

ABSTRACT

KIM, MOSES. On Galois 2-extensions of the Dihedral Group. (Under the direction of Amassa Fauntleroy.)

We give a criteria for solvability of the embedding problem $(E/k, D_n, \mu_2)$ by considering an identification of S_m in the orthogonal group $O_m = O(m \times \langle 1 \rangle)$ and restricting the 2-cocycle corresponding to the 2-extension of S_m to the group D_n (where $\#D_n = 2n = m$), which allows us to compute the obstruction of the embedding in an explicit way using Serre's obstruction formula. We will make heavy use of Galois cohomology in the context of pro-finite group cohomology as well as the general theory of quadratic forms to prove Serre's formula and hence give a criteria for solvability.

© Copyright 2012 by Moses Kim

All Rights Reserved

On Galois 2-extensions of the Dihedral Group

by
Moses Kim

A thesis submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Mathematics

Raleigh, North Carolina

2012

APPROVED BY:

Bojko Bakalov

Thomas Lada

Amassa Fauntleroy
Chair of Advisory Committee

DEDICATION

To my parents.

BIOGRAPHY

The author was raised in Santo Domingo, Dominican Republic, and given a bilingual education at New Horizons Bilingual School, graduating in 2004. He graduated from Davidson College in 2009 earning a Bachelor of Science degree in Mathematics. After some thought, he decided to enroll in the Master of Science program in Mathematics at North Carolina State University in 2010. His experience at NC State has been a good one, forming friendships and learning advanced mathematics.

ACKNOWLEDGEMENTS

I am grateful for the help given to me from all of my committee members: Amassa Fauntleroy, Bojko Bakalov, and Thomas Lada. I would also like to express gratitude for the friendships that I formed during my stay here, especially Austin Jones and George Lankford. I would also like to mention Ernest Stitzinger for answering technical questions about the program that I needed to know in order to finish the M.S. program without any abrupt transitions. Thank you all.

TABLE OF CONTENTS

Chapter 1 Introduction	1
Chapter 2 Galois Cohomology	5
2.1 Profinite Groups	5
2.2 Galois Cohomology Functor	10
2.3 Galois Descent	16
2.4 Étale and Galois Algebras	20
2.5 Group Extensions	22
Chapter 3 Quadratic Forms	26
3.1 Basics	26
3.2 Orthogonal groups and Clifford algebras	30
3.3 Galois cohomology of quadratic forms	34
3.4 Trace forms under Galois extensions	37
Chapter 4 Results	41
4.1 Quadratic Forms and Étale algebras	41
4.2 Serre's formula	42
4.3 2-extensions of D_n	45
References	48

Chapter 1

Introduction

The embedding problem is a particular case of the inverse Galois problem in Galois theory that asks the following question: given a group G that is Galois over some extension K/F and the epimorphism

$$\gamma : E \rightarrow G$$

does there exist a field extension K' of F such that the following two conditions are satisfied:

- i. $K' \supset K$ and $E = Gal(K'/F)$
- ii. $\gamma(x) = x \mid_K$

We can express the above problem in the language of group extensions. The only distinction being that we specify the nature of the normal subgroups of E via a monomorphic map $\iota : A \rightarrow E$ in the following sense:

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\gamma} G \longrightarrow 1$$

By the exactness at E , $\iota(A) \triangleleft E$. Moreover, if we assume that A is a G -module such that $\phi : G \rightarrow Aut(A)$ is the corresponding representation, the action of G extends to an action of E via inner automorphisms on A in the following way:

$$x \cdot a = x\iota(a)x^{-1} = \iota(\phi(\gamma(x))a) \text{ for all } x \in E, a \in A$$

This action is going to play an important role in defining the concept of equivalence of group extensions later on in Chapter 2.

We will follow the methodology of Berhuy's book [2] to tackle the embedding problem in the context of Galois cohomology and quadratic forms.

One important step we need to make before discussing in depth the techniques in Galois cohomology as it relates to the embedding problem is the isomorphism between groups extensions of G by A and 2-cocycles of G with values in A , with the assumption that A is a G -module. In our study of the embedding problem we will take G to be the Galois group of the separable extension k_s of a field k and let G act trivially on A . It is a well known theorem by Cayley, that any finite group can be represented as a group of permutations. Techniques in group cohomology allow us to study a cocycle of H , where H is a subgroup of G , by looking at the cocycles of G and restricting the domain to that of H . In this thesis, we study 2-extensions of D_n by restriction of S_n , where our groups are Galois over a separable extension of k , with $\text{char}k \neq 2$. Before we consider an embedding of a given group, we first look at its Galois correspondence to a field, say E , over the base field k . Because of the nature of S_n , we can indeed find a separable extension over which the group S_n is Galois. So it makes sense to focus our attention on this particular separable extension, which by definition, is an Étale algebra. Using the Krull topology on Galois groups, we find a Galois closure of E and denote it by E^{gal} . It will be clear in the context of infinite Galois theory that $Gal(E/k) = Gal(E^{gal}/k)$. We will denote this group by G_E .

As a consequence of abstract Galois descent, we have the following isomorphism of functors over k .

$$\begin{aligned} H^1(-, S_n) &\cong Et_n(-) \\ H^1(-, G) &\cong G-Gal(-) \end{aligned}$$

The first isomorphism is between 1-cocycles with values in S_n and Étale algebras of degree n ; and the second, between 1-cocycles with values in G and G -Galois algebras.

Let $e : \mathcal{G}_{k_s} \rightarrow S_n$ represent the Étale algebra E . By construction,

$$\text{im } e = \text{Gal}\left(\bigcup_{\chi \in X(E)} \chi(E)\right) = \text{Gal}(E^{gal}/k) = G_E, \text{ where } X(E) = \text{Hom}_{k\text{-alg}}(E, k_s)$$

So we obtain another map $f : \mathcal{G}_{k_s} \rightarrow G_E$ that represents the Galois algebra E^{gal} . Now using the above definitions, we may interpret the conditions for solvability as follows.

Given the group extension:

$$1 \longrightarrow A \longrightarrow G' \xrightarrow{\pi} G \longrightarrow 1$$

with corresponding 2-cocycle class $[c] \in H^2(G, A)$ and a surjective continuous morphism $f : \mathcal{G}_{k_s} \rightarrow G$, does there exist a morphism $f' : \mathcal{G}_{k_s} \rightarrow G'$ such that $\pi \circ f' = f$. Assuming that the action of G_{k_s} on A , G , and G' is trivial and applying the functor $H^*(k, -) := H^*(\mathcal{G}_{k_s}, -)$ to the above extension, we obtain

$$\cdots \longrightarrow H^1(k, G') \xrightarrow{\pi_*} H^1(k, G) \xrightarrow{\delta^1} H^2(k, A) \longrightarrow \cdots$$

By exactness at $H^1(k, G)$, $\pi \circ f' = f$ iff $f \in \text{im } \pi_*$ iff $\delta^1(f) = 0$. By group cohomology, we have the following equality

$$f^*(c) = \delta^1(f) \pmod{B^2(k, A)},$$

where $B^2(k, A)$ is the set of 2-coboundaries. $f^*(c)$ is known as the obstruction to the embedding problem.

We obtain the obstruction to the embedding problem:

$$1 \longrightarrow \mu_2(k_s) \longrightarrow \tilde{D}_n \longrightarrow D_n \longrightarrow 1$$

by restricting the 2-cocycle $s_m \in H^2(S_m, \mu_2)$ to D_n , where $\#D_n = m$, which implies the commutativity of the following diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mu_2(k_s) & \longrightarrow & \tilde{D}_n & \longrightarrow & D_n \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \mu_2(k_s) & \longrightarrow & \tilde{S}_m & \longrightarrow & S_n \longrightarrow 1 \end{array}$$

By group cohomology, we have the following:

$$f^*(Res(s_m)) = e^*(s_m) \pmod{B^2(k, \{\pm 1\})}$$

We will use tools in Galois cohomology and quadratic forms to compute the above obstruction $e^*(s_m)$. By identifying S_m with a subgroup of the orthogonal group O_m , we will be able to reduce the computation of the obstruction to a computation of quadratic forms of \AA tale algebras. And in so doing we obtain the obstruction formula due to Serre. This formula reduces the solvability of the embedding problem to finding quadratic forms of Galois extensions. We go over this aspect in detail in Chapter 3 before proving the obstruction formula and obtaining specific cases of 2-extensions of D_n for particular values of n in Chapter 4.

Chapter 2

Galois Cohomology

In order to introduce Galois cohomology we first need to make a foray into the theory of profinite groups G . Defining a G -action on a set A will induce morphisms from $G^{\times n}$ to A and putting constraints on these morphisms will produce cohomology sets $H^n(G, A)$. The Galois group of a field extension K/k is a profinite group with order being inclusion of sets and it is but natural to define an action of the Galois group on the set of field extensions as induced by group automorphisms. We will focus our attention on $H^1(G, _)$. In order to see how G -sets and $H^1(G, _)$ interact, we introduce the notion of group schemes and their action; this will be the subject of Galois descent. We will introduce Étale and Galois algebras and their properties as a consequence of Galois descent, which will be crucial in our interpretation of the embedding problem in the context of group extensions.

2.1 Profinite Groups

We first need a few basic definitions before we define profinite groups.

Definition 2.1.1 Given a partially ordered set $(I, <)$, I is said to be a directed set if $\forall i, j \in I$, there exists $k \in I$ such that $i < k, j < k$.

Definition 2.1.2 The collection of sets $(X_i)_{i \in I}$ together with maps $\pi_{ij} : X_j \rightarrow X_i$, where I is a directed set, is called a projective system of sets if the following properties are satisfied:

- i. $\pi_{ii} = id_{X_i}, \forall i \in I$

ii. $\pi_{ki} \circ \pi_{ij} = \pi_{kj}, \forall i, j, k \in I$

Definition 2.1.3 The inverse limit of a projective system of sets $(X_i)_{i \in I}$ is denoted by

$$\varprojlim_i X_i = \{(x_i)_{i \in I} \in \prod_i X_i \mid \pi_{ij}(x_j) = x_i, \forall i < j\},$$

where $\prod_i X_i$ is endowed with the product topology and the X_i are discrete.

Definition 2.1.4 We say that a topological group G is profinite if there exists a projective set of finite groups $(H_i)_{i \in I}$ such that

$$G \cong \varprojlim_i H_i$$

The set of field extensions over some base field k with partial order \subseteq is a directed set. Given an extension L/k , define $X_L = Gal(L/k)$. Moreover, define the map $\pi_{K,F} : X_F \rightarrow X_K$ by $\sigma \mapsto \sigma|_K$, where K is a subextension of F . Going over the above definition, we can easily see that the pair $((X_L), (\pi_{F,F'}))$ is a projective system of finite groups, mainly Galois groups of extensions. We immediately have an isomorphism of topological groups

$$Gal(\Omega/k) \cong \varprojlim_{L \subset \Omega} Gal(L/k)$$

Before discussing the concept of G -sets and G -groups. where G is profinite, we briefly discuss the topology we are working with on the set of Galois groups.

Definition 2.1.5 The Krull topology on $Gal(L/k)$ is given by the open neighborhoods:

$$\{\sigma Gal(L/L') \mid \sigma \in Gal(L/k) \text{ and } k \subset L' \subset L\}$$

To describe G -sets, we need to define what we mean by a continuous G -action.

Definition 2.1.6 Given a discrete topological space A and a profinite group G , we say that the left action of G is continuous if the subgroup

$$Stab_G a = \{g \in G \mid g \cdot a = a\}$$

is open for all $a \in A$.

An alternative characterization of the continuous left action of a profinite group G on a discrete topological space A is given by the following lemma.

Lemma 2.1.7 The left action of G on A is continuous if and only if the following equality holds:

$$A = \bigcup_U A^U,$$

where the U are normal and open in G .

All such A with a continuous left G -action are called G -sets. Furthermore, if A is a group and the G -action is given by group morphisms, then A is said to be a G -group. Commutative G -groups are called G -modules.

Examples 2.1.8

- i. If G acts trivially on A , A automatically becomes a G -set.
- ii. Given a Galois extension L/k with Galois group $\mathcal{G}_L = Gal(L/k)$, the action

$$\sigma \cdot l = \sigma(l), \forall \sigma \in \mathcal{G}_L, l \in L$$

gives L the structure of a \mathcal{G}_L -group.

Definition 2.1.9 Let A be a G -group. A continuous morphism $\alpha : G \rightarrow A$ is called a 1-cocycle if the following holds:

$$\alpha_{\sigma\tau} = \alpha_\sigma \sigma \cdot \alpha_\tau, \forall \sigma, \tau \in G$$

The set of 1-cocycles of G with values in A is denoted by $Z^1(G, A)$.

Lemma 2.1.10 If $\alpha : G \rightarrow A$ is a 1-cocycle, then so is $\beta : G \rightarrow A$ given by

$$\sigma \mapsto a\alpha_\sigma \sigma \cdot a^{-1} \text{ for some } a \in A$$

We refer the reader to [2, II.3] for the proof of the above lemma.

