_4 - 2x_3^2x_5 + 2x_3x_4^2 + 10x_3x_4x_5 - 6x_3x_5^2 - \\ & x_2^2x_4 - x_1x_5^2 - 10x_1x_3x_4 - 6x_1x_3x_5 - 6x_1x_4^2 - 6x_1x_4x_5 + 6x_1x_2x_3 - 10x_1x_2x_4 + \\ & 10x_1x_2x_5 + x_4^2x_5 \end{aligned}$$

which seem also worse compared to the preceding invariant.

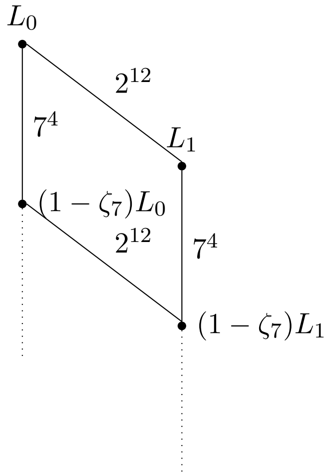
Similar to the examples of $\mathrm{PSL}_2(5)$ and $\mathrm{PSL}_2(7)$ one could construct a $(\mathbb{Q}(\sqrt{-11})/\mathbb{Q}, ^-)$-representation of G. We do not do this, because the resulting representation and the invariants would become too large to print.

7.3 $\mathrm{SL}_2(7)$

Let $G = \mathrm{SL}_2(7)$, $K = \mathbb{Q}(\zeta_7)$, $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$ and $F = \mathbb{Q}(\sqrt{-7})$. The objective is to realize G as subgroup of $\mathrm{GL}_4(K)$ which is defined over $\mathbb{Q}$. As seen before, we try to apply the construction of remark (7.1.1).

It is well known that up to isomorphism there exist two full $\mathbb{Z}_F\,\mathrm{SL}_2(7)$-lattices of rank 4 in each of the absolutely irreducible 4-dimensional $F\,\mathrm{SL}_2(7)$-modules. On both lattices there exists a (unique up to scalars) G-invariant hermitian form. Restricting scalars of those forms yields the root lattice D_8 and its dual. Let (P_1, h_1) be the Barnes lattice and (P_2, h_2) the hermitian G-invariant $\mathbb{Z}_F$-lattice of which the scalar restriction is D_8. One checks that the construction of remark (7.1.1) is applicable, hence one obtains a lattice $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice of dimension 24 with determinant 2^6. Denote by L_1 the $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice by applying (7.1.1) to the other G-invariant hermitian lattice. Let $M = \mathbb{Q} \otimes L_0$ be the $K * (G \rtimes \Gamma)$-module and Δ the corresponding representation.

By proposition (6.2.2) the isomorphism classes of full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in M are $L_{i,j} := (1-\zeta_7)^i L_j$ with $0 \le i \le 5$ and $1 \le j \le 2$. The Hasse diagram looks like



For each lattice there exists a unique, primitive form $\Phi_{L_{i,j}} \in \mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$. One computes the following table of normalized $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in M.

Lattice L	$\det(\Phi_L)$	$\min(\Phi_L)$	$\det(\Phi_{L^\Gamma})$	$\min(\Phi_{L^\Gamma})$
$L_{0,0}$	2^6	4	2	1
$L_{0,1}$	$2^6 \cdot 7^8$	6	$2 \cdot 7^2$	2
$L_{0,2}$	$2^6 \cdot 7^{16}$	12	2	1
$L_{0,3}$	2^6	4	2	1
$L_{0,4}$	$2^6 \cdot 7^8$	6	2	1
$L_{0,5}$	$2^6 \cdot 7^{16}$	12	$2 \cdot 7^2$	2
$L_{1,0}$	2^{18}	4	2^3	1
$L_{1,1}$	$2^{18} \cdot 7^8$	6	$2^3 \cdot 7^2$	1
$L_{1,2}$	$2^{18} \cdot 7^{16}$	14	2^3	1
$L_{1,3}$	2^{18}	4	2^3	1
$L_{1,4}$	$2^{18} \cdot 7^8$	6	2^3	1
$L_{1,5}$	$2^{18} \cdot 7^{16}$	14	$2^3 \cdot 7^2$	4

The lattices $(L_{0,0}, \Phi_{0,0})$ and $(L_{1,0}, \Phi_{1,0})$ correspond to the irreducible maximal finite subgroup of $\mathrm{GL}_{24}(\mathbb{Q})$ isomorphic to $(\mathrm{SL}_2(7) \times \mathrm{PSL}_2(7)) \rtimes \mathrm{C}_2$ [Neb96] and its dual.

One can choose a reduced $\mathbb{Z}$-basis of $L_{0,1}^\Gamma$ such that the GRAM matrix of $(L_{0,1}^\Gamma, \Phi_{L_{0,1}^\Gamma})$ is $\mathrm{diag}(2,1,1,1)$. This basis provides a $(K/\mathbb{Q}, {}^-)$-representation $\Delta_{\mathbb{Q}} : \mathrm{SL}_2(7) \to \mathrm{GL}_4(K)$ which differs from MASCHKE'S representation [Mas87] by an element $\mathrm{O}_4(\Phi_{L_{0,1}^\Gamma}, \mathbb{Z})$.

This realizes $\mathrm{SL}_2(7)$ as a subgroup of $\mathrm{GL}_4(K)$ which is defined over $\mathbb{Q}$ and generated by

$$\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \zeta_7 & 0 & 0 \\ 0 & 0 & \zeta_7^4 & 0 \\ 0 & 0 & 0 & \zeta_7 \end{pmatrix}, \frac{1}{\sqrt{-7}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & \zeta_7 + \zeta_7^6 & \zeta_7^2 + \zeta_7^5 & \zeta_7^3 + \zeta_7^4 \\ 2 & \zeta_7^2 + \zeta_7^5 & \zeta_7^3 + \zeta_7^4 & \zeta_7 + \zeta_7^6 \\ 2 & \zeta_7^3 + \zeta_7^4 & \zeta_7 + \zeta_7^6 & \zeta_7^2 + \zeta_7^5 \end{pmatrix} \rangle$$

The invariant of smallest degree is

$$i_4 := 2x_1^4 + 6x_1x_2x_3x_4 + x_2^3x_3 + x_3^3x_4 + x_4^3x_2$$

and in fact MASCHKE calculated fundamental invariants of this group [Mas87].

One can also use the hermitian $\mathbb{Z}_F$-structure on the D_8-lattice to realize $\mathrm{SL}_2(7)$ as a subgroup of $\mathrm{GL}_4(F)$ which is defined over $\mathbb{Q}$. Recall the hermitian G-invariant lattice (P_2, h_2) whose scalar restriction is D_8. The extension of the hermitian automorphism group of $\mathrm{Aut}((P_2, h_2))$ with the GALOIS group of $F/\mathbb{Q}$ is split inside $\mathrm{Aut}(\mathrm{D}_8)$. This turns D_8 into a $\mathbb{Z}_F * (\mathrm{SL}_2(7) \rtimes \mathrm{C}_2)$-lattice. One can choose a reduced $\mathbb{Z}$-basis of the Γ fixed lattice such that the GRAM matrix of is $\mathrm{diag}(1,1,1,2)$. Let $\alpha = (-1+\sqrt{-7})/2$, then the group is generated by

$$\langle \frac{1}{\sqrt{-7}} \begin{pmatrix} -2-\alpha & -1 & 0 & -2 \\ 1+\alpha & -\alpha-1 & 1 & -2 \\ 1 & 1+\alpha & \alpha & -2 \\ 0 & 1 & -\alpha-1 & -1 \end{pmatrix}, \frac{1}{\sqrt{-7}} \begin{pmatrix} 1+\alpha & -\alpha-1 & 1 & -2 \\ 0 & -1 & -\alpha & -2\alpha \\ -1 & -2 & \alpha & 0 \\ 1+\alpha & 0 & -1 & 1 \end{pmatrix} \rangle$$

where the first generator is of order 7 and the second of order 3. We compute the invariant of degree 4, which does not have such a pretty structure as in MASCHKE'S representation.

$$i_4 := 3x_1^2x_2^2 + 6x_1^3x_4 - 12x_1^2x_3x_4 - 3x_1x_2^2x_3 - 12x_1x_2^2x_4 - 3x_1x_2x_3^2 - 6x_1x_3^2x_4 - 6x_2^2x_3x_4 - 12x_2x_3^2x_4 - 6x_1^2x_2x_4 - 14x_4^4 - x_1^4 + 6x_3^3x_4 - 6x_1x_2x_3x_4 - 6x_1x_2^3 + 6x_2^3x_4 + 3x_2^2x_3^2 - 6x_2x_3^3 + 3x_1^2x_3^2 - 3x_1^2x_2x_3 - 6x_1^3x_3 - x_2^4 - x_3^4;$$

The subgroup of rational points is C_6 in either representation.

