



universität
wien

MASTERARBEIT

Titel der Masterarbeit

„Orthogonal groups and their non-abelian group
cohomology“

Verfasser

Dominik Gruber BSc.

angestrebter akademischer Grad

Master of Science (MSc.)

Wien, 2011

Studienkennzahl lt. Studienblatt: A 066 821

Studienrichtung lt. Studienblatt: Mathematik

Betreuer: Prof. Dr. Joachim Schwermer

Contents

Introduction	1
1 Quadratic Forms and orthogonal groups	5
1.1 Quadratic forms and quadratic spaces	5
1.2 Quadratic forms and symmetric matrices	11
1.3 Quadratic forms over quadratically closed fields	13
2 Special orthogonal groups as linear algebraic groups	15
2.1 Affine varieties, morphisms and products	15
2.2 Linear algebraic groups	16
2.3 $SO(Q)_K$ as a linear algebraic group	19
3 Non-abelian group cohomology	23
3.1 Definition of cohomology sets and first results	23
3.2 An exact sequence in cohomology	25
3.3 Twisting	26
4 Galois Cohomology	29
4.1 Galois groups as topological groups	29
4.2 Galois descent and Hilbert 90	30
5 Computations of cohomology sets	35
5.1 A lemma on commuting actions	35
5.2 Description of $H^1(\mathcal{G}, SO(J_n)_{\overline{F}})$	37
5.3 Computation of $H^1(\tau, SO(J_n)_F)$	39
5.4 Computation of $H^1(\mathcal{G}, {}^bSO(J_n)_{\overline{F}}^{\tau})$	42
6 A consideration of fixed point sets	45
Summary	51
Zusammenfassung (Deutsch)	53
References	55
Author's curriculum vitae	57

Introduction

Let $G := SO(p, q)_{\mathbb{R}}$ be a special orthogonal group over the real numbers. Then the map $\tau : M \mapsto (M^{-1})^t$ is an involution on G and $K := G^{\tau}$ is a maximal compact subgroup of G . If Γ is a discrete, torsion-free, τ -stable subgroup of G , we have a canonical right-action of Γ on $X := K \backslash G$ and we have an induced action of the group $\langle \tau \rangle$ generated by τ on X/Γ . J. Rohlfs has shown in [7, Proposition 1.3 and the remark thereafter] that the set $(X/\Gamma)^{\tau}$ of fixed points in X/Γ under τ decomposes into a disjoint union

$$(X/\Gamma)^{\tau} \cong \bigsqcup_{[b] \in H^1(\tau, \Gamma)} F(b).$$

Here $H^1(\tau, \Gamma)$ is the first non-abelian cohomology set of $\langle \tau \rangle$ with values in Γ . The $F(b)$'s are closed immersed submanifolds that depend only on the cohomology class of the cocycle b in $H^1(\tau, \Gamma)$, i. e. if b and c are cocycles in $Z^1(\tau, \Gamma)$ satisfying $[b] = [c]$ in $H^1(\tau, \Gamma)$, then $F(b)$ and $F(c)$ coincide. Thus the notation makes sense. We will show that for $b \in Z^1(\tau, \Gamma)$, the manifold $F(b)$ is a locally symmetric space whose type only depends on the cohomology class of b in $H^1(\tau, G)$, i. e. if b and c are cocycles in $Z^1(\tau, G)$ satisfying $[b] = [c]$ in $H^1(\tau, G)$, then $F(b)$ and $F(c)$ are diffeomorphic. Therefore, the cohomology set $H^1(\tau, G)$ is of interest for determining the possible types of locally symmetric spaces arising in this construction and thus for the computation of $(X/\Gamma)^{\tau}$. By [7, Proposition 1.9], the Euler characteristic of $(X/\Gamma)^{\tau}$ equals the Lefschetz number of $\langle \tau \rangle$ acting on (X/Γ) . For further details on Lefschetz numbers see [7] and [9].

In this thesis we will give a description of $H^1(\tau, G)$, where G is a special orthogonal group over an arbitrary field of characteristic $\neq 2$ in terms of Galois cohomology. Over the field of the reals, this is the cohomology set appearing above. We will reach the result:

Theorem 5.13 *Assume that F is perfect with $\text{char } F \neq 2$ and let $\mathcal{G} := \text{Gal}(\overline{F}/F)$. Let $n \not\equiv 2 \pmod{4}$ and let $Z := \{I_{r,s,r} J_n \mid r, s \in \mathbb{N}, 2r + s = n\}$. We have a bijection:*

$$H^1(\tau, SO(J_n)_F) \rightarrow \bigsqcup_{b \in Z} \ker(H^1(\mathcal{G}, {}^b SO(J_n)_{\overline{F}}^{\tau}) \rightarrow H^1(\mathcal{G}, SO(J_n)_{\overline{F}})),$$

where $\sqcup$ denotes a disjoint union.

Here $J_n = (\delta_{i,n-j+1})_{i,j}$, the $n \times n$ -matrix with entries 1 on the off-diagonal and zeros everywhere else. The groups ${}^b SO(J_n)_{\overline{F}}^{\tau}$ are the fixed point sets of the b -twisted action of τ on $SO(J_n)_{\overline{F}}$. J. Rohlfs and J. Schwermer have given a similar description of $H^1(\tau, Sp_n(F))$, where $Sp_n(F)$ is the symplectic group in

dimension $2n$, in [8, Proposition 3.3]. In that case, the (more elegant) formula $H^1(\tau, Sp_n(F)) \cong H^1(\text{Gal}(\overline{F}/F), U_n(\overline{F}))$ holds, where F is a totally real number field and $U_n(\overline{F})$ is the unitary group over $\overline{F}$. This was the starting point for this thesis.

We now give an overview of the objects and methods used to prove the result of this thesis and to interpret it.

Let F be a field with $\text{char } F \neq 2$. A quadratic form on an F -vector space V is a map $q : V \rightarrow F$ for which there exists a symmetric bilinear form $b_q : V \times V \rightarrow F$ such that for all $x \in V$ we have $q(x) = b_q(x, x)$. A quadratic space is a vector space V together with a quadratic form q . Taking the finite-dimensional vector space F^n , a quadratic form on F^n is defined by a homogeneous polynomial of degree 2 in n variables. The quadratic space (V, q) is said to be regular if b_q is non-degenerate.

A simple example of a quadratic space is $\mathbb{R}^n$ with the squared Euclidean norm, which is induced by the Euclidean scalar product. An important property of this quadratic form q on $\mathbb{R}^n$ is that there is no nonzero vector x satisfying $q(x) = 0$, i. e. there are no nontrivial vectors of length zero. For a general quadratic form q , this need not be the case and we may have nonzero vectors satisfying $q(x) = 0$. This possibility makes the treatment of quadratic spaces in general somewhat more difficult than in the case of the Euclidean space.

For two quadratic spaces (V, q) and (V', q') over a field F we have the notion of isometry, i. e. two quadratic spaces are isometric if there is a linear bijection $f : V \rightarrow V'$ satisfying $q = q' \circ f$. We can also define the orthogonal group (and thus the special orthogonal group) of a quadratic space as the group of isometries mapping V onto itself.

We will give a treatment of the structure of quadratic spaces over fields of characteristic not equal to 2 which is based on [6, Chapter IV]. One result will be that over an algebraically closed field, any two n -dimensional quadratic spaces are isometric. We will also treat the corresponding orthogonal group in the finite dimensional case and in particular show that it is generated by mirror symmetries.

Next, we will use algebraic geometry to obtain results on the arithmetic in special orthogonal groups. Let F be an algebraically closed field. Considered as a matrix group, a special orthogonal group $SO(Q)_F$ is defined by algebraic equations, namely by

$$M^t Q M = Q, \det M = 1$$

where Q is a fixed symmetric matrix inducing the considered quadratic form and M^t is the transpose of M . Hence it is natural to consider $SO(Q)_F$ as a linear algebraic group. For our purposes, a linear algebraic group simply is a

matrix group over an algebraically closed field that is defined by polynomial equations in its coordinates. We give a brief introduction into this matter based on [12]. A particularly useful result will be theorem 2.8, which implies that any semi-simple element of $SO(Q)_F$ lies in a maximal torus and that any two maximal tori are conjugate.

We will then introduce the notion of non-abelian group cohomology. For this we take a topological group $\mathcal{G}$ that acts continuously on a discrete group A and define the 1-cocycles of $\mathcal{G}$ with values in A to be the set of continuous maps $\alpha : \mathcal{G} \rightarrow A, \gamma \mapsto \alpha_\gamma$ satisfying

$$\forall \gamma, \delta \in \mathcal{G} : \alpha_{\gamma\delta} = \alpha_\gamma \gamma \alpha_\delta.$$

We also define an equivalence relation on these 1-cocycles and obtain a pointed set of equivalence classes denoted by

$$H^1(\mathcal{G}, A),$$

the first cohomology set of $\mathcal{G}$ with values in A .

We will discuss two different settings of group cohomology. First, we let $\text{Gal}(E/F)$ with the Krull-topology act on a special orthogonal group $SO(Q)_E$ over the field E (which is a matrix group over E) by simply applying the Galois-automorphisms to each entry of the corresponding matrices. This is a well-understood object in the theory of Galois cohomology, which can be discussed in a more general setting.

Let F be a field and E a Galois extension. Let X be some algebraic object over E (for example a quadratic form, a central simple algebra,...). Then an F -form of X is a similar algebraic object X' over F which, after extending scalars to E , becomes isomorphic to X . For example, if X is some E -algebra, an F -form X' of X is an F -algebra satisfying $X' \otimes_F E \cong X$. Similarly, if X is a quadratic space (V, q) over E , i. e. an E -vector space together with a quadratic form, then an F -form of X is a quadratic space (V', q') over F satisfying that $(V' \otimes_F E, q' \otimes 1)$ is isometric to (V, q) .

Such forms of algebraic objects can be described by Galois cohomology. We have for many types of objects X that

$$H^1(\text{Gal}(E/F), \text{Aut}(X)_E) \cong \{F - \text{equivalence classes of } F - \text{forms of } X\},$$

where $\text{Aut}(X)_E$ is a suitable isomorphism group of X defined over E and F is a corresponding notion of equivalence over the field F .

This correspondence between Galois cohomology sets and forms is covered in [5, Chapter 7], and also in [10, Chapter III, 1]. In this thesis we will show a variant of this result for quadratic forms, i. e. we will show for any regular quadratic form Q defined over a perfect field F with $\text{char } F \neq 2$ that

the set $H^1(\text{Gal}(\overline{F}/F), O(Q)_{\overline{F}})$ maps bijectively to the F -isometry classes of quadratic forms over F . Here $O(Q)_{\overline{F}}$ is the orthogonal group corresponding to Q over an algebraic closure $\overline{F}$ of F . We will get a similar characterization of $H^1(\text{Gal}(\overline{F}/F), SO(Q)_{\overline{F}})$. On our way, we will show a generalization of Hilbert's Satz 90.

For the second application of group cohomology, assume that F is a perfect field. We will consider $SO(Q)_F$ as the F -points of the linear algebraic group $SO(Q)_{\overline{F}}$. We have a Cartan involution

$$\tau : M \mapsto (M^{-1})^t$$

on $SO(Q)_F$ and $SO(Q)_{\overline{F}}$ for a suitable choice of Q . If we also denote by τ the 2-element group generated by τ and consider this finite group with the discrete topology, we can consider the cohomology sets $H^1(\tau, SO(Q)_F)$ and $H^1(\tau, SO(Q)_{\overline{F}})$.

We will then use a lemma due to J. Rohlfs and B. Speh (see [9, Lemma 1.1]) to describe the cohomology set $H^1(\tau, SO(J_n)_F)$ in terms of Galois cohomology sets to obtain the aforementioned result in theorem 5.13. Here, again, $J_n = (\delta_{i, n-j+1})_{i,j}$, the $n \times n$ -matrix with entries 1 on the off-diagonal and zeros everywhere else.

Finally we will consider the case $F = \mathbb{R}$ and, based on our results, prove an explicit formula for $|H^1(\tau, SO(J_n)_{\mathbb{R}})|$ where $n \not\equiv 2 \pmod{4}$. We will also give a more explicit form of the submanifolds $F(b)$ of $(X/\Gamma)^\tau$ (notation as above) and calculate their possible dimensions.

1 Quadratic Forms and orthogonal groups

We give an introduction to quadratic forms over fields F with $\text{char } F \neq 2$ and show some basic results. Among other results, we will show that orthogonal groups are generated by mirror symmetries and that over a quadratically closed field, any two regular quadratic forms are equivalent.

We henceforth assume $\text{char } F \neq 2$ for any field F .

1.1 Quadratic forms and quadratic spaces

This section uses definitions and proofs similar to [6, Chapter IV].

Definition 1.1. Let F be a field with $\text{char } F \neq 2$. Let V be an F -vector space. A bilinear map $b : V \times V \rightarrow F$ is called a symmetric bilinear form on V if it satisfies:

$$\forall x, y \in V : b(x, y) = b(y, x).$$

A quadratic form on V is a map $q : V \rightarrow F$ for which there exists a symmetric bilinear form b_q on V such that $\forall x \in V : q(x) = b_q(x, x)$. A quadratic space (V, q) over a field F is an F -vector space V together with a quadratic form q on V . Let (V, q) and (V', q') be two quadratic spaces over a field F . An injective linear map $\sigma : V \rightarrow V'$ satisfying $\forall x \in V : q'(\sigma(x)) = q(x)$ is called an isometry of V into V' . A surjective isometry $V \rightarrow V'$ is called an isometry of V onto V' . If an isometry of V onto V' exists, V and V' are called isometric. The group of isometries of V onto V is a subgroup of $GL(V)$ called the orthogonal group of V and denoted by $O(V, q)$. The subgroup $O(V, q) \cap SL(V)$ is called the special orthogonal group of (V, q) and denoted by $SO(V, q)$. We say two quadratic forms q and q' on V are equivalent if (V, q) and (V, q') are isometric, i. e. if there is a linear bijection $\sigma : V \rightarrow V'$ such that $q = q' \circ \sigma$.

Lemma 1.2. Let F be a field with $\text{char } F \neq 2$ and let (V, q) be a quadratic space over F . There is exactly one symmetric bilinear form b_q on V satisfying $\forall x \in V : b_q(x, x) = q(x)$.

Proof. Consider the map $b_q : V \times V, (x, y) \mapsto \frac{q(x+y) - q(x) - q(y)}{2}$. It can easily be shown that this is a symmetric bilinear form satisfying $\forall x \in V : b_q(x, x) = q(x)$. Furthermore, any such symmetric bilinear form must satisfy the defining equation for b_q and hence b_q is unique. $\square$

Definition 1.3. Let (V, q) be an n -dimensional quadratic space.

- The unique symmetric bilinear form associated to q is denoted by b_q .
- A base $(v_1, \dots, v_n)$ of V satisfying $b_q(v_i, v_j) = 0$ for all i, j with $i \neq j$ is called an orthogonal base of (V, q) .

- Let W be a subset of V . We define the subspace $W^\perp := \{x \in V \mid \forall w \in W : b_q(x, w) = 0\}$.

Theorem 1.4 (Orthogonal base theorem). *Any finite dimensional quadratic space has an orthogonal basis.*

Proof. Let (V, q) be a finite dimensional quadratic space. We proceed by induction to $\dim V$. For $\dim V = 1$ the statement is trivial. Now consider the case $\dim V = n$ for $n > 1$. If q is the zero map $V \rightarrow F$, any base of V will fulfill the proposed equations. Otherwise, choose $b_1 \in V$ with $q(b_1) \neq 0$. Now the linear form $V \rightarrow F, x \mapsto b_q(x, b_1)$ has image of dimension one and hence kernel of dimension $n - 1$. Also, $\langle b_1 \rangle \cap \langle b_1 \rangle^\perp = 0$. Therefore, $V = \langle b_1 \rangle \oplus \langle b_1 \rangle^\perp$. By our inductive assumption we have an orthogonal base $(b_2, \dots, b_n)$ of $\langle b_1 \rangle^\perp$ and now $(b_1, \dots, b_n)$ is an orthogonal base of V . $\square$

Definition 1.5. Let (V, q) be a quadratic space over F . Let b be a symmetric bilinear form on V .

- The bilinear form b is called non-degenerate if for all $v \in V$ with $v \neq 0$ there exists $x \in V$ such that $b(x, v) \neq 0$.
- The quadratic space (V, q) is called regular if b_q is non-degenerate.
- The quadratic form q is called regular if (V, q) is regular.

Definition 1.6. Let (V, q) be a quadratic space over F . Let W be a subspace of V .

- We define $\text{rad } W = W \cap W^\perp$.
- We say W is regular if $\text{rad } W = 0$. This is the case if and only if $(W, q|_W)$ is regular as a quadratic space.
- We say W splits V if and only if the equation $V = W \oplus W^\perp$ holds.
- If W' is a subspace of V , we say W and W' are orthogonal if $W^\perp \subset W'$ (or equivalently $(W')^\perp \subset W$).
- The direct sum of pairwise orthogonal subspaces $W_1, \dots, W_n$ of V is denoted by $W_1 \perp \dots \perp W_n$.

Lemma 1.7. Let (V, q) be an n -dimensional regular quadratic space over F . Denote by $b_q(-, v)$ the map $V \rightarrow F, x \mapsto b_q(x, v)$. Then $\phi : V \rightarrow V^*, v \mapsto b_q(-, v)$ is a linear isomorphism (where V^* denotes the dual space of V , i. e. the space of F -linear maps $V \rightarrow F$).

Proof. It is obvious that ϕ is linear. We show that ϕ is injective: Let $\phi(v) = \phi(w)$ for $v, w \in V$. Then, for all $x \in V$: $b_q(x, v) = b_q(x, w)$. Hence, $b_q(x, v - w) = 0$ for all $x \in V$ and hence, since V is regular, $v - w = 0$ or equivalently $v = w$. For dimensional reasons, ϕ is surjective. $\square$

The statement implies that for $k \leq n$ and given linearly independent vectors $v_1, \dots, v_k \in V$, we can find linearly independent vectors $w_1, \dots, w_k \in V$ such that $b_q(w_i, v_j) = \delta_{i,j}$.

Lemma 1.8. *Let (V, q) be an n -dimensional regular quadratic space. A subspace W splits V if and only if W is regular. The space W is regular if and only if $W^\perp$ is regular.*

Proof. Choose a base $w_1, \dots, w_k$ of W and consider the map $\varphi : V \rightarrow V, x \mapsto \sum_{i=1}^k b_q(x, w_i)w_i$. Since b_q is non-degenerate by our assumption for (V, q) , φ has image W . Hence, $\ker \varphi$ has dimension $n - \dim W$ and obviously $\ker \varphi = W^\perp$. Now, $W \cap W^\perp = 0$ if and only if W is regular. The second statement follows from the facts that obviously $W \subset (W^\perp)^\perp$ and that, as we have seen above, $(\dim W^\perp)^\perp = n - \dim W^\perp = n - (n - \dim W) = \dim W$. Hence, $W = (W^\perp)^\perp$ which implies the second claim. $\square$

Lemma 1.9. *Let (V, q) be a finite-dimensional regular quadratic space. Let $W_1, \dots, W_n$ be regular, pairwise orthogonal subspaces and let W denote their sum. Then W is regular and the direct sum of the W_i 's, i. e.*

$$W = W_1 \perp \dots \perp W_n.$$

Proof. Take $w = w_1 + \dots + w_n \in W$ with $w_i \in W_i$ for all i and assume $b(x, w) = 0$ for all $x \in W$. Fix i and take $x_i \in W_i$. We have $b_q(x_i, w) = b_q(x_i, w_i)$. Since this holds for all $x_i \in W_i$ and W_i is regular, we have $w_i = 0$. Since i was arbitrary, we have that $w = 0$ and hence W is regular. To show that the sum is direct, again fix i and take $x = \sum_{j \neq i} x_j \in W_i \cap \sum_{j \neq i} W_j$ with $x_j \in W_j$ for $j \neq i$. Then, for $y_i \in W_i$, we have $b_q(y_i, x) = b_q(y_i, \sum_{j \neq i} x_j) = \sum_{j \neq i} b_q(y_i, x_j) = 0$ since the considered spaces are orthogonal. Analogously, $b_q(x, y_j) = 0$ for any $y_j \in W_j$ for $j \neq i$ since $x \in W_i$. Hence $b_q(x, y) = 0$ for any $y \in W$ and thus, since W is regular, $x = 0$. $\square$

Definition 1.10. *Let (V, q) be a quadratic space.*

- *We say $v \in V$ is isotropic if and only if $q(v) = 0$.*
- *A two-dimensional subspace H of V having a base (v, w) satisfying $q(v) = q(w) = 0$ and $b_q(v, w) = 1$ is called a hyperbolic plane.*
- *A subspace of V consisting only of isotropic vectors is called isotropic.*
- *We say $v \in V$ is anisotropic if and only if $q(v) \neq 0$.*

- A subspace of V consisting only of anisotropic vectors and 0 is called *anisotropic*.
- If V is anisotropic (as subspace of V), q is called *anisotropic*.