Definition 2.1.11 Given 1-cocycles $\alpha, \beta : G \rightarrow A$, we say that α is cohomologous to β if there exists $a \in A$ such that

$$\beta_\sigma = a\alpha_\sigma \sigma \cdot a^{-1}, \forall \sigma \in G$$

Being cohomologous is an equivalence relation. Let us denote it by \sim . We call the quotient of the set $Z^1(G, A)$ by \sim the first cohomology set of G with values in A and denote it by

$$H^1(G, A) = Z^1(G, A) / \sim$$

Now we are ready to define higher cohomology sets in the more general setting of cochain complexes using the notation $(C^*(G, A), d)$. Given a G -module A we define $C^n(G, A)$ to be the set of continuous morphisms $\alpha : G^{\times n} \rightarrow A$ for $n \geq 1$ and define $C^0(G, A) = A$. The coboundary operator $d_n : C^n(G, A) \rightarrow C^{n+1}(G, A)$ is given by

$$d_n(\alpha)_{\sigma_1, \sigma_2, \dots, \sigma_{n+1}} = \sigma_1 \cdot \alpha_{\sigma_2, \dots, \sigma_{n+1}} + \sum_{i=1}^n (-1)^i \alpha_{\sigma_1, \sigma_2, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_{n+1}} + (-1)^{n+1} \alpha_{\sigma_1, \sigma_2, \dots, \sigma_n}$$

Thus, we obtain:

$$H^n(G, A) = \ker d_n / \text{im } d_{n-1}$$

The reader will take note that cohomology sets $H^n(G, A)$ behave functorially in A or G as the case arises. First we define what we mean by compatible maps in the setting of G -sets.

Definition 2.1.12 Given profinite groups G, G' and a G -set A and a G' -set A' , we call the maps $\phi : G' \rightarrow G$ and $f : A \rightarrow A'$ compatible if the following holds.

$$f(\phi(\sigma') \cdot a) = \sigma' \cdot f(a), \forall a \in A, \sigma' \in G'$$

Lemma 2.1.13 Keeping the notation from the above definition for G, G', A , and A' , we have the following well-defined map of pointed sets:

$$f_* : H^n(G, A) \rightarrow H^n(G', A'),$$

which is given by:

$$f_*(\alpha)_{\sigma'_1, \dots, \sigma'_n} = f(\alpha_{\phi(\sigma'_1), \dots, \phi(\sigma'_n)})$$

Now suppose G and G' are finite groups such that $G' < G$ and let A be a G -group. Then, it is natural to consider the inclusion morphism $\iota : G' \rightarrow G$ and the identity map $id : A \rightarrow A$. By lemma 2.1.13, setting $\phi = \iota$ and $f = id$, we obtain the following map

$$Res : H^n(G, A) \rightarrow H^n(G', A),$$

which we call the restriction map.

In the case where G and G' are profinite groups with given morphisms $\phi : G' \rightarrow G$ and $f = id : A \rightarrow A$, we use the following notation:

$$\phi^* : H^n(G, A) \rightarrow H^n(G', A)$$

Now we introduce a useful binary operation on the set of cohomology sets.

Let A and B be G -modules, where G is some profinite group. The continuous action of G on both A and B induces a continuous action on their tensor product $A \otimes_{\mathbb{Z}} B$ given by

$$G \times A \otimes_{\mathbb{Z}} B \rightarrow A \otimes_{\mathbb{Z}} B : (\sigma, a \otimes b) \mapsto \sigma \cdot (a \otimes b) = \sigma \cdot a \otimes \sigma \cdot b$$

Given the cocycles $\alpha \in Z^p(G, A)$ and $\beta \in Z^q(G, B)$, we define the following map.

$$\cup : Z^p(G, A) \times Z^q(G, B) \rightarrow Z^{p+q}(G, A \otimes B)$$

given by

$$(\alpha, \beta) \mapsto \alpha \cup \beta : (\sigma_1, \dots, \sigma_p, \sigma_{p+1}, \dots, \sigma_{p+q}) \mapsto \alpha_{\sigma_1, \sigma_2, \dots, \sigma_p} \otimes \sigma_1 \cdots \sigma_p \cdot \beta_{\sigma_{p+1}, \dots, \sigma_{p+q}}$$

Computation with the coboundary operator d_{p+q} shows that the induced map

$$\cup : H^p(G, A) \times H^q(G, B) \rightarrow H^{p+q}(G, A \otimes B)$$

is well-defined.

By identifying $A \otimes_{\mathbb{Z}} B$ with $B \otimes_{\mathbb{Z}} A$ as G -modules we have the following anti-commutative

rule:

$$[\alpha] \cup [\beta] = (-1)^{pq} [\beta] \cup [\alpha],$$

which gives a grading to the cohomology ring.

The binary operation \cup is called the cup product. Now, given G -modules A , B , and C , consider the \mathbb{Z} -bilinear map $\theta : A \times B \rightarrow C$ satisfying

$$\theta(\sigma \cdot a, \sigma \cdot b) = \sigma \cdot \theta(a, b), \quad \forall a \in A, b \in B, \sigma \in G$$

By the above condition, the map θ induces a \mathbb{Z} -bilinear map of G -modules: $A \otimes_{\mathbb{Z}} B \rightarrow C$, which also induces a morphism in cohomology as follows:

$$\theta_* : H^n(A \otimes B) \rightarrow H^n(G, C) : [\alpha] \mapsto [\theta \circ \alpha]$$

Composing \cup with θ_* , we obtain the map:

$$\cup_{\theta} : H^p(G, A) \times H^q(G, B) \rightarrow H^{p+q}(G, C) : ([\alpha] \cdot [\beta]) \mapsto \theta_*([\alpha \cup \beta]) = [\theta \circ (\alpha \cup \beta)],$$

which we call the cup product with respect to θ .

2.2 Galois Cohomology Functor

In the previous section, we showed that $\mathcal{G}_L = \text{Gal}(L/k)$ was a profinite group and that it acted continuously on a discrete set, mainly a field. By defining a group-valued functor we are able to define new G_L -groups. First, we need a few definitions.

Definition 2.2.1 A group scheme is a covariant functor from the category of algebraic extensions over some field k to the category of groups.

The following are some examples of group schemes that we shall encounter later:

- i. $\mu_m(L) = \{x \in L^\times \mid x^m = 1\}$
- ii. $GL(V)(L) = \{f : V_L \rightarrow V_L \mid f \text{ is a linear}\}$, where V is a vector space.
- iii. $O(V)(L) = \{f \in GL(V)(L) \mid q_R = q_R \circ f\}$, where (V, q) is a quadratic form over k

Observe that a group scheme is a subfunctor of the following functor

$$F : C_k \rightarrow Gps$$

from the category of field extensions over k to the category of groups. So it is enough to describe the induced continuous action of G_L on the L -points of the functor F .

It is useful to introduce some notation to simplify computation. For any inclusion of fields $\iota : L \rightarrow L'$, the image of $s \in F(L)$ under $F(\iota)$ will be denoted by $s_{L'}$.

Lemma 2.2.2 Let $F : C_k \rightarrow Gps$ be a covariant functor. The following map

$$G_L \times F(L) \rightarrow F(L) : (\sigma, s) \mapsto \sigma \cdot s = F(\sigma)(s)$$

induces an action of $G_L = Gal(L/k)$ on $F(L)$. Moreover, given the inclusion of fields $\iota : L \rightarrow L'$, we have the following equality

$$\sigma' \cdot s_{L'} = (\sigma' |_L \cdot s)_{L'}, \forall \sigma' \in G_{L'}, s \in F(L)$$

Proof. Let $s \in F(L)$. By the functoriality of F , observe that

$$id_L \cdot s = F(id_L)(s) = id_{F(L)}(s) = s$$

$$(\sigma\tau) \cdot s = F(\sigma\tau)(s) = F(\sigma)F(\tau)(s) = \sigma \cdot (\tau \cdot s), \forall \sigma, \tau \in G_L, s \in F(L)$$

Let L, L' be Galois extensions over k such that $L \subset L'$. Consider the commutative diagram below:

$$\begin{array}{ccc} L & \xrightarrow{\iota} & L' \\ \sigma' |_L \downarrow & & \downarrow \sigma' \\ L & \xrightarrow{\iota} & L' \end{array}$$

Applying the functor F to the above diagram induces the following commutative diagram:

$$\begin{array}{ccc}
F(L) & \xrightarrow{F(\iota)} & F(L') \\
F(\sigma' |_L) \downarrow & & \downarrow F(\sigma') \\
F(L) & \xrightarrow{F(\iota)} & F(L')
\end{array}$$

In other words, given $s \in F(L)$ and $\sigma' \in G_{L'}$,

$$\sigma' \cdot s_{L'} = F(\sigma')F(\iota)(s) = F(\iota)F(\sigma' |_L)(s) = (\sigma' |_L \cdot s)_{L'}$$

□

Let us remark that if we further assume that F is a group-valued functor then it immediately follows that $F(\sigma)$ is a group morphism for all $\sigma \in G_L$ and hence we have an action by group morphisms. Thus, in this particular case, $F(L)$ is a G_L -group.

Definition 2.2.3 A group scheme $F : Alg_k \rightarrow Gps$ is a Galois functor if the following two properties hold:

- i. The inclusion $F(L) \hookrightarrow F(L')$ induces the isomorphism

$$F(L) \cong F(L')^{Gal(L'/L)}$$

- ii. Given a Galois extension L' over k

$$F(L') = \bigcup_L \iota_{L,L'}(L),$$

where $\iota_{L,L'} : G(L) \rightarrow G(L')$ is induced by the inclusion $L \subset L'$

If properties i. and ii. hold, Lemma 2.1.7 implies that the action of G_L on $F(L)$ given by

$$G_L \times F(L) \rightarrow F(L) : (\sigma, l) \mapsto \sigma \cdot l = F(\sigma)(l)$$

is continuous. Moreover, since F is a group scheme, the above action is given by group morphisms. Thus, $F(L)$ is a G_L -group. By the steps in the previous section, we may now consider the set $H^n(G_L, F(L))$.

Consider the map $\bar{\phi} : Gal(\Omega'/L') \rightarrow Gal(\Omega/L)$ given by the equality $\tau \circ \phi = \phi \circ \bar{\phi}(\tau)$, where $\phi : \Omega \rightarrow \Omega'$ is an extension of the inclusion $L \hookrightarrow L'$ of field extensions over k and $\tau \in Gal(\Omega'/L')$. By construction, our map $\bar{\phi}$ is well-defined.

Now we turn our attention towards the cohomology set $H^n(\mathcal{G}_L, F(L))$. Consider the compatible maps $\bar{\phi} : \mathcal{G}_{\Omega'} \rightarrow \mathcal{G}_{\Omega}$ and $F(\phi) : F(\Omega) \rightarrow F(\Omega')$.

By Lemma 2.1.13, we have the following induced map:

$$R_{\phi} : H^n(\mathcal{G}_{\Omega}, F(\Omega)) \rightarrow H^n(\mathcal{G}_{\Omega'}, F(\Omega'))$$

R_{ϕ} is a well-defined map of pointed sets that only depends on the inclusion map $L \hookrightarrow L'$. Thus, we may consider Galois groups over algebraic closures of fields as well as their separable extensions. Again, applying Lemma 2.1.13 together with the compatible maps $\bar{\phi} : \mathcal{G}_{L_s} \rightarrow \mathcal{G}_{K_s}$ and $F(\phi) : F(K_s) \rightarrow F(L_s)$, we have a well-defined map of pointed sets:

$$R_{\phi} : H^n(\mathcal{G}_{K_s}, F(K_s)) \rightarrow H^n(\mathcal{G}_{L_s}, F(L_s))$$

It is easily seen that we have $R_{\psi \circ \phi} = R_{\psi} \circ R_{\phi}$, where $\phi : K_s \rightarrow L_s$ and $\psi : L_s \rightarrow M_s$ are extensions of the inclusion maps $K \hookrightarrow L$ and $L \hookrightarrow M$. It immediately follows then that any cohomology set of a Galois extension L/k is isomorphic to the direct limit of its subextensions as shown below:

$$H^n(\mathcal{G}_{L'}, F(L')) \cong \varinjlim_L H^n(\mathcal{G}_L, F(L)),$$

where the L are subextensions of L' . Thus, we denote the Galois cohomology functor by:

$$H^n(-, F(-)) : C_k \rightarrow Sets$$

Definition 2.2.4 Given a Galois functor $F : Alg_k \rightarrow Gps$, the n^{th} cohomology set of F is denoted by:

$$H^n(L, F) = H^n(\mathcal{G}_{L_s}, F(L_s))$$

Recall that $\mu_m : Alg_k \rightarrow Gps$ is a group scheme given by $\mu_m(F) = \{x \in F^{\times} \mid x^m = 1\}$. Since our embedding problem concerns 2-extensions, it will be useful to consider the

functor:

$$H^1(-, \mu_2(-)) : \text{Alg}_k \rightarrow \text{Sets}$$

We state a version of Hilbert 90.

Theorem 2.2.5 (Hilbert's Theorem 90) The functor $H^1(-, \mathbb{G}_m(-)) : \text{Alg}_k \rightarrow \text{Sets}$ is trivial, where $\mathbb{G}_m(F) = F^\times$, for all field extensions F over k .

Here is an important consequence of Hilbert 90 that we shall use in our proofs later on.