7.4 $\mathrm{SL}_2(13)$

Let $G = \mathrm{SL}_2(13)$, $K = \mathbb{Q}(\zeta_{13})$, χ an absolutely irreducible character of degree 6 of G and use the notation of example (5.4.5). Note that this fixes one of the possible 2 different $K * (G \rtimes \Gamma)$-structures in the sense of (2.4.1). The character $\widetilde{\chi}$ of $K * (G \rtimes \Gamma)$ has degree 72, rational values and SCHUR index 1 over $\mathbb{Q}$. Let M be a $K * (G \rtimes \Gamma)$-module affording this character. Viewing M as a $K\,\mathrm{SL}_2(13)$-module, there exists, up to isomorphism, a unique $\mathbb{Z}_K G$-lattice L in M. The isomorphism classes of full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices are $L_i := (1-\zeta_{13})^i L$ with $0 \le i \le 11$. One computes the following table of $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in M together with their unique primitive form in $\mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	13^{48}	≤ 26	13^4	7
L_1	13^{60}	≤ 52	13^4	7
L_2	1	≤ 6	1	1
L_3	13^{12}	≤ 8	13^2	3
L_4	13^{24}	≤ 12	13^2	3
L_5	13^{36}	≤ 12	13^4	3
L_6	13^{48}	≤ 26	13^4	3
L_7	13^{60}	≤ 52	1	1
L_8	1	≤ 6	1	1
L_9	13^{12}	≤ 8	1	1
L_{10}	13^{24}	≤ 12	13^2	2
L_{11}	13^{36}	≤ 12	13^2	2

Choosing a reduced $\mathbb{Z}$-basis of L_2^Γ such that the GRAM matrix of $(L_2^\Gamma, \Phi_{L_2^\Gamma})$ is the identity matrix, provides a $(K/\mathbb{Q}, {}^-)$-representation

$$\Delta_{\mathbb{Q}} : \mathrm{SL}_2(13) \to \mathrm{GL}_6(K)$$

with character χ. Due to its size we do not print the generating matrices. The denominators of those matrices all lie in the fractional ideal generated by

$(\sqrt{-13})^{-1}$ and the representation has the following invariant degree 4

$$\begin{aligned}
i_4 :=& 11x_1^3x_3 + 3x_1^3x_4 + 3x_1^2x_2^2 + 9x_1^2x_2x_5 + 3x_1^2x_3^2 - 9x_1^2x_3x_4 + 9x_1^2x_3x_6 - 3x_1^2x_4^2 + \\
& 6x_1^2x_4x_6 - 3x_1^2x_5^2 - 11x_1x_2^3 + 9x_1x_2^2x_5 - 9x_1x_2^2x_6 - 6x_1x_2x_5^2 - 27x_1x_2x_5x_6 - 9x_1x_3^2x_6 + \\
& 27x_1x_3x_4x_6 + 6x_1x_3x_6^2 + 9x_1x_4^2x_6 - 9x_1x_4x_6^2 - 3x_1x_5^3 + 9x_1x_5^2x_6 - 3x_2^3x_6 - 3x_2^2x_3^2 + \\
& 9x_2^2x_3x_4 + 3x_2^2x_4^2 + 6x_2^2x_5x_6 - 3x_2^2x_6^2 + 3x_2x_3^3 + 6x_2x_3^2x_4 - 9x_2x_3^2x_5 - 9x_2x_3x_4^2 + \\
& 27x_2x_3x_4x_5 + 11x_2x_4^3 + 9x_2x_4^2x_5 + 9x_2x_5^2x_6 - 9x_2x_5x_6^2 + 11x_3^3x_5 + 9x_3^2x_4x_5 + 3x_3^2x_5^2 - \\
& 3x_3^2x_6^2 + 6x_3x_4^2x_5 - 9x_3x_4x_5^2 + 9x_3x_4x_6^2 - 3x_3x_6^3 - 3x_4^3x_5 - 3x_4^2x_5^2 + 3x_4^2x_6^2 + \\
& 11x_4x_6^3 + 11x_5^3x_6 + 3x_5^2x_6^2
\end{aligned}$$

7.5 $\mathrm{SL}_2(25)$

Recently NEBE constructed a 72-dimensional, extremal even unimodular lattice Λ_{72} together with a subgroup $U := (\mathrm{PSL}_2(7) \times \mathrm{SL}_2(25)) \rtimes \mathrm{C}_2 \leq \mathrm{GL}_{72}(\mathbb{Z})$ of the automorphism group of Λ_{72} [Neb]. The hermitian construction of Λ_{72} will be reviewed shortly. Let $K = \mathbb{Q}(\zeta_7)$, $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$ and $F = \mathbb{Q}(\sqrt{-7})$. In his thesis [Hen09] HENTSCHEL classified all hermitian $\mathbb{Z}_F$-structures on the LEECH lattice. One of those is a 12-dimensional hermitian $\mathbb{Z}_F$-lattices (P, h) with hermitian automorphism group $\mathrm{SL}_2(25)$. It is isometric to its GALOIS conjugate and the extension of the hermitian automorphism group by $\mathrm{Gal}(F/\mathbb{Q})$ is split. The lattice Λ_{72} is the scalar restriction of the hermitian tensor product of (P, h) with the BARNES lattice. Note that the BARNES lattice is a CRAIG-lattice and use the ATLAS [CCN+85] to check that the construction of remark (7.1.1) applies. This turns Λ_{72} into an 72-dimensional $\mathbb{Z}_K * (\mathrm{SL}_2(25) \rtimes \Gamma)$-lattice. Let $M := \mathbb{Q} \otimes \Lambda_{72}$ the corresponding $\mathbb{Q}(\zeta_7) * (\mathrm{SL}_2(25) \rtimes \Gamma)$-module. Its character is $\widetilde{\chi_{16}}$, where χ_{16} is a faithful irreducible character of $\mathrm{SL}_2(25)$ in the ATLAS notation.

There exists another faithful irreducible character χ_{17} of $\mathrm{SL}_2(25)$ of degree 12. The corresponding character $\widetilde{\chi_{17}}$ of $K * (G \rtimes \Gamma)$ has degree 72 and SCHUR index 2 over $\mathbb{Q}$, which can be checked using the twisted FROBENIUS-SCHUR indicator (5.3.7).

The GALOIS group Γ acts on Λ_{72} and let H be a subgroup of Γ. Denote the bilinear form corresponding to Λ_{72} by Φ, and by $\Phi_{\Lambda_{72}^H} : \Lambda_{72}^H \times \Lambda_{72}^H \to \mathbb{Z}$: $(v, w) \mapsto v^{tr}\Phi w$ the form restricted to the fixed lattice under H. After rescaling $\Phi_{\Lambda_{72}^H}$, one computes the following table.

H	$\mathrm{rk}_{\mathbb{Z}}(\Lambda_{72}^H)$	$\det(\Phi_{L^H})$	$\min(\Phi_{\Lambda_{72}^H})$	$[\Lambda_{72} : (\Lambda_{72}^H \otimes \mathbb{Z}_K)]$
Γ	12	1	2	7^{30}
$\langle\sigma^2\rangle$	24	1	4	7^{12}
$\langle\sigma^3\rangle$	36	1	4	7^{6}

Note that the lattice $\Lambda_{72}^{\langle\sigma^2\rangle}$ is the LEECH lattice and Λ_{72}^{Γ} turns out to be the unique indecomposable unimodular lattice of dimension 12, which KNESER denoted K_{12} in [Kne57]. Choosing a reduced basis for the fixed lattice Λ_{72}^{Γ} gives a $(K/\mathbb{Q}, ^{-})$-representation:

$$\Delta_{\mathbb{Q}} : \mathrm{SL}_2(25) \to \mathrm{GL}_{12}(\mathbb{Q}(\zeta_7))$$

Due to its size we do not print the generating matrices nor the invariant of smallest degree. The denominators of the generating matrices all lie in the fractional ideal generated by $(\sqrt{-7})^{-1}$.

7.6 3. A_6

Let G be the VALENTINER group 3.A_6, χ one of the irreducible faithful characters of degree 3, and $K = \mathbb{Q}(\zeta_{15})$ with GALOIS group $\Gamma = \mathrm{C}_4 \times \mathrm{C}_2$. A computer calculation shows that, up to conjugation in $\mathrm{Aut}(G)$, there is a unique subgroup $U \cong \mathrm{C}_4 \times \mathrm{C}_2$ of $\mathrm{Aut}(G)$ which acts as GALOIS automorphisms on the character field $\mathbb{Q}(\sqrt{5}, \zeta_3)$ of χ.

There are two elements of order 2 in U, conjugate to each other in $\mathrm{Aut}(G)$, acting non trivially on the center of G and fixing the conjugacy classes of elements of order 5 of G. Hence, both elements induce the canonical complex conjugation on the character field of χ.

In fact, up to composition with an element of $\mathrm{Inn}(\mathrm{Aut}(G))$, there are two different possibilities for the isomorphism $^{-} : \Gamma \to U$. In terms of theorem (2.4.1) one expects two matrix groups which are not conjugate to each other by an element of $\mathrm{GL}_3(\mathbb{Q})$ and which are isomorphic to 3. A_6. Note that the two resulting twisted group rings $K * (G \rtimes \Gamma)$ are isomorphic $\mathbb{Q}$-algebras, but the canonical involution on $K * (G \rtimes \Gamma)$ is not respected.

The character $\widetilde{\chi}$ of $K * (G \rtimes \Gamma)$ has degree 24, rational values and SCHUR index 1 over $\mathbb{Q}$. Denote by M the corresponding $K * (G \rtimes \Gamma)$-module. Let $\Delta : G \to \mathrm{GL}_3(K)$ a representation affording χ. It is well known that $\Delta(\mathbb{Z}_K G)$ is a maximal $\mathbb{Z}_K$-order. Hence, up to isomorphism, there exists a unique $\mathbb{Z}_K G$-lattice in M and the equivalence classes of Γ-invariant ideals of $\mathbb{Z}_K$ are $(1 - \zeta_3)^i (1 - \zeta_5)^j$ for $0 \leq i \leq 1$ and $0 \leq j \leq 3$.

One computes the following table of $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in M together with their unique primitive form in $\mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$. Note that this table is the same for both choices of $^{-} : \Gamma \to U$.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	$3^{12} \cdot 5^{18}$	16	$3 \cdot 5^2$	2
L_1	$3^{12} \cdot 5^{18}$	16	$3^2 \cdot 5^2$	4
L_2	$3^{12} \cdot 5^6$	8	$3 \cdot 5$	1
L_3	$3^{12} \cdot 5^{18}$	16	3	1
L_4	$3^{12} \cdot 5^6$	8	$3^2 \cdot 5$	2
L_5	$3^{12} \cdot 5^6$	8	3	1
L_6	$3^{12} \cdot 5^{18}$	16	3^2	1
L_7	$3^{12} \cdot 5^6$	8	3^2	1

The lattices (L_2, Φ_2) and (L_5, Φ_5) correspond to an irreducible maximal finite subgroup of $\mathrm{GL}_{24}(\mathbb{Q})$ isomorphic to $(\mathrm{C}_2 \times \mathrm{C}_3 \,.\, \mathrm{PGL}_2(4) \times \mathrm{D}_{10}) .\, \mathrm{C}_2$ [Neb96].