Lemma 1.11. *Let (V, q) be a regular quadratic space and let $x_1, \dots, x_r \in V$ be pairwise orthogonal linearly independent isotropic vectors. Then there are pairwise orthogonal hyperbolic planes $H_1, \dots, H_r$ such that $x_i \in H_i$ for all i . Any hyperbolic plane is regular.*

Proof. We use induction to r . For $r = 0$, the statement is trivial. Now let $r > 0$. Let W denote the span of the x_i 's. Consider the map $\varphi : V \rightarrow W, x \mapsto \sum_{i=1}^r b_q(x, x_i)x_i$. Since b_q is non-degenerate, φ is surjective. Choose $v \neq 0$ in the preimage of the space generated by x_r . Then, $b_q(x_r, v) \neq 0$ and, by scaling v , we may assume $b_q(x_r, v) = 1$. Also, v is orthogonal to all x_i for $i \neq r$. Now set $\mu := -\frac{1}{2}b_q(v, v)$ and $y_r = \mu x_r + v$. Note that $b_q(x_r, y_r) = b_q(x_r, v) = 1$. We have:

$$\begin{aligned} b_q(y_r, y_r) &= b_q(\mu x_r + v, \mu x_r + v) \\ &= \mu^2 b_q(x_r, x_r) + 2\mu b_q(x_r, v) + b_q(v, v) \\ &= 2\mu + b_q(v, v) \\ &= 0. \end{aligned}$$

Thus, x_r and y_r are a base of a hyperbolic plane which we denote by H_r . We show that H_r is regular: Choose $x = \lambda_1 x_r + \lambda_2 y_r \in H_r$. If $x \in H_r^\perp$, we have:

$$\begin{aligned} 0 &= b_q(x, x_r) \\ &= b_q(\lambda_1 x_r, x_r) + b_q(\lambda_2 y_r, x_r) \\ &= \lambda_2, \end{aligned}$$

and similarly $\lambda_1 = 0$. Hence, b_q restricts to H_r as a non-degenerate symmetric bilinear form and H_r is regular. Hence we may apply our inductive assumption to the vectors $x_1, \dots, x_{r-1}$ in the regular quadratic space $H_r^\perp$ (with the restriction of q as quadratic form). $\square$

For any finite-dimensional regular quadratic space (V, q) , we will show that any two maximal isotropic subspaces are isometric. For this we need some notation: Suppose there is $x \in V$ such that $q(x) \neq 0$ (i. e. x is anisotropic) and consider the map:

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

For $v \in V$ we have:

$$\begin{aligned}
q(\tau_x(v)) &= b_q(\tau_x(v), \tau_x(v)) \\
&= b_q\left(v - \frac{2b_q(v, x)}{q(x)}x, v - \frac{2b_q(v, x)}{q(x)}x\right) \\
&= b_q(v, v) - 2\frac{2b_q(v, x)}{q(x)}b_q(v, x) + \left(\frac{2b_q(v, x)}{q(x)}\right)^2 b_q(x, x) \\
&= b_q(v, v) = q(v).
\end{aligned}$$

Thus, $\tau_x \in O(V, q)$ for any anisotropic vector x . We obviously have $\tau_x(x) = -x$ and for any $v \in \langle x \rangle^\perp$: $\tau_x(v) = v$. A map of the form τ_x for some anisotropic x is called a (mirror) symmetry.

Lemma 1.12. *Let (V, q) be an n -dimensional regular quadratic space. Then $O(V, q)$ is generated by symmetries. Every element of $O(V, q)$ may be written as product of at most $2n - 1$ symmetries.*

Proof. For $\dim V = 1$, let $x \in V$ anisotropic. Then $\tau_x x = -x$. Now let $\dim V = n$ for $n > 1$ and let $\sigma \in O(V, q)$. Let $x \in V$ anisotropic and let $W = \langle x \rangle^\perp$. Note that W is regular. Suppose $\sigma x = x$ or $\sigma x = -x$. Then we have that $\sigma W = W$ and we may view σ as composition of two isometries, one on $\langle x \rangle$ and one on W . Hence we can apply the inductive assumption. Now suppose σx and x are linearly independent. Consider:

$$q(x \pm \sigma x) = q(x) \pm 2b_q(x, \sigma x) + q(\sigma x) = 2(q(x) \pm b_q(x, \sigma x)).$$

Since $q(x) \neq 0$ we have that $x + \sigma x$ or $x - \sigma x$ is anisotropic. Consider the case $y = x + \sigma x$ is anisotropic. Then

$$\begin{aligned}
\tau_y \circ \sigma(x) &= \sigma x - 2\frac{b_q(\sigma x, x + \sigma x)}{b_q(x + \sigma x, x + \sigma x)}(x + \sigma x) \\
&= \sigma x - 2\frac{b_q(\sigma x, x) + q(\sigma x)}{q(x) + q(\sigma x) + 2b_q(x, \sigma x)}(x + \sigma x) \\
&= -x,
\end{aligned}$$

since $q(x) = q(\sigma x)$. Since $\tau_y \circ \sigma(x) = -x$, by our considerations above, $\tau_y \circ \sigma$ is a product of symmetries. Hence, so is $\tau_y \circ \tau_y \circ \sigma = \sigma$. Similarly, if $\sigma x - x$ is anisotropic, then $\tau_{\sigma x - x} \circ \sigma(x) = x$ and the same argument holds. $\square$

Lemma 1.13. *Let (V, q) be a finite-dimensional quadratic space. If two regular subspaces U and W are isometric, then so are $U^\perp$ and $W^\perp$.*

Proof. We use induction to $\dim U$. First, assume U and W have dimension 1 and choose $x \neq 0$ in U and $y \neq 0$ in W such that $q(x) = q(y) \neq 0$. Such x and

y exist since U and W are isometric and the restrictions of q to U or W are nonzero. Now, consider the equation:

$$q(x+y) + q(x-y) = 2q(x) + 2q(y) = 4q(x).$$

Hence, $q(x+y)$ or $q(x-y)$ is not zero. Possibly replacing y by $-y$ we may assume that $q(x-y) \neq 0$ and we may therefore consider the map τ_{x-y} . Now by inserting in our definition, we have $\tau_{x-y}(x) = y$ and, since τ_{x-y} is an isometry, we have $\tau_{x-y}(U^\perp) = \tau_{x-y}(U)^\perp = W^\perp$.

Now consider the case $\dim U > 1$. Let φ be an isometry of U onto W and choose non-trivial subspaces U_1 and U_2 of U such that $U = U_1 \perp U_2$. We then have $W = \varphi(U_1) \perp \varphi(U_2)$. Set $W_1 := \varphi(U_1)$ and $W_2 := \varphi(U_2)$. Applying our inductive assumption to the isometric spaces U_1 and W_1 , we get that $U_2 \perp U^\perp = U_1^\perp$ and $W_2 \perp W^\perp = W_1^\perp$ are isometric. Choose an isometry $\psi : W_2 \perp W^\perp \rightarrow U_2 \perp U^\perp$. Applying our inductive assumption to the quadratic space $U_2 \perp U^\perp$ yields that, since U_2 and $\psi(W_2)$ are isometric, $U^\perp$ and $\psi(W^\perp)$ are isometric and hence so are $U^\perp$ and $W^\perp$. $\square$

Theorem 1.14 (Witt's theorem). *Let (V, q) be a finite-dimensional regular quadratic space, let U be a subspace of V and let σ be an isometry of U into V . Then there is a prolongation of σ to an isometry of V onto V .*

Proof. Choose W to be a complementary subspace to $\text{rad } U$ in U , i. e. such that $U = W \perp \text{rad } U$. Note that W is regular. Let $x_1, \dots, x_r$ be a base for $\text{rad } U$. These x_i are pairwise orthogonal, linearly independent, isotropic vectors in $W^\perp$ and hence there are hyperbolic planes $H_1, \dots, H_r \leq W^\perp$ that are pairwise orthogonal with $\forall i : x_i \in H_i$. Set $H := H_1 \perp \dots \perp H_r$. Since H is a regular subspace of the quadratic space $W^\perp$, there is $S \leq W^\perp$ such that $W^\perp = H \perp S$ and hence

$$V = H \perp S \perp W.$$

Set $U' := \sigma(U)$, $W' := \sigma(W)$ and $\forall i : x'_i := \sigma(x_i)$. Then,

$$\text{rad } U' = \sigma(\text{rad } U) = \langle x'_1, \dots, x'_r \rangle.$$

Also,

$$U' = W' \perp \text{rad } U'.$$

Now choose hyperbolic planes $H'_1, \dots, H'_r$ in $W'^\perp$ similarly as above such that $\forall i : x'_i \in H'_i$ and set $H' := H'_1 \perp \dots \perp H'_r$. Again, choose $S' \leq W'^\perp$ such that $W'^\perp = H' \perp S'$ and hence $V = H' \perp S' \perp W'$. The spaces H and H' are obviously isometric via an isometry that restricts to $U \cap H$ as $\sigma|_{U \cap H}$. Also, W and W' are isometric via $\sigma|_W$. Our lemma above implies that $S = (H \perp W)^\perp$ and $S' = (H' \perp W')^\perp$ are isometric and thus we may extend σ to $H \perp W \perp S = V$. $\square$

Corollary 1.15. *Any two maximal isotropic subspaces W and W' of V are isometric.*

Proof. Since q restricts to W and W' as the zero map respectively, we only need to show that they are isomorphic as vector spaces which is the case if and only if they have the same dimension. Assume $\iota = \dim W \leq \dim W'$. Let $w_1, \dots, w_\iota$ be a base of W . As in the proof above, we have pairwise orthogonal hyperbolic planes $H_1, \dots, H_\iota$ with $w_i \in H_i$ for all i . Set $H := H_1 \perp \dots \perp H_\iota$. Now let $w'_1, \dots, w'_\iota$ be linearly independent vectors in W' and choose corresponding pairwise orthogonal hyperbolic planes $H'_1, \dots, H'_\iota$ with $w'_j \in H'_j$ for all j and set $H' := H'_1 \perp \dots \perp H'_\iota$. Then H and H' are obviously isometric.

By our theorem above, an isometry of H onto H' may be prolonged to an isometry σ of V . Now since W is a maximal isotropic subspace of V , so is $\sigma(W)$ which, by construction, is a subspace of the isotropic space W' . Hence maximality yields $W' = \sigma(W)$, which implies the claim. $\square$

Definition 1.16. *Let (V, q) be a non-degenerate quadratic space of finite dimension. The dimension of a maximal isotropic subspace is called the Witt-index of (V, q) .*

1.2 Quadratic forms and symmetric matrices

Let (V, q) be an n -dimensional quadratic space over F . Choosing a base $(v_1, \dots, v_n)$ of V , we may express b_q in coordinates as:

$$F^n \times F^n \rightarrow F, (x, y) \mapsto x^t Q y,$$

where $Q = (b(v_i, v_j))_{i,j} \in F^{n \times n}$. We may thus identify any symmetric $n \times n$ -matrix Q with a quadratic form on F^n .

Lemma 1.17. *An n -dimensional quadratic F -space (V, q) is regular if and only if for any base $(v_1, \dots, v_n)$ of V , the matrix $Q := (b_q(v_i, v_j))_{i,j}$ is regular.*

Proof. Consider the linear map $\beta : V \rightarrow V, x \mapsto \sum_{i=1}^n b_q(x, v_i) v_i$. The matrix Q is the expression of β with respect to the chosen base. Now if b_q is non-degenerate, β is surjective and hence for dimensional reasons a bijection. On the other hand, assume that β is a bijection. Let $x \in V$ such that $\forall y \in V : b_q(x, y) = 0$. Then $x \in \ker \beta$ and therefore, $x = 0$. $\square$

Now consider the space F^n together with regular quadratic forms q and q' . Let $e_1, \dots, e_n$ be the standard base of F^n . Set $Q := (b_q(e_i, e_j))_{i,j}$ and $Q' := (b_{q'}(e_i, e_j))_{i,j}$. Then q and q' are equivalent if and only if there is a linear bijection $u : F^n \rightarrow F^n$ represented by a matrix U (with respect to the chosen base) such that for all $x, y \in F^n$:

$$x^t Q' y = (Ux)^t Q (Uy) = x^t (U^t Q U) y,$$

which is the case if and only if $U^tQU = Q'$. Similarly, if $q = q'$, U is an isometry of (F^n, q) if and only if $U^tQU = Q$. We define, in analogy to definition 1.1:

Definition 1.18. *Let F be a field and let $n \in \mathbb{N}$. Let Q be a regular symmetric $n \times n$ -matrix.*

- *Two regular symmetric $n \times n$ F -matrices S and S' are called F -equivalent if there is $U \in GL_n(F)$ such that $U^tSU = S'$.*
- *We define $O(Q)_F := \{M \in GL_n(F) | M^tQM = Q\}$, the orthogonal group of Q . We define $O_n(F) := O(I_n)_F$, where I_n is the $n \times n$ -identity matrix.*
- *We define $SO(Q)_F := \{M \in SL_n(F) | M^tQM = Q\}$, the special orthogonal group of Q . We define $SO_n(F) := SO(I_n)_F$, where I_n is the $n \times n$ -identity matrix.*

By our considerations, the identification of symmetric matrices and quadratic forms induces a bijection between the set of regular quadratic forms of F^n and the set of regular symmetric $n \times n$ matrices. The bijection preserves the notion of equivalence.

We will need the notion of a pointed set:

Definition 1.19. *A pointed set is a pair (X, x) where $x \in X$. The element x is called the base point. If (X, x) and (Y, y) are pointed sets, a map of pointed sets $(X, x) \rightarrow (Y, y)$ is a map $\phi : X \rightarrow Y$ satisfying $\phi(x) = y$. The kernel of ϕ , denoted $\ker \phi$, is the preimage of $\{y\}$ under ϕ , i. e. $\ker \phi = \phi^{-1}(\{y\})$. The notion of an exact sequence of pointed sets is defined in analogy to the notion of an exact sequence of groups.*

A pointed set (X, x) may be viewed as a set X containing a distinguished point.

Definition 1.20. *Let F be a field and let $n \in \mathbb{N}$. Let Q be a regular symmetric $n \times n$ -matrix.*

- *We define $F\text{-Isom}(Q)$ to be the pointed set of equivalence classes of regular quadratic forms of F^n (or equivalently, the set of F -equivalence classes of regular symmetric $n \times n$ matrices over F) with $[Q]$ as base point.*
- *We define the discriminant map $\text{disc} : F\text{-Isom}(Q) \rightarrow F^*/(F^*)^2$ by $[S] \mapsto \det(S) \cdot (F^*)^2$.*
- *We define $F\text{-Isom}^1(Q)$ to be the pointed set of equivalence classes of regular quadratic forms of F^n that have the same discriminant as $[Q]$ with $[Q]$ as base point.*

The following lemma will prove useful:

Lemma 1.21. *Let Q and S be two F -equivalent regular symmetric $n \times n$ -matrices and let $U \in GL_n(F)$ such that $U^tQU = S$. Then*

$$SO(Q)_F = USO(S)_FU^{-1}.$$

Proof. Let $x \in USO(S)_FU^{-1}$. Then $x = UyU^{-1}$ for some $y \in SO_F(S)$. We have $x^tQx = (U^{-1})^ty^tU^tQUyU^{-1} = (U^{-1})^ty^tSyU^{-1} = (U^{-1})^tSU^{-1} = Q$. Hence $USO(S)_FU^{-1} \subset SO(Q)_F$. An analogous calculation shows $U^{-1}SO(Q)U \subset SO(S)$ and our claim holds. $\square$

1.3 Quadratic forms over quadratically closed fields

Recall that a field F is quadratically closed if and only if $\{x^2 | x \in F\} = F$. Equivalently, every polynomial of degree 2 in F has zeros in F .

Lemma 1.22. *Let F be quadratically closed and V an n -dimensional vector space over F . Any two regular quadratic forms on V are equivalent.*

Proof. Let q and q' be two regular quadratic forms on V . Choose an orthogonal base $v_1, \dots, v_n$ of V with respect to q and an orthogonal base $v'_1, \dots, v'_n$ of V with respect to q' . Then there are λ_i and λ'_i in F^* for $i \in \{1, \dots, n\}$ such that $q(v_i) = \lambda_i$ and $q'(v'_i) = \lambda'_i$. The linear map $V \rightarrow V$ defined by $v_i \mapsto \sqrt{\frac{\lambda_i}{\lambda'_i}}v'_i$ for all i is an isometry of (V, q) onto (V, q') . $\square$

Lemma 1.23. *Let F be a quadratically closed field. Let (V, q) be a quadratic F -space with $\dim V > 1$. Then V contains a nonzero isotropic vector.*

Proof. Choose x and y linearly independent in V . For $\mu \in F$ consider:

$$b_q(x + \mu y, x + \mu y) = \mu^2 b_q(y, y) + 2b_q(x, y)\mu + b_q(x, x).$$

Now set μ to be a zero of the polynomial $b_q(y, y)X^2 + 2b_q(x, y)X + b_q(x, x)$. Then, $v := x + \mu y$ is a nonzero vector with $q(v) = 0$. $\square$

Corollary 1.24. *Any regular quadratic space (V, q) of dimension n over a quadratically closed field has Witt-index $\lfloor \frac{n}{2} \rfloor$.*

Proof. This can be proved by induction to n . For $n = 0$ and $n = 1$, the claim holds. For $n > 2$, choose a hyperbolic plane H in V and restrict q to the space $H^\perp$. By the inductive assumption, we can find $\lfloor \frac{n-2}{2} \rfloor = \lfloor \frac{n}{2} \rfloor - 1$ pairwise orthogonal linearly independent isotropic vectors in $H^\perp$. Also, we can obviously find one nonzero isotropic vector in H . Since $H \cap H^\perp = 0$ we have found $\frac{n}{2}$ pairwise orthogonal linearly independent isotropic vectors in V . Now lemma 1.11 ensures that this number is maximal. $\square$

Denote by J_n the Element of $F^{n \times n}$ having the form:

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

The matrix J_n is the $n \times n$ matrix that has ones on the off diagonal and zeros everywhere else. Note that $\det(J_n) = (-1)^{\lfloor \frac{n}{2} \rfloor}$. Also note that J_n may be considered over any field (in fact, over any ring with unit).

Corollary 1.25. *Let F be a quadratically closed field and let q be a quadratic form on F^n . There is a basis $(v_1, \dots, v_n)$ with respect to which q is represented by J_n .*

Proof. Let $\iota = \lfloor \frac{n}{2} \rfloor$. As in lemma 1.11 choose pairwise orthogonal hyperbolic planes $H_1, \dots, H_\iota$ and isotropic vectors v_i, v_{n-i+1} for $i \in \{1, \dots, \iota\}$ such that v_i and v_{n-i+1} span H_i and that $b_q(v_i, v_{n-i+1}) = 1$. If n is even, $v_1, \dots, v_n$ is a base of F^n with respect to which q is represented by J_n . If n is odd, there is a one-dimensional space $W := (H_1 \perp \dots \perp H_\iota)^\perp$. Since W is regular and F is quadratically closed, we may choose $v_{\iota+1} \in W$ with $q(v_{\iota+1}) = 1$. $\square$

2 Special orthogonal groups as linear algebraic groups

We now proceed to introduce the notion of a linear algebraic group, which requires some basic algebraic geometry. We will see that orthogonal groups over algebraically closed fields can be viewed as linear algebraic groups. We will state some general results on linear algebraic groups. Most importantly, theorem 2.8 will be useful in section 5 for determining cohomology sets.

The definitions and results of subsection 1 and 2 of this section are taken from [12, Chapters 1 and 2]. Another introduction to linear algebraic groups and results may be found in [1]. Subsection 3 will deal with applying the general results to special orthogonal groups.

2.1 Affine varieties, morphisms and products

Let K be an algebraically closed field. Set $S := K[T_1, \dots, T_n]$, the ring of polynomials in n variables over K for some $n \in \mathbb{N}$. If the number of variables we are considering is clear from context, we abbreviate $K[T] := K[T_1, \dots, T_n]$. We may interpret an element p of S as a K -valued function on $V := K^n$. We say, $x \in V$ is a zero of $p \in S$ if $p(x) = 0$ and we say $x \in V$ is a zero of an ideal I of S if x is a zero of all elements of I .

