

Notes on Cohomology

Luis Arenas-Carmona. ¹

Universidad de Chile,
Facultad de Ciencias.
Casilla 653, Santiago, Chile.
learenas@uchile.cl

¹Supported by Fondecyt, proyecto No. 3010018, and the Chilean Catedra Presidencial in Number Theory.

Chapter 1

Introduction.

Galois cohomology is a fundamental tool for the classification of certain algebraic structures. To be precise, let k be a field, G a linear algebraic group acting on a space V , both defined over k . It is known [4], that if G is defined as the set of automorphisms of a tensor τ on V , e.g., a quadratic form or an algebra structure, the cohomology set $H^1(K/k, G_K)$ classifies the K/k -forms of τ , i.e., those tensors of the same type also defined over k that become isomorphic to τ over the larger field K (§4.1). Results of this type, however, hold in much more general settings. In this notes, we give the general facts about cohomology that allow the use of cohomology sets for classification, and give examples of applications to many parts of field theory and number theory. In particular, we devote a whole chapter to the study of the relation between lattices and cohomology.

Such a theory is already hinted at in [11]. In this reference, two finiteness results are proven. The first one deals with the finiteness of the local cohomology set $H^1(\mathcal{G}_w, \Gamma_w)$, for an arithmetically defined group Γ . Notations are as in [11]. The second one deals with the finiteness of the kernel of the map

$$H^1(\mathcal{G}, \Gamma) \longrightarrow \prod_{v \text{ place of } k} H(\mathcal{G}_{w(v)}, \Gamma_{w(v)}),$$

where we have fixed a place $w(v)$ of K dividing each place v of k . It is the proof of the second result which requires expressing the given kernel in terms of the set of double cosets

$$G_k \backslash G_{\mathbb{A}_k} / \prod_w \Gamma_w$$

(see corollary 3.3 in [11]). These double cosets are the same ones that classify the classes of lattices in a genus. This relation is pursued in chapter (crossreference).

1.0.1 Notations

In all of this notes, k, K, E denote number or local fields of characteristic 0, or algebraic extensions of them. If k is a number field, $\Pi(k)$ denotes the set of

places of k .

Remark 1.0.1. By an algebraic group, we mean a linear algebraic group. All algebraic groups are assumed to be subgroups of the general linear group of a vector space V , of finite dimension, over a sufficiently large algebraically closed field Ω of characteristic 0. We assume that all localizations of number fields inject into Ω . G denotes an algebraic group over Ω . $GL(V), SL(V)$ denote the general and special linear groups over Ω . When we work over a fixed local or number field k , we say that G is defined over k if the equations defining G have coefficients in k (see section 2.1.1 in [10]). *This is the case for all groups considered here.* For any field E , $k \subseteq E \subseteq \Omega$, we write G_E for the set of E -points of G , e.g., if $G = GL(V)$, the set of E points is denoted $GL_E(V)$. The same conventions apply to spaces and algebras. All spaces and algebras are assumed to be finite dimensional.

Exceptions to this rule are the multiplicative and additive groups. We denote $\mathbb{G}_m = \Omega^*$, $\mathbb{G}_a = \Omega$ when considered as algebraic groups. For the set of k -points we write k^*, k . Instead of $(\mathbb{G}_m)_k, (\mathbb{G}_a)_k$.

The orthogonal group of a quadratic form Q on V is written $\mathcal{O}_n(Q)$ or $\mathcal{O}_n(Q, V)$, where $n = \dim_{\Omega}(V)$. The set of E -points is denoted $\mathcal{O}_{n,E}(Q)$.

The field on which a particular lattice is defined is always written as a subindex. If K/k an extension of local or number fields and Λ_k is a lattice in V_k , Λ_K denotes the \mathcal{O}_K -lattice in V_K generated by Λ_k .

If G is an algebraic group acting on a space V , both defined over k , and Λ_k is a \mathcal{O}_k -lattice on V_k , the stabilizer of Λ_k in G_k is denoted G_k^{Λ} . If $G = GL(V)$, this set is denoted $GL_k^{\Lambda}(V)$. Similar conventions apply to special linear or orthogonal groups.

Remark 1.0.2. Whenever K/k is a Galois extension of a number field k , and v a place of k , w denotes a place of K dividing v . We assume that one fixed such w has been chosen for every v . This convention is also applied for infinite extension, e.g., $K = \bar{k}$.