We discuss the two different choices of the map $^{-} : \Gamma \to \mathrm{Aut}(G)$ and the influence on the fixed lattices. For one choice there exists a reduced $\mathbb{Z}$-basis of $(L_5^\Gamma, \Phi_{L_5^\Gamma})$ such that after rescaling the GRAM matrix is $\mathrm{diag}(1,1,3)$. In this case, up to an element of $\mathrm{O}_3(\Phi_{L_5^\Gamma}, \mathbb{Z})$, we find that the group $3.\mathrm{A}_6$ is generated by the matrices

$$\begin{pmatrix} \zeta_{15} & 0 & 0 \\ 0 & \zeta_{15}^4 & 0 \\ 0 & 0 & -1-\zeta_{15}^5 \end{pmatrix}$$

and

$$\frac{1}{\sqrt{-15}} \begin{pmatrix} -2+2\zeta_{15}^7+\zeta_{15}^4-2\zeta_{15}^3-2\zeta_{15}^6+2\zeta_{15}^2 & 2-2\zeta_{15}^7-3\zeta_{15}-2\zeta_{15}^4+\zeta_{15}^3+\zeta_{15}^6+2\zeta_{15}^5 & -3+3\zeta_{15}^7-3\zeta_{15}^3-3\zeta_{15}^6 \\ -1+2\zeta_{15}^7-\zeta_{15}^4-\zeta_{15}^3-\zeta_{15}^6 & \zeta_{15}+2\zeta_{15}^6 & 3-3\zeta_{15}^7-3\zeta_{15}-3\zeta_{15}^4+3\zeta_{15}^3+3\zeta_{15}^6+3\zeta_{15}^5 \\ 1-\zeta_{15}^2 & 2-\zeta_{15}^7-\zeta_{15}-\zeta_{15}^4+\zeta_{15}^3+\zeta_{15}^5 & -1+2\zeta_{15}^7+\zeta_{15}+\zeta_{15}^4-2\zeta_{15}^3+2\zeta_{15}^2-\zeta_{15}^5 \end{pmatrix}$$

This representation is precisely the one WIMAN found in [Wim96] by studying the geometry of the VALENTINER group and of which he calculated the invariant of smallest degree:

$$i_6 := 27x_3^6 + 9x_1^5x_3 - 45x_1^2x_2^2x_3^2 - 135x_1x_2x_3^4 + 10x_1^3x_2^3 + 9x_2^5x_3$$

The second choice of $\Gamma \to \mathrm{Aut}(G)$ leads to GRAM matrix of $(L_5^\Gamma, \Phi_{L_5^\Gamma})$ being

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

It is easy to check that those GRAM matrices represent non isometric quadratic forms over $\mathbb{Q}$.

Since the representation is quite similar to WIMANS, we give only the invariant of degree 6.

$$\begin{aligned} i_6 = &-15x_1^4x_3^2 - 15x_1^2x_2^4 - 9x_1x_3^5 + 90x_1x_2^2x_3^3 + 15x_1^4x_2x_3 + 30x_1^2x_2x_3^3 + 30x_1^2x_2^3x_3 - \\ &45x_1^2x_2^2x_3^2 - 90x_1x_2^3x_3^2 + 10x_2^6 + 10x_3^6 - 15x_1^4x_2^2 - 15x_1^2x_3^4 + 9x_1x_2^5 - 30x_2^5x_3 + \\ &60x_2^4x_3^2 - 70x_2^3x_3^3 + 60x_2^2x_3^4 - 30x_2x_3^5 + x_1^6 \end{aligned}$$

We observe that WIMANS representation provides better invariants.

7.7 2. A_7

Let $G = 2.\mathrm{A}_7$, $K = \mathbb{Q}(\sqrt{-7})$ and χ an absolutely irreducible character of degree 4. One finds that K is the character field of χ. There are two isoclinic split extensions of G by an outer automorphism of order 2. In both cases χ and its complex conjugate character fuse to a single character ψ of degree 8 and with rational values. Using MAGMA one checks that in one extension, denoted by $E := G \rtimes \mathrm{C}_2$, the character ψ has SCHUR index 1 over $\mathbb{Q}$. Hence there exists an 8-dimensional $\mathbb{Q}E$-module M with character ψ. Let φ be the generator of $\mathrm{C}_2 \leq \mathrm{Aut}(G)$ and note that φ interchanges the two conjugacy classes of elements of order 7 and 14 respectively. This shows that C_2 acts on the character field $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{-7})$ as GALOIS automorphisms. Let $^- : \Gamma \to \mathrm{Aut}(G)$ defined by $\sigma \mapsto \varphi$, then this choice turns M into a $K * (G \rtimes \Gamma)$-module.

There are 2-non isomorphic $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices L_0, L_1 in M and for each there exists a unique primitive form $\Phi_{L_i} \in \mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$. One computes the following table.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	1	2	2	2
L_1	1	2	1	2

Both lattices (L_i, Φ_{L_i}) are isometric to the famous E_8-lattice. Thus the E_8 lattice induces a representation $\Delta : 2.\mathrm{A}_7 \to \mathrm{GL}_4(K)$ having fundamental invariants with rational coefficients. In this representation $2.\mathrm{A}_7$ is generated by the matrices:

$$\langle \frac{1}{\sqrt{-7}} \begin{pmatrix} 0 & -1-2\alpha & 0 & 0 \\ -\alpha-1 & 0 & -1+\alpha & -1 \\ 1 & 0 & \alpha & 2 \\ -1+\alpha & 0 & -1 & -\alpha \end{pmatrix}, \frac{1}{\sqrt{-7}} \begin{pmatrix} \alpha & -1 & 1+\alpha & -\alpha-1 \\ -1 & -1+\alpha & 0 & 1+\alpha \\ -\alpha & 0 & \alpha+2 & 1 \\ \alpha & -\alpha & 1 & 1+\alpha \end{pmatrix} \rangle$$

where $\alpha = (-1+\sqrt{-7})/2$ and the generators have order 12 and 6, respectively. The subgroup of rational points is isomorphic to S_4. We do not print the polynomial invariant of degree 8, since it consist of 117 summands. It should be noted that the largest absolute value among the coefficient is 24, which is rather small.

We construct another representation of $2.\mathrm{A}_7$ with character χ over $K = \mathbb{Q}(\zeta_7)$. Using the twisted FROBENIUS-SCHUR (5.3.7) indicator and the ATLAS [CCN+85] one checks that, up to conjugation in $\mathrm{Aut}(G)$, there exists a unique automorphism $\varphi \in \mathrm{Aut}(G)$ with the following properties:

- It is not an inner automorphism.
- Let $^- : \Gamma \to \mathrm{Aut}(G) : \sigma \mapsto \varphi$, then the $K * (G \rtimes \Gamma)$ character $\widetilde{\chi}$ has degree 24, rational values and SCHUR index 1 over $\mathbb{Q}$.

Let M be the module corresponding to $\widetilde{\chi}$. One computes the following table of normalized $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices (L_i, Φ_i) in M.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	7^{16}	12	7^2	2
L_1	1	4	1	1
L_2	7^8	6	7^2	1
L_3	7^{16}	12	1	1
L_4	1	4	1	1
L_5	7^8	6	1	1

The lattices (L_1, Φ_1) and (L_4, Φ_4) are isometric to the famous LEECH lattice. For those one can choose a reduced $\mathbb{Z}$-basis of $(L_i^\Gamma, \Phi_{L_i^\Gamma})$ such that the GRAM matrix is the identity matrix. This basis provides a $(K/\mathbb{Q}, ^-)$-representation

$$\Delta_\mathbb{Q} : 2.\mathrm{A}_7 \to \mathrm{GL}_4(K)$$

and one of them differs from KLEIN'S representation [Kle87] by an element $\mathrm{O}_3(\mathbb{Z})$. The corresponding matrix group is generated by

$$\left\langle \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -\zeta_7 & 0 & 0 \\ 0 & 0 & -\zeta_7^4 & 0 \\ 0 & 0 & 0 & -\zeta_7^2 \end{pmatrix}, \frac{1}{\sqrt{-7}} \begin{pmatrix} 0 & -\zeta_7^3+\zeta_7^4 & -\zeta_7^5+\zeta_7^2 & \zeta_7-\zeta_7^6 \\ \zeta_7^3-\zeta_7^4 & 0 & \zeta_7^6-\zeta_7 & \zeta_7^2-\zeta_7^5 \\ \zeta_7^5-\zeta_7^2 & \zeta_7-\zeta_7^6 & 0 & \zeta_7^3-\zeta_7^4 \\ \zeta_7^6-\zeta_7 & \zeta_7^5-\zeta_7^2 & -\zeta_7^3+\zeta_7^4 & 0 \end{pmatrix} \right\rangle$$

and the invariant of smallest degree is

$$\begin{aligned} i_8 = {} & 21x_4^4x_1x_2^2x_3 - 21x_1^2x_4^2x_2^2x_3^2 + 21x_3^4x_4^2x_1x_2 + 3x_4^7x_1 - x_1^8 + 28x_4^4x_2x_3^3 + \\ & 28x_3x_4^3x_2^4 - 21x_4^5x_1^2x_3 - 42x_1^3x_3^2x_4^3 - 42x_2^3x_1^3x_4^2 + 7x_2x_1^4x_4^3 - 7x_4^6x_2^2 - \\ & 7x_3^6x_4^2 - 42x_2x_4x_1^5x_3 + 21x_2^4x_4x_3^2x_1 - 7x_3^2x_2^6 + 3x_1x_2^7 + 3x_3^7x_1 + 7x_2^3x_3x_1^4 + \\ & 28x_3^4x_2^3x_4 - 21x_1^2x_4x_2^5 + 7x_1^4x_3^3x_4 - 21x_3^5x_1^2x_2 - 42x_1^3x_3^3x_2^2 \end{aligned}$$

7.8 $\mathrm{U}_3(4)$

Let $G = \mathrm{U}_3(4)$, $K = \mathbb{Q}(\zeta_{13})$ with group Γ and χ the irreducible faithful character of degree 12. The character χ has rational values and SCHUR index 2 over $\mathbb{Q}$. There are 2-conjugacy classes of automorphisms of order 13 of G which are not inner automorphisms. Choose a representative of one of those classes and use it to define $^- : \Gamma \to \mathrm{Aut}(G)$. Since χ is Γ invariant, the character $\widetilde{\chi}$ of $K * (G \rtimes \Gamma)$ has degree 144 and values in $\mathbb{Q}$.