For an ideal I of S we set $\mathcal{V}(I)$ to be the set of all zeros of I . Conversely, for a subset X of V , we set $\mathcal{I}(X)$ to be the ideal of elements of S , such that all elements of X are zeros of all elements of S , i.e. $\mathcal{I}(X) = \{p \in S \mid \forall x \in X : p(x) = 0\}$, the ideal of elements of S vanishing on X . For an ideal I of S , set $\sqrt{I}$ the ideal whose elements p satisfy that $p^k \in I$ for some $k \in \mathbb{N}$.

We define a topology on V by setting the closed sets of V to be all sets of the form $\mathcal{V}(I)$ for ideals I of S . This is called the Zariski topology. We call a closed set of V an algebraic set. If X is an algebraic set in V , the Zariski topology on X is defined as the subset topology induced by the Zariski topology on V . The Zariski topology on an algebraic set is T_1 , noetherian and quasi-compact. (See [12, p. 2].)

Definition 2.1. *An affine algebraic variety over K is a pair $(X, K[X])$ where:*

- *X is an algebraic subset of $V = K^n$ for some $n \in \mathbb{N}$ viewed as topological space with the Zariski topology.*
- *$K[X]$ is the set of restrictions of elements of the polynomial ring $S = K[T_1, \dots, T_n]$ (viewed as functions $V \rightarrow K$) restricted to X . We identify $K[X]$ with the isomorphic K -algebra $S/\mathcal{I}(X)$.*

We will simply write X for the affine variety $(X, K[X])$. If $Y \subset X$ is closed in X , it is closed in V since X is closed in V . Hence, $(Y, K[Y])$ is a variety. We

call Y a subvariety of X .

Definition 2.2. Let $X \subset K^n$ and $Y \subset K^m$ be two affine K -varieties. Denote the polynomial ring corresponding to K^n as $K[T_1, \dots, T_n]$ and the one corresponding to K^m as $K[U_1, \dots, U_m]$. A morphism $\phi : X \rightarrow Y$ of affine varieties is a map $\phi : X \rightarrow Y$ of the form $x = (x_1, \dots, x_n) \mapsto (p_1(x), \dots, p_m(x))$ where $p_i \in K[X]$ for all i . Note that ϕ induces a homomorphism $\phi^* : K[Y] \rightarrow K[X], p(U_1, \dots, U_m) \mapsto p(p_1(T), \dots, p_m(T))$. Also note that ϕ is continuous.

Let X and Y be affine K -varieties where $I = \mathcal{I}(X)$ with $I \leq K[T_1, \dots, T_n]$ and $J = \mathcal{I}(Y)$ with $J \leq K[U_1, \dots, U_m]$. Consider the product of sets $X \times Y \leq K^n \times K^m = K^{n+m}$. If we view the polynomial algebra $K[T_1, \dots, T_n, U_1, \dots, U_m]$ as $K[T] \otimes_K K[U]$, we have $\mathcal{I}(X \times Y) = M$, where M is the ideal generated (as a $K[T] \otimes K[U]$ -module) by elements of the form $p \otimes 1$ for $p \in I$ and $1 \otimes q$ for $q \in J$. The resulting variety is called the product variety of X and Y and is denoted by $X \times Y$. We have that $K[X \times Y] \cong K[X] \otimes_K K[Y]$. Note that the Zariski topology of $X \times Y$ is generally distinct from and finer than the product topology of X and Y .

2.2 Linear algebraic groups

Definition 2.3. A linear algebraic group over an algebraically closed field K is an affine K -variety G with a distinguished element e (neutral element), a morphism $\mu : G \times G \rightarrow G, (g, h) \mapsto gh$ (multiplication) and a morphism $i : G \rightarrow G, g \mapsto g^{-1}$ (inversion) such that these maps define a group structure on G with e as neutral element. If G and G' are algebraic groups, a homomorphism of algebraic groups is a group homomorphism that is also a morphism of varieties.

Note that if H is a closed (in the Zariski topology) subgroup of a linear algebraic group G , H is an algebraic group.

Examples: We construct a few well-known groups as algebraic groups.

1) K^* , the multiplicative group of K : Consider K^2 and denote the corresponding polynomial ring by $K[T, Z]$. Set $I := (p)$, where $p = TZ - 1$. Set $G := \mathcal{V}(I)$. The multiplication $(x_1, x_2)(y_1, y_2) := (x_1y_1, x_2y_2)$ defines a group structure on G which is a morphism $G \times G \rightarrow G$. The corresponding inversion map is given by $(x_1, x_2)^{-1} = (x_2, x_1)$ which, again, is a morphism. Hence, G is a linear algebraic group which is obviously isomorphic to K^* as a group.

2) $SL_n(K)$: Consider the space K^{n^2} , which, as a K -vector space, we may also write as $M_n(K)$. Denote its polynomial ring by $K[T] := K[T_{11}, T_{1,2}, \dots, T_{1,n}, T_{2,1}, T_{2,2}, \dots, T_{n,n}]$. Set $I := (p)$, where $p = \det((T_{i,j})) - 1$. Then, $SL_n(K) := \mathcal{V}(I)$. The multiplication and the inversion map in $SL_n(K)$ are defined by polynomial equations, and therefore they are morphisms of varieties. Hence, $SL_n(K)$ is a linear algebraic group.

3) We use the techniques of 1) and 2) to construct $GL_n(K)$: Consider the space K^{n^2+1} which, as a K -vector space, we may also write as $M_n(K) \times K$. Denote its polynomial ring by $K[T, Z] := K[T_{11}, T_{1,2}, \dots, T_{2,1}, T_{2,2}, \dots, T_{n,n}, Z]$. Set $I := (p)$, where $p = \det((T_{i,j}))Z - 1$. Set $G := \mathcal{V}(I)$. Then, $G = \{(g, d) | (\det g)d = 1\}$. We have a multiplication $(g, d)(g', d') := (gg', dd')$, where the multiplication in the first component is matrix multiplication, the one in the second component is multiplication in K . This multiplication and the corresponding inversion map are defined by polynomial equations. Hence, G is a linear algebraic group which, as a group, is obviously isomorphic to $GL_n(K)$.

4) Let Q be a symmetric matrix in $GL_n(K)$. Consider the group $SO(Q)_K = \{M \in SL_n(K) | M^t Q M = Q\}$, where M^t denotes the transpose matrix of M . Obviously, transposition is a morphism $SL_n(K) \rightarrow M_n(K)$. Hence we may write $SO(Q)_K$ as the preimage of the closed set $\{Q\} \subset M_n(K)$ under the map $SL_n(K) \rightarrow M_n(K), M \mapsto M^t Q M$. Hence $SO(Q)_K$ is closed in $SL_n(K)$ and thus a linear algebraic group.

5) Let $D_n(K)$ denote the invertible diagonal $n \times n$ -matrices over K . Then $D_n(K)$ is closed in $GL_n(K)$.

Remark: From our remarks on the topology of $G \times G$ it follows that an algebraic group is not required to be a topological group. In fact, it is a topological group if and only if it is finite. (This follows from the following lemma together with the fact that algebraic varieties are T_1 . Any topological group that is T_1 is also T_2 and a nonempty irreducible T_2 -space consists of a single point.) However, for $x \in G$, the maps $\lambda_x : G \rightarrow G, g \mapsto xg$ as well as $\rho_x : G \rightarrow G, g \mapsto gx$ are morphisms of varieties. (In terms of K -coordinates of $g \in G \subset K^n$, xg is a polynomial expression in the coordinates of g whose coefficients are polynomials in the coordinates of x .)

We state some results for algebraic groups:

Lemma 2.4. *Let G be a linear algebraic group. The unique connected component G^0 of G containing e is a closed normal subgroup of finite index. G^0 is an irreducible topological space. Any closed subgroup of G of finite index contains G^0 .*

Proof. The proof can be found in [12, p. 25].

Let $X = \mathcal{V}(I)$ be an affine K -variety, where I is an ideal in some $K[T]$. Note that X is an irreducible topological space if and only if I is a prime ideal. Now the lemma shows that if G is a linear algebraic group which is an irreducible topological space, then G is connected.

Corollary 2.5. *The linear algebraic group K^* is connected.*

Proof. The defining polynomial $TZ - 1$ is prime and hence K^* is irreducible. $\square$

Definition 2.6. Let G be a linear algebraic group over K . A torus in G is a subgroup that is isomorphic to $D_n(K)$ for some $n \in \mathbb{N}$, where D_n is the subgroup of diagonal matrices in $GL_n(K)$. A maximal torus is a torus that is maximal with respect to the inclusion of sets.

Definition 2.7. Let G be a linear algebraic group over K . An element x of G is called semi-simple if for all homomorphisms of algebraic groups $\phi : G \rightarrow GL_n(K)$ for all $n \in \mathbb{N}$, $\phi(x)$ is diagonalizable.

Theorem 2.8. Let G be a connected linear algebraic group. Then we have:

- Every semi-simple element of G lies in a maximal torus.
- Two maximal tori of G are conjugate.

Proof. This non-elementary result can be found in [12, p. 108-109].

Corollary 2.9. Let G be a linear algebraic group. Let T be a maximal torus in G . Then G is connected if and only if $N_G(T) \leq G^0$.

Proof. Suppose $N_G(T) \leq G^0$. Let $x \in G$. We will show $x \in G^0$. We have $T' := xTx^{-1}$ is connected and hence subgroup of G^0 . Also, T' is a maximal torus in G^0 and by theorem 2.8 there is $z \in G^0$ such that $zT'z^{-1} = T$. We have $zxTx^{-1}z^{-1} = T$ and hence $zx \in N_G(T)$. Therefore, by assumption $zx \in G^0$ and since $z \in G^0$ we have $x \in G^0$. The converse implication is clear, since $G = G^0$ if G is connected. $\square$

The following result will prove useful later on:

Lemma 2.10. Let K be an algebraically closed field with $\text{char } K \neq 2$ and G be a linear algebraic group. Let $x \in G$ with $x^2 = 1$. Then x is semi-simple.

Proof. Let $x \in G$. Then for any homomorphism of algebraic groups $\phi : G \rightarrow GL_m(K)$ we have $\phi(x)^2 = 1$. Hence we show that $y \in GL_m(K)$ is diagonalizable if $y^2 = 1$. Since $y^2 = 1$, all eigenvalues of y lie in $\{1, -1\}$. We have an additive Jordan decomposition: $y = y_s + y_n$, where $y_s \in GL_m(K)$ is diagonalizable and y_n is in $M_m(K)$ is nilpotent and $y_sy_n = y_ny_s$. (This fact is proven in [12, Section 2.4].) Also, the characteristic polynomials of y and y_s are the same. By assumption we have:

$$1 = y^2 = (y_s + y_n)^2 = y_s^2 + 2y_sy_n + y_n^2.$$

Now since y_s is diagonalizable and has only eigenvalues in $\{1, -1\}$ we have $y_s^2 = 1$. This implies $-2y_sy_n = y_n^2$. Since $-2y_s$ is bijective, we have $\dim_K(\ker y_n) = \dim_K(\ker y_n^2)$. Hence we have $\ker y_n = \ker y_n^2$ and hence $y_n = 0$. $\square$

2.3 $SO(Q)_K$ as a linear algebraic group

We now consider special orthogonal groups as linear algebraic groups. We first proceed by finding a maximal torus in the group of matrices $SO(J_n)_F$ for

$$J_n = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \dots & \dots & 1 & \dots & \dots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix},$$

our standard form for a quadratic form over an algebraically closed field, which we introduced in chapter 1. We always assume that fields have a characteristic different from 2.

Lemma 2.11. *Let F be a field with more than three elements and let $n \in \mathbb{N}$ and set $q := \lfloor \frac{n}{2} \rfloor$. Let T be the subgroup of $G := SO(J_n)_F$ consisting of all diagonal matrices in $SO(J_n)_F$, i.e.*

$$T = \{\text{diag}(\lambda_1, \dots, \lambda_q, 1, \lambda_q^{-1}, \dots, \lambda_1) \mid \forall i : \lambda_i \in F^*\}.$$

(If n is even, skip the entry 1 at position $q + 1$.) Then we have: $T = Z_G(T)$ and hence T is a maximal abelian subgroup of G .

Proof. Let $x \in T$ such that x has an Eigenvalue, say, λ_k for $k \in \{1, \dots, q, n - q + 1, \dots, n\}$ or, equivalently, λ_k^{-1} of multiplicity 1 and let $z \in Z_G(T)$. Such an x exists since by our assumption on F , the multiplicative group F^* contains an element λ satisfying $\lambda \neq \lambda^{-1}$. Then we have:

$$ze_k = x^{-1}zxe_k = x^{-1}z\lambda_k e_k = \lambda_k x^{-1}ze_k.$$

Hence, ze_k is an Eigenvector of x^{-1} corresponding to λ_k^{-1} and hence in the space $\langle e_k \rangle$. Therefore, e_k is an Eigenvector of z and by analogy, all $e_1, \dots, e_q, e_{n-q+1}, \dots, e_n$ are eigenvectors of z . If n is even, we have shown that z is a diagonal matrix. If n is odd, ze_{q+1} is orthogonal to all $e_1, \dots, e_q, e_{n-q+1}, \dots, e_n$ and hence lies in the space e_{q+1} which means that e_{q+1} is an eigenvector as well. Therefore, z is a diagonal matrix. Now, since $z \in SO(Q)_F$, z lies in T . $\square$

Corollary 2.12. *Let F be a quadratically closed field and let Q be a symmetric regular 2×2 -matrix. Then the groups $SO(J_2)_F$, $SO(Q)_F$ and F^* are all isomorphic.*

Proof. As we have seen in 1.22, all non-degenerate quadratic forms of F^2 are equivalent. Hence, there exists $x \in GL_2(F)$, such that $x^t J_2 x = Q$. By lemma 1.21 we have $SO_2(Q) = x^{-1}SO(J_2)_F x$. Hence $x^{-1}Tx$ (where T is defined as above) is a subgroup of $SO_2(F)$ coinciding with its own centralizer. Obviously, T and hence $x^{-1}Tx$ is isomorphic to F^* . Now it is an easy exercise to show that $SO(J_2) = T$ and thus our claim holds. $\square$

Corollary 2.13. *Let K be algebraically closed and Q a symmetric regular 2×2 -matrix. Then $SO(Q)_K$ is a connected linear algebraic group.*

Proof. This holds since the isomorphism $K^* \rightarrow SO(Q)_K$ is obviously one of algebraic groups and by corollary 2.5, K^* is connected. $\square$

We now introduce the notion of the Weyl group of the maximal torus T in $SO(J_n)_F$ which will show us how elements of T transform under conjugacy with an element of the normalizer of T .

Lemma 2.14. *Let F be a field that has more than three elements. Let $G := SO(J_n)_F$ and let T be the maximal abelian subgroup of diagonal matrices as above. The Weyl group of T in $G := SO(J_n)_F$ is defined as $W = N_G(T)/Z_G(T)$. W acts on T as follows: $(wZ_G(T), t) := wt w^{-1}$. This action is well defined. We claim:*

- *Let $n = 2q + 1$. If $\bar{w} \in W$ and $t = \text{diag}(\lambda_1, \dots, \lambda_q, 1, \lambda_q^{-1}, \dots, \lambda_1^{-1})$, then there is a map $\epsilon : \{1, \dots, q\} \rightarrow \{0, 1\}$ and an element $\sigma \in S_q$ with:*

$$(\bar{w}, t) = \text{diag}(\lambda_{\sigma(1)}^{1-2\epsilon(1)}, \dots, \lambda_{\sigma(q)}^{1-2\epsilon(q)}, 1, \lambda_{\sigma(q)}^{2\epsilon(q)-1}, \dots, \lambda_{\sigma(1)}^{2\epsilon(1)-1}).$$

Conversely, $\bar{w}$ is uniquely determined by ϵ and σ . In fact,

$$W \cong S_q \ltimes (\mathbb{Z}/2\mathbb{Z})^q.$$

- *Let $n = 2q$. If $\bar{w} \in W$ and $t = \text{diag}(\lambda_1, \dots, \lambda_q, \lambda_q^{-1}, \dots, \lambda_1^{-1})$, then there is a map $\epsilon : \{1, \dots, q\} \rightarrow \{0, 1\}$ satisfying $\sum_{i=1}^q \epsilon(i) \equiv 0 \pmod{2}$ and an element $\sigma \in S_q$ with:*

$$(\bar{w}, t) = \text{diag}(\lambda_{\sigma(1)}^{1-2\epsilon(1)}, \dots, \lambda_{\sigma(q)}^{1-2\epsilon(q)}, \lambda_{\sigma(q)}^{2\epsilon(q)-1}, \dots, \lambda_{\sigma(1)}^{2\epsilon(1)-1}).$$

Conversely, $\bar{w}$ is uniquely determined by ϵ and σ . In fact,

$$W \cong S_q \ltimes (\mathbb{Z}/2\mathbb{Z})^{q-1}.$$

Proof. The first part of the proof is similar to the one of the lemma above. One can show, that an element ν of $N_G(T)$ maps eigenspaces of elements of T to eigenspaces, i. e. it can be viewed as composition of a diagonal matrix $\delta \in T$ with a permutation π of the vectors $e_1, \dots, e_n$ satisfying certain conditions because ν lies in G . Note that the simultaneous inversions $\lambda_k \mapsto \lambda_k^{-1}$ and $\lambda_k^{-1} \mapsto \lambda_k$ correspond to the transposition of two elements λ_k and λ_{n-k+1} . Conjugation with δ leaves elements of T invariant, and hence we can concern ourselves with the permutation part only, which is described by ϵ and σ as in the claim. In the case that n is even, π must satisfy that its corresponding matrix has determinant 1 which restricts the sign of π . If n is odd, however,

the matrix P corresponding to π may have 1 or -1 at $P_{q+1,q+1}$ hence π need not need fulfill any requirement for its sign. Therefore we must distinguish the two cases. $\square$

In the following lemmas, we identify the group of K -linear isometries $SO(V, q)$ with its corresponding matrix group for a chosen base. We assume K to be algebraically closed and therefore we may consider $SO(V, q)$ as an algebraic group. Note that the chosen base is irrelevant since by lemma 1.21, two different coordinate representations of the group are conjugate to one another via an element of $GL_{\dim V}(K)$.

Lemma 2.15. *Let (V, q) be a regular quadratic space with $n := \dim V \geq 4$ over an algebraically closed field K . Then $SO(V, q)$ is connected.*

Proof. Let $g \in SO(V, q) =: G$. By lemma 1.12 there are $N \in \mathbb{N}$ and $v_1, \dots, v_N \in V$ anisotropic vectors such that $g = \tau_{v_1} \circ \tau_{v_2} \circ \dots \circ \tau_{v_N}$. Since $\det g = 1$, we have that N is even. Let $i \in \{1, 3, \dots, N-1\}$ be odd. We show that $\tau_{v_i} \circ \tau_{v_{i+1}} \in G^0$. If this holds for all odd i , then $g \in G^0$. Consider the space $W := \langle v_i, v_{i+1} \rangle$. First, assume that W is regular. Then $V = W \perp W^\perp$ and $\tau_{v_i} \circ \tau_{v_{i+1}}$ leaves every element of $W^\perp$ fixed. Now consider the map $\phi_W : SO(W, q|_W) \rightarrow SO(V, q)$ which extends every map on W to V by defining $\phi_W(\lambda)|_{W^\perp} = \text{id}|_{W^\perp}$. This map is an injective morphism of algebraic groups, which in particular is continuous. Hence, since $SO(W, q|_W)$ is connected by corollary 2.13, $\phi(SO(W, q|_W))$ is connected and thus lies in G^0 . Therefore we have $\tau_{v_i} \circ \tau_{v_{i+1}} \in \phi(SO(W, q|_W)) \subset G^0$.

If W is not regular, we need to modify our proof by finding $v \in V$ anisotropic such that $\langle v_i, v \rangle$ and $\langle v_{i+1}, v \rangle$ are regular. We then replace $\tau_{v_i} \circ \tau_{v_{i+1}}$ by $\tau_{v_i} \circ \tau_v \circ \tau_v \circ \tau_{v_{i+1}}$ (which is the same map since $\tau_v \circ \tau_v = \text{id}_V$) and show as above that $\tau_{v_i} \circ \tau_v$ as well as $\tau_v \circ \tau_{v_{i+1}}$ are in G^0 which again yields the desired result. Consider $W^\perp$. We have that $\dim W^\perp = n - 2$. Since the Witt-index of V is $\lfloor \frac{n}{2} \rfloor$, $W^\perp$ contains an anisotropic vector v , if $n > 4$.