Let Ω be Galois and cyclic over k of degree n with Galois group $\mathcal{G}_\Omega = \langle \gamma \rangle$. Consider the 1-cocycle $\alpha \in H^1(\mathcal{G}_\Omega, \Omega^\times)$. Since $\gamma^n = 1$ and α is a 1-cocycle, we have:

$$1 = \alpha_{\gamma^n} = \alpha_{\gamma^{n-1}\gamma} = \alpha_{\gamma^{n-1}}\gamma^{n-1} \cdot \alpha_\gamma = \alpha_{\gamma^{n-2}}\gamma^{n-2} \cdot \alpha_\gamma \gamma^{n-1} \cdot \alpha_\gamma = \prod_{i=1}^{n-1} \gamma^i \cdot \alpha_\gamma = N_{\Omega/k}(\alpha_\gamma)$$

Thus, $x \in \Omega^\times$ such that $N_{\Omega/k}(x) = 1$ completely determines the 1-cocycle given by

$$\alpha_{\gamma^m} = \prod_{i=1}^{m-1} \gamma^i \cdot x, \quad m = 0, 1, \dots, n-1$$

By Hilbert 90, we have that α is trivial, which means that there exists some element $a \in \Omega^\times$ such that $\alpha_\sigma = \frac{\sigma(a)}{a}$, $\forall \sigma \in \mathcal{G}_\Omega$. Replacing σ with the generator, we obtain $\alpha_\gamma = \gamma^0 \cdot x = x = \gamma(a)/a$. Hilbert 90 gives us the following:

$$\alpha_\gamma = \frac{\gamma(a)}{a}$$

Notice that Hilbert 90 still applies if we had chosen a cocycle from the set $H^1(K, \mu_2(K))$ since $H^1(-, \mu_2(-))$ is a subfunctor of $H^1(-, \mathbb{G}_m(-))$. An application of Hilbert 90 is Kummer theory, which we state as a proposition.

Proposition 2.2.6 Let k be a field such that $\text{char} k$ is prime to some positive integer m . Then we have a canonical isomorphism

$$\phi : k^\times / k^{\times m} \rightarrow H^1(k, \mu_m(k))$$

given by

$$\bar{a} \mapsto \alpha : \sigma \mapsto \frac{\sigma(a)}{a},$$

where $x^m = a$ for some $x \in k_s$.

Proof. Let $\bar{a} \in k^\times/k^{\times m}$. We immediately note that, since $\text{char} k \nmid m$, the polynomial $x^m - a$ is separable over k . This means that the map $k^\times \rightarrow k^\times$ given by $x \mapsto x^m$ is surjective. So we may consider the following exact sequence:

$$1 \longrightarrow \mu_m(k) \longrightarrow k^\times \xrightarrow{-m} k^\times \longrightarrow 1$$

Applying the functor $H^*(k, -)$, we obtain a long exact sequence in cohomology:

$$\cdots \longrightarrow k^\times \xrightarrow{-m} k^\times \xrightarrow{\delta^0} H^1(k, \mu_m(k)) \longrightarrow \cdots$$

The isomorphism is given by exactness at $H^1(k, \mu_m(k))$ and Hilbert 90 via the zeroth connecting homomorphism:

$$\delta^0 : k^\times/k^{\times m} \rightarrow H^1(k, \mu_m(k)) : \bar{a} \mapsto \delta^0(a)$$

where $\delta^0(a) = \alpha : \mathcal{G}_{k_s} \rightarrow \mu_m(k_s) : \sigma \mapsto \sigma(x)/x$, where $x \in k_s$ such that $x^m = a$. It is clear that the cocycle α does not depend on the choice of a . We have shown that δ^0 is injective. Now, suppose $\alpha \in H^1(k, \mu_m(k))$. Then, by Hilbert 90, there exists some $x \in k_s$ such that $\alpha_\sigma = \sigma(x)/x, \forall \sigma \in \mathcal{G}_{k_s}$. Since $\alpha_\sigma^m = 1$, we have $1 = \alpha_\sigma^m = (\sigma(x)/x)^m = \sigma(x^m)/x^m$. Cross-multiplying, we obtain $\sigma(x^m) = x^m$ so that our choice is $a = x^m$ and hence $a \in k^\times$. \square

Using the above isomorphism we are ready to explain some results concerning cup products in $H^n(k, \mu_2(k_s))$. When we add elements in $H^n(k, \mu_2(k_s))$, we will use additive notation while in $\mu_2(k_s)$, we will use multiplicative notation. By definition, we have the following:

$$[\alpha] + [\beta] = [\alpha\beta], \forall \alpha, \beta \in H^n(k, \mu_2(k_s))$$

Using Proposition 2.2.6, let us denote the image of a square class $\bar{a} \in k^\times/k^{\times 2}$ under δ^0 by α_a and the square root of a by x_a . Since $\mu_2(k_s)$ is commutative, we have $(x_a x_b)^2 = x_a^2 x_b^2 = ab$ for some square classes $a, b \in k^\times/k^{\times 2}$. This implies that $\alpha_a \alpha_b$ represents the square class ab . Thus,

$$(a) + (b) = (ab)$$

Consider the bilinear map $\phi : \mu(k_s) \times \mu_2(k_s) \rightarrow \mu_2(k_s)$ given by $((-1)^p, (-1)^q) \mapsto (-1)^{pq}$ and let us denote $\cup_\phi = \cup$. Keeping the same notation for α_a and α_b , we introduce a new map. By Hilbert 90, we have

$$\alpha_a : \sigma \rightarrow \sigma(x_a)/x_a = (-1)^{\epsilon_a(\sigma)}, \alpha_b : \tau \mapsto \tau(x_b)/x_b = (-1)^{\epsilon_b(\tau)},$$

where $\epsilon_a, \epsilon_b : \mathcal{G}_{k_s} \rightarrow \{0, 1\}$. Thus,

$$\alpha_a \cup \alpha_b : \mathcal{G}_{k_s} \times \mathcal{G}_{k_s} \rightarrow \mu_2(k_s) : (\sigma, \tau) \mapsto (-1)^{\epsilon_a(\sigma)\epsilon_b(\tau)}$$

2.3 Galois Descent

An example that illustrates the Galois descent problem, or a motivation if you will, is the problem of conjugacy of matrices. Is it true that if a matrix is conjugate to some fixed matrix M_o over a field extension L/k , it is conjugate over the base field k ? Given a Galois functor $F : C_k \rightarrow M_n$, where $M_n(K) = \{\text{matrices with entries in } K \text{ of size } n\}$, Galois cohomology allows us to measure the degree to which matrices are conjugate to M_o over k by relating the conjugacy classes of M_o to the set of 1-cocycles in $H^1(\mathcal{G}_L, Z_F(M_o)(L))$, where $Z_F(M_o)(L) = \{A \in F(L) \mid AM_oA^{-1} = M_o\}$ via the map

$$A \mapsto \alpha^A : \sigma \mapsto A/\sigma \cdot A^{-1}$$

Let us denote by $*$ the conjugate action; that is $A * M_o = AM_oA^{-1}$. If we look carefully we can see that the set $Z_F(M_o)(L)$ is nothing but the stabilizer of M_o in $F(L)$. So once we define an action on $F(L)$ we may restrict it to a subset, mainly a stabilizer, and generate 1-cocycles.

In order to generalize the concept of the conjugacy problem for matrices we need to extend it to other algebraic objects and their conjugacy over fields. In order to facilitate this, we introduce the notion of a functor acting on another.

Definition 2.3.1 Let $G : C_k \rightarrow Grps$ be a covariant functor. We say that G acts on the functor $F : C_k \rightarrow Sets$ if the diagram

$$\begin{array}{ccc}
G(L) \times F(L) & \xrightarrow{*} & F(L) \\
(G(\iota), F(\iota)) \downarrow & & \downarrow F(\iota) \\
G(L') \times F(L') & \xrightarrow[*]{} & F(L')
\end{array}$$

commutes. Let $(g, a) \in G(L) \times F(L)$. Commutativity of the diagram implies that

$$F(\iota)(g * a) = G(\iota)(g) * F(\iota)(a)$$

In the case where the map ι is substituted by an automorphism $\sigma \in \text{Aut}(L)$, we write:

$$\sigma \cdot (g * a) = (\sigma \cdot g) * (\sigma \cdot a)$$

Now we are ready to introduce some new terminology to denote what we mean by two elements in $F(L)$ becoming equivalent over some extension L'/L .

Definition 2.3.2 Let $a, a' \in F(K)$. We say that a is equivalent to a' over K if there exists some element $g \in G(K)$ such that $a' = g * a$ and denote it by

$$a \sim_K a'$$

Using the above language, we restate the Galois descent problem. Given elements $a, a' \in F(L)$ for some extension L/k such that $a \sim_L a'$, do we also have that $a \sim_k a'$?

Definition 2.3.3 Let $G : C_k \rightarrow \text{Grps}$ be a functor acting on $F : C_k \rightarrow \text{Sets}$ and let $a \in F(k)$. We say that $a' \in F(K)$, for some extension K/k , is a K -twisted form of a if

$$a_\Omega \sim_\Omega a'_\Omega$$

for some Galois extension Ω/K .

Note that the action of $G(\Omega)$ restricts to K -twisted forms since $a_\Omega \sim_\Omega a'_\Omega$ and $a' \sim_K a''$ implies that $a_\Omega \sim_\Omega a''_\Omega$. In other words, the action is well-defined on equivalence classes.

Now we introduce the following set:

$$F_a(\Omega/K) = \{[a'] \mid a' \in F(K), a'_\Omega \sim_\Omega a_\Omega\}$$

We want to show that F_a is a functor, but, first, we need to show what we mean by $F_a(\iota) : F_a(K) \rightarrow F_a(K')$, where $\iota : K \hookrightarrow K'$ is a morphism of field extensions. Our task is to show that K -twisted forms are also K' -twisted forms via the map ι . So suppose a' is a K -twisted form of a . Then, by definition, there exists a Galois extension Ω/K such that $a_\Omega \sim_\Omega a'_\Omega$; that is, $g * a_\Omega = a'_\Omega$ for some $g \in G(\Omega)$. Assume also that we have an extension $\phi : \Omega \rightarrow \Omega'$ of $\iota : K \rightarrow K'$. The various inclusions of field extensions induce the following commutative diagram:

$$\begin{array}{ccc} F(K) & \longrightarrow & F(K') \\ \downarrow & & \downarrow \\ F(\Omega) & \longrightarrow & F(\Omega') \end{array}$$

so that, given $x \in F(K)$, $(x_{K'})_{\Omega'} = (x_\Omega)_{\Omega'}$.

Observe that $g_{\Omega'} * (a'_{K'})_{\Omega'} = g_{\Omega'} * (a'_\Omega)_{\Omega'} = (g * a'_\Omega)_{\Omega'} = (a_\Omega)_{\Omega'} = a_{\Omega'}$. Let us denote $F_a(K) = F_a(K_s/K)$, where K/k is a field extension. Then, $\iota : K \rightarrow K'$ induces the map

$$F_a(\iota) : F(K) \rightarrow F(K') : [x] \mapsto [x_{K'}]$$

Thus, $F_a : C_k \rightarrow Sets$ is a functor.

So to rephrase the Galois descent problem is to ask the following: given a Galois extension Ω/k , is it true that $F_a(\Omega/k) = \{[a]\}$?

Definition 2.3.4 Let $F : C_k \rightarrow Sets$ be a functor with the following properties:

- i. $\iota : K \rightarrow K'$ induces an injective morphism $F(\iota) : F(K) \rightarrow F(K')$
- ii. Given any extension Ω/K , $F(K) \cong F(\Omega)^{G_\Omega}$.

We say that such F satisfies the Galois descent condition.

Now it is convenient to introduce an analogue of the term $Z_F(M_o)(L)$ in the context of functorial action G on F . Keeping the previous definitions for these terms, we have

the following:

Definition 2.3.5 Given $a \in F(k)$, the stabilizer of a in G over some extension L/k is denoted by

$$\text{Stab}_{Ga}(L) = \{g \in G(L) \mid g * a_L = a_L\}$$

Consider the inclusion of fields $\iota : L \hookrightarrow L'$ and the induced map $G(L) \rightarrow G(L')$. Suppose $g \in \text{Stab}_{Ga}(L)$. Then, by definition, we have $g * a_L = a_L$. Observe that

$$g_{L'} * a_{L'} = (g * a_L)_{L'} = (a_L)_{L'} = a_{L'}$$

This implies that the functor G restricts to Stab_{Ga} . Thus, $\text{Stab}_{Ga} : C_k \rightarrow \text{Sets}$ is a functor. Keeping our notation for G and F as before, we will state the following lemma without proof.

Lemma 2.3.6 If F satisfies the Galois descent condition and G is a Galois functor acting on F , then $\text{Stab}_{Ga} : C_k \rightarrow \text{Grps}$ is a Galois functor for some $a \in F(k)$. Furthermore, given any extension L/k , $\text{Stab}_{Ga}(L)$ is a \mathcal{G}_L -group.

Note that we have the following Galois cohomology functor with respect to Stab_{Ga} :

$$H^1(-, \text{Stab}_{Ga}(-)) : C_k \rightarrow \text{Sets}$$

We present a particular case of the Galois descent lemma.

Lemma 2.3.7 Let G be a group-valued functor acting on a functor $F : C_k \rightarrow \text{Sets}$ that satisfies the Galois descent condition. Let $a \in F(k)$. If $H^1(-, G(-)) = 1$, then we have the following bijection of functors:

$$F_a(-) \cong H^1(-, \text{Stab}_{Ga}(-))$$

We will refer the reader to [2, III.8] for the proof of the above lemma.