A computer calculation shows that there exists a cyclic and Γ-invariant subgroup of order 13 in G. Similar to example (5.4.5) one can use induction to see that $\widetilde{\chi}$ has SCHUR index 1 over $\mathbb{Q}$. Let M be a $K * (G \rtimes \Gamma)$-module affording this character. Viewing M as a $K\mathrm{U}_3(4)$-module there exists, up to isomorphism, two $\mathbb{Z}_K G$-lattice L_0, L_1 in M. Hence the isomorphism classes of full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices are $L_{j,i} := (1-\zeta_{13})^i L_j$ with $0 \le i \le 11$ and $0 \le j \le 1$. One computes the following table of normalized $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices in M with minimal determinant.

Lattice L	$\det(\Phi_{L_i})$	$\min(\Phi_{L_i})$	$\det(\Phi_{L_i^\Gamma})$	$\min(\Phi_{L_i^\Gamma})$
L_0	2^{72}	≤ 12	2^6	2
L_1	2^{72}	≤ 12	2^6	2
L_2	2^{72}	≤ 12	2^6	1
L_3	2^{72}	≤ 12	2^6	1

There exists a $(K/\mathbb{Q}, ^-)$-representation

$$\Delta_\mathbb{Q} : \mathrm{U}_3(4) \to \mathrm{GL}_{12}(K)$$

with character χ. Due to its size we do not print the generating matrices nor the invariant of smallest degree.

7.9 Extraspecial groups

7.9.1 $\mathbf{D}_8 \otimes \mathbf{Q}_8$

Let G be the extraspecial 2-group $\mathrm{D}_8 \otimes \mathrm{Q}_8$ and $K = \mathbb{Q}(i)$ with GALOIS group Γ. Use the KRONECKER product of the elements of

$$\mathrm{D}_8 = \langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle$$

and the matrix group Q_8 given in example (5.1.8) to construct G as a finite subgroup of $\mathrm{GL}_4(K)$ which is invariant under complex conjugation. This turns $M := K^{4\times 1}$ into a $K * (G \rtimes \Gamma)$-module. A computer calculation shows that there are 192 non isomorphic full $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices L_i in M and each has a unique primitive form in $\mathcal{F}_{\Delta,>0}(K * (G \rtimes \Gamma))$. There are 32-lattices (L_i, Φ_{L_i}) isometric to the E_8-lattice, 30 isometric to the standard lattice $(\mathbb{Z}^{8\times 1}, \mathrm{I}_8)$, 70 isometric to $\mathrm{D}_4 \perp \mathrm{D}_4$ and 30 represent the root lattice D_8 and the dual D_8^*, respectively.

Viewing all those lattices as hermitian $\mathbb{Z}[i]$-lattices, we compute the hermitian automorphism group:

Lattice L	$\lvert \mathrm{Aut}_{\mathbb{Z}[i]}(L, \Phi_L) \rvert$	solvable
E_8	$2^{10} \cdot 3^2 \cdot 5$	no
Std	$2^{11} \cdot 3$	yes
$\mathrm{D}_4 \perp \mathrm{D}_4$	$2^8 \cdot 3^2$	yes
D_8	$2^{11} \cdot 3$	yes

We consider the case that (L, Φ) is isometric to the E_8-lattice. The hermitian automorphism group of those lattices is the complex reflection group $G := G_{31}$, which is an extension of

$$\mathrm{C}_4 \curlyvee (\mathrm{D}_8 \curlyvee \mathrm{Q}_8)$$

by the symmetric group S_6. This turns E_8 into an $\mathbb{Z}_K * (G_{31} \rtimes \Gamma)$-lattice and one can choose a reduced $\mathbb{Z}$-basis of $(\mathrm{E}_8^\Gamma, \Phi_{\mathrm{E}_8^\Gamma})$ such that the GRAM matrix is the identity matrix. This basis provides a $(K/\mathbb{Q}, ^-)$-representation

$$\Delta_{\mathbb{Q}} : \mathrm{G}_{31} \to \mathrm{GL}_4(K)$$

As a matrix group G_{31} is generated by

$$G_{31} := \left\langle \frac{1}{2} \begin{pmatrix} 1 & 1 & i & -i \\ -1 & 1 & i & i \\ i & -i & -1 & -1 \\ -i & -i & -i & 1 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} -i & -i & 1 & 1 \\ 1 & -i-1 & -1 & 0 \\ 1 & i & -i & 1 \\ -i & 0 & -i & -i-1 \end{pmatrix} \right\rangle$$

where the generators are of order 6 and 8, respectively. Computing the invariant of smallest degree, one finds

$$\begin{aligned} i_8 :=& x_1^8 - 7x_1^4x_2^4 - 42x_1^4x_2^2x_4^2 + 14x_1^4x_3^4 - 7x_1^4x_4^4 - 42x_1^2x_2^4x_3^2 + 84x_1^2x_2^2x_3^2x_4^2 \\ &- 42x_1^2x_3^2x_4^4 + x_2^8 - 7x_2^4x_3^4 + 14x_2^4x_4^4 - 42x_2^2x_3^4x_4^2 + x_3^8 - 7x_3^4x_4^4 + x_4^8 \end{aligned}$$

In the nineteenth century, MASCHKE constructed a representation of this group where the generating matrices have entries in the 8-th cyclotomic field [Mas89]. Using the techniques of the previous examples, one finds $\mathrm{E}_8 \perp \mathrm{E}_8$ as a $\mathbb{Z}[\zeta_8] * (\mathrm{G}_{31} \rtimes \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}))$-lattice. MASCHKE'S representation can be obtained taking a reduced $\mathbb{Z}$-basis of the fixed point lattice under the action of the GALOIS group of $\mathbb{Q}(\zeta_8)$ on $\mathrm{E}_8 \perp \mathrm{E}_8$. The invariant of smallest degree in MASCHKE'S representation is

$$\begin{aligned} i_8 =& 14x_2^4x_3^4 + x_4^8 + 168x_1^2x_4^2x_2^2x_3^2 + x_1^8 + 14x_1^4x_4^4 + 14x_1^4x_2^4 + 14x_1^4x_3^4 + \\ & 14x_4^4x_3^4 + 14x_4^4x_2^4 + x_3^8 + x_2^8 \end{aligned}$$

An obvious difference between those invariants is the number of real solutions of the equation $i_8(x) = 0$ in $\mathbb{R}^4$.

7.9.2 Odd p

Let p be an odd prime and G an extraspecial p-group of order p^3. There are exactly two non isomorphic groups of such type and they admit the following presentations:

$$\begin{aligned} p_+^{2+1} &= \langle a, b, c \mid a^p = b^p = c^p = 1, ba = abc, ca = ac, cb = bc \rangle \\ p_-^{2+1} &= \langle a, b, c \mid a^p = b^p = c, c^p = 1, ba = abc, ca = ac, cb = bc \rangle \end{aligned}$$

It is immediate that the first group has exponent p and the second p^2, thus the exponent distinguishes both.

Let $\varphi : \mathrm{S}_p \to \mathrm{GL}_p(\mathbb{Z})$ be the permutation representation corresponding to the natural S_p action on $\{1, ..., p\}$. One finds the following matrix representations:

$$\Delta : p_+^{2+1} \to \mathrm{GL}_p(\mathbb{Q}(\zeta_p))$$

$$\begin{aligned} & a \mapsto \varphi((1, 2, ..., p)),\ b \mapsto \mathrm{diag}(1, \zeta_p, \zeta_p^2, ..., \zeta_p^{p-1}) \\ & c \mapsto \mathrm{diag}(\zeta_p, ..., \zeta_p) \end{aligned}$$

and

$$\Delta : p_-^{2+1} \to \mathrm{GL}_p(\mathbb{Q}(\zeta_{p^2}))$$

$$\begin{aligned} & a \mapsto \mathrm{diag}(\zeta_{p^2}, \zeta_{p^2}^{p+1}, \zeta_{p^2}^{2p+1}, ..., \zeta_{p^2}^{(p-1)p+1})\varphi((1, 2, ..., p)) \\ & b \mapsto \mathrm{diag}(\zeta_{p^2}, \zeta_{p^2}^{p+1}, \zeta_{p^2}^{2p+1}, ..., \zeta_{p^2}^{(p-1)p+1}),\ c \mapsto \mathrm{diag}(\zeta_{p^2}^p, ..., \zeta_{p^2}^p) \end{aligned}$$

where ζ_p and ζ_{p^2} are primitive p-th respectively p^2-th roots of unity. Both representation are faithful, absolutely irreducible and the corresponding matrix group is defined over $\mathbb{Q}$. This turns $\mathbb{Z}[\zeta_p]^{p\times 1}$ and $\mathbb{Z}[\zeta_{p^2}]^{p\times 1}$ into a $\mathbb{Z}[\zeta_p] * (p_+^{2+1} \rtimes \Gamma)$ respectively $\mathbb{Z}[\zeta_{p^2}] * (p_-^{2+1} \rtimes \Gamma)$-lattice, where $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q})$ respectively.