We are left with the case $n = 4$ and $\dim W^\perp = 2$. Assuming $W^\perp$ to be isotropic in this case, however, will yield that the matrix corresponding to an associated base is singular: Choose an orthogonal base (b_1, b_2) of W . Since we assume that W is not regular, we may assume b_2 to be isotropic. We assume that W is not isotropic, $W^\perp$ is isotropic and that $W \cap W^\perp \neq 0$. Hence there is $b_3 \in W^\perp \setminus W$ isotropic. We extend the vectors b_1, b_2, b_3 by a fourth vector b_4 to a basis (b_1, b_2, b_3, b_4) of W with respect to which q has the form:

$$\begin{pmatrix} \mu & 0 & 0 & \lambda_1 \\ 0 & 0 & 0 & \lambda_2 \\ 0 & 0 & 0 & \lambda_3 \\ \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \end{pmatrix},$$

where $\lambda_i = q(b_4, b_i)$ for all i . This matrix is singular, which contradicts the assumption that V is regular. Hence $W^\perp$ is not isotropic and as above, we may find an anisotropic vector $v \in W^\perp$. $\square$

Lemma 2.16. *Let (V, q) be regular quadratic space with $\dim V = 3$ over an algebraically closed field K . Then $SO(V, q)$ is connected.*

Proof. Corollary 1.25 shows that we may assume $V = K^3$ and $q : (x, y) \mapsto x^t J_3 x$. Let $G := SO(J_3)_K$. Then we have shown that the subgroup T of diagonal matrices is a maximal torus in G . In lemma 2.14 we have shown that $N_G(T) = T \cup nT$, where

$$n = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

If we can show that $n \in G^0$, corollary 2.9 yields the desired result. The map n fixes the vector $v = (1, 0, 1)^t$ which is not isotropic and thus generates the regular quadratic space $W := \langle v \rangle$. Now $W^\perp$ is a regular quadratic space as well and $n|_{W^\perp} \in SO(W^\perp, q|_{W^\perp})$.

The map $\phi : SO(W^\perp, q|_{W^\perp}) \rightarrow SO(V, q)$ that extends maps λ on $W^\perp$ to V by setting $\phi(\lambda)|_W = \text{id}|_W$ is an injective homomorphism of algebraic groups which in particular is continuous. Since $SO(W^\perp, q|_{W^\perp})$ is connected, so is $\phi(SO(W, q|_{W^\perp}))$. Hence $n \in \phi(SO(W, q|_{W^\perp})) \subset G^0$ and our claim holds due to corollary 2.9. $\square$

Corollary 2.17. *Let (V, q) be an n -dimensional regular quadratic space over an algebraically closed field K . Then $SO(V, q)$ is connected.*

Proof. This is a direct consequence of the preceding two lemmas and corollary 2.13. $\square$

3 Non-abelian group cohomology

We now introduce group cohomology for non-abelian groups. Cohomology sets have a wide variety of interpretations and uses, two of which will be discussed in the last two sections of this thesis. We base our definitions and statements on [5, pp. 383-387]. We only define the cohomology sets $H^i(\mathcal{G}, A)$ for $i = 0, 1$, where $\mathcal{G}$ and A are groups. There is an efficient way to generalize this definition for higher i if A is an abelian group. This, however, will generally not be the case in our considerations and therefore we omit this construction. It can be found in [11, Chapter VII].

3.1 Definition of cohomology sets and first results

An action of a group $\mathcal{G}$ on a set X is a map $\mathcal{G} \times X, (\gamma, x) \mapsto \gamma x$ satisfying:

- $\forall x \in X : 1x = x$, where 1 is the neutral element in $\mathcal{G}$.
- $\forall \gamma, \delta \in \mathcal{G}, x \in X : \gamma(\delta x) = (\gamma\delta)x$.

A topological group $\mathcal{G}$ is a group whose underlying set is endowed with a topology such that the multiplication $\mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}, (x, y) \mapsto xy$ and the inversion $\mathcal{G} \rightarrow \mathcal{G}, x \mapsto x^{-1}$ are continuous maps. An action of a topological group $\mathcal{G}$ on a topological space X is called continuous if the map $\mathcal{G} \times X, (\gamma, x) \mapsto \gamma x$ is continuous, where $\mathcal{G} \times X$ is endowed with the induced product topology. In our considerations, the set X which is acted upon by a group $\mathcal{G}$ will always carry the discrete topology.

Lemma 3.1. *Let $\mathcal{G}$ be a topological group acting on a discrete topological space X . The action of $\mathcal{G}$ on X is continuous if and only if for every $x \in X$, the subgroup $\text{Stab}(x) = \{\gamma \in \mathcal{G} | \gamma x = x\}$ is open in $\mathcal{G}$. The subgroup $\text{Stab}(x)$ is called the stabilizer of x .*

Proof. Suppose the stabilizer of each element in X is open. In order to show that the action of $\mathcal{G}$ on X is continuous, we need to verify that the preimage of each open set in X under the action $\alpha : \mathcal{G} \times X \rightarrow X$ is open in $\mathcal{G} \times X$. Since X is discrete and hence any open subset of X is the union of open sets containing one element each, it suffices to verify that the preimage under α of $\{x\}$ is open for any given $x \in X$. Let $(\gamma, y) \in \alpha^{-1}(\{x\})$. Since $\gamma y = x$, we have for $\sigma \in \text{Stab}(y)$: $(\gamma\sigma)y = \gamma(\sigma y) = \gamma y = x$ and hence the open set $\gamma\text{Stab}(y) \times \{y\}$ is contained in $\alpha^{-1}(\{x\})$. This observation yields:

$$\alpha^{-1}(\{x\}) = \bigcup_{(\gamma, y) \in \alpha^{-1}(\{x\})} \gamma\text{Stab}(y) \times \{y\}.$$

Being a union of open sets, this is an open set in $\mathcal{G} \times X$. Conversely, suppose that the action α is continuous. For $x \in X$, consider the intersection of open

sets: $\alpha^{-1}(\{x\}) \cap \mathcal{G} \times \{x\}$. This is easily seen to be $\text{Stab}(x) \times \{x\}$ and hence $\text{Stab}(x)$ is open. $\square$

We define:

Definition 3.2. Let A be a set with the discrete topology and $\mathcal{G}$ a topological group which operates continuously on A . We set:

$$H^0(\mathcal{G}, A) := \{a \in A \mid \forall \gamma \in \mathcal{G} : \gamma a = a\},$$

the set of $\mathcal{G}$ -invariant Elements of A . We also write:

$$A^{\mathcal{G}} := H^0(\mathcal{G}, A).$$

Now suppose A is a group. In this case, if we speak of a continuous action of a topological group $\mathcal{G}$ on A , we assume that A has the discrete topology and that $\mathcal{G}$ acts via group automorphisms, i. e. that $\forall \gamma \in \mathcal{G}, a, b \in A : \gamma(ab) = (\gamma a)(\gamma b)$. Such a group A is called a $\mathcal{G}$ -group. In this case, $H^0(\mathcal{G}, A)$ is a subgroup of A .

Recall our definition of pointed sets given in definition 1.19.

Definition 3.3. Let $\mathcal{G}$ be a topological group and A a $\mathcal{G}$ -group. A continuous map $\alpha : \mathcal{G} \rightarrow A, \gamma \mapsto \alpha_\gamma$ satisfying

$$\forall \gamma, \delta \in \mathcal{G} : \alpha_{\gamma\delta} = \alpha_\gamma \alpha_\delta$$

is called a 1-cocycle of $\mathcal{G}$ with values in A . The set of 1-cocycles of $\mathcal{G}$ with values in A is denoted by $Z^1(\mathcal{G}, A)$. Two cocycles $\alpha, \beta \in Z^1(\mathcal{G}, A)$ are said to be equivalent (or cohomologous), if there is $a \in A$, such that the following equation holds:

$$\forall \gamma \in \mathcal{G} : \beta_\gamma = a \alpha_\gamma \gamma a^{-1}.$$

This is an equivalence relation. Denoting this relation by $\sim$, we define:

$$H^1(\mathcal{G}, A) := Z^1(\mathcal{G}, A) / \sim,$$

the first cohomology set of $\mathcal{G}$ with values in A . If $\alpha \in Z^1(\mathcal{G}, A)$, we denote by $[\alpha]$ its cohomology class in $H^1(\mathcal{G}, A)$. The cohomology set $H^1(\mathcal{G}, A)$ is a pointed set with $[(\gamma \mapsto 1)]$ as base point.

If A is abelian, $Z^1(\mathcal{G}, A)$ has an evident group structure given by $(\alpha\beta)_\gamma := \alpha_\gamma \beta_\gamma$. This structure carries over to $H^1(\mathcal{G}, A)$. We have two basic facts:

Lemma 3.4 (Cohomology and products). Let $\mathcal{G}$ be a topological group and A and B two $\mathcal{G}$ -groups. Let $A \times B$ be the direct product of A and B , which becomes a $\mathcal{G}$ -group by setting $\gamma(a, b) := (\gamma a, \gamma b)$ for $\gamma \in \mathcal{G}, a \in A, b \in B$. Then there is a bijection of pointed sets:

$$H^1(\mathcal{G}, A) \times H^1(\mathcal{G}, B) \rightarrow H^1(\mathcal{G}, A \times B), ([\alpha], [\beta]) \mapsto [(\alpha, \beta)].$$

Proof. The proof is straightforward. For two cocycles $\alpha \in Z^1(\mathcal{G}, A)$ and $\beta \in Z^1(\mathcal{G}, B)$, we have for $\gamma, \delta \in \mathcal{G}$:

$$(\alpha_{\gamma\delta}, \beta_{\gamma\delta}) = (\alpha_{\gamma}\gamma\alpha_{\delta}, \beta_{\gamma}\gamma\beta_{\delta}) = (\alpha_{\gamma}, \beta_{\gamma})(\gamma\alpha_{\delta}, \gamma\beta_{\delta}) = (\alpha, \beta)_{\gamma}\gamma(\alpha, \beta)_{\delta}.$$

Hence, $(\alpha, \beta) \in Z^1(\mathcal{G}, A \times B)$. Equivalence of cocycles may be computed component-wise again and thus, the map is a well defined map of cohomology sets. Projecting cocycles in $Z^1(\mathcal{G}, A \times B)$ onto A and B respectively induces a map $H^1(\mathcal{G}, A \times B) \rightarrow H^1(\mathcal{G}, A) \times H^1(\mathcal{G}, B)$ that is obviously left- and right-inverse to our proposed map and thus our claim holds. $\square$

Lemma 3.5 (Cohomology and $\mathcal{G}$ -homomorphisms). *Let $\mathcal{G}$ be a topological group and A and B two $\mathcal{G}$ -groups. Let $\varphi : A \rightarrow B$ be a homomorphism of $\mathcal{G}$ -groups, i. e. a group homomorphism satisfying $\forall a \in A, \gamma \in \mathcal{G} : \varphi(\gamma a) = \gamma\varphi(a)$. Then there is a well-defined homomorphism*

$$\varphi^* : H^1(\mathcal{G}, A) \rightarrow H^1(\mathcal{G}, B), [\alpha] \mapsto [\varphi \circ \alpha].$$

If φ is bijective, then so is φ^ .*

Proof. Let $\alpha \in Z^1(\mathcal{G}, A)$ and consider $\beta := \varphi \circ \alpha$. For $\gamma, \delta \in \mathcal{G}$ we have:

$$\beta_{\gamma\delta} = \varphi(\alpha_{\gamma\delta}) = \varphi(\alpha_{\gamma}\gamma\alpha_{\delta}) = \varphi(\alpha_{\gamma})\gamma\varphi(\alpha_{\delta}) = \beta_{\gamma}\gamma\beta_{\delta}.$$

Hence, $\beta \in Z^1(\mathcal{G}, B)$. Consider a cocycle α' that is equivalent to α . Then there is $x \in A$ satisfying $\forall \gamma \in \mathcal{G} : \alpha'_{\gamma} = x\alpha_{\gamma}x^{-1}$. Then $\forall \gamma \in \mathcal{G} : (\varphi^*\alpha')_{\gamma} = \varphi(x)\beta_{\gamma}\gamma\varphi(x)^{-1}$ and hence, φ^* maps equivalent cocycles to equivalent cocycles. Therefore, it is well defined. If φ is bijective, there is an obvious left- and right-inverse, namely $(\varphi^{-1})^* : H^1(\mathcal{G}, B) \rightarrow H^1(\mathcal{G}, A), [\beta] \mapsto [\varphi^{-1} \circ \beta]$. $\square$

3.2 An exact sequence in cohomology

We will now derive a particularly useful exact sequence of cohomology sets. It is an exact sequence of pointed sets. For groups, the base point will always be the neutral element.

Let B be a $\mathcal{G}$ -group and A a $\mathcal{G}$ -subgroup, i. e. a subgroup of B which is stable under the action of $\mathcal{G}$. Consider the pointed set of left cosets of A in B , i. e. $B/A = \{bA | b \in B\}$. Since A is stable under the action of $\mathcal{G}$, there is a well defined action of $\mathcal{G}$ on B/A : $\mathcal{G} \times B/A \rightarrow B/A, (\gamma, bA) \mapsto (\gamma b)A$. The quotient topology on B/A is discrete since we assume the $\mathcal{G}$ -group B to be discrete, and by the definition of the quotient topology, the induced action is again continuous. We therefore may consider $H^0(\mathcal{G}, B/A) = (B/A)^{\mathcal{G}}$. Obviously, $B^{\mathcal{G}}$ projects naturally onto $(B/A)^{\mathcal{G}}$. Now, take an element $bA \in (B/A)^{\mathcal{G}}$ and consider the map $\alpha : \mathcal{G} \rightarrow A, \gamma \mapsto b^{-1}\gamma b$. This map has values in A , since $\gamma bA = bA$ and

hence $b^{-1}\gamma bA = A$ for any $bA \in (B/A)^{\mathcal{G}}$, $\gamma \in \mathcal{G}$. Also, it is easy to see that α is in $Z^1(\mathcal{G}, A)$. Taking a different element of bA , say ba for some $a \in A$, and making the same construction as above yields a 1-cocycle $\alpha' : \mathcal{G} \rightarrow A, \gamma \mapsto a^{-1}b^{-1}\gamma b\gamma a$, which is equivalent to α in $H^1(\mathcal{G}, A)$. We thus have a well-defined map:

$$\delta^0 : (B/A)^{\mathcal{G}} \rightarrow H^1(\mathcal{G}, A), bA \mapsto [(\gamma \mapsto b^{-1}\gamma b)].$$

Now, there is an exact sequence:

Lemma 3.6. *Let $\mathcal{G}$ be a topological group. Let B be a $\mathcal{G}$ -group and let A be a $\mathcal{G}$ -subgroup of B . The sequence of pointed sets*

$$1 \rightarrow A^{\mathcal{G}} \rightarrow B^{\mathcal{G}} \rightarrow (B/A)^{\mathcal{G}} \xrightarrow{\delta^0} H^1(\mathcal{G}, A) \rightarrow H^1(\mathcal{G}, B)$$

is exact, where δ^0 is defined as above and the other maps are the maps induced by the inclusion $A \rightarrow B$ and the projection $B \rightarrow B/A$ respectively.

Proof. Exactness at $B^{\mathcal{G}}$ is obvious. For exactness at $(B/A)^{\mathcal{G}}$ consider bA for some $b \in B^{\mathcal{G}}$. Then $b^{-1}\gamma b = 1$ for any $\gamma \in \mathcal{G}$ and therefore, $\delta^0(bA)$ is the class of the trivial cocycle in $H^1(\mathcal{G}, A)$. On the other hand, consider an element in the kernel of δ^0 , i. e. a left coset bA for some $b \in B$ for which there exists an $a \in A$, such that $\forall \gamma \in \mathcal{G} : b^{-1}\gamma b = a^{-1}\gamma a$. Then, $\forall \gamma \in \mathcal{G} : \gamma(ba^{-1}) = ba^{-1}$ and thus, $bA = ba^{-1}A$ lies in the image of $B^{\mathcal{G}}$.

Now it is obvious that the image of δ^0 lies in the kernel of the map $H^1(\mathcal{G}, A) \rightarrow H^1(\mathcal{G}, B)$. For the converse inclusion, consider a class of 1-cocycles in that kernel, represented by some 1-cocycle α . The cocycle α has values in A and there is $b \in \mathcal{G}$ such that $\forall \gamma \in \mathcal{G} : \alpha_{\gamma} = b^{-1}\gamma b$. Then $(\gamma b)A = b\alpha_{\gamma}A = bA$ and which implies $bA \in (B/A)^{\mathcal{G}}$. Therefore, $[\alpha]$ is the image of bA under δ^0 . $\square$

Corollary 3.7. *The map δ^0 induces a bijection between the orbit set of $B^{\mathcal{G}}$ in $(B/A)^{\mathcal{G}}$ and $\ker(H^1(\mathcal{G}, A) \rightarrow H^1(\mathcal{G}, B))$.*

Proof. Let $bA \in (B/A)^{\mathcal{G}}$ and $\beta \in B^{\mathcal{G}}$. Then, $\delta^0(\beta bA) = [b^{-1}\beta^{-1}\gamma(\beta b)] = [b^{-1}\gamma b]$ and thus the proposed map is well-defined. It follows from lemma 3.6 that it is surjective. To show that it is injective, choose bA and $b'A$ in $(B/A)^{\mathcal{G}}$ such that $\delta^0(bA) = \delta^0(b'A)$. Then, there is $a \in A$ such that $\forall \gamma \in \mathcal{G} : b^{-1}\gamma b = ab'^{-1}\gamma(b'a^{-1})$ or equivalently $\gamma(b'a^{-1}b^{-1}) = b'a^{-1}b^{-1}$. Now, $b'a^{-1}b^{-1} \in B^{\mathcal{G}}$ and $b'A = (b'a^{-1}b^{-1})bA$. Thus bA and $b'A$ lie in the same $B^{\mathcal{G}}$ -orbit. $\square$

3.3 Twisting

We introduce the notion of twisting, which will be a useful technical tool later on. Let $\mathcal{G}$ be a topological group and let B be a $\mathcal{G}$ -group and A a normal $\mathcal{G}$ -subgroup of B . Let $\alpha \in Z^1(\mathcal{G}, B)$. We define a new operation $*_{\alpha}$ of $\mathcal{G}$ on A by:

$$\gamma *_{\alpha} x := \alpha_{\gamma}\gamma(x)\alpha_{\gamma}^{-1}$$

for $\gamma \in \mathcal{G}$ and $x \in A$. This is an operation on A via automorphisms and it is continuous since α is a continuous map. If we consider A as a $\mathcal{G}$ -group with respect to this new operation (which depends on α) we write ${}^\alpha A$. (As groups, $A = {}^\alpha A$. As $\mathcal{G}$ -groups, however, this need not be the case.)

Lemma 3.8. *Let A be a $\mathcal{G}$ -group and let $b \in Z^1(\mathcal{G}, A)$. Then there is a bijection*

$$\rho_b : H^1(\mathcal{G}, {}^b A) \rightarrow H^1(\mathcal{G}, A), [\alpha] \mapsto [\alpha b],$$

satisfying

$$\rho_b([1]) = [b].$$

Proof. Let $\alpha \in Z^1(\mathcal{G}, {}^b A)$. First we show that $\alpha b \in Z^1(\mathcal{G}, A)$. We have for $\gamma, \delta \in \mathcal{G}$:

$$\begin{aligned} (\alpha b)_{\gamma\delta} &= \alpha_{\gamma\delta} b_{\gamma\delta} \\ &= \alpha_\gamma \gamma *_b (\alpha_\delta) b_\gamma \gamma b_\delta \\ &= \alpha_\gamma b_\gamma \gamma (\alpha_\delta) b_\gamma^{-1} b_\gamma \gamma b_\delta \\ &= (\alpha b)_\gamma \gamma (\alpha b)_\delta. \end{aligned}$$

Now let $\alpha, \beta \in Z^1(\mathcal{G}, {}^b A)$. Then $\alpha \sim \beta$ holds if and only if there is $a \in A$ such that for all $\gamma \in \mathcal{G}$ we have $\beta_\gamma = a \alpha_\gamma \gamma *_b a^{-1}$. This is equivalent to $\beta_\gamma b_\gamma = a \alpha_\gamma b_\gamma \gamma a^{-1} b_\gamma^{-1} b_\gamma$, or equivalently $(\beta b)_\gamma = a (\alpha b)_\gamma \gamma a^{-1}$. This shows that our map is injective. It obviously has an inverse map $\rho_{b^{-1}}$ and hence our claim holds. $\square$

Lemma 3.9. *Let A and B be $\mathcal{G}$ -groups and let $i : A \rightarrow B$ be a homomorphism of $\mathcal{G}$ -groups. Let $b \in Z^1(\mathcal{G}, A)$. Then $i \circ b \in Z^1(\mathcal{G}, B)$ and the following diagram commutes:*

$$\begin{array}{ccc} H^1(\mathcal{G}, {}^b A) & \xrightarrow{i^*} & H^1(\mathcal{G}, {}^{i \circ b} B) \\ \downarrow \rho_b & & \downarrow \rho_{i \circ b} \\ H^1(\mathcal{G}, A) & \xrightarrow{i^*} & H^1(\mathcal{G}, B) \end{array}$$

Here we use the notation of the previous lemma.