2.4 Étale and Galois Algebras

Definition 2.4.1 Let k be a field with nonzero characteristic. A commutative k -algebra E is Étale if it satisfies any of the following equivalent conditions:

- i. $E_{k_s} \cong k_s^{\times n}$, where k_s is a separable extension of k .
- ii. $\dim_k E = \#X(E)$, where $X(E) = \text{Hom}_{k\text{-alg}}(E, k_s)$.
- iii. $E \cong k[X]/\langle f \rangle$, where f is a separable polynomial in $k[X]$.

We introduce some examples of Étale algebras that we will refer to later on:

Examples 2.4.2

- i. Any finite separable extension E over k is Étale over k .
- ii. $k^{\times n}$ is called the split Étale algebra over k of degree n .

In view of condition ii. of the above definition, we have that, given any morphism of field extensions, say $\iota : L \rightarrow L'$ and an Étale algebra E over L , $E_{L'}$ is Étale over L' . Thus, we obtain a functor:

$$\acute{E}t_n : C_k \rightarrow \text{Sets}$$

By definition, all Étale algebras over K of dimension n are K -twisted forms of $K^{\times n}$. So by Galois descent, we obtain the isomorphism:

$$\acute{E}t_n(-) \cong H^1(-, \text{Aut}_{k\text{-alg}}(K^{\times n}))$$

Lemma 2.4.3 $\text{Aut}(K^n) \cong S_n$

We state the above isomorphism of functors in a proposition.

Proposition 2.4.5 $\acute{E}t_n(-) \cong H^1(-, S_n)$.

Galois algebras are a special case of Étale algebras and, as we might expect, we obtain similar results when applying the Galois descent lemma. Let us recall that G -algebras

over k are k -algebras on which G acts by k -algebra automorphisms. For any G -algebra L over k , there is a natural right action of G on $X(L) = \text{Hom}_{k\text{-alg}}(L, k_s)$ given by

$$(\xi \cdot g)(l) = \xi(g \cdot l), \forall l \in L$$

Definition 2.4.6 Let G be a group of order n and L , a G -algebra over k of degree n . We say that L is a G -Galois algebra if L is \acute{E} tale over k and the right action of G on $X(L)$ is transitive.

In the same way we applied Galois descent to twisted forms of the split \acute{E} tale algebra over k , we introduce its Galois version. Let G be a group of order n and let us index the elements in $k^{\times n}$ by the elements in G . Denote by $(e_g)_{g \in G}$ be the n idempotents in $k^{\times n}$. Now we define an important automorphism. Let $f_g \in \text{Aut}_{k\text{-alg}}(k^{\times n})$ be given by

$$e_h \mapsto e_{gh}$$

So there exists an induced action of G on $k^{\times n}$ via the map f_g :

$$G \times k^{\times n} \rightarrow k^{\times n} : (g, x) \mapsto f_g(x)$$

This action endows $k^{\times n}$ with the structure of a Galois G -algebra, which we denote by L_o . Given a Galois G -algebra L of degree n , by proper indexing and permutation of idempotents, we obtain the following isomorphism of k -algebras under the action of G :

$$L \cong_G L_o$$

Theorem 2.4.7 Given a G -algebra L over k of degree n with $\#G = n$, we have the following equivalent conditions:

- i. L is a Galois G -algebra
- ii. $L_{k_s} \cong_G (L_o)_{k_s}$
- iii. L is \acute{E} tale with $L^G = k$

Consider the map $\phi_g : L_o \rightarrow L_o$ given by $e_h \mapsto e_{hg^{-1}}, \forall g, h \in G$. By construction, the map $g \mapsto \phi_g$ defines an isomorphism of groups:

$$G \cong \text{Aut}_{G\text{-alg}}(L_o)$$

Assuming that \mathcal{G}_{k_s} acts trivially on G , we have the following proposition due to the Galois descent lemma:

Proposition 2.4.8 $G\text{-Gal} \cong H^1(-, G)$

2.5 Group Extensions

In this section, we will study group extensions of G by A , where both A and G are finite groups. We further assume that A is abelian and a G -module. Our attempt to classify equivalence classes of group extensions will lead us to the construction of corresponding 2-cocycles of G with values in A . Once the classification by 2-cocycles is accomplished, we turn our discussion towards defining the obstruction to a given embedding problem.

Definition 2.5.1 Let A be a G -module with corresponding representation $\phi : G \rightarrow \text{Aut}(A)$. A group extension of G by A is a short exact sequence:

$$1 \longrightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$$

Note that the image of A under the injective map ι is normal in E . This allows us to induce an action of E on A via inner automorphisms in the following way:

$$x \cdot a = x \cdot \iota(a) = x\iota(a)x^{-1}, \forall x \in E, a \in A$$

which also extends to an action of G via π as follows:

$$x\iota(a)x^{-1} = \iota(\phi(\pi(x))(a)), \forall x \in E, a \in A$$

We know that not all group extensions arise as direct products $A \times G$ if we choose, for instance, cyclic groups. Both \mathbb{Z}_8 and $\mathbb{Z}_4 \times \mathbb{Z}_2$ are extensions of \mathbb{Z}_4 by \mathbb{Z}_2 but are not

isomorphic. So we need to make the isomorphism between E and $A \times G$ clear using the information given by the group extension above.

We need a map s which is the right inverse of π under composition of maps with the additional condition that $s(1) = 1$. Regardless of the latter, we call s a set-theoretic section of π if $\pi s = id_G$. Let $x \in E$ and define $g = \pi(x)$. Consider the element $xs(g)^{-1}$ in E . Mapping it under π , we have

$$\pi(xs(g)^{-1}) = \pi(x)\pi s(g^{-1}) = gg^{-1} = 1$$

By the exactness at E and the injectivity of ι , there exists a unique element $a \in A$ such that $\iota(a) = xs(g)^{-1}$. Thus, once our section s is chosen such that $s(1) = 1$, we obtain a bijection from E to $A \times G$ given by

$$x \mapsto \iota(a)s(g)$$

Multiplication in E and the bijection of sets just described will induce a particular operation on $A \times G$. Let $x, x' \in E$ and denote $g = \pi(x)$ and $g' = \pi(x')$ such that $x = \iota(a)s(g)$ and $x' = \iota(a')s(g')$ for some $a, a' \in A$. Then, $xx' = \iota(a)s(g)\iota(a')s(g') = \iota(a)s(g)\iota(a')s(g)^{-1}s(g)s(g') = \iota(a)(s(g)\iota(a')s(g)^{-1})(s(g)s(g')s(gg')^{-1})s(gg')$.

Let us denote the action of G on A by $g \cdot a$. Recall that the action of E on A by inner automorphisms extends to an action of G by mapping under ι so that $s(g)\iota(a')s(g)^{-1} = \iota((\pi s(g)) \cdot a) = \iota(g \cdot a)$. Since s is a section, $s(g)s(g')s(gg')^{-1} \in \ker \pi$. Thus, there exists a unique element $\alpha_{g,g'}^{(s)} \in A$ such that $\iota(\alpha_{g,g'}^{(s)}) = s(g)s(g')s(gg')^{-1}$.

Since ι is a group morphism, we collect terms to obtain:

$$(\iota(a)s(g))(\iota(a')s(g')) = \iota(a)\iota(g \cdot a)\iota(\alpha_{g,g'}^{(s)})s(gg') = \iota(a\alpha_{g,g'}^{(s)}g \cdot a)s(gg')$$

So we have obtained a multiplication that endows $A \times G$ with a group structure as follows:

$$(a, g)(a', g') = (a\alpha_{g,g'}^{(s)}g \cdot a, gg'),$$

which we denote by $A \times_\alpha G$.

It is easy to check that $\alpha^{(s)} : G \times G \rightarrow A : (g, g') \mapsto s(g)s(g')s(gg')^{-1}$ is a cocycle.

Theorem 2.5.2 Let A be a G -module with representation $\phi : G \rightarrow Aut(G)$. There

exists an isomorphism between the set of 2-cocycles in $H^2(G, A)$ and the set of equivalence classes of group extensions of G by A .

Proof. We say that two extensions E, E' are equivalent if there exists an isomorphism $f : E \rightarrow E'$ of groups with commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow id_A & & \downarrow f' & & \downarrow id_G & & \\ 1 & \longrightarrow & A & \xrightarrow{\iota'} & E' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

Recall that given any extension E and a section of π there exists a 2-cocycle $\alpha^{(s)} \in H^2(G, A)$ such that $E \cong A \times_{\alpha^{(s)}} G$. To prove the theorem, it is enough to show that, given two different sections s and t of π , the cocycles $\alpha^{(s)}$ and $\alpha^{(t)}$ differ by a coboundary. So let us assume that s and t are two different sections of π . It is clear that for all $g \in G$, $s(g)t(g)^{-1}$ maps to 1 under π . By exactness at E , there exists a unique element γ_g such that $\iota(\gamma_g) = s(g)t(g)^{-1}$ or $s(g) = \iota(\gamma_g)t(g)$. Thus, $\alpha_{g,g'}^{(s)} = s(g)s(g')s(gg')^{-1} = \iota(\gamma_g)t(g)\iota(\gamma_{g'})t(g')t(gg')^{-1}\iota(\gamma_{gg'})^{-1} = \iota(\gamma_g)(t(g)\iota(\gamma_{g'})t(g)^{-1})(t(g)t(g')t(gg')^{-1})\iota(\gamma_{gg'})^{-1} = \iota(\gamma_g)\iota(g \cdot \gamma_{g'})\iota(\gamma_{g,g'}^{(t)})\iota(\gamma_{gg'}^{-1}) = \iota(\alpha_{g,g'}^{(t)}\gamma_g g \cdot \gamma_{g'}\gamma_{gg'}^{-1})$ \square

Let G act trivially on the abelian group A and consider the extension

$$1 \longrightarrow A \longrightarrow G' \xrightarrow{\pi} G \longrightarrow 1$$

We have the following lifting problem: given a group morphism $f : \mathcal{G}_{k_s} \rightarrow G$, does there exist a morphism $f' : \mathcal{G}_{k_s} \rightarrow G'$ such that $\pi \circ f' = f$? Let us reformulate the question in the following way. Assume that the action of \mathcal{G}_{k_s} on A , G , and G' is trivial and apply the functor $H^*(k, -)$ to the above extension. We obtain a long exact sequence in cohomology:

$$\cdots \longrightarrow H^1(k, G') \xrightarrow{\pi_*} H^1(k, G) \xrightarrow{\delta^1} H^2(k, A) \longrightarrow \cdots$$

The condition $\pi \circ f' = f$ for some $f' \in H^1(k, G')$ is the same as requiring $f \in \ker \delta^1$. We call the class $[\delta^1(f)]$ the obstruction to the embedding problem. Since it is cumbersome to calculate $\delta^1(f)$ we find a simpler 2-cocycle. Let s be a section of π with $s(1) = 1$. We use the fact that $s(f_\sigma)$ is a preimage of f_σ under π to construct a 2-cocycle $\gamma : \mathcal{G}_{k_s} \times \mathcal{G}_{k_s} \rightarrow A$ that represents the class $[\delta^1(f)]$. Given the section s

above, we find that the 2-cocycle γ is completely determined by the equalities: $\iota(\gamma_{g,g'}) = s(f_g)s(f_{g'})s(f_{gg'})^{-1} = s(f_g)s(f_{g'})s(f_g f_{g'})^{-1}$, $\forall g, g' \in \mathcal{G}_{k_s}$; the second one coming from the fact that f is a 1-cocycle and that \mathcal{G}_{k_s} acts trivially on A . Observe that the equality $\iota(\alpha_{\sigma,\sigma'}) = s(\sigma)s(\sigma')s(\sigma\sigma')^{-1}$, $\forall \sigma, \sigma' \in G$ completely determines the cocycle $\alpha^{(s)}$. So the cocycle $\gamma^{(s)}$ is precisely the cocycle $f^*(\alpha)$.

Chapter 3

Quadratic Forms

In this chapter, we introduce quadratic forms and other algebraic objects such as Clifford algebras and groups that the forms generate. We will also define maps between these objects, especially isometries, that will allow us to construct short exact sequences and, in turn, use Galois cohomology to interpret Hasse invariants of quadratic forms in a cohomological context.

3.1 Basics

Definition 3.1.1 A quadratic form over a commutative ring R is a pair (V, q) of a vector space V over R together with a map $q : V \rightarrow R$ satisfying the following:

- i. $q(ax) = a^2x, \forall x \in V, a \in R$
- ii. the map $b_q(\cdot, \cdot) : V \times V \rightarrow R$ given by $(x, y) \mapsto \frac{1}{2}(q(x+y) - q(x) - q(y))$ is bilinear.

Note that b_q completely determines q since $b_q(x, x) = q(x), \forall x \in V$. We say that two quadratic forms (V, q) and (V', q') are isomorphic if there exists an isomorphism of R -modules $f : V \rightarrow V'$ such that $q'(f(x)) = q(x), \forall x \in V$. If $V = V'$, we call such f an isometry of (V, q) .

We want to define a quadratic form on the scalar extension of V by some ring R' . The following bilinear form defines the quadratic form we need:

$b_{q_{R'}} : V \otimes_R R' \times V \otimes_R R' \rightarrow R' : (x \otimes a, x' \otimes a') \mapsto aa'\phi(b_q(x, x'))$, where $\phi : R \rightarrow R'$ is a ring morphism.

Definition 3.1.2 A quadratic form (V, q) is regular over R if the map $V \rightarrow V^*$ given by $x \mapsto b_q(x, \cdot)$ is an isomorphism of R -modules.