7.9.3 3-groups

Assume that $p = 3$, $K = \mathbb{Q}(\zeta_3)$ and

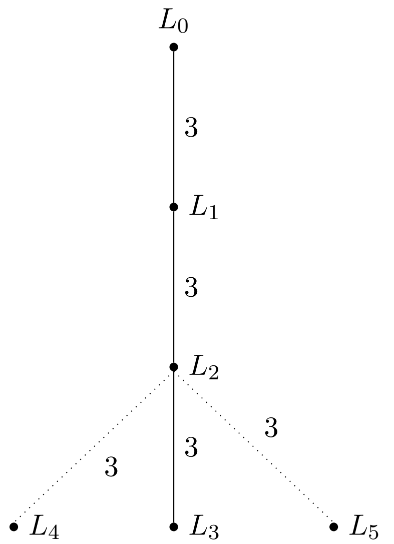
$$G = 3_+^{2+1} = \langle \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3^2 \end{pmatrix}, \begin{pmatrix} \zeta_3 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3 \end{pmatrix} \rangle$$

The space of invariants of smallest degree is

$$\lambda_1(x_1^3 + x_2^3 + x_3^3) + \lambda_2(x_1 x_2 x_3) \text{ with } \lambda_1, \lambda_2 \in \mathbb{Q}(\zeta_3)$$

hence 2-dimensional. Geometrically, this invariant space is directly connected to the HESSE pencil [AD09].

Recall that $L_0 := \mathbb{Z}[\zeta_3]^{3\times 1}$ is a $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice. View L_0 as a $\mathbb{Z}_K G$-lattice and using MAGMA one obtains the HASSE diagram of all full $\mathbb{Z}_K G$ sublattices of L_0:



The dotted lines indicate that L_4 and L_5 are not $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices. Hence, up to isomorphism, the $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices are $(1-\zeta_3)^j L_i$ with $0 \le j \le 1$ and $1 \le i \le 3$. On all those lattices there existes a unique primitive form $\Phi_{i,j}$.

One checks that $(L_2, \Phi_{2,0})$ is isometric to the root lattice E_6-lattice. The $\mathbb{Z}_K * (G \rtimes \Gamma)$-structure on E_6 turns it into an hermitian $\mathbb{Z}[\zeta_3]$-lattice and the hermitian automorphism group is the complex reflection group $G_{26} = \mathrm{C}_2 \times 3^{1+2}.\mathrm{SL}_2(3)$. The quotient $G_{26}/\,\mathrm{C}(G_{26})$ is isomorphic to $\mathbb{F}_3 \rtimes \mathrm{SL}_2(\mathbb{F}_3)$ and is called the HESSIAN group. Hence, E_6 is an $\mathbb{Z}_K * (G_{26} \rtimes \Gamma)$-lattice.

Choosing a reduced $\mathbb{Z}$-basis of the Γ-fixed lattice $(\mathrm{E}_6^\Gamma, \Phi_{\mathrm{E}_6^\Gamma})$ such that the Gram matrix is the identity matrix, provides a $(K/\mathbb{Q}, ^-)$-representation

$$\Delta_{\mathbb{Q}} : \mathrm{G}_{26} \to \mathrm{GL}_3(K)$$

and generating matrices are

$$G_{26} := \left\langle \frac{1}{\sqrt{-3}} \begin{pmatrix} -1 & -\zeta_3 & -1 \\ -1 & 1+\zeta_3 & 1+\zeta_3 \\ -1 & -1 & -\zeta_3 \end{pmatrix}, \begin{pmatrix} \zeta_3 & 0 & 0 \\ 0 & -\zeta_3 - 1 & 0 \\ 0 & 0 & \zeta_3 \end{pmatrix} \right\rangle$$

where the first matrix is of order 18 and the second of order 3. This is a primitive matrix group i.e. it is not conjugate to a subgroup of

$$H \wr \mathrm{S}_k := \langle \mathrm{diag}(h_1, ..., h_k), P \otimes \mathrm{I}_{\frac{m}{k}} \mid h_i \in H, P \text{ a permutation matrix } \rangle$$

for some $H < \mathrm{GL}_{\frac{m}{k}}(K)$.

The invariant of smallest degree is

$$i_6 := x_1^6 + x_2^6 + x_3^6 - 10(x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3)$$

which is the same as Maschke calculated in [Mas89]. This shows that the classical representation of G_{26}, from which Maschke calculated fundemental invariants, admits an arithmetical construction using a $\mathbb{Z}$-basis of the Γ-fixed lattice E_6^Γ.

We turn to the second extraspecial 3-group of order 3^3. Let $K = \mathbb{Q}(\zeta_{p^2})$ and

$$G = 3_-^{2+1} = \langle \begin{pmatrix} 0 & 0 & \zeta_9 \\ \zeta_9^4 & 0 & 0 \\ 0 & \zeta_9^7 & 0 \end{pmatrix}, \begin{pmatrix} \zeta_9 & 0 & 0 \\ 0 & \zeta_9^4 & 0 \\ 0 & 0 & \zeta_9^7 \end{pmatrix}, \begin{pmatrix} \zeta_9^3 & 0 & 0 \\ 0 & \zeta_9^3 & 0 \\ 0 & 0 & \zeta_9^3 \end{pmatrix} \rangle$$

The invariant of smallest degree is

$$i_3 = x_1^2x_3 + x_2^2x_1 + x_2x_3^2$$

Recall that $\mathbb{Z}[\zeta_9]^{3\times 1}$ is a $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattice. A computer calculation reveals that there are 324 non isomorphic $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices, which are all equipped with an unique primitive form Φ. The most interesting lattice (L, Φ) corresponds to an irreducible maximal finite subgroup of $\mathrm{GL}_{18}(\mathbb{Q})$ isomorphic to $((\mathrm{C}_2 \times 3^{1+4} : \mathrm{Sp}(4,3)). \mathrm{C}_2$ of [NP95].

Blichfeld showed that every finite subgroup of $\mathrm{GL}_3(\mathbb{C})$ which contains $\Delta(G) = p_-^{1+2}$ is not primitive [Bli17, Chapter V]. Hence, the finite subgroups of $\mathrm{GL}_3(\mathbb{C})$ constructed from Γ-fixed points of the $\mathbb{Z}_K * (G \rtimes \Gamma)$-lattices are of not much interest.

Chapter 8

The quotient map

Let K be an algebraically closed field and G a finite subgroup of $\mathrm{GL}_n(K)$ with natural module $V := K^n$. The main result of this chapter is the following theorem, which was proposed by Plesken.

Theorem 8.0.1. *Let G be a finite subgroup of $\mathrm{GL}_n(K)$, p a point in K^n and assume that the characteristic of K does not divide $|G|$. The rank of the* Jacobian *matrix, evaluated at p, of any system of fundamental polynomial invariants equals the dimension of the subspace of fixed points under the stabilizer G_p of p in G.*

If K has characteristic zero, a similar result is mentioned in [Bay04, Proposition 4] which is neither proven nor explained in any form. Here this theorem is a result of a more general study between the geometric properties of the quotient map [DK02, Chapter 2]

$$\pi : K^n \to K^n/G$$

and the group theoretic properties of the natural action of G on V.

Denote by $\mathrm{T}_p(V)$ the tangent space and by $\mathrm{T}_p^*(V)$ the cotangent space. The stabilizer G_p acts linearly on both spaces and as a KG_p-module the cotangent space is the dual of the natural G_p module. Identify the cotangent space with V^*. In the first section it is proven that the image of the cotangent map induced by π is $\mathrm{Fix}_{G_p}(V^*)$, which is isomorphic to $\mathrm{Fix}_{G_p}(V)$ if the characteristic of K and $|G|$ are coprime. Theorem (8.0.1) is obtained by choosing fundamental polynomial invariants.

Assume that L is a subfield of K and that G is a subgroup of $\mathrm{GL}_n(L)$. For any L-valued point $p \in V$ that is $p \in L^n$, the fixed space $\mathrm{Fix}_{G_p}(V^*)$ is the scalar extension of $\mathrm{Fix}_{G_p}((L^n)^*)$ by K. Hence the results remain true under restriction to L-valued points of V. Choose $K = \mathbb{C}$ and $L = \mathbb{R}$ to obtain the finite group version of a result by Procesi and Schwarz for compact, real Lie-groups [PS85, Proposition 1.5].

In the last section the results are applied to study the geometry of a natural map associated to the normalizer of G_p acting on the fixed points under G_p. Theorem (8.0.1) combined with elementary group theory is used to compute the orbit type stratification of K^n. The complex reflection group G_{31} shows that this method is superior to the methods described in [Bay04], which do not work for this group. More theoretically, for reflection groups (8.0.1) implies a generalization of a result of STEINBERG [Ste60] on the factorization of the JACOBIAN determinant.

8.1 Singularities of the quotient map

Let G be a finite subgroup of $\mathrm{GL}_n(K)$ and $V := K^{n\times 1}$ its natural module. Then G acts on the dual space V^* by $g\omega := \omega \circ g^{-1}$. Choosing a basis $x_1, ..., x_n$ of V^*, one can identify the ring of polynomial functions on V with $K[x_1, ..., x_n]$ and gets an action of G on $K[x_1, ..., x_n]$. The **ring of invariants** is denoted by $K[x_1, ..., x_n]^G$ and by a result of NOETHER it is finitely generated [DK02, Thm. 2.2.10].

The **quotient variety** V/G is the algebraic variety with coordinate ring $\mathcal{O}_{V/G} = K[x_1, ..., x_n]^G$ and the points are identified with orbits. The natural embedding $K[x_1, ..., x_n]^G \to K[x_1, ..., x_n]$ induces the quotient map $\pi : V \to V/G : p \mapsto {}^G p$ and this map is a **good geometric quotient** c.f. [DK02, Chapter 2].

Let $p \in K^{n\times 1}$ be a point, G_p its stabilizer in G and $\mathrm{m}_{\pi(p)}, \mathrm{m}_p$ denote the maximal ideals of $\mathcal{O}_{\pi(p),V/G}$ and $\mathcal{O}_{p,V}$ respectively. The quotient map induces the map

$$\pi^*_{|p} : \mathrm{m}_{\pi(p)} / \mathrm{m}^2_{\pi(p)} \to \mathrm{m}_p / \mathrm{m}^2_p : f + \mathrm{m}^2_{\pi(p)} \mapsto f \circ \pi + \mathrm{m}^2_p$$

on the cotangent space. The first objective is to describe the image of this map. This is done using the ideas of the proof of [Dré04, Proposition 4.11], hence generalizing this proposition.