Proof. Let $[\alpha] \in H^1(\mathcal{G}, A)$. Then it is obvious that $i \circ \alpha \in Z^1(\mathcal{G}, B)$. We have:

$$\begin{aligned} \rho_{i \circ b} i^* [\alpha] &= [(i \circ \alpha)(i \circ b)] \\ &= [i \circ (\alpha b)] \\ &= i^* [\alpha b] \\ &= i^* \circ \rho_b [\alpha]. \end{aligned}$$

$\square$

4 Galois Cohomology

We now introduce the notions necessary to define and calculate Galois cohomology sets. We start by endowing Galois groups with a topology, the so-called Krull topology. Then we use the technique of Galois descent to prove a generalization of Hilbert's Satz 90. In the next section, we will give an interpretation of Galois cohomology sets with values in (special) orthogonal groups.

4.1 Galois groups as topological groups

Let F be a field and E a Galois extension of F . Let $\mathcal{E}$ be the set of Galois extensions of F contained in E which have finite degree over F . Now let $L, K \in \mathcal{E}$ with $K \subseteq L$. Since K is a normal field extension of F , the elements of $\text{Gal}(L/F)$ restricted to K are elements of $\text{Gal}(K/F)$. This restriction obviously is a group homomorphism $\text{Gal}(L/F) \rightarrow \text{Gal}(K/F)$ and we denote it by $\text{res}_{L/K}$. Now consider the direct product $P := \prod_{K \in \mathcal{E}} \text{Gal}(K/F)$. We shall consider the subset $\mathcal{G}'$ of P , whose elements $\varphi = (\varphi_K)_{K \in \mathcal{E}}$ satisfy the following equation for any $K, L \in \mathcal{E}$ with $K \subseteq L$:

$$\text{res}_{L/K}(\varphi_L) = \varphi_K.$$

It can easily be seen that $\mathcal{G}'$ is a group under the component-wise iteration of maps. Now consider $\mathcal{G} := \text{Gal}(E/F)$. The map $\Phi : \mathcal{G} \rightarrow P, \varphi \mapsto (\text{res}_{E/K})_{K \in \mathcal{E}}$ is an injective homomorphism with values in $\mathcal{G}'$. We will show that its image is $\mathcal{G}'$. Let $(\varphi_K)_{K \in \mathcal{E}}$ be in $\mathcal{G}'$. Consider the map $\varphi : E \rightarrow E, x \mapsto \varphi_{F(x)}(x)$. We will show that this is a field automorphism of E fixing F and thus an element of $\mathcal{G}$ which maps to $(\varphi_K)_{K \in \mathcal{E}}$ under Φ . Let x, y be in E . We have:

$$\begin{aligned} \varphi(x+y) &= \varphi_{F(x+y)}(x+y) \\ &= \varphi_{F(x,y)}(x+y) \\ &= \varphi_{F(x,y)}(x) + \varphi_{F(x,y)}(y) \\ &= \varphi_{F(x)}(x) + \varphi_{F(y)}(y) \\ &= \varphi(x) + \varphi(y), \end{aligned}$$

and analogously:

$$\varphi(xy) = \varphi(x)\varphi(y).$$

Also, since $\varphi_F \in \text{Gal}(F, F)$, φ restricts to the identity on F and thus, φ is in $\text{Gal}(E/F)$. It is obvious, that $\Phi(\varphi) = (\varphi_K)_{K \in \mathcal{E}}$. Hence Φ is surjective and, since we have already noted that it is an injective group homomorphism, it is a group isomorphism.

Now, if we consider the finite groups $\text{Gal}(K/F)$ with $K \in \mathcal{E}$ as discrete topological spaces, we get an induced product topology on P and an induced

topology on the subset $\mathcal{G}'$ which makes $\mathcal{G}'$ a topological group. Since $\mathcal{G}$ is isomorphic to $\mathcal{G}'$, we may carry over the topology on $\mathcal{G}'$ to $\mathcal{G}$ setting a subset of $\mathcal{G}$ to be open if and only if its image under Φ is open in $\mathcal{G}'$. Then the cosets $\gamma \text{Gal}(E/K)$ where K/F is a finite field extension and $\gamma \in \mathcal{G}$ form a base of the topology on $\mathcal{G}$.

Note that $\mathcal{G}'$ is a closed subset of P since its complement is easily seen to be open in P . Since all the groups $\text{Gal}(K/F)$ with $K \in \mathcal{E}$ are finite and hence compact, P is compact and so is the closed subset $\mathcal{G}'$.

Lemma 4.1. *Let E/F be a Galois extension of fields and let $\mathcal{G} := \text{Gal}(E/F)$ (considered as a topological group). Let $\mathcal{G}$ act on a discrete topological space X . The action is continuous if and only if for each $x \in X$, the stabilizer of x in $\mathcal{G}$ contains a Galois group $\text{Gal}(E/K)$, where K/F is a field extension of finite degree.*

Proof. By lemma 3.1 the considered action of $\mathcal{G}$ on X is continuous if and only if for every $x \in X$ the group $\text{Stab}(x) := \{\gamma \in \mathcal{G} | \gamma x = x\}$ is open in $\mathcal{G}$.

First assume that $\text{Stab}(x)$ is open. Then it must contain some coset $\gamma \text{Gal}(E/K)$ where K/F is a field extension of finite degree. This implies that $\gamma \in \text{Stab}(x)$ and hence so is γ^{-1} . Therefore $\text{Gal}(E/K) = \gamma^{-1} \gamma \text{Gal}(E/K)$ is contained in $\text{Stab}(x)$.

For the converse, assume that $\text{Stab}(x)$ contains some group $\text{Gal}(E/K)$ where K/F is a field extension of finite degree. The set $\text{Gal}(E/K)$ is open in $\mathcal{G}$ and hence so is $\text{Stab}(x) = \cup_{\gamma \in \text{Stab}(x)} \gamma \text{Gal}(E/K)$. $\square$

4.2 Galois descent and Hilbert 90

Let E/F be a Galois extension of a field F and $\mathcal{G}$ the corresponding Galois group. Let V be an E -vector space. We say, $\mathcal{G}$ operates on V by semilinear automorphisms, if the following holds:

$$\forall \gamma \in \mathcal{G}, v, w \in V, \lambda \in E : \gamma * (v + \lambda w) = \gamma * v + \gamma(\lambda) \gamma * w.$$

Lemma 4.2 (Galois descent). *Let E/F be a Galois extension and V an E -vector space with the discrete topology on which $\mathcal{G} := \text{Gal}(E/F)$ operates by continuous semilinear automorphisms. Then the following statements hold:*

- $V^{\mathcal{G}} = \{v \in V | \gamma * v = v\}$ is an F -vector space.
- The map $\varphi : V^{\mathcal{G}} \oplus_F E \rightarrow V, v \otimes \lambda \mapsto \lambda v$ is an isomorphism of E -vector spaces.

Proof. The proof is similar to the one given in [5, p. 280]. For the first statement, assume v and w to be in $V^{\mathcal{G}}$ and λ in F . Then, for $\gamma \in \mathcal{G}$ we have:

$$\gamma * (v + \lambda w) = \gamma * v + \gamma(\lambda) \gamma * w = v + \lambda w.$$

Therefore, $V^{\mathcal{G}}$ is an F -vector space.

Now we show that φ is surjective by constructing a preimage for arbitrary $v \in V$. Since $\mathcal{G}$ operates continuously on the discrete space V , by lemma 4.1 there is a finite Galois extension M/F contained in E such that v is stable under the action of $\text{Gal}(E/M)$. Let $n = [M : F]$ and $(m_i)_{1 \leq i \leq n}$ be a basis of M over F . Since $\text{Gal}(E/F)/\text{Gal}(E/M) \cong \text{Gal}(M/F)$, there are n left-cosets of $\text{Gal}(E/M)$ in $\text{Gal}(E/F)$. Choose $\gamma_1, \dots, \gamma_n$ to be representatives of these with γ_1 being the identity on E . Now, the restrictions $\gamma_1|_M, \dots, \gamma_n|_M$ are the n distinct elements of $\text{Gal}(M/F)$ and hence linearly independent over M by a theorem of Dedekind, which can be found in [3, p. 163]. Now, consider the matrix:

$$A := \begin{pmatrix} \gamma_1(m_1) & \dots & \gamma_n(m_1) \\ \dots & \dots & \dots \\ \gamma_1(m_n) & \dots & \gamma_n(m_n) \end{pmatrix}.$$

This matrix lies in $M_n(M)$ since any F -automorphism of E leaves the normal extension M invariant. Now if, say, the k -th column of A were to be a linear combination over M of the other columns, $\gamma_k|_M$ would be a linear combination of the other $\gamma_i|_M$'s as well, since the F -homomorphisms $\gamma_1|_M, \dots, \gamma_n|_M$ are determined by their values on the F -basis $m_1, \dots, m_n$ of M . Therefore, A is an invertible matrix. Set $(b_{i,j})_{i,j} := A^{-1}$. Now, consider the vectors $v_i := \sum_{j=1}^n (\gamma_j * v) \gamma_j(m_i)$. We have:

$$\begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix} = A \begin{pmatrix} \gamma_1 * v \\ \dots \\ \gamma_n * v \end{pmatrix}$$

Since we chose the γ_i 's to be representatives of the left-cosets of $\text{Gal}(E/M)$ in $\mathcal{G}$, we have for $\gamma \in \mathcal{G}$ that there is a permutation $\sigma \in S_n$, such that for any $k \in \{1, \dots, n\}$: $\gamma \gamma_k \text{Gal}(E/M) = \gamma_{\sigma(k)} \text{Gal}(E/M)$. Now, since $\text{Gal}(E/M)$ acts trivially on both v and the m_i 's, we have:

$$\gamma * v_i = \sum_{j=1}^n \gamma * (\gamma_j * v) \gamma_j(m_i) = \sum_{j=1}^n (\gamma_{\sigma(j)} * v) \gamma_{\sigma(j)}(m_i) = v_i.$$

Therefore, the v_i 's lie in $V^{\mathcal{G}}$ and

$$v = \gamma_1 * v = \sum_{j=1}^n b_{1j} v_j = \varphi \left(\sum_{j=1}^n v_j \otimes b_{1j} \right).$$

Therefore, $v \in \varphi(V^{\mathcal{G}} \oplus_F E)$ and φ is surjective.

Now, to prove injectivity of φ , choose $k > 0$ minimal such that there exists $x \in \ker \varphi$ satisfying $x = \sum_{i=1}^k x_i \otimes \lambda_i$ for $x_i \in V^{\mathcal{G}}$, $\lambda_i \in E$ with the x_i 's linearly

independent over F . We may assume that $\lambda_1 \in F$. Then, there is $\gamma \in \mathcal{G}$ such that for some λ_i : $\gamma(\lambda_i) \neq \lambda_i$, for otherwise the x_i 's would be linearly dependent over F . Consider $y = x - \gamma x = \sum_{i=2}^k x_i \otimes (\lambda_i - \gamma(\lambda_i))$. Then y is nonzero, lies in $\ker \varphi$ and the x_i 's are still linearly independent over F . This contradicts the minimality of k . Hence, any element of $\ker \varphi$ must be 0. $\square$

With the help of this lemma, we can prove a useful result about Galois-cohomology:

Theorem 4.3. *Let E/F be a Galois extension and A a central simple F -algebra of finite dimension. We have:*

$$H^1(\text{Gal}(E/F), (A \otimes_F E)^*) = 1.$$

Here the operation of $\text{Gal}(E/F)$ on $(A \otimes_F E)^*$ is the one induced by $\forall \gamma \in \mathcal{G}, a \in A, \lambda \in E : \gamma(a \otimes \lambda) := a \otimes \gamma(\lambda)$.

Proof. The proof is an adaption of the one given in [5, p. 393]. Set $A_E := A \otimes_F E$ with the discrete topology and $\mathcal{G} := \text{Gal}(E/F)$. The considered operation of $\mathcal{G}$ on A_E^* is obviously continuous and satisfies for $\gamma \in \mathcal{G}, a, b \in A_E : \gamma(ab) = (\gamma a)(\gamma b)$, i. e. it is an action by group automorphisms. Let $\alpha \in Z^1(\mathcal{G}, A_E^*)$. We define a new operation $*$ of $\mathcal{G}$ on A_E by:

$$\forall \gamma \in \mathcal{G}, a \in A_E : \gamma * a := \alpha_\gamma \gamma(a).$$

This operation, restricted to A_E^* , is again continuous since α and the multiplication of A_E are continuous maps. It is also a semilinear operation on A_E in the sense of lemma 4.2. Therefore we have that $U := \{a \in A_E \mid \forall \gamma \in \mathcal{G} : \gamma * a = a\}$ is an F -vector space and $f : U \otimes_F E \rightarrow A_E, (u \otimes \lambda) \mapsto u\lambda$ is an isomorphism of E -vector spaces. For $u \in U, a \in A, \gamma \in \mathcal{G}$ we have:

$$\gamma * (u(a \otimes 1)) = \alpha_\gamma \gamma(u(a \otimes 1)) = \alpha_\gamma \gamma(u)(a \otimes 1) = (\gamma * u)(a \otimes 1) = u(a \otimes 1).$$

Hence $u(a \otimes 1) \in U$ and, by identifying $A \cong A \otimes 1$, U is an A -right module. Since $U \otimes_F E \cong A \otimes_F E$ we have that $\dim_E(U \otimes E) = \dim_E(A \otimes E)$ and hence $\dim_F U = \dim_F A$. Now, since A is central and simple, by Wedderburn's Theorem (see [5, p. 4]) we have a division algebra D over F such that $A \cong M^{n \times n}(D)$ as F -algebras. Since U is an A -module, U is isomorphic to $D^{r \times n}$ for some $r \in \mathbb{N}$ operated on by the elements of $M^{n \times n}(D) \cong A$ by matrix-multiplication from the right. Since $\dim_F U = \dim_F A$ we have $r = n$ and hence, A and U are isomorphic as A -right modules. Let $g : A \rightarrow U$ be an isomorphism of A -right modules. Set:

$$\varphi := f \circ (g \otimes \text{id}_E) : A_E \rightarrow A_E, a \otimes \lambda \mapsto g(a)\lambda.$$

φ is a bijection. For $a, b \in A, \lambda, \mu \in E$ we have:

$$\begin{aligned}\varphi((a \otimes \lambda)(b \otimes \mu)) &= f(g(ab) \otimes \lambda\mu) \\ &= f(g(a)(b \otimes 1) \otimes \lambda\mu) \\ &= g(a)(b \otimes 1)\lambda\mu \\ &= g(a)\lambda(b \otimes \mu) \\ &= \varphi(a \otimes \lambda)(b \otimes \mu).\end{aligned}$$

Hence, φ is an isomorphism of A_E -right modules and therefore it is the left-multiplication by $a := \varphi(1 \otimes 1) = g(1) \in U \cap A_E^*$. Now we have $\forall \gamma \in \mathcal{G} : a = \gamma * a = \alpha_\gamma \gamma(a)$ or equivalently $\alpha_\gamma = a\gamma(a^{-1})$. Therefore, α is equivalent to the trivial cocycle and since α was arbitrary our claim holds. $\square$

Corollary 4.4. *Let E/F be a Galois extension and $n \in \mathbb{N}$. Then we have:*

$$H^1(\text{Gal}(E/F), GL_n(E)) = 1.$$

Proof. Choose the central simple F -algebra $M_n(F)$ of $n \times n$ matrices with entries in F and apply the theorem. $\square$

Corollary 4.5 (Satz 90). *Let E/F be a finite Galois extension such that $\mathcal{G} := \text{Gal}(E/F)$ is a cyclic group generated by γ . Then all elements x of E satisfying $N_{E/F}(x) = 1$ are of the form $y\gamma(y^{-1})$ for some $y \in E$.*

Proof. Let $n := [E : F]$ and let α be in $Z^1(\mathcal{G}, E^*)$, where E^* denotes the multiplicative group of E . Then we have for any $k \geq 1$: $\alpha_{\gamma^k} = \alpha_\gamma \gamma(\alpha_{\gamma^{k-1}})$. Hence α is determined by $\alpha_\gamma =: x$. We have $1 = \alpha_1 = \alpha_{\gamma^n} = x\gamma(x)\gamma^2(x)\dots\gamma^{n-1}(x) = N_{E/F}(x)$. Conversely any element of norm 1 induces a 1-cocycle in this manner. Now the corollary above yields that there is $y \in E$ such that $x = \alpha_\gamma = y\gamma(y^{-1})$. $\square$

Now let E/F be a Galois extension and consider $GL_n(E)$ for some n . Set $\mathcal{G} := \text{Gal}(E/F)$. The determinant map is a surjective homomorphism $\det : GL_n(E) \rightarrow E^*$. Also, $\det$ commutes with the action of $\mathcal{G}$ on $GL_n(E)$ and E^* respectively, i. e. for $M \in GL_n(E), \gamma \in \mathcal{G} : \det(\gamma M) = \gamma(\det(M))$. The kernel of $\det$ is $SL_n(E)$. We have an exact sequence:

$$1 \rightarrow SL_n(E) \rightarrow GL_n(E) \xrightarrow{\det} E^* \rightarrow 1.$$

By lemma 3.6, this sequence induces an exact sequence of pointed sets:

$$1 \rightarrow SL_n(F) \rightarrow GL_n(F) \xrightarrow{\det} F^* \rightarrow H^1(\mathcal{G}, SL_n(E)) \rightarrow 1.$$

Here we use: $SL_n(E)^\mathcal{G} = SL_n(F)$, $GL_n(E)^\mathcal{G} = GL_n(F)$, $(GL_n(E)/SL_n(E))^\mathcal{G} \cong (E^*)^\mathcal{G} = F^*$ and $H^1(\mathcal{G}, GL_n(E)) = 1$. Hence, there is a bijection:

$$H^1(\mathcal{G}, SL_n(E)) \rightarrow F^* / \det(GL_n(F)) = 1.$$

Corollary 4.6. *We have shown:*

$$H^1(\mathrm{Gal}(E/F), SL_n(E)) = 1.$$

5 Computations of cohomology sets

We will now use the results developed in the previous sections to describe certain cohomology sets. For any field F we always assume $\text{char } F \neq 2$.

5.1 A lemma on commuting actions

In order to compute some cohomology sets, the following lemma will prove useful. It is similar to [8, p. 153].

Lemma 5.1. *Let $\mathcal{G}$ and T be two groups operating on a group G via automorphisms such that the actions commute, i.e. $\forall \gamma \in \mathcal{G}, \tau \in T, g \in G$:*

$$\gamma(\tau(g)) = \tau(\gamma(g)).$$

Then, there is a bijection between the orbit set of $G^{\mathcal{G}}$ in $(G/G^T)^{\mathcal{G}}$ and the orbit set of G^T in $(G/G^{\mathcal{G}})^T$.