Given a finite dimensional quadratic form (V, q) and a basis $\mathcal{B} = \{e_1, e_2, \dots, e_n\}$, we have a representative matrix $Mat(q, \mathcal{B}) = (b_q(e_i, e_j))$. For any vector $x = x_1e_1 + \dots + x_n e_n$, we have $q(x) = \vec{x}^t Mat(q, \mathcal{B}) \vec{x}$, where $\vec{x} = [x_1 \ x_2 \ \dots \ x_n]^t$ is a column vector.

Keeping the same notation as above, if we further assume that (V, q) is regular, then it is clear that $Mat(q, \mathcal{B})$ is invertible. Thus, we may take its determinant, which we denote by

$$det(q) = det(Mat(q, \mathcal{B}))$$

We use the above notation to refer to its square class in $R^\times/R^{\times 2}$. Also observe that for any extension $\phi : R \rightarrow R'$, $det(q_{R'}) = \phi(det(q)) \in R^\times/R^{\times 2}$.

Definition 3.1.3 The degree of a quadratic form (V, q) over R is the dimension of V over R or its rank as a R -module.

Consider the form (R^n, q) , where q is given by

$$R^n \rightarrow R : (x_1, x_2, \dots, x_n) \mapsto a_1x_1^2 + a_2x_2^2 + \dots + a_nx_n^2$$

for some $a_i \in R$, $i = 1, 2, \dots, n$.

We denote this particular quadratic form by $\langle a_1, a_2, \dots, a_n \rangle$. Moreover, we say that a quadratic form (V, q) of degree n is diagonalisable if it is isomorphic to $\langle a_1, a_2, \dots, a_n \rangle$ for some $a_i \in R$. In the case where $a = a_i \ \forall i$, we will denote the corresponding form by $n \times \langle a \rangle$.

We introduce an operation on the set of quadratic forms over R that endows it with a ring structure. Given two quadratic forms (V, q) and (V', q') , the orthogonal sum q and q' is the Cartesian product $V \times V'$ with the map $V \times V' \rightarrow R$ given by $(v, v') \mapsto q(v) + q(v')$, $\forall v \in V, v' \in V'$. We denote this map by $q \perp q'$. If we repeat this operation m times on a quadratic space (V, q) , we simplify notation by denoting the space by $m \times q$.

On the other hand, the tensor product of two quadratic spaces (V, q) and (V', q') is the space $V \otimes V'$ together with the map $b_{q \otimes q'} : V \otimes V' \times V \otimes V' \rightarrow R$ given by $(v_1 \otimes w_1, v_2 \otimes w_2) \mapsto b_q(v_1, v_2)b_{q'}(w_1, w_2)$, $\forall v_1, v_2 \in V, w_1, w_2 \in V'$. The regularity property

is preserved under both \perp and \otimes .

Now consider a quadratic form (V, q) of degree n over a field F . Let $a \in F^\times$ such that $q(x) = a$ for some $x \in V$. Note that by the nature of q , x cannot be zero. We call such a an element representable by q or that q represents a . We denote the set of such elements by:

$$D(q) = \{a \in F^\times \mid q(x) = a \text{ for some } x \in V\}$$

The following lemma illustrates how we can use the information given by $D(q)$ to determine a diagonalization.

Lemma 3.1.4 Given a regular quadratic form (V, q) and $a \in D(q)$, there exists (V', q') such that $V \cong V' \perp \langle a \rangle$.

We can see that by applying induction on the degree of a quadratic form we can diagonalize it. This is very useful since we can diagonalize a quadratic form using representable elements that we know, such as the field norm.

Under the operations \otimes and \perp , quadratic forms over a field F become a commutative semiring, which we denote by $M(F)$. We say that $M(F)$ is a semiring since not all quadratic forms have additive inverses. By the construction of the orthogonal sum operation \perp , we obtain the so called Witt cancellation theorem:

$$q \perp q_1 \cong q \perp q_2 \Rightarrow q_1 \cong q_2, \forall q, q_1, q_2 \in M(F)$$

Thus, $M(F)$ is a commutative cancellation monoid. Now we are ready to apply Grothendieck's construction to any such monoid M . Define a relation \sim on $M \times M$ as follows:

$$(a, b) \sim (a', b') \text{ if and only if } a + b' = b + a'$$

Note that the addition given by

$$(a, b) + (a', b') = (a + a', b + b')$$

is well-defined with the inverse of (a, b) being (b, a) . The relation \sim induces on the set $M \times M$ a group structure, which we denote by $Groth(M) = M \times M / \sim$. We have a special notation in the case where $M = M(F)$:

$$\widehat{W}(F),$$

which we call the Witt-Grothendieck ring of F .

By addition on $M \times M / \sim$, $(x, y) = (x - y, 0)$. So the inclusion map $\iota : M(F) \rightarrow Groth(M) : x \mapsto (x, 0)$ allows us to view $Groth(M)$ as the additive group generated by $M(F)$. $Groth(M)$ has the universal property with respect to monoid homomorphisms $f : M \rightarrow G$, where G is some abelian group; that is, f extends uniquely to a map $Groth(M) \rightarrow G$.

Recall that a hyperbolic space is the orthogonal sum of hyperbolic planes, which are 2-dimensional quadratic spaces isomorphic to $\langle 1, -1 \rangle$. Now denote by $\mathbb{Z} \cdot \mathbb{H}$ the set of hyperbolic spaces and their additive inverses. We obtain the Witt ring of a field F as the quotient of $\widehat{W}(F)$ by the ideal $\mathbb{Z} \cdot \mathbb{H}$:

$$W(F) = \widehat{W}(F) / \mathbb{Z} \cdot \mathbb{H}$$

The equivalence relation is given as follows. $q \sim q'$ if and only if there exist positive integers r and r' such that:

$$q \perp r \times \langle 1, -1 \rangle \cong q' \perp r' \times \langle 1, -1 \rangle$$

Under the above relation, $W(K)$ becomes a commutative ring with additive identity $[\langle 0 \rangle]$ and unity $[\langle 1 \rangle]$.

Let us use the bar notation to denote the canonical projection of \mathbb{Z} onto \mathbb{Z}_2 . Let K/k be a field extension and consider the following map

$$W(K) \rightarrow \mathbb{Z} : q \mapsto \dim(q)$$

Via the projection of \mathbb{Z} onto \mathbb{Z}_2 , we obtain

$$W(K) \rightarrow \mathbb{Z}_2 : q \mapsto \overline{\dim(q)}$$

Consider the ideal which is the kernel of the above map. We denote it as follows.

$$I(K) = \{q \in W(K) \mid \dim(q) \text{ is even}\}$$

Now consider the the following quadratic form:

$$\langle 1, -a_1 \rangle \otimes \langle 1, -a_2 \rangle \otimes \cdots \otimes \langle 1, -a_n \rangle$$

for some positive integer n . We denote the above by $\langle\langle a_1, a_2, \dots, a_n \rangle\rangle$ and call it a n -fold Pfister form. Observe that $[\langle a, b \rangle] = [\langle\langle a \rangle\rangle] - [\langle\langle b \rangle\rangle]$, which implies that $I(K)$ is additively generated by 1-fold Pfister forms $\langle\langle a \rangle\rangle$, $\forall a \in K$. Let us denote the subset of $I(K)$ generated by n -fold Pfister forms by $I^n(K)$ with $I^0(K) = W(K)$.

3.2 Orthogonal groups and Clifford algebras

Throughout this section, we will assume that our quadratic forms are defined over fields k with characteristic 0.

Definition 3.2.1 Let (V, q) be a quadratic form of degree n . The orthogonal group q is given by:

$$O(q)(R) = \{f \in GL(V)(R) \mid q_R \circ f = q_R\},$$

where R is a commutative ring.

Note that $q_R \circ f = q_R$ implies that $\det(f) \in \mu_2(R)$. So we have the following morphism of group schemes:

$$\det : O(q) \rightarrow \mu_2$$

Definition 3.2.2 Let q be a quadratic form. The special orthogonal group of q is a sub-group scheme of $O(q)$ given by:

$$O^+(q)(R) = \{f \in O(q)(R) \mid \det(f) = 1\}$$

Since we have a bilinear form $b_q(\cdot, \cdot)$ on V we may consider the x -hyperplanes H which we define as follows:

$$H = \{y \in V \mid b_q(x, y) = 0\}$$

Given the hyperplane H , we may also define a reflection on its set as follows:

$$\tau_x : V \rightarrow V : v \mapsto v - 2 \frac{b_1(x, v)}{b_q(x, x)} x$$

Note that $\tau_x(x) = -x$ and $\tau_x(y) = y$, $\forall y \in H$. Composing a finite number of reflections, we obtain an isometry. In fact, we can make this statement even stronger.

Lemma 3.2.3 Any isometry in $O(q)$ is a product of reflections.

By construction of the special orthogonal group. we have the following short exact sequence:

$$1 \longrightarrow O^+(q)(k_s) \longrightarrow O(q)(k_s) \xrightarrow{\det} \mu_2(k_s) \longrightarrow 1$$

where q has degree n and k_s is a separable closure of k .

Let (V, q) be a quadratic form and consider the tensor algebra $T(V) = \bigoplus_{n \geq 0} T_n(V)$, where $T_0(V) = R$ and $T_n(V) = V^{\otimes n}$, $n \geq 1$. $T(V)$ possesses a two-sided ideal given by $\mathcal{I}(q) = \langle v \otimes v - q(v) \mid v \in V \rangle$. So we may mod the tensor algebra out by this particular ideal to obtain the quotient algebra:

$$C(V, q) = T(V)/\mathcal{I}(q),$$

which we name the Clifford algebra of q .

We use the bar notation to denote the canonical projection $T(V) \rightarrow C(V, q) : x \mapsto \bar{x}$. Observe that \bar{M} generates $C(V, q)$. So it is natural to consider maps of M with values in M . But first, let us introduce the canonical involution on the tensor algebra $T(V)$:

$$(x_1 \otimes x_2 \otimes \cdots \otimes x_n)^t = x_n \otimes x_{n-1} \otimes \cdots \otimes x_1$$

Since $_t$ fixes $\mathcal{I}(q)$, it induces an involution on $C(V, q)$ as well, which we denote by the same notation. The map $M \rightarrow M : v \mapsto -v$ induces an automorphism on $C(V, q)$ which

we denote by

$$\gamma : C(V, q) \rightarrow C(V, q)$$

The above map endows $C(V, q)$ with a \mathbb{Z}_2 -grading as follows:

$$C_0(V, q) = \{x \in C(V, q) \mid \gamma(x) = x\}$$

$$C_1(V, q) = \{x \in C(V, q) \mid \gamma(x) = -x\}$$

The Clifford algebra has the following properties, which we state in a proposition.

Proposition 3.2.4 Given a regular quadratic space (V, q) , the following hold:

- i. $C(V, q)_R \cong C(V_R, q_R)$ for some ring R
- ii. $b_q(x, y) = \frac{1}{2}(\bar{x}\bar{y} + \bar{y}\bar{x}), \forall x, y \in V$
- iii. \bar{x} is invertible if $q(x) \neq 0$
- iv. Given an orthogonal basis $\{e_1, e_2, \dots, e_n\}$ of (V, q) , the set $\{\bar{e}_1^{m_1}, \bar{e}_2^{m_2}, \dots, \bar{e}_n^{m_n}\}$, where $m_i = 0, 1 \forall i$ forms a k -basis for $C(V, q)$

To simplify notation we drop the bar notation. Let us now choose an invertible element x such that $q(x) \neq 0$ and let $y \in V$. Mapping y under the reflection τ_x , we obtain: $\tau_x(y) = y - 2\frac{b_q(x, y)}{b_q(x, x)}x = y - 2\frac{xy - yx}{2x^2}x = y - (xy + yx)x^{-1} = -xyx^{-1} = \gamma(x)yx^{-1}$. Since all isometries are products of reflections, we have the following lemma:

Lemma 3.2.5 Let (V, q) be a quadratic form. Any isometry $f : V \rightarrow V$ can be expressed as $f(x) = \gamma(s_f)xs_f^{-1}$ for some invertible element $s_f \in C(V, q)$.

The above definition is a motivation in defining an important subset of the Clifford algebra $C(V, q)$.

Definition 3.2.6 The Clifford group of a quadratic space (V, q) is denoted by:

$$\Gamma(V, q)(R) = \{s \in C(V, q)_R^\times \mid \gamma(s)V_Rs^{-1} = V_R\}$$

for some ring R .

So given any $s \in \Gamma(V, q)(R)$, we may define the map: $\alpha_s : V_R \rightarrow V_R : x \mapsto \gamma(s)xs^{-1}$,

which defines a morphism of group schemes given by

$$\alpha : \Gamma(V, q) \rightarrow GL(V),$$

where $\alpha_R(s) = \alpha_s : V_R \rightarrow V_R$.

By construction, we have the following lemma:

Lemma 3.2.7 *ker* $\alpha_R = R^\times$ for any k -algebra R .

Let (V, q) be a quadratic form over R . We define the norm map on $C(V, q)$ as follows: $C(V, q) \rightarrow C(V, q) : s \mapsto s^t s$, which we denote by N_R . Note that $N_R(v) = q(v) = v^2, \forall v \in V$. By definition of the map γ and the above lemma, $N_R(\gamma(s)) = \gamma(s)^t \gamma(s) = \gamma(s^t s) = s^t s = N_R(s)$.