Theorem 8.1.1. *The stabilizer G_p acts naturally on $\mathrm{m}_p / \mathrm{m}^2_p$ and the image of $\pi^*_{|p}$ is the space of fixed points under this action that is $\pi^*_{|p}(\mathrm{m}_{\pi(p)} / \mathrm{m}^2_{\pi(p)}) = \left(\mathrm{m}_p / \mathrm{m}^2_p\right)^{G_p}$.*

Proof. From the definition of $\pi^*_{|p}$ the inclusion

$$\pi_{*|p}(\mathrm{m}_{\pi(p)} / \mathrm{m}^2_{\pi(p)}) \subseteq \left(\mathrm{m}_p / \mathrm{m}^2_p\right)^{G_p} \tag{8.1}$$

is immediate for all $p \in V$.

Identify $\left(\mathrm{m}_p / \mathrm{m}^2_p\right)^{G_p}$ with the space of invariant polynomials of degree one, which vanish at p.

Let $u \neq 0$ be an element of $\left(\mathrm{m}_p / \mathrm{m}^2_p\right)^{G_p}$, then there exists an $\widetilde{f} \in \mathrm{m}_p^{G_p}$ with the following properties:

- The image of $\widetilde{f}$ is u in $\mathrm{m}_p / \mathrm{m}^2_p$
- The restriction of $\widetilde{f}$ to the G orbit of p vanishes only at p

Define

$$f := \prod_{g \in G/G_p} {}^g\tilde{f}$$

Then $f \in \mathrm{m}_p \cap K(V)^G$ and we can compute the image of f in $\mathrm{m}_p \,/\, \mathrm{m}_p^2$ as the linear part of the TAYLOR expansion in p. Let $1 \leq i \leq n$, using the product rule we have:

$$\frac{\partial}{\partial_{x_i}}_{|p} f = (\frac{\partial}{\partial_{x_i}}_{|p} \widetilde{f}) \cdot \underbrace{(\prod_{g \in G/G_p, g \notin G_p} {}^g\tilde{f})_{x=p}}_{\neq 0} + \underbrace{\widetilde{f}(p)}_{=0} \cdot (\frac{\partial}{\partial_{x_i}}_{|p} \prod_{g \in G/G_p, g \notin G_p} {}^g\tilde{f})$$

This shows that the linear part of the TAYLOR expansion of f is a non zero scalar multiple of the linear part of $\widetilde{f}$. By construction this is a non zero scalar multiple of u in $\mathrm{m}_p \,/\, \mathrm{m}_p^2$.

Since f is G-invariant it can be considered as an element of $\mathrm{m}_{\pi(p)} \,/\, \mathrm{m}_{\pi(p)}^2$ and one has equality in (8.1). This proves the theorem. $\square$

Recall that the differential

$$\pi_{*|p} : \mathrm{T}_p\, V \to \mathrm{T}_{\pi(p)}\, V/G$$

of π is the dual map of $\pi^*_{|p}$.

From now on assume that the characteristic of K does not divide the order of G. The linear action of G_p on $\mathrm{m}_p \,/\, \mathrm{m}_p^2$ turns this into a KG_p-module, which is isomorphic to the dual of the natural module V of G_p. Both modules are completly reducible and contain the same number of copies of the trivial module. This implies that $\left(\mathrm{m}_p \,/\, \mathrm{m}_p^2\right)^{G_p}$ and the space of fixed points

$$\mathrm{Fix}_{G_p}(V) := \{v \in V \mid gv = v \text{ for all } g \in G_p\}$$

are isomorphic vector spaces. Use this and theorem (8.1.1) to determine the rank of $\pi_{*|p}$ and note that dual maps have the same rank.

Corollary 8.1.2. *Let K be of characteristic coprime to $|G|$ and p be an point in V, then:*

$$\mathrm{rk}(\pi_{*|p}) = \dim_K \left(\mathrm{m}_p \,/\, \mathrm{m}_p^2\right)^{G_p} = \dim_K(\mathrm{Fix}_{G_p}(V))$$

Remark 8.1.3. In the modular case $\mathrm{rk}(\pi_{*|p}) = \dim_K \left(\mathrm{m}_p \,/\, \mathrm{m}_p^2\right)^{G_p}$ remains true, but in general this differs from $\dim_K(\mathrm{Fix}_{G_p}(V))$.

Choose a system of fundamental invariants $\{h_i\}_{i=1,..,l}$. This induces a closed embedding of the quotient variety into affine l-space

$$\varphi : V/G \to K^{l\times 1} : {}^G p \mapsto \left(h_1(p), ..., h_l(p)\right)$$

One obtains the following commutative diagram.

$$\begin{tikzcd} V \arrow[r, "\pi"] \arrow[dr, "\varphi\circ\pi=:\psi"'] & V/G \arrow[d, "\varphi"] \\ & K^{l\times 1} \end{tikzcd}$$

For any point p this leads to a commutative diagram on the tangent spaces.

$$\begin{tikzcd} \mathrm{T}_p V \arrow[r, "\pi_{*|p}"] \arrow[dr, "\psi_{*|p}"'] & \mathrm{T}_{\pi(p)} V/G \arrow[d, "\varphi_{*|\pi(p)}"] \\ & \mathrm{T}_{\psi(p)} K^{l\times 1} \end{tikzcd}$$

It is a basic fact that the differential $\psi_{*|p}$ of ψ at p can be identified with the Jacobian matrix $\mathrm{Jac}(\psi)_{|p} := (\frac{\partial h_j}{\partial x_i})_{|p} \in K^{n\times l}$. Since φ is a closed embedding the rank of $\psi_{*|p}$ is the same as the rank of $\pi_{*|p}$. By corollary (8.1.2) one has that $\mathrm{rk}(\pi_{*|p}) = \dim_K(\mathrm{Fix}_{G_p}(V))$ and this proves the main theorem (8.0.1).

Remark 8.1.4. Theorem (8.0.1) does not hold in every characteristic. Assume that $G := \mathrm{GL}_3(\mathbb{F}_2)$ is given in the natural representation and that $V := \overline{\mathbb{F}_2}^{3\times 1}$ is the natural module. The Dickson invariants ([Wil83])

$$\begin{aligned}
h_1 &= x_1^4 + x_1^2x_2^2 + x_1^2x_2x_3 + x_1^2x_3^2 + x_1x_2^2x_3 + x_1x_2x_3^2 + x_2^4 + x_2^2x_3^2 + x_3^4\\
h_2 &= x_1^4x_2^2 + x_1^4x_2x_3 + x_1^4x_3^2 + x_1^2x_2^4 + x_1^2x_2^2x_3^2\\
&\quad + x_1^2x_3^4 + x_1x_2^4x_3 + x_1x_2x_3^4 + x_2^4x_3^2 + x_2^2x_3^4\\
h_3 &= x_1^4x_2^2x_3 + x_1^4x_2x_3^2 + x_1^2x_2^4x_3 + x_1^2x_2x_3^4 + x_1x_2^4x_3^2 + x_1x_2^2x_3^4
\end{aligned}$$

are a set of fundamental invariants and the Jacobian matrix is

$$\mathrm{Jac} = \begin{pmatrix} x_2^2x_3 + x_2x_3^2 & x_1^2x_3 + x_1x_3^2 & x_1^2x_2 + x_1x_2^2\\ x_2^4x_3 + x_2x_3^4 & x_1^4x_3 + x_1x_3^4 & x_1^4x_2 + x_1x_2^4\\ x_2^4x_3^2 + x_2^2x_3^4 & x_1^4x_3^2 + x_1^2x_3^4 & x_1^4x_2^2 + x_1^2x_2^4 \end{pmatrix}$$

For an arbitrary, non-zero point $p \in \mathbb{F}_2^3$ the stabilizer G_p of p is isomorphic to the symmetric group S_4. The space of fixed points under G_p is one dimensional and spanned by p, but the Jacobian is always zero evaluated at p. This is consistent with remark (8.1.3), since the dual representation of the natural representation of G_p has no non trivial fixed points.

8.2 Applications and examples

We want to use the results of the last section to study the geometric properties of the map

$$\iota : \mathrm{Fix}_{G_p}(V)/\,\mathrm{N}_G(G_p) \to V/G \ : \ {}^{\mathrm{N}_G(G_p)}x \mapsto {}^{G}x$$

induced by the natural action of the normalizer $\mathrm{N}_G(G_p)$ of G_p on the space of fixed points $\mathrm{Fix}_{G_p}(V)$. This gives the map

$$\tilde{\iota} : \mathbb{C}[V]^G \to \mathbb{C}[\mathrm{Fix}_{G_p}(V)]^{\mathrm{N}_G(G_p)} \;:\; p \mapsto p_{|\,\mathrm{Fix}_{G_p}(V)}$$

on the coordinate rings. Analyzing the proof of (8.1.1) one obtains the following corollary.

Corollary 8.2.1. *Let $\tilde{\pi}$ be the quotient map $\mathrm{Fix}_{G_p}(V) \to \mathrm{Fix}_{G_p}(V)/\,\mathrm{N}_G(G_p)$, K an arbitrary algebraically closed field and*

$$E := \{x \in \mathrm{Fix}_{G_p}(V) \mid G_x = G_p\}$$

be the set of points in $\mathrm{Fix}_{G_p}(V)$ whose stabilizer is G_p. Then

1. *the restriction of ι to $\tilde{\pi}(E)$ is injective.*
2. *for every $x \in E$, the induced map*

$$\iota_{*|\tilde{\pi}(x)} : \mathrm{T}_{\tilde{\pi}(x)}\,\mathrm{Fix}_{G_p}(V)/\,\mathrm{N}_G(G_p) \to \mathrm{T}_{\pi(x)}\,V/G$$

is injective

Proof. Since elements in the same G-orbit have conjugate stabilizers the injectivity of ι restricted to $\tilde{\pi}(E)$ is immediate.