Proof. Consider a coset gG^T in $(G/G^T)^{\mathcal{G}}$. For any $\gamma \in \mathcal{G}$ we have $g^{-1}\gamma(g) \in G^T$. Thus, for any $\gamma \in \mathcal{G}, \tau \in T$ we have:

$$g^{-1}\gamma(g) = \tau(g^{-1}\gamma(g)) = \tau(g^{-1})\tau(\gamma(g)) = \tau(g^{-1})\gamma(\tau(g)),$$

and hence:

$$g\tau(g^{-1}) = \gamma(g)\gamma(\tau(g^{-1})) = \gamma(g\tau(g^{-1})).$$

Therefore, $g^{-1}G^{\mathcal{G}} \in (G/G^{\mathcal{G}})^T$. Now, choosing a different representative $g' = gt$ for some $t \in G^T$ yields the element $t^{-1}g^{-1}G^{\mathcal{G}}$ in $(G/G^{\mathcal{G}})^T$ which lies in the G^T -orbit of $gG^{\mathcal{G}}$. Also, choosing a different element sgG^T for $s \in G^{\mathcal{G}}$ in the $G^{\mathcal{G}}$ -orbit of gG^T yields the same coset $g^{-1}s^{-1}G^{\mathcal{G}} = g^{-1}G^{\mathcal{G}}$. Therefore, we have a well-defined map: $G^{\mathcal{G}} \setminus (G/G^T)^{\mathcal{G}} \rightarrow G^T \setminus (G/G^{\mathcal{G}})^T, [gG^T] \mapsto [g^{-1}G^{\mathcal{G}}]$. Obviously, there is an inverse map and thus we have a bijection. $\square$

Corollary 5.2. *Under the assumptions of the lemma and adding the assumption that $\mathcal{G}$ and T be topological groups and the considered actions be continuous, we have a bijection of pointed sets:*

$$\ker\left(H^1(T, G^{\mathcal{G}}) \rightarrow H^1(T, G)\right) \longrightarrow \ker\left(H^1(\mathcal{G}, G^T) \rightarrow H^1(\mathcal{G}, G)\right).$$

Proof. This follows from corollary 3.7 and the preceding lemma. The bijection has the following form: Let $[\alpha] \in \ker(H^1(T, G^{\mathcal{G}}) \rightarrow H^1(T, G))$. Then there is $g \in G$ such that $\forall \tau \in T : \alpha_{\tau} = g^{-1}\tau g$. The corresponding element in $\ker(H^1(\mathcal{G}, G^T) \rightarrow H^1(\mathcal{G}, G))$ is the class of the cocycle $\gamma \mapsto g\gamma g^{-1}$. $\square$

Recall the definition

$$J_n = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \dots & \dots & 1 & \dots & \dots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix},$$

i. e. J_n is the $n \times n$ -matrix with entries 1 on the off diagonal and zeros in the other entries. We may view J_n over any field F . We define the map $\tau : GL_n(F) \rightarrow GL_n(F), M \mapsto (M^{-1})^t$. We identify τ , which is a group automorphism of order two, with the two-element group generated by it. For any subgroup $G \leq GL_n(F)$ that is preserved by τ (i. e. $\tau(G) \subset G$), we will identify $\tau|_G = \tau$. The group τ obviously operates on G and considering τ and G with the respective discrete topologies, this action is continuous. A cocycle $\alpha \in Z^1(\tau, G)$ is determined by its value α_τ at the element τ , since $\alpha_1 = 1$. We will identify the cocycle α with its value α_τ at τ . We have that $1 = \alpha_1 = \alpha_{\tau^2} = \alpha_\tau \tau \alpha_\tau$ and hence $\alpha_\tau = \tau \alpha_\tau^{-1} = \alpha_\tau^t$. Hence the elements of $Z^1(\tau, G)$ are simply symmetric matrices. We now show that τ preserves $SO(J_n)_F$:

Lemma 5.3. *Let F be a field and τ defined as above. Then we have:*

$$\tau(SO(J_n)_F) \subset SO(J_n)_F.$$

Proof. Let $G := SO(J_n)_F$. Since τ is the composition of the inversion map and the transposition map and since the inversion map certainly preserves G , we only need to show that for any $M \in G$, we have $M^t \in G$. This is the case if and only if $M J_n M^t = J_n$. Note that $M^t J_n M = J_n$ and $J_n^2 = 1$. We calculate:

$$\begin{aligned} J_n &= J_n (M^t)^{-1} M^t \\ &= J_n (M^t)^{-1} J_n^2 M^t \\ &= J_n (M^t)^{-1} M^t J_n M J_n M^t \\ &= J_n^2 M J_n M^t \\ &= M J_n M^t \end{aligned}$$

□

Corollary 5.4. *Let F be a perfect field and let $\bar{F}$ be an algebraic closure of F . Set $\mathcal{G} := \text{Gal}(\bar{F}/F)$. Let $n \in \mathbb{N}$ and let $b \in Z^1(\tau, SO(J_n)_F)$. Then the action of $\mathcal{G}$ commutes with the b -twisted action of τ . There is a bijection of pointed sets:*

$$\begin{aligned} \ker \left(H^1(\tau, {}^b SO(J_n)_F) \rightarrow H^1(\tau, {}^b SO(J_n)_{\bar{F}}) \right) &\longrightarrow \\ \ker \left(H^1(\mathcal{G}, {}^b SO(J_n)_{\bar{F}}) \rightarrow H^1(\mathcal{G}, SO(J_n)_{\bar{F}}) \right). \end{aligned}$$

Proof. We apply 5.2, setting $G = SO(J_n)_{\bar{F}}$, $\tau = T$ and, as defined, $\mathcal{G} = \text{Gal}(\bar{F}/F)$. The action of $\mathcal{G}$ on $SO(J_n)_{\bar{F}}$ is defined by $(\gamma, (x_{i,j})_{i,j}) \mapsto (\gamma(x_{i,j}))_{i,j}$

for $\gamma \in \mathcal{G}$ and $(x_{i,j})_{i,j}$ in $SO(J_n)_{\overline{F}}$ (i. e. by applying the field automorphism γ to each entry of the matrix $(x_{i,j})_{i,j}$). This action is in fact continuous (where, as we defined in section 3, $SO(J_n)_{\overline{F}}$ is regarded with the discrete topology). Then $G^{\mathcal{G}} = SO(J_n)_F$ and $G^T = SO(J_n)_{\overline{F}}^{\tau}$. $\square$

The set $H^1(\tau, SO(J_n)_F)$ appears in the computation of certain fixed point sets, as we will see in section 6. First we will give a description of the Galois-cohomology sets appearing in the corollary. Then we will give a description of $H^1(\tau, SO(J_n)_F)$ in terms of Galois cohomology and look at the example $F = \mathbb{R}$.

5.2 Description of $H^1(\mathcal{G}, SO(J_n)_{\overline{F}})$

Let F be a perfect field and let $\overline{F}$ be an algebraic closure of F . Set $\mathcal{G} := \text{Gal}(\overline{F}/F)$. As mentioned above, the topological group $\mathcal{G}$ acts continuously on the discrete group $GL_n(\overline{F})$ by $(\gamma, (x_{i,j})_{i,j}) \mapsto (\gamma(x_{i,j}))_{i,j}$ for $\gamma \in \mathcal{G}$ and $(x_{i,j})_{i,j}$ in $GL_n(\overline{F})$. This action may obviously be restricted to $SO(Q)_{\overline{F}}$ where Q is a symmetric $n \times n$ matrix defined over F . It may also be restricted to $SL_n(\overline{F})$. We will determine the set $H^1(\mathcal{G}, SO(J_n)_{\overline{F}})$. Let Q be a regular, symmetric $n \times n$ matrix over F . As we have seen above, the symmetric matrix Q may be considered as an element of $Z^1(\tau, GL_n(F)) \subset Z^1(\tau, GL_n(\overline{F}))$. Consider the Q -twisted action of τ on $SL_n(\overline{F})$, which we defined as $\tau *_Q x = Q^{-1}(x^{-1})^t Q$ for $x \in SL_n(\overline{F})$. It is an easy calculation to show: ${}^Q SL_n(F)^{\tau} = SO(Q)_{\overline{F}}$. Corollary 5.2 yields a bijection:

$$\ker\left(H^1(\tau, {}^Q SL_n(F)) \rightarrow H^1(\tau, {}^Q SL_n(\overline{F}))\right) \longrightarrow \ker\left(H^1(\mathcal{G}, SO(Q)_{\overline{F}}) \rightarrow H^1(\mathcal{G}, SL_n(\overline{F}))\right).$$

Now corollary 4.6 yields $H^1(\mathcal{G}, SL_n(\overline{F})) = 1$. We will calculate $H^1(\tau, {}^Q SL_n(F))$ to gain a description of $H^1(\mathcal{G}, SO(Q)_{\overline{F}})$. For this purpose, we will need a brief lemma.

Lemma 5.5. *Let F be a field and let Q and Q' be two equivalent regular, symmetric matrices over F having the same determinant. There is a matrix $x \in SL_n(F)$ such that $Q' = x^t Q x$.*

Proof. By our assumption, there is $y \in GL_n(F)$ such that $y^t Q' y = Q$. Now, since $\det Q' = \det Q$, we have $\det y \in \{1, -1\}$. If $\det y = 1$, we are done. Otherwise, choose an orthogonal base $v_1, \dots, v_n$ of the bilinear form Q and set $\bar{v}$ the matrix $(v_1, \dots, v_n)$. Define the matrix $v := (v_1, \dots, v_{n-1}, \det \bar{v}^{-1} v_n)$ and $w := (v_1, \dots, v_{n-1}, -\det \bar{v}^{-1} v_n)$. Then $\det v = 1$ and $\det w = -1$. There is a diagonal matrix D such that $Q = (v^{-1})^t D v^{-1} = (w^{-1})^t D w^{-1}$. We have $D = w^t y^t Q' y w$ and $Q = (v^{-1})^t w^t y^t Q' y w v^{-1} = (y w v^{-1})^t Q' (y w v^{-1})$. Since $\det y w v^{-1} = 1$, we have proven our claim. $\square$

Lemma 5.6. *Let F be a field and let Q be a regular symmetric $n \times n$ -matrix over F with $\text{disc}[Q] = \delta$. There is a bijection of pointed sets between the set of equivalence classes of quadratic forms with discriminant δ with base point $[Q]$, denoted by $F - \text{Isom}^1(Q)$, and $H^1(\tau, {}^QSL_n(F))$.*

Proof. We construct a bijection. Consider $\alpha \in Z^1(\tau, {}^QSL_n(F))$. We have $1 = \alpha_1 = \alpha_{\tau^2} = \alpha_{\tau} \tau *_Q \alpha_{\tau}$. Set $M := \alpha_{\tau}$. Then, $MQ(M^{-1})^t Q^{-1} = 1$ and hence $M = QM^t Q^{-1}$ or $QM^t = MQ$. By $Q = Q^t$, this is equivalent to $MQ = (MQ)^t$ and so, MQ induces a quadratic form. Since $\det M = 1$ we have $\det MQ = \det Q$ and thus, $\text{disc}[MQ] = \text{disc}[Q]$. Now consider another cocycle α' with $\alpha'_{\tau} = N$. Then, α and α' are cohomologous if and only if there is $x \in SL_n(F)$ such that $M = xN\tau *_Q (x^{-1}) = xNQx^t Q^{-1}$ or equivalently $MQ = xNQx^t$. Hence MQ and NQ are equivalent as quadratic forms if and only if α and α' are cohomologous.

We thus have a well-defined injective map of pointed sets $\Phi : H^1(\tau, {}^QSL_n(F)) \rightarrow F - \text{Isom}^1(Q)$, $[\alpha] \mapsto [\alpha_{\tau}Q]$. Now for surjectivity consider an equivalence class κ of quadratic forms with discriminant δ . Then, there is a representative Q' in this class having the same determinant as Q . Now, $Q'Q^{-1}$ defines an element $\beta \in Z^1(\tau, {}^QSL_n(F))$ via $\beta_{\tau} = Q'Q^{-1}$. Then we have $\kappa = \Phi(\beta)$ and therefore the map Φ is surjective and thus bijective. $\square$

Corollary 5.7. *Let the field F be quadratically closed. Then $H^1(\tau, {}^QSL_n(F)) = 1$.*

Proof. This holds since by corollary 1.25, over a quadratically closed field any two regular quadratic forms are equivalent. $\square$

Corollary 5.8. *Suppose F is perfect and let $\mathcal{G} := \text{Gal}(\overline{F}/F)$ where $\overline{F}$ is an algebraic closure of F . Then there is a bijection Φ_Q of pointed sets between $H^1(\mathcal{G}, SO(Q)_{\overline{F}})$ and the set $F - \text{Isom}^1(Q)$ of equivalence classes of quadratic forms on F^n with discriminant $[\det Q]$ with $[Q]$ as the base point.*

Proof. This follows from the exact sequence at the beginning of this subsection together with corollary 4.6 and the preceding corollary, since an algebraically closed field is in particular quadratically closed. $\square$

We write out the map Φ_Q explicitly: Let $[\alpha] \in H^1(\mathcal{G}, SO(Q)_{\overline{F}})$. Then there is $M \in SL_n(\overline{F})$ such that $\forall \gamma \in \mathcal{G} : \alpha_{\gamma} = M^{-1}\gamma M$. The cohomology class $[\alpha]$ is mapped to $[\beta] \in H^1(\tau, {}^QSL_n(\overline{F}))$, where $\beta_{\tau} = M\tau *_Q M^{-1} = MQM^t Q^{-1}$. This maps to the class of quadratic forms $[MQM^t]$.

Remark: Note that by exchanging $SL_n(\overline{F})$ with $GL_n(\overline{F})$ we gain a description for $H^1(\mathcal{G}, O(Q)_{\overline{F}})$. There is a bijection of this cohomology set onto the pointed

set of non-degenerate quadratic forms of F^n modulus equivalence with $[Q]$ as base point. This result can also be found in [10, p.] or [5, p. 405].

5.3 Computation of $H^1(\tau, SO(J_n)_F)$

Lemma 5.9. *Let $b \in Z^1(\tau, O(J_n)_F)$. Let $\mathcal{S}$ be the set of $SO(J_n)_F$ -conjugacy classes of elements x in the coset $SO(J_n)_F b J_n$ satisfying $x^2 = 1$. The map $\Phi : H^1(\tau, {}^b SO(J_n)_F) \rightarrow \mathcal{S}, [\alpha] \mapsto [\alpha_\tau b J_n]$ is a bijection mapping $[1]$ to $[b J_n]$.*

Proof. We have $1 = b\tau(b) = b(b^{-1})^t$ and hence $b = b^t$. Also, since $b \in O(J_n)_F$, we have $b J_n b = J_n$. Now let $M \in Z^1(\tau, {}^b SO(J_n)_F)$. Then

$$\begin{aligned} 1 &= M\tau *_b M \\ &= Mb(M^{-1})^t b^{-1} \end{aligned}$$

Hence, $Mb = bM^t$. Since $J_n Mb = (M^{-1})^t b^{-1} J_n$ we have

$$\begin{aligned} Mb J_n &= bM^t J_n \\ &= b J_n M^{-1} \\ &= J_n b^{-1} M^{-1} \\ &= (Mb J_n)^{-1}. \end{aligned}$$

Hence, $(Mb J_n)^2 = 1$. Now let $N \in Z^1(\tau, {}^b SO(J_n)_F)$ a cocycle equivalent to M . Then there is $T \in SO(J_n)_F$ such that $N = TM\tau *_b T^{-1} = TMbT^t b^{-1}$. Therefore,

$$\begin{aligned} Nb J_n &= TMbT^t J_n \\ &= TMb J_n T^{-1}. \end{aligned}$$

Thus our proposed map is well-defined. Computing our calculations in reverse order shows that it is a bijection. $\square$

Lemma 5.10. *Let F be a quadratically closed field. Then $H^1(\tau, SO(J_2)_F) = 1$.*

Proof. . The group $SO(J_2)_F$ coincides with the maximal abelian subgroup of diagonal matrices T (see lemma 2.11) and therefore it is isomorphic to F^* . Since F is quadratically closed, we have $\{x^2 | x \in SO(J_2)_F\} = SO(J_2)_F$. Now, for $t \in T$, we obviously have $J_2 t^{-1} = t J_2$. Hence, we have $t J_2 t^{-1} = t^2 J_2$. By lemma 5.9, every element of $H^1(\tau, SO(J_2)_F)$ corresponds to the conjugacy class over $SO(J_2)_F$ of an element $x J_2$ for some $x \in SO(J_2)_F$. As we have seen, the class of $x J_2$ equals $\{t^2 x J_2 | t \in SO(J_2)_F\} = SO(J_2)_F J_2$ and hence there is only one class. Hence, $H^1(\tau, SO(J_2)_F) = 1$. $\square$

For $r, s \in \mathbb{N}$, denote by $I_{r,s,r}$ the diagonal $2r+s \times 2r+s$ matrix $\text{diag}(-I_r, I_s, -I_r)$ which has r times the entry -1 , s times the entry 1 and again r times the entry -1 on the diagonal.

Theorem 5.11. *Let $\bar{F}$ be an algebraically closed field.*

- *Suppose $\lfloor \frac{n}{2} \rfloor$ is even. Then we have:*

$$H_1(\tau, SO(J_n)_{\bar{F}}) = \{[I_{r,s,r}J_n] : 2r + s = n\},$$

where $[...]$ denotes cohomology classes. Also $[I_{r,s,r}J_n] \neq [I_{r',s',r'}J_n]$ for $r \neq r'$ (and equivalently $s \neq s'$).

- *Suppose n is odd and $\lfloor \frac{n}{2} \rfloor$ is odd. Then we have:*

$$H_1(\tau, SO(J_n)_{\bar{F}}) = \{[-I_{r,s,r}J_n] : 2r + s = n\},$$

where $[...]$ denotes cohomology classes. Also $[-I_{r,s,r}J_n] \neq [-I_{r',s',r'}J_n]$ for $r \neq r'$ (and equivalently $s \neq s'$).

- *Suppose $n \not\equiv 2 \pmod{4}$. Then:*

$$|H^1(\tau, SO(J_n)_{\bar{F}})| = 1 + \left\lfloor \frac{n}{2} \right\rfloor.$$

Proof. If q is even, we have $\det J_n = 1$ and hence $J_n \in SO(J_n)_{\bar{F}}$. Lemma 5.9 implies that $[\alpha] \mapsto [\alpha_\tau J_n]$ defines a bijection of classes of cocycles in $H^1(\tau, SO(J_n)_{\bar{F}})$ onto conjugacy classes of elements x in $SO(J_n)_{\bar{F}}$ that satisfy $x^2 = 1$. (Choose $b=1$ in the lemma.) Now, these elements x are all semisimple by lemma 2.10. Hence, theorem 2.8 implies that each one is conjugate to an element t of the maximal torus of diagonal matrices T (see lemma 2.11) that satisfies $t^2 = 1$. Such elements t are matrices $t = \text{diag}(\epsilon_1, \dots, \epsilon_q, 1, \epsilon_q, \dots, \epsilon_1)$ (omitting 1 at $t_{q+1,q+1}$ if n is even), where $\epsilon_i \in \{-1, 1\}$ for all i . As we have seen when computing the Weyl group of T in $SO(J_n)_{\bar{F}}$, any two such elements t of T are conjugate to one another if and only if they have the same number of entries -1 on the diagonal. Now using the inverse of the bijection in lemma 5.9 to go back to cohomology classes yields the result.

If n is odd and q is odd, J_n does not lie in $SO(J_n)_{\bar{F}}$, $-J_n$ does, however. Hence we may choose $b = -1$ in the lemma above and observe that the -1 -twisted action of τ on $SO(J_n)_{\bar{F}}$ coincides with the regular one.

The third statement is an obvious consequence of the first two. $\square$

Remark: Let $S := \{t \in T | t^2 = 1\}$. Then S is a subgroup of T and the operation of the Weyl group W of T in $SO(J_n)_{\bar{F}}$ restricts to an operation on S . For $n \not\equiv 2 \pmod{4}$ we have shown:

$$H^1(\tau, SO(J_n)_{\bar{F}}) \cong S/W,$$

where S/W denotes the orbit set in S of the action of the Weyl group.