Consider $\alpha_s : V_R \rightarrow V_R$ for some $s \in \Gamma(V, q)$ and let $v \in V_R$. Then, $q_R(\alpha_s(v)) = \alpha_s(v)^t \alpha_s(v) = (\gamma(s) v s^{-1})^t (\gamma(s) v s^{-1}) = (s^{-1})^t v^t \gamma(s)^t \gamma(s) v s^{-1} = (s^{-1})^t v N_R(s) v s^{-1} = N_R(s) N_R(s^{-1}) q_R(v) = N_R(s) N_R(s)^{-1} q_R(v) = q_R(v)$

Thus, we have the following lemma.

Lemma 3.2.8 Given any $s \in \Gamma(V, q)$, α_s is an isometry of q_R .

By lemmas 3.2.7 and 3.2.8, we have the following short exact sequence:

$$1 \longrightarrow K^\times \longrightarrow \Gamma(V, q)(K) \xrightarrow{\alpha_K} O(q)(K) \longrightarrow 1,$$

where K/k is a field extension.

We define a subset of $\Gamma(V, q)$ by choosing those elements with norm equal to 1 and denote it by

$$Pin(q)(K) = \{x \in \Gamma(V, q)(K) \mid N_R(x) = 1\}$$

By lemma 3.2.5, given an element $x \in V$, $\alpha_K(x) = \tau_x$. In view of the fact that $N_R(x) = q_R(x) = x^2$, notice that $N_R(\pm \frac{x}{\sqrt{q(x)}}) = 1$ so that $\tau_x(y) = \gamma(\frac{x}{\sqrt{q(x)}}) y (\frac{x}{\sqrt{q(x)}})^{-1}, \forall y \in V_R$. In other words, $\alpha_R^{-1}(\tau_x) = \{\pm \frac{x}{\sqrt{q(x)}}\}$, which gives the following lemma.

Lemma 3.2.8 Given a quadratic form (V, q) over R , we have the following exact sequence:

$$1 \longrightarrow \mu_2(K) \longrightarrow \text{Pin}(q)(K) \xrightarrow{\alpha_K} O(q)(K) \longrightarrow 1,$$

3.3 Galois cohomology of quadratic forms

Let us introduce some notation first. Given any field extension K/k , let us denote by $F(K)$ the set of quadratic forms on V_K . And for every morphism of field extensions $\iota : L \rightarrow L'$, let $F(\iota)$ be given by $F(L) \rightarrow F(L') : q \mapsto q_{L'}$. Thus, we obtain the following functor:

$$F : C_k \rightarrow \text{Sets}$$

Let us define an action of the functor $GL(V) : C_k \rightarrow \text{Grps}$ on F as follows:

$$f \cdot q = q \circ f^{-1}, \forall f \in GL(V)(K), q \in F(K)$$

We use the notation $Quad_n(L)$ to denote the set of quadratic forms on V_L with base point q_L . Since all quadratic forms of degree n become isomorphic over a closed separable field extension, $Quad_n(-) : C_k \rightarrow \text{Sets}$ is the functor of twisted forms of q . By Galois descent, we have the following:

Proposition 3.3.1 Given a quadratic form (V, q) , we have an isomorphism of functors:

$$Quad_n(-) \cong H^1(-, O(q))$$

Given a quadratic form q of degree n over a field k , there exists $a_i \in k$ such that $q \cong \langle a_1, \dots, a_n \rangle$, which we call a diagonalization of q . Now consider the map $k^\times \times k^\times \rightarrow H^2(k, \mu_2) : (a, b) \mapsto a \cup b$, where $x \in k^\times$ represents the class $[x] \in k^\times/k^{\times 2} \cong H^1(k, \mu_2)$ and the symbol \cup is the cup product we defined in Chapter 2.

Definition 3.3.2 The Hasse invariant of a quadratic form q over k with diagonalization $\langle a_1, \dots, a_n \rangle$ is given by

$$w_2(q) = \sum_{i < j} (a_i) \cup (a_j)$$

By the bilinearity of the cup product and the equality $(ab) = (a) + (b)$, $\forall a, b \in k^\times/k^{\times 2}$, we have the following.

Given two quadratic forms q, q' :

- i. $w_2(\lambda q) = w_2(q) + (n-1)(\lambda) \cup \det(q) + \binom{n}{2}(-1) \cup (\lambda)$
- ii. $w_2(q \perp q') = w_2(q) + \det(q) \cup \det(q') + w_2(q')$

The above properties follow immediately if we choose two diagonalizations of q and q' , respectively.

Applying lemma 3.2.8 to $K = k_s$, we have the following exact sequence

$$1 \longrightarrow \mu_2(k_s) \longrightarrow \text{Pin}(q)(k_s) \xrightarrow{\alpha_{k_s}} O(q)(k_s) \longrightarrow 1,$$

It is important that we choose a separable closure k_s of k so that we can use Proposition 3.3.1. The first connecting homomorphism map of the long exact sequence induced by the functor $H^*(k, -)$ on the above sequence will send a quadratic form to a 2-cocycle of \mathcal{G}_{k_s} with values in $\mu_2(k_s)$.

Theorem 3.3.3 $\delta^1(q') = w_2(q) + w_2(q') + \det(q) \cup \det(q')$

Proof. Let q and q' be two quadratic forms defined on V . Choose orthogonal bases $\{e_1, \dots, e_n\}$ and $\{e'_1, \dots, e'_n\}$ for q and q' , respectively, and define the following: $a_i = q(e_i)$, $b_i = q'(e'_i)$, and $c_i = b_i a_i^{-1}$. We will not distinguish between e_i and $e_i \otimes 1$ and refer to $\{e_i\}$ and $\{e'_i\}$ as bases for q_{k_s} and q'_{k_s} .

Hilbert 90 gives us the corresponding 1-cocycles for a_i and c_i :

$$\sigma \mapsto \frac{\sigma(\sqrt{a_i})}{\sqrt{a_i}} = (-1)^{\epsilon_i(\sigma)}, \quad \tau \mapsto \frac{\tau(\sqrt{c_i})}{\sqrt{c_i}} = (-1)^{s_i(\tau)},$$

where $\epsilon_i, s_i : \mathcal{G}_{k_s} \rightarrow \mathbb{Z}/2\mathbb{Z}, \forall i$.

Let us define $f : V_{k_s} \rightarrow V_{k_s}$ by $e'_i \mapsto \sqrt{c_i} e_i$. Observe that $q_{k_s} \circ f(e'_i) = q_{k_s}(\sqrt{c_i} e_i) = c_i a_i = b_i = q'_{k_s}(e_i)$. Thus, $f \cdot q'_{k_s} = q_{k_s}$ and we have the following cocycle representing q' : $\xi : \sigma \mapsto f \circ \sigma \cdot f^{-1}$. Note that ξ_σ is an isometry in $O(q)(k_s)$. So we need to know where it maps each of the e_i .

$$\xi_\sigma(e_i) = f(\sigma \cdot f^{-1}(\sigma^{-1}(e_i))) = f(\sigma \cdot f^{-1}(e_i)) = f\left(\sigma \cdot \frac{1}{\sqrt{c_i}} e_i\right) = f\left(\frac{1}{(-1)^{s_i(\sigma)} \sqrt{c_i}} e'_i\right) =$$

$$(-1)^{-s_i(\sigma)} e_i.$$

This implies that the isometry ξ_σ is given by a product of reflections such that $\xi_\sigma = \tau_{e_1}^{s_1(\sigma)} \circ \dots \circ \tau_{e_n}^{s_n(\sigma)}$. By the discussion of lemma 3.2.8, we know that the positive preimage of ξ_σ in $Pin(q)(k_s)$ is $\tilde{\xi}_\sigma = \frac{1}{\sqrt{a_1}^{s_1(\sigma)} \dots \sqrt{a_n}^{s_n(\sigma)}} e_1^{s_1(\sigma)} \dots e_n^{s_n(\sigma)}$. Acting σ on $\tilde{\xi}_\tau$, we obtain

$$\begin{aligned} \sigma \cdot \tilde{\xi}_\tau &= \frac{(-1)^{\sum_i \epsilon_i(\sigma) s_i(\tau)}}{\sqrt{a_1}^{s_1(\tau)} \dots \sqrt{a_n}^{s_n(\tau)}} e_1^{s_1(\tau)} \dots e_n^{s_n(\tau)}. \text{ By anticommutativity of the } e_i, \text{ we obtain:} \\ \tilde{\xi}_\sigma \sigma \cdot \tilde{\xi}_\tau &= \frac{(-1)^{\sum_i \epsilon_i(\sigma) s_i(\sigma) + \sum_{i < j} s_i(\sigma) s_j(\tau)}}{\sqrt{a_1}^{s_1(\sigma) + s_1(\tau)} \dots \sqrt{a_n}^{s_n(\sigma) + s_n(\tau)}} e_1^{s_1(\sigma) + s_1(\tau)} \dots e_n^{s_n(\sigma) + s_n(\tau)} \end{aligned}$$

Consider the cocycle $\alpha : \mathcal{G}_{k_s} \rightarrow \mu_2(k_s)$ given by $\sigma \mapsto (-1)^{s_i(\sigma)}$. Since \mathcal{G}_{k_s} acts trivially on $\mu_2(k_s)$, the map $s_i : \mathcal{G}_{k_s} \rightarrow \mathbb{Z}/2\mathbb{Z}$ is a group morphism. Thus, $s_i(\sigma\tau) - s_i(\sigma) - s_i(\tau) \in 2\mathbb{Z}$.

Let us denote $m_{\sigma,\tau}^{(i)} = \frac{1}{2}(s_i(\sigma) + s_i(\tau) - s_i(\sigma\tau)) \in \mathbb{Z}$. Thus, $e_i^{s_i(\sigma) + s_i(\tau)} = e_i^{2m_{\sigma,\tau}^{(i)} + s_i(\sigma\tau)} = a_i^{m_{\sigma,\tau}^{(i)}} e_i^{s_i(\sigma\tau)}$ and $\sqrt{a_i}^{s_i(\sigma) + s_i(\tau)} = a_i^{m_{\sigma,\tau}^{(i)}} \sqrt{a_i} e_i^{s_i(\sigma\tau)}$, giving us

$$\tilde{\xi}_\sigma \sigma \cdot \tilde{\xi}_\tau = \frac{(-1)^{\sum_i \epsilon_i(\sigma) s_i(\sigma) + \sum_{i < j} s_i(\sigma) s_j(\tau)}}{\sqrt{a_1}^{s_1(\sigma\tau)} \dots \sqrt{a_n}^{s_n(\sigma\tau)}} e_1^{s_1(\sigma\tau)} \dots e_n^{s_n(\sigma\tau)} \text{ so that}$$

$$\tilde{\xi}_\sigma \sigma \cdot \tilde{\xi}_\tau \tilde{\xi}_{\sigma\tau}^{-1} = (-1)^{\sum_i \epsilon_i(\sigma) s_i(\sigma) + \sum_{i < j} s_i(\sigma) s_j(\tau)}.$$

The 2-cocycle $\beta : \mathcal{G}_{k_s} \times \mathcal{G}_{k_s} \rightarrow \mu_2(k_s)$ defined by $(\sigma, \tau) \mapsto (-1)^{\sum_i \epsilon_i(\sigma) s_i(\sigma) + \sum_{i < j} s_i(\sigma) s_j(\tau)}$ represents the class $[\delta^1(q')] \in H^2(k, \mu_2(k_s))$.

Using the properties of cup products,

$$\begin{aligned} \delta^1(q') &= \sum_i (a_i) \cup (c_i) + \sum_{i < j} (c_i) \cup (c_j) \\ &= \sum_i (a_i) \cup (b_i a_i^{-1}) + \sum_{i < j} (b_i a_i^{-1}) \cup (b_j a_j^{-1}) = \sum_i (a_i) \cup (a_i b_i) + \sum_{i < j} (a_i b_i) \cup (a_j b_j) \\ &= \sum_i (a_i) \cup (a_i) + \sum_{i < j} (a_i) \cup (a_j) + \sum_{i < j} (b_i) \cup (b_j) + \sum_{i,j} (a_i) \cup (b_j) \\ &= \sum_i (a_i) \cup (-1) + \sum_{i < j} (a_i) \cup (a_j) + \sum_{i < j} (b_i) \cup (b_j) + (\sum_i (a_i)) \cup (\sum_j (b_j)) \\ &= \det(q) \cup (-1) + w_2(q) + w_2(q') + \det(q) \cup \det(q') \\ &= w_2(q) + w_2(q') + \det(q) \cup -\det(q'). \end{aligned} \quad \square$$

Recall the ideal $I^n(K)$ generated by n -fold Pfister forms. By construction, we have the following nested sequence of ideals:

$$W(K) \supset I(K) \supset I^2(K) \supset \dots \supset I^n(K) \supset I^{n+1}(K) \supset \dots$$

Now consider the following map.

$$e_n : I^n(K) \rightarrow H^n(K, \mu_2) : \langle\langle a_1, \dots, a_n \rangle\rangle \mapsto a_1 \cup \dots \cup a_n$$

In the case $n = 2$, we have the following isomorphism given by e_2 .

Theorem 3.3.4 $I^2(K)/I^3(K) \cong H^2(K, \mu_2)$

Now we introduce an invariant on the set $W(K)$ involving the Hasse invariant.