Let $x \in E$ and consider the quotient maps $\sigma : V/\,\mathrm{N}_G(G_p) \to V/G$ and $\widehat{\pi} : V \to V/\,\mathrm{N}_G(G_p)$. Denote by $\mathrm{m}_{\widehat{\pi}(x)}$ the maximal ideal of $\mathcal{O}_{\widehat{\pi}(x),V/\,\mathrm{N}_G(G_p)}$. Use $G_p \leq \mathrm{N}_G(G_p)$ and the proof of (8.1.1) to see that the cotangent map

$$\sigma^*_{|\widehat{\pi}(x)} : \mathrm{m}_{\pi(x)}\,/\,\mathrm{m}^2_{\pi(x)} \to \widehat{\mathrm{m}}_{\widehat{\pi}(x)}/\widehat{\mathrm{m}}^2_{\widehat{\pi}(x)}$$

is surjective. Hence the differential of σ is injective. Note that the natural map $\tau : \mathrm{Fix}_{G_p}/\,\mathrm{N}_G(G_p) \to V/\,\mathrm{N}_G(G_p)$ is a closed embedding and that $\iota = \sigma \circ \tau$. This proofs the corollary. □

We discuss the special case when $\mathrm{Fix}_{G_p}(V)$ is 1-dimensional. If G has no non trivial fixed points on V and if it can be realized as a subgroup of $\mathrm{GL}_n(\mathbb{R})$, then there is an easy group theoretic criterion to decide if the map $\tilde{\iota}$ is surjective. If $\tilde{\iota}$ is surjective then ι is a closed embedding, which is a stronger statement than corollary (8.2.1). One can make the following remark.

Remark 8.2.2. Assume that G is a subgroup of $\mathrm{GL}_n(\mathbb{R})$ and that G has no non trivial fixed points on $V = \mathbb{C}^n$. Let $p \in V$ be a point such that $\mathrm{Fix}_{G_p}(V)$ is 1-dimensional. The map $\tilde{\iota}$ is surjective if and only if $[\mathrm{N}_G(G_p) : G_p] = 2$.

Proof. Since $\mathrm{N}_{G_p}(G_p)$ acts on the one dimensional space $\mathrm{Fix}_{G_p}(V)$ it induces a 1-dimensional, real representation of $\mathrm{N}_{G_p}(G_p)/G_p$. Therefore G_p is either self normalizing or $[\mathrm{N}_G(G_p) : G_p] = 2$. Assume that G_p is self normalizing, then $\mathbb{C}[\mathrm{Fix}_{G_p}(V)]^{\mathrm{N}_G(G_p)} = \mathbb{C}[\mathrm{Fix}_{G_p}(V)]$ and since G has no fixed points, the map cannot be surjective.

One can assume that p is the first standard basis vector and if $[\mathrm{N}_G(G_p) : G_p] = 2$ then $\mathbb{C}[\mathrm{Fix}_{G_p}(V)]^{\mathrm{N}_G(G_p)}$ is $\mathbb{C}[x_1^2]$. It is enough to show that there exists an element of degree 2 in $\mathbb{C}[V]^G$, which does not vanish at p. Since G is a real matrix group the invariant polynomial corresponding to a positive definite G-invariant bilinear form has this property. □

In other words the last remark says that the map

$$\iota : \mathrm{Fix}_{G_p}(V)/\,\mathrm{N}_G(G_p) \to V/G$$

is a closed embedding, if and only if the G-orbit of p is stable under the C_2-action $x \mapsto -x$.

Turning to theorem (8.0.1) we can use this to calculate the orbit type stratification of V. Let H be a subgroup of G and $[H]$ denote its conjugacy class. The stratum associated to $[H]$ is

$$V^{[H]} := \{p \in V \mid G_p \in [H]\}$$

Since G is finite there are only a finite number of strata and each stratum is a locally closed non-singular subvariety of V. For proofs of these assertions see [VP89, Section 6.9].

If G is given as a subgroup of $\mathrm{GL}_n(\mathbb{R})$, one could use the work [AS83] to obtain a description in terms of equalities and inequalities of the the stratification of $\varphi(\mathbb{R}^n/G)$. For $1 \leq k \leq n$ denote by $V_{\leq k}$ the Zariski-closure of the union of all strata of dimension less or equal to k. Note that this is the union of all fixed point spaces, with a dimension less or equal to k, of subgroups of G.

Corollary 8.2.3. *For $1 \leq k \leq n$ let Jac_k be the ideal generated by the $k \times k$ minors of the* Jacobian *of a chosen set of fundamental invariants. Then the radical of Jac_k is the ideal corresponding to $V_{\leq k-1}$.*

Proof. A point p lies in the zero set of Jac_k if and only if the rank of the Jacobian evaluated at p is less than k. By theorem (8.0.1) this is the case if and only if the dimension of the space of fixed points under the stabilizer G_p is less than k. This is equivalent to p being an element of $V_{\leq k-1}$. □

Remark 8.2.4. Geometrically the zero set of Jac_k is a union of subspaces of dimension less than k, which are pointwise fixed by some subgroup of G. For example if $G \leq \mathrm{SL}_3(\mathbb{C})$ is the symmetry group of a platonic solid, these are the symmetry axes.

Consider G to be a finite, unitary reflection group. In this case it is possible to give a more specific description of the prime components of the radical of Jac_k. Specifically for $k = n$ one obtains a description of the factorization of the Jacobian determinant, which is a well known result of Steinberg [Ste60]. This result is also mentioned in [Bay04, 3.2 Proposition 6], but the proof is less transparent.

Proposition 8.2.5. *The prime components of the radical of Jac_k are the ideals corresponding to $(k-1)$-dimensional fixed point spaces under subgroups of the finite, unitary reflection group G.*

Proof. From corollary (8.2.3) one knows that only ideals corresponding to fixed point spaces with a dimension less than k occur in the primary decomposition. Hence it remains to show that every fixed point space with a dimension less than $k-1$ lies in a $k-1$ dimensional fixed point space. Assume that X is a fixed point space of dimension $k-l$ with $1 < l < k$. It is well known that X can be obtained as an intersection of $n-k+l$ independent reflection hyperplanes [OT92, Theorem 6.27]. Taking the intersection of only $n-k+1$ of those hyperplanes, one gets a $k-1$ dimensional fixed point space containing X. □

Remark 8.2.6. It is clear that (8.2.5) does not hold for non reflection groups. For example it fails for the 2-dimensional rational irreducible representation of the cyclic group of order 4.

Assume that G is an arbitrary finite subgroup of $\mathrm{GL}_n(K)$. To determine the orbit type stratification of V, we will compute a set of representatives of the conjugacy classes of subgroups appearing as point stabilizers. From corollary (8.2.3) it follows that one has to do the following steps for $1 \leq k \leq n$:

- Compute the prime components of the radical of Jac_k (cf. [BW93]).
- Find representatives of the G-orbits on this set.
- For all representatives P, choose a generic point p of the zero set $\mathcal{V}(P)$ that is a point with $\mathrm{Fix}_{G_p}(K^{n\times 1}) = \mathcal{V}(P)$

The stabilizers of the generic points are the desired representatives.

This procedure should be compared with the algorithms proposed in [Bay04, Section 4]. The first step, that is the decomposition of the radical of Jac_k, is the same in both algorithms. Apart from computing a set of fundamental invariants this is the main bottleneck of this approach. This is because there might be many prime components, although all of them are linear.

Finding generic points can be compared to the orbit length computation in [Bay04]. Bayer used commutative algebra for this. Generic points can easily be found by choosing "random" points in the spaces $\mathcal{V}(P)$ and computing the intersection of stabilizers in G of those points.

We shortly mention a group theoretic application: If G is a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$. In this case the orbit type stratification can be used to describe how the $\mathbb{F}_q G$-module $\mathbb{F}_q \otimes \mathbb{Z}^{n\times 1}$ decomposes into G orbits (cf. [PP87]) for any prime q.

The following example shows the difficulty when lots of prime components are involved.

Example 8.2.7. Consider the the finite unitary reflection group denoted G_{31} in Shephard-Todd [ST54] given as a matrix group in (7.9.1). As an abstract group it is an extension of

$$\mathrm{C}_4 \curlyvee (\mathrm{D}_8 \curlyvee \mathrm{Q}_8)$$

by the symmetric group S_6.

The degrees of the fundamental invariants are $8, 10, 20, 24$ and the subgroups appearing as stabilizers can be found in [OT92, Appendix C]. Using theorem

(8.2.5) the primary decomposition of the radical of Jac_k for $1 \leq k \leq 4$ is completely determined. However, trying to compute this decomposition with MAGMA ([BCP97]) for $k = 2$ and 3 was stopped after 3 days. This is mainly because the radical of Jac_2 has 1500 and of Jac_3 has 710 prime components.

The example shows that one has to provide more group theoretic information. Compute the fixed space $\mathrm{Fix}(g_\nu)$ of a set of representatives g_ν of the conjugacy classes of prime order elements. Denote the corresponding ideals I_{g_ν} and define $\mathrm{Jac}_{k,\nu}$ as the ideal generated by Jac_k and I_{g_ν}. Compute the prime components of the radical of $\mathrm{Jac}_{k,\nu}$ for every k, ν.

It is clear that the G orbit of every fixed point space has a representative contained in some $\mathrm{Fix}(g_\nu)$. Another way to say this is that every prime component of the radical of Jac_k can be found in the G-orbit of a component of the radical of $\mathrm{Jac}_{k,\nu}$. So one obtains the desired primary decomposition.

Remark 8.2.8. Geometrically this method works by restricting to representatives of the fixed spaces that are maximal with respect to inclusion. The advantage of this comes from the observation that the number of fixed spaces, which are contained in a fixed representative, is significantly smaller than in the whole space.

Example 8.2.9. Consider example (8.2.7) again. Since G is a finite unitary reflection group the maximal, with respect to inclusion, fixed spaces are the reflection hyperplanes. Note that there is only one conjugacy class of reflections in G_{31}, so it is enough to consider just one hyperplane. The zero set of $\langle x_1 \rangle$ is such a hyperplane and with this choice MAGMA is now able to compute the primary decomposition of the radical of $\langle \mathrm{Jac}_k, x_1 \rangle$ for $k = 2$ and 3, respectively. One sees that for $k = 2$ there are 127 and for $k = 3$ there are 31 prime components, which is significantly less compared to the 1500 and prime components of Jac_2 and the 710 of Jac_3, respectively. From these data one recomputes the table of [OT92, Appendix C].