Lemma 5.12. *Let F be a field and $\bar{F}$ its algebraic closure. Let $n \in \mathbb{N}$. Let $b \in Z^1(\tau, SO(J_n)_F)$. Let $\iota : SO(J_n)_F \rightarrow SO(J_n)_{\bar{F}}$ be the inclusion map and consider the induced map*

$$\iota^* : H^1(\tau, SO(J_n)_F) \rightarrow H^1(\tau, SO(J_n)_{\bar{F}}).$$

We have a bijection:

$$(\iota^*)^{-1}([b]) \rightarrow \ker(H^1(\tau, {}^b SO(J_n)_F) \rightarrow H^1(\tau, {}^b SO(J_n)_{\bar{F}}))$$

given by

$$\rho_{b^{-1}} : [\alpha] \mapsto [\alpha b^{-1}].$$

Proof. By lemma 3.9 we have a commutative diagram:

$$\begin{array}{ccc} H^1(\tau, {}^b SO(J_n)_F) & \longrightarrow & H^1(\tau, {}^b SO(J_n)_{\bar{F}}) \\ \downarrow \rho_b & & \downarrow \rho_b \\ H^1(\tau, SO(J_n)_F) & \xrightarrow{\iota^*} & H^1(\tau, SO(J_n)_{\bar{F}}) \end{array}$$

The vertical arrows are bijections. Now considering $(\rho_b)^{-1} = \rho_{b^{-1}}$ yields the claim. $\square$

Theorem 5.13. *Assume that F is perfect and let $\mathcal{G} := \text{Gal}(\bar{F}/F)$. Let $n \not\equiv 2 \pmod{4}$ and let $Z := \{I_{r,s,r} J_n \mid r, s \in \mathbb{N}, 2r + s = n\}$. We have a bijection:*

$$H^1(\tau, SO(J_n)_F) \rightarrow \bigsqcup_{b \in Z} \ker(H^1(\mathcal{G}, {}^b SO(J_n)_{\bar{F}}) \rightarrow H^1(\mathcal{G}, SO(J_n)_{\bar{F}})),$$

where $\sqcup$ denotes a disjoint union.

Proof. By the theorem above, Z is a set of representative cocycles for the cohomology set $H^1(\tau, SO(J_n)_{\bar{F}})$ if $\lfloor \frac{n}{2} \rfloor$ is even. Hence $H^1(\tau, SO(J_n)_F)$ decomposes into a disjoint union of sets $(\iota^*)^{-1}([b])$ for $b \in Z$, which we have described in the preceding lemma. Now the existence of the claimed bijection follows from corollary 5.4. For the case that n is odd and $\lfloor \frac{n}{2} \rfloor$ is odd note that $-Z$ is a representative set of cocycles and that the b -twisted action of τ on $SO(J_n)_{\bar{F}}$ coincides with the $-b$ -twisted action for any cocycle b . $\square$

We now characterize the groups ${}^b SO(J_n)_{\bar{F}}$ for a field F . Let $b = I_{r,s,r} J_n$ and $M \in {}^b SO(J_n)_{\bar{F}}$. Since $M \in SO(J_n)_F$, we have $J_n \tau(M) J_n = M$. Also, $M \in {}^b SO(J_n)_{\bar{F}}$ yields:

$$\begin{aligned} \tau *_b(M) &= b \tau(M) b^{-1} \\ &= I_{r,s,r} J_n \tau(M) J_n I_{r,s,r} \\ &= I_{r,s,r} M I_{r,s,r}. \end{aligned}$$

Hence M commutes with $I_{r,s,r}$. Now let M be of the form:

$$\begin{pmatrix} M_{1,1} & M_{1,2} & M_{1,3} \\ M_{2,1} & M_{2,2} & M_{2,3} \\ M_{3,1} & M_{3,2} & M_{3,3} \end{pmatrix},$$

where $M_{1,1}$ and $M_{3,3}$ are $r \times r$ -blocks, $M_{2,2}$ is an $s \times s$ -block and the other block sizes are chosen accordingly. Then we have:

$$I_{r,s,r} M I_{r,s,r} = \begin{pmatrix} M_{1,1} & -M_{1,2} & M_{1,3} \\ -M_{2,1} & M_{2,2} & -M_{2,3} \\ M_{3,1} & -M_{3,2} & M_{3,3} \end{pmatrix}$$

and hence $M_{1,2}, M_{2,1}, M_{2,3}$ and $M_{3,2}$ are all zero. The matrix

$$\begin{pmatrix} M_{1,1} & M_{1,3} \\ M_{3,1} & M_{3,3} \end{pmatrix}$$

lies in $O(J_{2r})_F$ and $M_{2,2}$ lies in $O(J_s)_F$. We have $\det M = 1$. Now denote by $S(O(J_{2r})_F \times O(J_s)_F)$ the kernel of the map $O(J_{2r})_F \times O(J_s)_F \rightarrow F, (A, B) \mapsto \det A \det B$. Then we get:

$${}^bSO(J_n)_F^\tau \cong S(O(J_{2r})_F \times O(J_s)_F).$$

Note that the considered isomorphism commutes with the action of $\text{Gal}(F/k)$ for any Galois extension F/k .

5.4 Computation of $H^1(\mathcal{G}, {}^bSO(J_n)_{\overline{F}}^\tau)$

Let F be a field and let E/F be a Galois extension. Set $\mathcal{G} := \text{Gal}(E/F)$. Let S_1 and S_2 be two regular symmetric matrices over F , S_1 of size $p \times p$, S_2 of size $q \times q$. Consider the homomorphism $d : GL_p(E) \times GL_q(E) \rightarrow E^*, (x, y) \mapsto \det x \det y$. For any subgroups $G_p \leq GL_p(E)$ and $G_q \leq GL_q(E)$ set $S(G_p \times G_q) := \ker d|_{G_p \times G_q}$, i.e. the subgroup of $G_p \times G_q$ whose elements (x, y) satisfy $\det x \det y = 1$.

Since d is surjective, we have an exact sequence:

$$1 \rightarrow S(GL_p(E) \times GL_q(E)) \rightarrow GL_p(E) \times GL_q(E) \xrightarrow{d} E^* \rightarrow 1.$$

As in the proof of corollary 4.6 and using the fact that by lemma 3.4 we have $H^1(\mathcal{G}, GL_p(E) \times GL_q(E)) \cong H^1(\mathcal{G}, GL_p(E)) \times H^1(\mathcal{G}, GL_q(E)) = 1 \times 1 = 1$, we obtain an exact sequence:

$$\begin{aligned} 1 \rightarrow S(GL_p(F) \times GL_q(F)) &\rightarrow GL_p(F) \times GL_q(F) \xrightarrow{d} F^* \\ &\rightarrow H^1(\mathcal{G}, S(GL_p(E) \times GL_q(E))) \rightarrow 1. \end{aligned}$$

Again, we derive: $H^1(\mathcal{G}, S(GL_p(E) \times GL_q(E))) = 1$.

Now consider the S_1 -twisted action of τ on ${}^{S_1}GL_p(E)$ and the S_2 -twisted action of τ on ${}^{S_2}GL_q(E)$. We have ${}^{S_1}GL_p(E)^\tau = O(S_1)_E$ and ${}^{S_2}GL_q(E)^\tau = O(S_2)_E$. Also, we have an induced action of τ on ${}^{S_1}GL_p(E) \times {}^{S_2}GL_q(E) : (x, y) \mapsto (\tau_{*S_1}(x), \tau_{*S_2}(y))$. We have: $S({}^{S_1}GL_p(E) \times {}^{S_2}GL_q(E))^\tau = S(O(S_1)_E \times O(S_2)_E)$. We again obtain a bijection of pointed sets:

$$\ker\left(H^1(\tau, S({}^{S_1}GL_p(F) \times {}^{S_2}GL_q(F))) \rightarrow H^1(\tau, S({}^{S_1}GL_p(E) \times {}^{S_2}GL_q(E)))\right) \longrightarrow H^1\left(\mathcal{G}, S(O(S_1)_{\overline{F}} \times O(S_2)_{\overline{F}})\right)$$

Lemma 5.14. *Let F be a perfect field and $\overline{F}$ an algebraic closure of F . Let S_1 and S_2 be regular symmetric matrices over F of sizes $p \times p$ and $q \times q$ respectively. Let $\mathcal{G} := \text{Gal}(\overline{F}/F)$. There is a bijection of pointed sets Φ_{S_1, S_2} between $H^1(\mathcal{G}, S(O(S_1)_{\overline{F}} \times O(S_2)_{\overline{F}}))$ and the subset $(F - \text{Isom}(S_1) \times F - \text{Isom}(S_2))^1$ of the Cartesian product of equivalence classes of regular quadratic forms on F^p and F^q respectively whose elements $([x], [y])$ satisfy $\text{disc}([x]) \text{disc}([y]) = \text{disc}([S_1]) \text{disc}([S_2])$.*

Proof. The proof is similar to the one of corollary 5.8, only in two coordinates. $\square$

We may apply this lemma to $S(O(J_{2r})_F \times O(J_s)_F)$ as in the previous subsection.

Example: We now determine the cardinality of the cohomology sets $H^1(\tau, SO(J_n)_{\mathbb{R}})$ for $n = 4$. We know that for $k \in \mathbb{N}$, there are exactly $k + 1$ distinct equivalence classes of quadratic forms on $\mathbb{R}^k$, which are parametrized by their signatures. By the preceding subsection we have:

$$|H^1(\tau, SO(J_4)_{\mathbb{R}})| = \sum_{r=0}^2 |\ker(H^1(\mathcal{G}, S(O(J_{2r}))_{\mathbb{C}} \times O(J_{4-2r})_{\mathbb{C}}) \rightarrow H^1(\mathcal{G}, SO(J_4)_{\mathbb{C}}))|,$$

where $\mathcal{G} := \text{Gal}(\mathbb{C}/\mathbb{R})$. The elements of $\ker(H^1(\mathcal{G}, S(O(J_{2r}))_{\mathbb{C}} \times O(J_{4-2r})_{\mathbb{C}}) \rightarrow H^1(\mathcal{G}, SO(J_4)_{\mathbb{C}}))$ correspond to two-tuples (X, Y) of equivalence classes of regular quadratic forms over $\mathbb{R}$ which satisfy that their signatures add up to $(2, 2)$. This leaves the following options (where we consider matrices as quadratic forms):

2r	s	Possible forms
0	4	$(I_0, I_{2,2})$
2	2	$(I_{1,1}, I_{1,1}), (I_{2,0}, I_{0,2}), (I_{0,2}, I_{2,0})$
4	0	$(I_{2,2}, I_0)$

Hence we get $|H^1(\tau, SO(J_4)_{\mathbb{R}})| = 5$. Now consider arbitrary dimension n . Note that after choosing the block sizes $2r$ and hence $s = n - 2r$, the signature of the form in one block determines the signature of the form in the other. For the smaller block, we can always choose any signature and simply adjust the other block. Hence we see:

$$|H^1(\tau, SO(J_n)_{\mathbb{R}})| = \sum_{r=0}^{\lfloor \frac{n}{2} \rfloor} (\min(2r, n - 2r) + 1) = 1 + \left\lfloor \frac{n}{2} \right\rfloor + \sum_{r=0}^{\lfloor \frac{n}{2} \rfloor} \min(2r, n - 2r),$$

if $n \not\equiv 2 \pmod{4}$. This computes to

$$|H^1(\tau, SO(J_n)_{\mathbb{R}})| = 1 + n \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{2} \right\rfloor^2 - n \left\lfloor \frac{n}{4} \right\rfloor + 2 \left\lfloor \frac{n}{4} \right\rfloor^2 + 2 \left\lfloor \frac{n}{4} \right\rfloor,$$

which for $n \equiv 0 \pmod{4}$ equals $1 + \frac{n}{2} + \frac{n^2}{8}$.

6 A consideration of fixed point sets

We will now describe a method used by J. Rohlfs in [7] and by Rohlfs and J. Schwermer in [8] to utilize cohomology sets in determining the fixed point set of the action of the Cartan involution τ on locally symmetric spaces. Rohlfs has shown in [7, Proposition 1.9] that the Euler characteristic of such a fixed point set equals the Lefschetz number of τ and Γ . For further details on Lefschetz numbers see [7].

In this section, all groups will be considered over $\mathbb{R}$ and therefore we will drop the subscript for the field we are considering. The groups considered will be considered as Lie groups, i. e. with their real topology, not with the Zariski-topology introduced earlier. For $p, q \in \mathbb{N}$, let $O(p, q) := O(I_{p,q})_{\mathbb{R}}$, where $I_{p,q} = \text{diag}(I_p, -I_q)$, the diagonal matrix with p times 1 and q times -1 on the diagonal and zeros everywhere else. Set $SO(p, q) := O(p, q) \cap SL_{p+q}(\mathbb{R})$.

Recall our notation: The matrix J_n is the $n \times n$ matrix which has ones on the second diagonal and zeros in all other entries. The map τ is defined as $\tau : GL_n(\mathbb{R}) \rightarrow GL_n(\mathbb{R}), M \mapsto (M^t)^{-1}$. The cyclic group of order two generated by τ will also be denoted by τ . Let $G' := SO(J_n)$, $K' := SO(J_n)^\tau$ and $\Gamma' \leq G'$ a torsion-free τ -stable discrete subgroup.

The discrete group τ operates continuously on G' and since K' is τ -stable, τ operates continuously on $K' \backslash G' =: X'$. There is an obvious right-action of Γ' on $K' \backslash G'$, namely $(K'x, \gamma) \mapsto K'x\gamma^{-1}$ for $x \in G'$ and $\gamma \in \Gamma'$. We show that there is an induced action of τ on X'/Γ' , the set of orbits of the Γ' -action on X' : Let $[K'x] = [K'y] \in X'/\Gamma'$. Then there are $k \in K'$ and $g \in \Gamma'$ such that $kxg = y$. Then $\tau(k)\tau(x)\tau(g) = \tau(kxg) = \tau(y)$ and hence $[K'\tau(x)] = [K'\tau(y)]$. Hence the action $\tau([K'x]) = [K'\tau(x)]$ for all $x \in G'$ is in fact well-defined.

We want to describe the space $(K' \backslash G' / \Gamma')^\tau$ of fixed points of $K' \backslash G' / \Gamma'$ under the τ -action. In order to do so, we will transform G' and K' into groups that allow somewhat easier calculations. Since over the reals any symmetric $n \times n$ -matrix is diagonalizable via an element of $SO(n)$, there is $t \in SO(n)$ such that $tG't^{-1} = SO(p, q)$ with $q = \lfloor \frac{n}{2} \rfloor$ and $p = n - q$. Set $G := SO(p, q)$. We consider $K := S(O(p) \times O(q))$ as a subgroup of G via $K \rightarrow G, (x, y) \mapsto \text{diag}(x, y)$. Then

$$\begin{aligned} tK't^{-1} &= t(G' \cap O(p+q))t^{-1} \\ &= G \cap tO(p+q)t^{-1} \\ &= G \cap O(p+q) \\ &= S(O(p) \times O(q)). \end{aligned}$$

The last equation follows from matrix calculations similar to those exercised in subsection 5.3. By [2, Chapter IX, Lemmas 4.3 and 4.4] we have that G has exactly two connected components, each of which contains one of the two

connected components of K . Hence $G/K \cong G^0/K^0$, where G^0 and K^0 denote identity components respectively. Also, by [2, Chapter VI, theorem 2.2], K^0 is a maximal compact subgroup of G^0 . Hence K is a maximal compact subgroup of G . We obviously have $K = G^\tau$ and thus K is in particular τ -stable. Also, set $\Gamma := t\Gamma't^{-1}$. Then Γ is a torsion-free τ -stable discrete subgroup of G . We define $X := K \backslash G$. As above, since K is τ -stable, we have an induced action of τ on X . Also, since Γ is τ -stable, we have an induced action of τ on X/Γ .

The map $\text{Int}_t : G' \rightarrow G, x \mapsto txt^{-1}$ induces a bijection $K' \backslash G' \rightarrow K \backslash G$. Suppose there is $g \in \Gamma'$ such that $K'x = K'yg$. Then $Ktxt^{-1} = Ktygt^{-1} = Ktyt^{-1}tgt^{-1}$. Hence we have an induced bijection $K' \backslash G' / \Gamma' \rightarrow K \backslash G / \Gamma$. Now suppose $\tau(\bar{x}) = \bar{x}$ for $\bar{x} = [K'x] \in K' \backslash G' / \Gamma'$. Then there is a $g \in \Gamma'$ such that $K'\tau(x)g = K'x$. Then

$$\begin{aligned} K\tau(txt^{-1})tgt^{-1} &= tK't^{-1}t\tau(x)t^{-1}tgt^{-1} \\ &= tK'\tau(x)gt^{-1} \\ &= tK'xt^{-1} \\ &= tK't^{-1}txt^{-1} \\ &= Ktxt^{-1} \end{aligned}$$

and thus $[Ktxt^{-1}] \in (X/\Gamma)^\tau$. Hence the map Int_t induces a bijection $(X'/\Gamma')^\tau \rightarrow (X/\Gamma)^\tau$, which is obviously a diffeomorphism. We will give a description of the fixed point set $(X/\Gamma)^\tau$.

Let $b \in Z^1(\tau, G)$. Recall that the b -twisted action of τ on bG is defined by $\tau *_b x = b\tau(x)b^{-1}$ for $x \in G$. We also define a (so called) b -twisted action of τ on ${}^bX = X$ by $\tau \times {}^bX : (\tau, x) \mapsto \tau(x)b^{-1}$. Note that for $b \in \Gamma$, the induced b -twisted action of τ on ${}^bX/\Gamma$ coincides with the usual induced τ -action on X/Γ . For an arbitrary $b \in Z^1(\tau, G)$ we define $X(b) := {}^bX^\tau$. We also define $\Gamma(b) := {}^b\Gamma^\tau$. We will see that $(X/\Gamma)^\tau$ decomposes into manifolds of the form $X(b)/\Gamma(b)$. First we need the following lemma, which is an adaption of [4, lemma 3.23]:

Lemma 6.1. *The discrete, torsion free group Γ acts freely on $X = K \backslash G$, i. e. for any $x \in X$ and $\gamma \in \Gamma$ we have that $x\gamma = x$ implies $\gamma = 1$.*

Proof. We show that for any $x \in X$ we have a neighborhood U of x such that $U\gamma \cap U \neq \emptyset$ implies $\gamma = 1$. This obviously implies the claim.

Since K is compact and any discrete subgroup of G is closed, we have that any discrete subgroup of K is finite. This implies $K \cap \Gamma' = \{1\}$ for any discrete torsion-free subgroup Γ' of G . Now let $x = Kg$. Then $K \cap g\Gamma g^{-1} = \{1\}$. Since Γ is closed, we may choose an open set $W \supset K$ in G such that $\Gamma \cap W = \{1\}$. The map $\mu : G \times G \times G \rightarrow G, (g_1, g_2, g_3) \mapsto g_1g_2g_3$ is continuous. We have $K \times K \times K \subset \mu^{-1}(K)$. Now Wallace's lemma implies that there is an open

neighborhood of V such that $V \times V \times V \subset \mu^{-1}(W)$. By possibly shrinking V we may assume $V = V^{-1}$. We have $V^{-1}V^2 \cap g\Gamma g^{-1} = \{1\}$.

Denote by π the canonical projection $G \rightarrow X$. We claim that $U := \pi(Vg)$ is a neighborhood of x as proposed above. Since π is an open map, U is a neighborhood of x . Let $\gamma \in \Gamma$ with $U\gamma \cap U \neq \emptyset$. Let $Kv_1g\gamma = Kv_2g$ in this intersection with $v_1, v_2 \in V$. Then we have $v_1g\gamma = kv_2g$ for some $k \in K$. We thus have $g\gamma g^{-1} = v_1^{-1}kv_2 \in V^{-1}V^2$ and thus $\gamma = 1$. $\square$

Lemma 6.2. *Let $b \in Z^1(\tau, G)$ and let f be the map $f : X(b)/\Gamma(b) \rightarrow (X/\Gamma)^\tau, [x] \mapsto [x]$, where $x \in X(b)$ is viewed as element of X and the brackets denote $\Gamma(b)$ and Γ -orbits respectively. Denote its image by $F(b)$. Then f is injective and a diffeomorphism onto $F(b)$.*

Proof. We show that f is injective: Let x and $y \in G$ such that Kx and $Ky \in X(b)$ and such that $[Kx] = [Ky]$ in X/Γ . Then there is $\gamma \in \Gamma$ such that $Kx = Ky\gamma$. We show that $\gamma \in \Gamma(b)$, i. e. $\tau *_b(\gamma) = \gamma$. By our assumptions we have $K\tau(x)b^{-1} = Kx = Ky = K\tau(y)b^{-1}$ and hence $K\tau(x) = K\tau(y)b^{-1}\gamma b$. Applying τ to this equation and noting $\tau(b) = b^{-1}$ yields $Kx = Kyb\tau(\gamma)b^{-1} = Ky\tau *_b(\gamma)$. Now by lemma 6.1, the discrete torsion-free group Γ acts freely on the space X and hence $Ky\gamma = Ky\tau *_b(\gamma)$ implies $\gamma = \tau *_b(\gamma)$. Therefore f is injective.