Definition 3.3.5 Given a quadratic form q of order n . The Clifford invariant of q is given by

$$c(q) = w_2(q) + \begin{cases} 0 & n \equiv 1, 2 \pmod{8} \\ (-1) \cup (-\det(q)) & n \equiv 3, 4 \pmod{8} \\ (-1) \cup (-1) & n \equiv 5, 6 \pmod{8} \\ (-1) \cup (\det(q)) & n \equiv 7, 8 \pmod{8} \end{cases}$$

and depends only on the Witt class of q .

Remark 3.3.6 Careful computations will show that $c(\langle\langle a, b \rangle\rangle) = (a) \cup (b)$, which implies that $c|_{I^2} = e_2$.

3.4 Trace forms under Galois extensions

Given a quadratic form q over a field K and a nontrivial F -linear functional $s : K \rightarrow F$, we can define a quadratic form over F with the same vector space V as follows:

$$s \circ b_q(\cdot, \cdot) : V \times V \rightarrow F,$$

which we denote by (V, sq) . The map s is known as the Scharlau transfer.

Let $r : L \rightarrow L'$ be a morphism of field extensions over k . By the functorial properties of $\widehat{W}(-)$, r induces a map on the set of Witt-Grothendieck rings $\widehat{W}(K)$, where $K \supset k$, which we denote by

$$\hat{r}^* : \widehat{W}(L) \rightarrow \widehat{W}(L')$$

and is given by

$$V \rightarrow V_{L'}$$

The 1-dimensional quadratic space over k with bilinear form $(x, y) \mapsto xy, \forall x, y \in k$ is denoted by $\langle 1 \rangle_k$. The trace form of a field extension K/k , where K is separable, is denoted by $tr_K : K \times K \rightarrow k : (a, b) \mapsto tr_{K/k}(ab)$.

Let (V, q) be a quadratic space defined over K . Consider the action of K on V via an element $\sigma \in Aut(K)$ as follows:

$$a * v = \sigma(a)v, \forall a \in K, v \in V$$

with bilinear form $\sigma^{-1}b_q(\cdot, \cdot) : V \times V \rightarrow K$. Observe that $\sigma^{-1}b_q(a*x, y) = \sigma^{-1}b_q(\sigma(a)x, y) = \sigma^{-1}(\sigma(a)b_q(x, y)) = a\sigma^{-1}b_q(x, y)$, which shows the linearity of $\sigma^{-1}b_q$ with respect to the action of K on V . In particular, if $\langle a \rangle$ is a 1-dimensional K -form, then $\langle a \rangle^\sigma = \langle \sigma^{-1}(a) \rangle$ by definition. This induces a right action of $Aut(K)$ on $W(K)$ given by $(\langle a \rangle, \sigma) \mapsto \langle a \rangle^\sigma$.

Given a separable field extension K/F and a K -quadratic form q , we are able to relate orthogonal sums of twisted forms of q , mainly q^σ for $\sigma \in Aut(K)$, to scalar extensions of the form $tr_*(q)$, which we state below.

Theorem 3.5.1 Let the extension K/F be separable with Galois group G . Given a quadratic form (V, q) , we have the following isometry of quadratic forms:

$$K \otimes_F tr_*(q) \cong \perp_{\sigma \in G} q^\sigma$$

One consequence of the above is that $\perp_{\sigma \in G} q^\sigma$ lies in the image of the induced map r^* , where r is the inclusion $F \hookrightarrow K$.

Proof. First we need some notation to designate bilinear forms and quadratic spaces to both $K \otimes_F tr_*(q)$ and $\perp_{\sigma \in G} q^\sigma$. The underlying vector space of $K \otimes_F tr_*(q)$ is simply $K \otimes_F V$ whose bilinear form we denote by \tilde{B} . Keeping the notation used for twisted forms, the form $\perp_{\sigma \in G} q^\sigma$ has underlying vector space $\perp V^\sigma$. There is a natural way of defining an isometry from $K \otimes_F V$ to $\perp V^\sigma$ as follows:

$$f : K \otimes_F V \rightarrow \perp V^\sigma : k \otimes v \mapsto \sum_{\sigma \in G} k * v$$

Now we show that f indeed preserves inner products.

$$B^\sigma(f(k_1 \otimes v), f(k_2 \otimes v')) = \sigma^{-1}B(f(k_1 \otimes v), f(k_2 \otimes v')) = \sigma^{-1}B(\sum k_1 * v, \sum k_2 * v') = k_1 k_2 \sum \sigma^{-1}B(v, v') = k_1 k_2 \sum \tau B(v, v') = k_1 k_2 \text{tr}(B(v, v')) = K \otimes_F \text{tr}_*(q)((k_1 \otimes v), (k_2 \otimes v')) = \tilde{B}((k_1 \otimes v), (k_2 \otimes v')).$$

Note that $\dim_F K \otimes_F V = (\dim_k V)([K : F]) = \dim_F(\perp V^\sigma)$. Since we chose a separable extension, \tilde{B} is regular. Suppose there exists $z \in K \otimes_F V$ such that $f(z) = 0$. Then, z is in the radical of \tilde{B} by the above computation. But, \tilde{B} is regular, which implies that $z = 0$ and hence f is injective. \square

In view of the above theorem, $\text{im} r^* \subset W(K)^G$, where $G = \text{Gal}(K/F)$. So we may consider the following composition of maps:

$$W(K)^G \xrightarrow{\text{tr}_*} W(F) \xrightarrow{r^*} W(K)^G$$

Let the quadratic form q be in $W(K)^G$. By definition, $q \cong q^\sigma, \forall \sigma \in G$. Using the map constructed in the theorem, we have

$$r^*(\text{tr}_*(q)) = \sum q^\sigma = \sum q = n \cdot q,$$

which leads us to the following corollary:

Corollary 3.5.2 If r^* is injective, then $\text{tr}_*(\langle 1 \rangle_K) = n \cdot \langle 1 \rangle_F$.

Given a separable extension K/F , we have the trace map $\text{tr} : K \rightarrow F$, which induces a nontrivial F -form on the field K via the bilinear map $(x, y) \mapsto \text{tr}(xy)$. We shall denote this particular trace form of K by \mathcal{T}_K .

Theorem 3.5.3 Let E/k be a separable extension and E' be a subextension such that $[E : E'] = m$ is odd. Then, $\mathcal{T}_E \cong m \cdot \mathcal{T}_{E'}$.

Proof. By the functorial properties of the Scharlau transfer map tr_* , we have the following: $\text{tr}_{E/k_*}(\langle 1 \rangle_E) = \text{tr}_{E'/k_*} \circ \text{tr}_{E/E'_*}(\langle 1 \rangle_E) = \text{tr}_{E'/k_*}(m \cdot \langle 1 \rangle_{E'}) \cong m \cdot \mathcal{T}_{E'}$ \square

Lemma 3.5.4 Let K/F be a quadratic extension such that $K = F(\sqrt{a})$ for some non-square $a \in F$. Then, $\mathcal{T}_K \cong \langle 2, 2a \rangle$.

Proof. We use the result from lemma 3.1.4 that all regular quadratic forms q can be diagonalized by representable elements in $D(q)$.

Let $\{1, \sqrt{a}\}$ be an ordered basis for K . The symmetric matrix corresponding to \mathcal{T}_K is given by:

$$\begin{pmatrix} \text{tr}(1) & \text{tr}(\sqrt{a}) \\ \text{tr}(\sqrt{a}) & \text{tr}(a) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2a \end{pmatrix}$$

Thus, by lemma 3.1.4, $\mathcal{T}_K \cong \langle 2, 2a \rangle$.

□

Chapter 4

Results

4.1 Quadratic Forms and Étale algebras

In chapter 3, we briefly mentioned the quadratic form \mathcal{T}_E , where E is some separable extension of k . Keeping the same notation, we introduce it in the context of Étale algebras over k .

Definition 4.1.1 Let E be an Étale algebra of rank n over k . The trace form on E is given by:

$$E \rightarrow k : x \mapsto tr_{E/k}(x^2),$$

and is denoted by \mathcal{T}_E .

We will state some properties of trace forms of Étale algebras: Let E and E' be Étale algebras over k and K/k , a field extensions. Then,

- i. $tr_{E \times E'}((e, e')) = tr_{E/k}(e) + tr_{E'/k}(e')$
- ii. $tr_{E_K/K}(e \otimes 1) = tr_{E/k}(e)$
- iii. Given an isomorphism of algebras $f : E \rightarrow E'$, $tr_{E/k}(e) = tr_{E'/k}(f(e))$

In view of the properties above, we have the following lemma:

Lemma 4.1.2 Let E and E' be Étale algebras of rank n over k and let K be a field extension of k . Then,

- i. $\mathcal{T}_{E \times E'} \cong \mathcal{T}_E \perp \mathcal{T}_{E'}$
- ii. $\mathcal{T}_{E_K} \cong (\mathcal{T}_E)_K$
- iii. $E \cong E' \Rightarrow \mathcal{T}_E \cong \mathcal{T}_{E'}$

Let E be an Étale algebra of rank n over k . Then, we have the isomorphism of k -algebras

$$E_{k_s} \cong k_s^n$$

Let's call the above isomorphism f . By techniques in group cohomology, we obtain a cocycle $\alpha \in H^1(k, S_n)$ that represents the algebra E . Such α is defined as follows:

$$\alpha : \sigma \mapsto f \circ \sigma \cdot f^{-1}$$

By the above lemma, note that the trace form \mathcal{T}_E becomes isomorphic to $n \cdot \langle 1 \rangle$ via the isomorphism of the scalar extension of E by k_s with k_s^n . Thus, by Galois descent, composing our cocycle α with the inclusion $\iota : S_n \hookrightarrow O_n$ induces a cocycle $\iota \circ \alpha$ that represents the quadratic form \mathcal{T}_E . So we have the following important map:

$$H^1(k, S_n) \rightarrow H^1(k, O_n) : E \mapsto \mathcal{T}_E$$

4.2 Serre's formula

Now we are ready to discuss the main result of this chapter. As discussed earlier, given a group extension G by A , where G is Galois over a separable field extension E/k , we obtain the obstruction to the embedding problem by computing $e^*(s_n)$, where $e : \mathcal{G}_{k_s} \rightarrow S_n$ represents the Étale algebra E and $s_n \in H^2(S_n, \mu_2)$ represents the 2-extension of the symmetric group S_n whose restriction leads to the cocycle $e^*(s_n)$.

Since we are able to represent S_n in O_n as the group of permutation matrices over k_s , we should also be able to find the corresponding restriction of the extension Pin to the group S_n . In other words, we have the following commutative diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2(k_s) & \longrightarrow & X & \xrightarrow{\pi} & S_n & \longrightarrow & 1 \\
& & \downarrow \text{id}_{\mu_2(k_s)} & & \downarrow & & \downarrow \iota & & \\
1 & \longrightarrow & \mu_2(k_s) & \longrightarrow & Pin_n(k_s) & \xrightarrow{\alpha_{k_s}} & O_n(k_s) & \longrightarrow & 1
\end{array}$$

where $X = \alpha_{k_s}^{-1}(O_n(k_s))$ and $\pi = \iota^{-1} \circ \alpha_{k_s}$. Let the class $(2) \in H^2(k, \mu_2)$ be represented by the cocycle $\alpha : \mathcal{G}_{k_s} \rightarrow \mu_2$ given by $\sigma \mapsto \sigma(\sqrt{2})/\sqrt{2} = (-1)^{\chi(\sigma)}$. Moreover, let the signature morphism $\epsilon : S_n \rightarrow \{\pm 1\}$ be given by $\epsilon(\sigma) = (-1)^{\nu(\sigma)}$.

Lemma 4.2.1 The following two extensions:

$$1 \longrightarrow \mu_2(k_s) \longrightarrow X \xrightarrow{\alpha_{k_s}} S_n \longrightarrow 1,$$

and

$$1 \longrightarrow \mu_2(k_s) \longrightarrow \tilde{S}_n \xrightarrow{\alpha_{k_s}} S_n \longrightarrow 1$$

are equivalent.

Moreover, \mathcal{G}_{k_s} acts on X as follows: $\sigma \cdot x = (-1)^{\chi(\sigma)\nu(\pi(\sigma))}$, $\forall \sigma \in \mathcal{G}_{k_s}, x \in X$.

Proof. We need to show that the elements in X behave just like the elements in \tilde{S}_n keeping in mind the commutativity of the above diagram. Let $\{e_i\}_{1 \leq i \leq n}$ be the canonical basis for k_s^n . Then, the set $\{e_i\}$ is an orthonormal basis for $q_0 = n \times \langle 1 \rangle = \langle 1, \dots, 1 \rangle$. Via the orthogonal representation of S_n , let us identify the image of a transposition $(ij) \in S_n$ with $f_{ij} \in O_n(k_s)$. We want to show that $f_{ij} = \tau_{e_i - e_j}$. Now mapping $e_i - e_j$ under q_0 , we obtain

$$q_0(e_i - e_j) = q_0(e_i, e_i) - 2b_{q_0}(e_i, e_j) + q_0(e_j, e_j) = 2$$

Thus, $\tau_{e_i - e_j}$ is given by

$$a \mapsto a - b_{q_0}(e_i - e_j, a)(e_i - e_j)$$

Hence, $\tau_{e_i - e_j}(e_i) = e_i - b_{q_0}(e_i - e_j, e_i)(e_i - e_j) = e_i - (e_i - e_j)$ and $\tau_{e_i - e_j}(e_j) = e_j - b_{q_0}(e_i - e_j, e_j)(e_i - e_j) = e_j + (e_i - e_j) = e_i$.