Consider the modular case and recall remark (8.1.3). It is clear that one cannot expect corollary (8.2.3) to hold in this case. The special case $k = n$ remains true, since $\dim(\mathrm{Fix}_G(V)) = n$ if and only if the group G is trivial.

Corollary 8.2.10. *The radical of* Jac_n *is the ideal corresponding to* $V_{\leq n-1}$.

Remark 8.2.11. In other words the last corollary says that a point p has a non trivial stabilizer if and only if the rank of the Jacobian evaluated at p is less then n.

It might also happen that the radical of Jac_k is the same for all $k \in \{1...n\}$. The following example shows such a case.

Example 8.2.12. Let $G = \mathrm{GL}_3(\mathbb{F}_3)$ in its natural representation and $V := \overline{\mathbb{F}_3}^3$ the natural module. The Dickson invariants are a system of fundamental invariants. Use MAGMA to see that prime components of the radical of Jac_k for $k \in \{1, 2, 3\}$ are the ideals corresponding to the 13 subspaces of dimension 2 spanned by elements of $\mathbb{F}_3^3$. Note that for every such 2-dimensional subspace the dual representation of the pointwise stabilizer has no non trivial fixed points. Hence those subspaces must appear as prime components of the radical of all the Jac_k.

In this case it is better to work with the ideals Jac_k and not with their radicals. If one does so, then Jac_1 contains all non-zero points of $\mathbb{F}_3^3$ as embedded components and zero appears as an embedded component of Jac_2.

Bibliography

[AD09] Michela Artebani and Igor Dolgachev. The Hesse pencil of plane cubic curves. *Enseign. Math. (2)*, 55(3-4):235–273, 2009.

[AS83] M. Abud and G. Sartori. The geometry of spontaneous symmetry breaking. *Ann. Physics*, 150(2):307–372, 1983.

[Bay04] Thomas Bayer. Optimal descriptions of orbit spaces and strata of finite groups. *ISSAC 2004*, pages 19–26, 2004.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Bli17] Hans Frederik Blichfeldt. *Finite collineation groups, with an introduction to the theory of groups of operators and substitution groups.* Chicago, Ill., The University of Chicago Press, 1917.

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[BZ85] H. Benz and H. Zassenhaus. Über verschränkte Produktordnungen. *J. Number Theory*, 20(3):282–298, 1985.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups.* Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[CS99] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[Die51] Jean Dieudonné. On the automorphisms of the classical groups. With a supplement by Loo-Keng Hua. *Mem. Amer. Math. Soc.,*, 1951(2):vi+122, 1951.

[DK02] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[Dré04] Jean-Marc Drézet. Luna's slice theorem and applications. In *Algebraic group actions and quotients*, pages 39–89. Hindawi Publ. Corp., Cairo, 2004.

[Elk99] Noam D. Elkies. The Klein quartic in number theory. In *The eightfold way*, volume 35 of *Math. Sci. Res. Inst. Publ.*, pages 51–101. Cambridge Univ. Press, Cambridge, 1999.

[GS06] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[Hen09] Michael Hentschel. *On Hermitian theta series and modular forms*. PhD thesis, RWTH, 2009.

[Hup67] B. Huppert. *Endliche Gruppen. I*. Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[Isa76] I. Martin Isaacs. *Character theory of finite groups*. Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. Pure and Applied Mathematics, No. 69.

[Jam] Sebastian Jambor. An L_3-U_3-quotient algorithm. *In preparation*.

[Jon11] Jan Jongen. The Brauer-Clifford group and rational forms of finite groups. *J. Algebra*, 335:282–300, 2011.

[Kle72] Felix Klein. Ueber Liniengeometrie und metrische Geometrie. *Math. Ann.*, 5(2):257–277, 1872.

[Kle79] Felix Klein. Ueber die transformation elfter ordnung der elliptischen functionen. *Mathematische Annalen*, 15:533–555, 1879. 10.1007/BF02086276.

[Kle87] Felix Klein. Zur Theorie der allgemeinen Gleichungen sechsten und siebenten Grades. *Math. Ann.*, 28(4):499–532, 1887.

[Kle93] Felix Klein. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*. Birkhäuser Verlag, Basel, 1993. Reprint of the 1884 original, Edited, with an introduction and commentary by Peter Slodowy.

[Kle99] Felix Klein. On the order-seven transformation of elliptic functions. In *The eightfold way*, volume 35 of *Math. Sci. Res. Inst. Publ.*, pages 287–331. Cambridge Univ. Press, Cambridge, 1999. Translated from the German and with an introduction by Silvio Levy.

[KM90] Noriaki Kawanaka and Hiroshi Matsuyama. A twisted version of the Frobenius-Schur indicator and multiplicity-free permutation representations. *Hokkaido Math. J.*, 19(3):495–508, 1990.

[Kne57] Martin Kneser. Klassenzahlen definiter quadratischer Formen. *Arch. Math.*, 8:241–250, 1957.

[Kün04] Matthias Künzer. On representations of twisted group rings. *J. Group Theory*, 7(2):197–229, 2004.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[Mas87] Heinrich Maschke. Ueber die quaternäre, endliche, lineare Substitutionsgruppe der Borchardt'schen Moduln. *Math. Ann.*, 30(4):496–515, 1887.

[Mas89] Heinrich Maschke. Aufstellung des vollen Formensystems einer quaternären Gruppe von 51840 linearen Substitutionen. *Math. Ann.*, 33(3):317–344, 1889.

[MM] I. Marin and J. Michel. Automorphisms of complex reflection groups. *To appear in Representation Theory.*

[MM64] Hideyuki Matsumura and Paul Monsky. On the automorphisms of hypersurfaces. *J. Math. Kyoto Univ.*, 3:347–361, 1963/1964.

[Neb] Gabriele Nebe. An even unimodular 72-dimensional lattice of minimum 8. *J. Reine und Angew. Math.*

[Neb96] Gabriele Nebe. Finite subgroups of $\mathrm{GL}_{24}(\mathbf{Q})$. *Experiment. Math.*, 5(3):163–195, 1996.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NP95] G. Nebe and W. Plesken. Finite rational matrix groups. *Mem. Amer. Math. Soc.*, 116(556):viii+144, 1995.

[NS36] T. Nakayama and K. Shoda. Über die Darstellung einer endlichen Gruppe durch halblineare Transformationen. *Japan. J. Math.*, 12:109–122, 1936.

[OT92] Peter Orlik and Hiroaki Terao. *Arrangements of hyperplanes*, volume 300 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1992.

[Ple83] Wilhelm Plesken. *Group rings of finite groups over p-adic integers*, volume 1026 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1983.

[PP87] H. Pahlings and W. Plesken. Group actions on Cartesian powers with applications to representation theory. *J. Reine Angew. Math.*, 380:178–195, 1987.

[PS85] Claudio Procesi and Gerald Schwarz. Inequalities defining orbit spaces. *Invent. Math.*, 81(3):539–554, 1985.

[Que95] H.-G. Quebbemann. Modular lattices in Euclidean spaces. *J. Number Theory*, 54(2):190–202, 1995.

[Rei75] I. Reiner. *Maximal orders*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975. London Mathematical Society Monographs, No. 5.

[Sat71] I. Satake. *Classification theory of semi-simple algebraic groups*. Marcel Dekker Inc., New York, 1971. With an appendix by M. Sugiura, Notes prepared by Doris Schattschneider, Lecture Notes in Pure and Applied Mathematics, 3.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[Sho38a] Kenjiro Shoda. Über die Äquivalenz der Darstellungen endlicher Gruppen durch halblineare Transformationen. *Proc. Imp. Acad.*, 14(8):278–280, 1938.

[Sho38b] Kenjiro Shoda. Über die Invarianten der endlichen Gruppen halblinearer Transformationen. *Proc. Imp. Acad.*, 14(8):281–285, 1938.

[SS83] M. A. Shahabi Shojaei. Schur indices of irreducible characters of SL(2, q). *Arch. Math. (Basel)*, 40(3):221–231, 1983.

[ST54] G. C. Shephard and J. A. Todd. Finite unitary reflection groups. *Canadian J. Math.*, 6:274–304, 1954.

[Ste60] Robert Steinberg. Invariants of finite reflection groups. *Canad. J. Math.*, 12:616–618, 1960.

[Tei40] Oswald Teichmüller. Über die sogenannte nichtkommutative Galoissche Theorie und die Relation $\xi_{\lambda,\mu,\nu}\xi_{\lambda,\mu\nu,\pi}\xi^{\lambda}_{\mu,\nu,\pi} = \xi_{\lambda,\mu,\nu\pi}\xi_{\lambda,\mu,\nu,\pi}$. *Deutsche Math.*, 5:138–149, 1940.

[Tur94a] Alexandre Turull. Clifford theory with Schur indices. *J. Algebra*, 170(2):661–677, 1994.

[Tur94b] Alexandre Turull. Clifford theory with Schur indices. *J. Algebra*, 170(2):661–677, 1994.

[Tur00] Alexandre Turull. Clifford theory for cyclic quotient groups. *J. Algebra*, 227(1):133–158, 2000.

[Tur09a] Alexandre Turull. Brauer-Clifford equivalence of full matrix algebras. *J. Algebra*, 321(12):3643–3658, 2009.

[Tur09b] Alexandre Turull. The Brauer-Clifford group. *J. Algebra*, 321(12):3620–3642, 2009.

[VP89] È. B. Vinberg and V. L. Popov. Invariant theory. In *Algebraic geometry, 4 (Russian)*, Itogi Nauki i Tekhniki, pages 137–314, 315. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989.

[Wil83] Clarence Wilkerson. A primer on the Dickson invariants. In *Proceedings of the Northwestern Homotopy Theory Conference (Evanston, Ill., 1982)*, volume 19 of *Contemp. Math.*, pages 421–434, Providence, RI, 1983. Amer. Math. Soc.

[Wim96] A. Wiman. Ueber eine einfache Gruppe von 360 ebenen Collineationen. *Math. Ann.*, 47:531–556, 1896.