Obviously, f is a smooth and open map onto its image and hence our claim holds. $\square$

Remark: Let us drop for a minute the requirement that Γ be torsion-free and let us assume that $b = \pm I_{p,q} \in \Gamma$. (This can only be the case in certain dimensions, namely if $n \not\equiv 2 \pmod{4}$. Note that the sign will have no impact on the following calculations and is only used to adjust the determinant of b .) Suppose $[Kx] \in X/\Gamma$ is a Γ -orbit. Note that $b \in K$ and $b = b^{-1} \in \Gamma$. We calculate:

$$\begin{aligned} \tau([Kx]) &= [K\tau(x)] \\ &= [Kb\tau(x)b^{-1}] \\ &= [K\tau *_b(x)] \\ &= [Kx]. \end{aligned}$$

Hence we have shown: $(X/\Gamma)^\tau = X/\Gamma$. Also, we have $\forall g \in G : g^tbg = b$ and hence the only cocycle in the cohomology class of b is b itself. Whenever the assumption that Γ is torsion-free holds, b cannot lie in Γ since b has order two, and therefore, no cocycle equivalent to b may lie in Γ . We will show in the following that in this case, for dimensional reasons, $(X/\Gamma)^\tau \neq X/\Gamma$.

We show that $F(b)$ depends only on the class of b in $H^1(\tau, \Gamma)$:

Lemma 6.3. *Let b and c be two equivalent cocycles in $Z^1(\tau, G)$ and $g \in G$ such that $b = gcg^t$. Then we have a diffeomorphism:*

$$X(b) \rightarrow X(c), Kx \mapsto Kxg.$$

We have an induced diffeomorphism:

$$X(b)/\Gamma(b) \rightarrow X(c)/g^{-1}\Gamma(b)g.$$

Proof. Let $x \in G$ such that $Kx \in X(b)$. Then, $K\tau(xg)c^{-1} = K\tau(x)(g^t)^{-1}c^{-1} = K\tau(x)b^{-1}g = Kxg$. Hence Kxg is in $X(c)$. Right-multiplication by g^{-1} is obviously an inverse map. The second statement is obvious. $\square$

Corollary 6.4. *Now let b and c be two equivalent cocycles in $Z^1(\tau, \Gamma)$ and let $\gamma \in \Gamma$ such that $b = \gamma c \gamma^t$. Then we obviously have $[Kx] = [Kx\gamma]$ in $(X/\Gamma)^\tau$ for any $x \in G$ with $[Kx] \in (X/\Gamma)^\tau$ and hence $F(b) = F(c)$.*

Due to this corollary the notion $F(b)$ for $[b] \in H^1(\tau, \Gamma)$ is well-defined. We can state the following result due to J. Rohlfs, which follows from proposition 1.3 in [7, p. 275] and the remark thereafter:

Theorem 6.5. *We have:*

$$(X/\Gamma)^\tau \cong \bigsqcup_{[b] \in H^1(\tau, \Gamma)} F(b),$$

where $\bigsqcup$ denotes a disjoint union.

We will now give a characterization of the manifolds $F(b)$ appearing in the theorem.

Lemma 6.6. *Let $b \in Z^1(\tau, K)$. The inclusion map ${}^bK \rightarrow {}^bG$ induces a bijection $H^1(\tau, {}^bK) \rightarrow H^1(\tau, {}^bG)$.*

Proof. See [7, p. 276].

Hence any $c \in Z^1(\tau, \Gamma)$ is equivalent (considered as a cocycle with values in G) to a cocycle $b \in Z^1(\tau, K)$, which, since Γ is torsion free, is distinct from $\pm I_{p,q}$ by our remark above. Using lemma 6.3, we can gain a description of $F(c)$ by considering $X(b)$ modulus the right-action of some discrete subgroup of G . Now let $b \in Z^1(\tau, K)$. Then the defined action of τ on bX is the one induced by the actions of τ on bG and the τ -subgroup bK . Thus, by lemma 3.6 we have an exact sequence:

$$1 \rightarrow {}^bK^\tau \rightarrow {}^bG^\tau \rightarrow {}^b(K \backslash G)^\tau \rightarrow H^1(\tau, {}^bK) \rightarrow H^1(\tau, {}^bG).$$

Since $\ker(H^1(\tau, {}^bK) \rightarrow H^1(\tau, {}^bG)) = 1$ by lemma 6.6, corollary 3.7 implies:

$${}^bK^\tau \backslash {}^bG^\tau \cong {}^bX^\tau = X(b).$$

The considered bijection is obviously a diffeomorphism.

Each cocycle in $b \in Z^1(\tau, K)$ corresponds to $b = \text{diag}(A, B)$, where A and B two symmetric orthogonal matrices of size $p \times p$ and $q \times q$ respectively with $\det A \det B = 1$. We know that such a cocycle b can be diagonalized via a matrix in K . Since we have that τ acts as the identity on K , we obtain that every element b of $Z^1(\tau, K)$ is equivalent to an element of $S := \{\text{diag}(I_\alpha, -I_\beta, I_\gamma, -I_\delta) \mid \alpha + \beta = p, \gamma + \delta = q, \beta + \delta \equiv 0(2)\}$. Again, if b stems from a cocycle in the torsion-free group Γ , we have $b \neq \pm I_{p,q}$. Hence we assume that $b = \text{diag}(I_\alpha, -I_\beta, I_\gamma, -I_\delta) \in S \setminus \{\pm I_{p,q}\}$.

We have that $SO(b) = {}^bSL_{p+q}(\mathbb{R})^\tau$ and thus ${}^bG^\tau = SO(p, q) \cap SO(b)$. We calculate ${}^bG^\tau$. Note that $b = b^{-1}$, $I_{p,q} = I_{p,q}^{-1}$ and $bI_{p,q} = \text{diag}(I_\alpha, -I_{\beta+\gamma}, I_\delta)$. For $x \in SO(p, q) \cap SO(b)$ we have $x^t = bx^{-1}b$ and $x^t I_{p,q} x = I_{p,q}$. Hence we have $bx^{-1}bI_{p,q}x = I_{p,q}$ or equivalently $x = bI_{p,q}xbI_{p,q}$. Let

$$x = \begin{pmatrix} X_{1,1} & X_{1,2} & X_{1,3} \\ X_{2,1} & X_{2,2} & X_{2,3} \\ X_{3,1} & X_{3,2} & X_{3,3} \end{pmatrix} \in {}^bG^\tau,$$

with $X_{1,1} \in M_{\alpha,\alpha}(\mathbb{R})$, $X_{2,2} \in M_{\beta+\gamma,\beta+\gamma}(\mathbb{R})$ and $X_{3,3} \in M_{\delta,\delta}(\mathbb{R})$ and the other blocks of according dimensions. Then we have:

$$\begin{aligned} bI_{p,q}xbI_{p,q} &= \begin{pmatrix} I_\alpha & 0 & 0 \\ 0 & -I_{\beta+\gamma} & 0 \\ 0 & 0 & I_\delta \end{pmatrix} \begin{pmatrix} X_{1,1} & X_{1,2} & X_{1,3} \\ X_{2,1} & X_{2,2} & X_{2,3} \\ X_{3,1} & X_{3,2} & X_{3,3} \end{pmatrix} \begin{pmatrix} I_\alpha & 0 & 0 \\ 0 & -I_{\beta+\gamma} & 0 \\ 0 & 0 & I_\delta \end{pmatrix} \\ &= \begin{pmatrix} X_{1,1} & -X_{1,2} & X_{1,3} \\ -X_{2,1} & X_{2,2} & -X_{2,3} \\ X_{3,1} & -X_{3,2} & X_{3,3} \end{pmatrix}. \end{aligned}$$

Hence $X_{1,2} = 0$, $X_{2,1} = 0$, $X_{2,3} = 0$ and $X_{3,2} = 0$. We see that the matrix $\begin{pmatrix} X_{1,1} & X_{1,3} \\ X_{3,1} & X_{3,3} \end{pmatrix} \in O(\alpha, \delta)$ and $X_{2,2} \in O(\beta, \gamma)$. Hence we see that

$${}^b(G)^\tau \cong S(O(\alpha, \delta) \times O(\beta, \gamma)).$$

A similar calculation shows

$${}^bK^\tau \cong S(O(\alpha) \times O(\delta) \times O(\beta) \times O(\gamma)).$$

Hence we obtain

$$X(b) \cong S(O(\alpha) \times O(\delta) \times O(\beta) \times O(\gamma)) \setminus S(O(\alpha, \delta) \times O(\beta, \gamma)).$$

A direct consequence is:

Theorem 6.7. *Let $b = \text{diag}(I_\alpha, -I_\beta, I_\gamma, -I_\delta)$ with $\alpha + \beta = p, \gamma + \delta = q$ and $\beta + \delta \equiv 0(2)$. Then there is a discrete, torsion-free subgroup $\Gamma_1 \leq S(O(\alpha, \delta) \times O(\beta, \gamma))$ such that*

$$F(b) \cong S(O(\alpha) \times O(\delta) \times O(\beta) \times O(\gamma)) \backslash S(O(\alpha, \delta) \times O(\beta, \gamma)) / \Gamma_1.$$

In particular, $F(b)$ is connected.

Now the projection

$$SO(\alpha, \delta) \times SO(\beta, \gamma) \rightarrow S(O(\alpha) \times O(\delta) \times O(\beta) \times O(\gamma)) \backslash S(O(\alpha, \delta) \times O(\beta, \gamma))$$

is surjective and induces a diffeomorphism:

$$X(b) \cong (S(O(\alpha) \times O(\delta)) \backslash SO(\alpha, \delta)) \times (S(O(\beta) \times O(\gamma)) \backslash SO(\beta, \gamma)).$$

As above, we see from [2, Chapter IX, Lemmas 4.3 and 4.4] that for any p, q we have $S(O(p) \times O(q)) \backslash SO(p, q) \cong (SO(p) \times SO(q)) \backslash SO^0(p, q)$, where $SO^0(p, q)$ is the identity component of $SO(p, q)$. Hence we get

$$X(b) \cong ((SO(\alpha) \times SO(\delta)) \backslash SO^0(\alpha, \delta)) \times ((SO(\beta) \times SO(\gamma)) \backslash SO^0(\beta, \gamma)).$$

Example: We now consider the possible dimensions of the manifolds $F(b)$. First note that the space $X = S(O(p) \times O(q)) \backslash SO(p, q)$ has dimension:

$$\begin{aligned} \dim X &= \dim SO(p, q) - \dim S(O(p) \times O(q)) \\ &= \frac{(p+q)(p+q-1)}{2} - \frac{(p)(p-1)}{2} - \frac{(q)(q-1)}{2} \\ &= pq. \end{aligned}$$

This we obtain by looking at the corresponding Lie algebras. Hence we have $\dim X/\Gamma = pq$. Similarly, the space $Y := (S(O(\alpha) \times O(\delta)) \backslash SO(\alpha, \delta))$ has dimension $\alpha\delta$ and $Z := (S(O(\beta) \times O(\gamma)) \backslash SO(\beta, \gamma))$ has dimension $\beta\gamma$. Hence all possible dimensions for $F(b)$ are $\{\alpha\delta + \beta\gamma \mid \alpha + \beta = p, \gamma + \delta = q, \beta + \gamma \equiv 0(2), (\alpha, \delta) \neq (p, q), (\beta, \gamma) \neq (p, q)\}$, which equals

$$\{pq - p\gamma - q\beta + 2\beta\gamma \mid 0 \leq \beta \leq p, 0 \leq \gamma \leq q, \beta + \gamma \equiv 0(2), (\beta, \gamma) \neq (0, 0), (\beta, \gamma) \neq (p, q)\}.$$

We see that $F(b)$ has dimension strictly less than pq .

We consider for example the case $n = 5$ and hence $p = 3$ and $q = 2$. Then X/Γ has dimension 6. For arbitrary $b \in Z^1(b, \Gamma)$ we are in one of the following cases:

α	β	γ	δ	$\dim F(b)$
0	3	1	1	3
1	2	0	2	2
1	2	2	0	4
2	1	1	1	3
3	0	2	0	0

Summary

This thesis deals with orthogonal groups over fields F with $\text{char } F \neq 2$ and non-abelian group cohomology with values in these orthogonal groups.

Chapter one introduces the notions of quadratic forms and the corresponding orthogonal groups. We show some basic results about quadratic spaces. In particular we introduce the notion of isotropy, prove Witt's theorem (theorem 1.14) and show that any two n -dimensional regular quadratic spaces over quadratically closed fields are isometric (corollary 1.25). We also show that orthogonal groups are generated by mirror symmetries (lemma 1.12).

In chapter two, we consider special orthogonal groups over algebraically closed fields as linear algebraic groups. We give a quick introduction to the required concepts of algebraic geometry and state theorem 2.8 on the conjugacy of maximal tori in connected linear algebraic groups. Then we show that special orthogonal groups over algebraically closed fields are connected (corollary 2.17) and thus permit the application of said theorem.

Chapter three is devoted to defining non-abelian group cohomology sets and developing tools for calculating cohomology sets. A useful result is the exact sequence in cohomology proven in lemma 3.6. We also introduce the technical tool of twisting. In chapter four we apply these techniques to prove some standard results of Galois cohomology. In particular, we prove the lemma on Galois descent (lemma 4.2) and a generalization of Hilbert's Theorem 90 (theorem 4.3).

In chapter five, we apply our developed results and techniques to compute cohomology sets. First we give a number-theoretic description of the cohomology sets $\text{Gal}(\bar{F}/F, SO(Q)_{\bar{F}})$ for perfect fields F with $\text{char } F \neq 2$ (corollary 5.8). We then proceed to tackle the aim of this thesis, namely giving a description of the cohomology set $H^1(\tau, SO(J_n)_F)$ in terms of the Galois cohomology. In theorem 5.13 we reach the result that it can be described as a disjoint union of Galois cohomology sets if $n \not\equiv 2 \pmod{4}$. Here J_n is the symmetric $n \times n$ -matrix $(\delta_{i, n-j+1})_{i,j}$ and τ is the Cartan involution $M \mapsto (M^{-1})^t$.

Chapter six illustrates the use of the knowledge of the cohomology sets $H^1(\tau, SO(J_n)_{\mathbb{R}})$ for computing the connected components of the fixed point set of the operation of τ on a locally symmetric space X/Γ corresponding to said orthogonal group. In particular, we determine the possible dimensions (as real manifolds) of said connected components (see example on page 50).

Zusammenfassung (Deutsch)

Die vorliegende Arbeit behandelt orthogonale Gruppen über Körpern F mit $\text{char } F \neq 2$ und nicht-abelsche Gruppenkohomologie mit Werten in solchen orthogonalen Gruppen.

Im ersten Kapitel werden quadratische Formen und die zugehörigen orthogonalen Gruppen eingeführt und grundlegende Resultate über quadratische Räume bewiesen. Insbesondere führen wir den Begriff der Isotropie ein, beweisen den Satz von Witt (Satz 1.14) und zeigen, dass je zwei n -dimensionale, reguläre quadratische Räume über einem quadratisch abgeschlossenen Körper isometrisch sind (Korollar 1.25). Weiters zeigen wir, dass orthogonale Gruppen von Spiegelungen erzeugt werden (Lemma 1.12).

Das zweite Kapitel behandelt orthogonale Gruppen über algebraisch abgeschlossenen Körpern als lineare algebraische Gruppen. Zu diesem Zweck werden die notwendigen Konzepte aus der algebraischen Geometrie eingeführt. Wir formulieren einige Resultate über lineare algebraische Gruppen, insbesondere Satz 2.8 über maximale Tori in zusammenhängenden linearen algebraischen Gruppen. Danach zeigen wir, dass spezielle orthogonale Gruppen zusammenhängend sind (Korollar 2.17) und daher die Anwendung dieses Satzes erlauben.

In Kapitel drei werden nicht-abelsche Kohomologiemengen definiert und Methoden zu deren Behandlung eingeführt. Ein nützliches Resultat ist die exakte Kohomologiesequenz aus Lemma 3.6. Wir führen das Hilfsmittel des 'Twistens' ein. In Kapitel vier werden diese Methoden, um Standardresultate über Galoiskohomologie zu beweisen. Unter anderem zeigen wir das Lemma über Galois-Abstieg (Lemma 4.2) und beweisen eine Verallgemeinerung von Hilberts Satz 90 (Satz 4.3).

Im fünften Kapitel verwenden wir unsere bisherigen Resultate und Hilfsmittel, um spezielle Kohomologiemengen zu berechnen. Zuerst geben wir eine zahlentheoretische Interpretation der Kohomologiemengen $H^1(\text{Gal}(\overline{F}/F), SO(Q)_{\overline{F}})$ für perfekte Körper F mit $\text{char } F \neq 2$ (Korollar 5.8). Danach beschäftigen wir uns mit dem eigentlichen Ziel der Arbeit, die Kohomologiemenge $H^1(\tau, SO(J_n)_F)$ durch Galoiskohomologie zu beschreiben und kommen in Satz 5.13 zu dem Resultat, dass sie sich für $n \not\equiv 2 \pmod{4}$ als disjunkte Vereinigung von Galoiskohomologiemengen beschreiben lässt. Hier bezeichnet J_n die symmetrische $n \times n$ -Matrix $(\delta_{i, n-j+1})_{i,j}$ und τ die Cartan-Involution $M \mapsto (M^{-1})^t$.

In Kapitel sechs illustrieren wir den Nutzen der Kenntnis der Kohomologiemengen $H^1(\tau, SO(J_n)_{\mathbb{R}})$ zur Berechnung der Zusammenhangskomponenten der Fixpunktmenge der Operation von τ auf einem lokalsymmetrischen Raum X/Γ , der zu dieser orthogonalen Gruppe gehört. Im Speziellen bestimmen wir die möglichen Dimensionen (als reelle Mannigfaltigkeiten) dieser Zusammenhangskomponenten (siehe Seite 50).

References

- [1] A. Borel, Linear Algebraic Groups, 2nd enlarged ed., Springer-Verlag New York 1991.
- [2] S. Helgason, Differential Geometry and Symmetric Spaces, Academic Press New York 1962.
- [3] J. C. Jantzen and J. Schwermer, Algebra, Springer-Verlag Berlin Heidelberg 2006.
- [4] S. Kionke, Zur Arithmetik und Geometrie der SL_2 über Ordnungen in Quaternionenalgebren, master's thesis, Universität Wien 2010.
- [5] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The Book of Involutions, AMS Colloquium Publications Vol. 44 (1998).
- [6] O. T. O'Meara, Introduction to Quadratic Forms, Springer-Verlag Berlin Göttingen Heidelberg 1963.
- [7] J. Rohlfs, The Lefschetz number of an involution on the space of classes of positive definite quadratic forms, Comment. Math. Helvetici 56 (1981), pp. 272-296.
- [8] J. Rohlfs and J. Schwermer, An Arithmetic Formula for a Topological Invariant of Siegel modular varieties, Topology Vol. 37 (1998), pp. 149-159.
- [9] J. Rohlfs and B. Speh, Lefschetz numbers and twisted stabilized orbital integrals, Math. Ann. 296 (1993), pp. 191-214.
- [10] J. P. Serre, Cohomologie Galoisienne, Springer-Verlag Berlin Heidelberg New York 1965.
- [11] J. P. Serre, Local Fields, Springer Verlag New York 1979.
- [12] T. A. Springer, Linear Algebraic Groups, 2nd ed., Birkhäuser Boston 1998.

Author's curriculum vitae

Full name: Dominik Johannes Gruber
Date of birth: December 23, 1986
Place of birth: Kirchdorf a. d. Krems, Austria
Citizenship: Austria
E-mail address: dominik.gruber@univie.ac.at

Education

- 2010 - 2011 University of Vienna
MSc in mathematics,
specialization: algebra,
thesis: Orthogonal groups and their non-abelian group cohomology,
advisor: Prof. Joachim Schwermer.
- 2008 - 2010 University of Vienna
BSc in mathematics (summa cum laude),
bachelor theses: Ornamentgruppen (wallpaper groups),
Gruppenerweiterungen (group extensions),
advisor: Prof. Joachim Mahnkopf.
- 2007 - 2009 University of Vienna
Physics, discontinued.
- 2006 - 2007 Vienna University of Technology
Technical mathematics, discontinued.
- 2005 - 2006 Proyecto Salesiano Chicos de la Calle, Ecuador
Social work with street children; en lieu of mandatory military service.
- 2002 - 2003 Edisto High School, South Carolina, USA
Exchange student for one year.
- 1997 - 2005 Khevenhüller Gymnasium Linz
High school graduation (Matura) with distinction.

Scholarships

Performance scholarships awarded by the University of Vienna for the academic years 2007 - 2008, 2008 - 2009 and 2009 - 2010.