By lemma 3.2.8, the preimages of $f_{ij} = \tau_{e_i - e_j}$ are $\pm \frac{1}{\sqrt{2}}(e_i - e_j)$. Squaring the quantity,

we have $(\pm \frac{1}{\sqrt{2}}(e_i - e_j))^2 = \frac{1}{2}q_0(e_i - e_j) = \frac{1}{2}(2) = 1$. Thus, the elements $\pm \frac{1}{\sqrt{2}}(e_i - e_j)$ in $Pin_n(k_s)$ have order 2. Similarly, given two disjoint transpositions $(ij), (kl) \in S_n$, the image of $(ij)(kl)$ in $O_n(k_s)$ under ι is $\tau_{e_i - e_j} \circ \tau_{e_k - e_l}$ whose preimage under π is $(\frac{1}{\sqrt{2}}(e_i - e_j))(\frac{1}{\sqrt{2}}(e_k - e_l)) = \frac{1}{2}(e_i - e_j)(e_k - e_l)$. Since $e_i - e_j$ and $e_k - e_l$ are mutually orthogonal, they anticommute. Thus,

$$\left(\frac{1}{2}(e_i - e_j)(e_k - e_l)\right)^4 = \left(-\frac{1}{4}(e_i - e_j)^2(e_k - e_l)^2\right)^2 = \left(-\frac{1}{4}q_0(e_i - e_j)q_0(e_k - e_l)\right)^2 = (-1)^2 = 1$$

Hence, the element $\frac{1}{2}(e_i - e_j)(e_k - e_l)$ has order 4. This structure on the set X is precisely the structure we find on \tilde{S}_n . Let $\pi(x) = (i_1 j_1)(i_2 j_2) \cdots (i_r j_r)$ be a product of disjoint transpositions. Then, as above, $x = \pm \frac{1}{\sqrt{2}}(e_{i_1} - e_{j_1}) \cdots (e_{i_r} - e_{j_r})$. Thus, $\sigma \cdot x = (-1)^{\chi(\sigma)\nu(\pi(x))}x$. \square

Theorem 4.2.2 $e^*(s_n) = w_2(\mathcal{T}_E) + (2) \cup (d_E)$

Proof. Recall the following commutative diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mu_2(k_s) & \longrightarrow & X & \xrightarrow{\pi} & S_n \longrightarrow 1 \\ & & \downarrow id_{\mu_2(k_s)} & & \downarrow & & \downarrow \iota \\ 1 & \longrightarrow & \mu_2(k_s) & \longrightarrow & Pin_n(k_s) & \xrightarrow{\alpha_{k_s}} & O_n(k_s) \longrightarrow 1 \end{array}$$

Applying the functor $H^*(k, -)$ to the above diagram, we obtain the following commutative diagram:

$$\begin{array}{ccc} H^1(k, S_n) & \xrightarrow{\delta^1} & H^2(k, \mu_2(k_s)) \\ \iota_* \downarrow & & \downarrow id \\ H^1(k, O_n) & \longrightarrow & H^2(k, \mu_2(k_s)) \end{array}$$

Given an Étale algebra E of rank n and its corresponding morphism $e : \mathcal{G}_{k_s} \rightarrow S_n$, by commutativity, we obtain: $\delta^1(E) = w_2(\iota_*(E)) = w_2(\mathcal{T}_E)$.

Now let t be a section of π with the condition that $t((1)) = 1$. Then, the class corresponding to the extension X is represented by the cocycle $\alpha : S_n \times S_n \rightarrow \mu_2$, uniquely determined by t as follows : $\alpha_{s_1, s_2} = t(s_1)t(s_2)t(s_1 s_2)^{-1}$, $\forall s_1, s_2 \in S_n$.

Define $x_\sigma = t(e_\sigma)$, $\forall \sigma \in \mathcal{G}_{k_s}$. Notice that $\pi(x_\sigma) = e_\sigma$. From the results in the last section of chapter 2, recall that $\delta^1(E)$ is represented by $\beta : \mathcal{G}_{k_s} \times \mathcal{G}_{k_s} \rightarrow \mu_2$ given by $\beta_{\sigma,\tau} = x_\sigma \sigma \cdot x_\tau x_{\sigma\tau}^{-1}$, $\forall \sigma, \tau \in \mathcal{G}_{k_s}$. By the above lemma,

$$x_\sigma \sigma \cdot x_\tau x_{\sigma\tau}^{-1} = x_\sigma (-1)^{\chi(\sigma)\nu(\pi(x_\tau))} x_\tau x_{\sigma\tau}^{-1} = (-1)^{\chi(\sigma)\nu(e_\tau)} x_\sigma x_\tau x_{\sigma\tau}^{-1}$$

Recall that the cocycle $\sigma \mapsto (-1)^{\chi(\sigma)}$ represents (2) and that $\epsilon : a \mapsto (-1)^{\nu(a)}$ is nothing but the signature morphism of S_n . Thus, the cocycle $\tau \mapsto (-1)^{\nu(e_\tau)}$ represents $\epsilon \circ e = d_E$. By the properties of cup products with values in μ_2 , the 2-cocycle $(\sigma, \tau) \mapsto (-1)^{\chi(\sigma)\nu(e_\tau)}$ represents (2) \cup d_E . Observe that $x_\sigma x_\tau x_{\sigma\tau}^{-1} = t(e_\sigma)t(e_\tau)t_{\sigma\tau}^{-1} = \alpha_{e_\sigma, e_\tau} = e^*(\alpha)_{\sigma, \tau}$. Since α is cohomologous to s_n , we obtain $\delta^1(E) = (2) \cup d_E + e^*(s_n)$.

Thus,

$$e^*(s_n) = w_2(\mathcal{T}_E) + (2) \cup d_E$$

□

4.3 2-extensions of D_n

Now we are ready to use the full machinery of Galois cohomology and quadratic forms to solve the embedding problem for 2-extensions of D_n . First let us note that $D_n \cong S_n$ for $n \leq 3$, which means that D_n is solvable since S_n already is. So we need only worry about $n > 3$. It is useful to denote the cardinality of D_n by some even integer m . The n -odd case we will treat using the results in section 3.5 while the n -even case, we will study using Clifford invariants of Witt classes of quadratic forms.

n -odd

Let D_n be Galois over a separable field extension E/k . The subgroup G_1 generated by rotations has index 2 in D_n . Thus, the field $K = E^{G_1}$ is quadratic. Since $[E : K] = n$ is odd, by Theorem 3.5.3, $E \cong n \cdot \langle K \rangle$. Furthermore, since K is quadratic, there exists some nonsquare $a \in F$ such that $K = k(\sqrt{a})$. By lemma 3.5.4, we obtain

$$\mathcal{T}_E \cong n \cdot \langle 2, 2a \rangle$$

Note that $\det(\mathcal{T}_E) = d_E = 4a = a \in k^\times/k^{\times 2}$. By Serre's formula, we have

$$\begin{aligned}
e^*(s_{2n}) &= w_2(\mathcal{T}_E) + (2) \cup (d_E) \\
&= \frac{n(n+1)}{2}(2) \cup (2a) + \frac{(n-1)(n)}{2}(2) \cup (2a) + (2) \cup d_E \\
&= 2n^2(2) \cup (2a) + (2) \cup d_E \\
&= (2) \cup d_E \\
&= (2) \cup (a)
\end{aligned}$$

Thus, the embedding problem is solvable if and only if a and $2a$ are norms in $k(\sqrt{2})/k$.

n -even

When we take tensor products of quadratic forms, we also take tensor products of the corresponding representative matrices. Thus, we have the following.

$$\mathcal{T}_{E \otimes E'} \cong \mathcal{T}_E \otimes \mathcal{T}_{E'},$$

where E and E' are two separable field extensions of k . Since n is even and greater than 3, we can write $2n = 2^r m$, where $r \geq 2$ is maximal and m is odd. Observe that there are n reflections x and a cyclic group of order n generated by y . However, only two elements of order 2 commute in D_n and these are x and $y^{n/2}$ since $xy = y^{-1}x$. By the theory of finite abelian groups, $\langle x, y^{n/2} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

By Galois correspondence, we have two disjoint quadratic extensions E_1 and E_2 over k . We can find a separable extension E' over k such that:

$$E \cong E_1 \otimes E_2 \otimes E'.$$

Thus,

$$\mathcal{T}_E \cong \mathcal{T}_{E_1} \otimes \mathcal{T}_{E_2} \otimes \mathcal{T}_{E'}$$

Now it is immediate that $\mathcal{T}_E \in I^3(k)$ if we apply the Scharlau transfer map. By theorem 3.3.4, \mathcal{T}_E corresponds to the zeroth class in $H^2(k, \mu_2)$. Thus, $e_2(\mathcal{T}_E) = 0$ and hence $c(q) = 0$.

If $2n \equiv 0 \pmod{8}$, then $w_2(\mathcal{T}_E) + (-1) \cup (\det(\mathcal{T}_E)) = 0$. Since all cocycles have values in μ_2 , $w_2(\mathcal{T}_E) = (-1) \cup (\det(\mathcal{T}_E))$. By Serre's obstruction formula, $e^*(s_{2n}) = w_2(\mathcal{T}_E) + (2) \cup d_E = (-1) \cup (\det(\mathcal{T}_E)) + (2) \cup (\det(\mathcal{T}_E)) = (-2) \cup 2(\det(\mathcal{T}_E)) = 0$.

If $2n \equiv 2 \pmod{8}$, then $w_2(\mathcal{T}_E) = 0$. Serre's formula gives $e^*(s_{2n}) = w_2(\mathcal{T}_E) + (2) \cup d_E = 0 + (2) \cup \det(\mathcal{T}_E) = (2) \cup \det(\mathcal{T}_E)$.

If $2n \equiv 4 \pmod{8}$, then $w_2(\mathcal{T}_E) + (-1) \cup (-\det(\mathcal{T}_E)) = 0$. Thus, $w_2(\mathcal{T}_E) = (-1) \cup (\det(\mathcal{T}_E))$. By Serre's formula, $e^*(s_{2n}) = w_2(\mathcal{T}_E) + (2) \cup d_E = (-1) \cup (-\det(\mathcal{T}_E)) + (2) \cup (\det(\mathcal{T}_E)) = (-2) \cup (-\det(\mathcal{T}_E))^2$. Note that $-\det(\mathcal{T}_E)^2$ is a norm of $k(\sqrt{-2})/k$. Thus, $e^*(s_{2n}) = 0$.

If $2n \equiv 6 \pmod{8}$, then $w_2(\mathcal{T}_E) + (-1) \cup (-1) = 0$; that is, $w_2(\mathcal{T}_E) = (-1) \cup (-1)$. By Serre's formula, $e^*(s_{2n}) = w_2(\mathcal{T}_E) + (2) \cup d_E = (-1) \cup (-1) + (2) \cup \det(\mathcal{T}_E) = (-2) \cup (-\det(\mathcal{T}_E))$.

From the above cases, we can see that the only obstructions are:

$$(2) \cup \det(\mathcal{T}_E) \text{ and } (-2) \cup (-\det(\mathcal{T}_E))$$

If $\det(\mathcal{T}_E)$ is a norm in $k(\sqrt{2})/k$, then the embedding problem is solvable whenever $m \equiv 2 \pmod{8}$. However, the case where $m \equiv 6 \pmod{8}$ requires the value of $\det(\mathcal{T}_E)$ to be negative since all norms in $k(\sqrt{2})/k$ are of the form $a^2 + 2b^2$ for some $a, b \in k$. After this is confirmed, then we check that $-\det(\mathcal{T}_E)$ is a norm in $k(\sqrt{-2})/k$.

Theorem 4.3.1 The embedding problem $(E/k, D_n, \mu_2)$ is solvable if:

- i. a is a norm in $k(\sqrt{2})/k$, where a is the discriminant of E , if n is odd.
- ii. $\det(\mathcal{T}_E)$ is a norm in $k(\sqrt{2})/k$ if $2n \equiv 2 \pmod{8}$
- iii. $-\det(\mathcal{T}_E)$ is a norm in $k(\sqrt{-2})/k$ if $2n \equiv 6 \pmod{8}$

REFERENCES

- [1] Bastida, Julio R. *Field Extensions and Galois Theory*. Encyclopedia of Mathematics and its Applications, Vol. 22 Addison-Wesley Publishing Company, Menlo Park, California. 1984.
- [2] Berhuy, Grégory *An Introduction to Galois Cohomology and its Applications*. Cambridge University Press, Cambridge, UK. 2010.
- [3] Gille, P. & Tamás, S. *Central Simple Algebras and Galois Cohomology*. Cambridge University Press, Cambridge, UK. 2006.
- [4] Hilton, P.J. & Stammach, U. *A Course in Homological Algebra*. Second Edition. Springer-Verlag, New York. 1996.
- [5] Lam, T.Y. *Introduction to Quadratic Forms over Fields*. Graduate Studies in Mathematics, Vol. 67 American Mathematical Society, Providence, Rhode Island. 2004.
- [6] Ledet, Arne *Brauer Type Embedding Problems*. Field Institute Monographs, No.21 American Mathematical Society, Providence, Rhode Island. 2005.