Remark 1.0.3. $\mathcal{G}_{K/k}$ denotes the Galois group of the extension K/k . If there is no risk of confusion, we write simply \mathcal{G} . If K is not specified, we assume $K = \bar{k}$. If k is a number field and $v \in \Pi(k)$, we also use the notation $\mathcal{G}_w = \mathcal{G}_{K_w/k_v}$.

If Γ is a group acting on a set S , S/Γ denotes the set of orbits and S^{Γ} the set of invariant points. The action of $\gamma \in \Gamma$ is denoted $s \mapsto s^{\gamma}$, for $s \in S$.

Chapter 2

Cohomology and classification

In this chapter we introduced the basic results that are required to connect cohomology and classification. The results in this section are found in chapter 1 in [5], and p. 13-26 in [10].

Definition 2.0.4. Let \mathcal{G} be a finite group, and let A a group provided with a \mathcal{G} -action. $H^1(\mathcal{G}, A)$ is defined as the quotient

$$H^1(\mathcal{G}, A) = \{\alpha : \mathcal{G} \mapsto A \mid \alpha(hg) = \alpha(h)\alpha(g)^h\} / \equiv,$$

where $\alpha \equiv \beta$ if and only if there exists $a \in A$ such that $\alpha(g) = a^{-1}\beta(g)a^g$ for all $g \in \mathcal{G}$. If \mathcal{G} acts trivially on A , then $H^1(\mathcal{G}, A) \cong \text{Hom}(\mathcal{G}, A)/A$, where A acts on $\text{Hom}(\mathcal{G}, A)$ by conjugation. In what follows we write α_g instead of $\alpha(g)$.

In case that $A \subseteq B$ is a subgroup, there is a long exact sequence

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

and furthermore, under the natural action ¹ of $B^{\mathcal{G}}$ on $(B/A)^{\mathcal{G}}$,

$$(B/A)^{\mathcal{G}}/B^{\mathcal{G}} \cong \ker(H^1(\mathcal{G}, A) \longrightarrow H^1(\mathcal{G}, B)). \quad (2.1)$$

To simplify notations, in all that follows we assume that whenever a sequence of pointed sets

$$\dots \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow X \longrightarrow Y \longrightarrow Z$$

is written, X, Y, Z denote pointed sets, W, V, U, \dots denote groups, and W acts on X with

$$X/W \cong \ker(Y \longrightarrow Z).$$

¹ This result is not found in [5], but can be found in [10] p.22.

to classifying twisted actions on \mathcal{G} on G that turn the set G into a principal homogeneous G -space.

Let X be the group of all maps from \mathcal{G} to G . Then X is a \mathcal{G} -group with an action $f \mapsto f^\sigma$ satisfying $f^\sigma(\lambda) = f(\lambda\sigma^{-1})$. A twisted semi-action of \mathcal{G} on G is a map $\rho : G \times \mathcal{G} \rightarrow G$ which satisfy $\rho(hg, \sigma) = h^\sigma \rho(g, \sigma)$ and $\rho(1, 1) = 1$. A twisted semi-action ρ is a twisted action if it satisfies the relation

$$\rho(\rho(g, \sigma), \lambda) = \rho(g, \sigma\lambda),$$

for all g in G and all σ and λ in \mathcal{G} . The group X acts transitively on the set T of twisted semi-actions by

$$(\alpha \cdot \rho)(g, \sigma) = \rho(g\alpha(\sigma)^{-1}, \sigma)\alpha(1),$$

for all α in X , all ρ in T , all g in G , and all σ in \mathcal{G} . The stabilizer of ρ_0 , where $\rho_0(g, \sigma) = g^\sigma$, is the set of maps satisfying $\alpha(\sigma)^\sigma = \alpha(1)$. This maps form a subgroup G' of X which is isomorphic to G as a \mathcal{G} -group. The quotient set $X/G' \cong T$ has a natural \mathcal{G} action which is translated to to an action on T as $\rho^{\lambda^{-1}}(1, \sigma) = \rho(1, \sigma\lambda)^{\lambda^{-1}} \rho(1, \lambda)^{-\lambda^{-1}}$. With this action, a twisted semi-action ρ is invariant if and only if

$$\rho(1, \sigma\lambda) = \rho(1, \sigma)^\lambda \rho(1, \lambda) = \rho(\rho(1, \sigma), \lambda),$$

and premultiplying both sides by $g^{\sigma\lambda}$ we see that a \mathcal{G} -invariant action is the same as a twisted action. The following lemma follows easily from proposition 2.1.1.

Lemma 2.1.2. *The set of twisted actions on G is in natural correspondence, up to isomorphisms of (G, \mathcal{G}) -actions, with the kernel of the map $H^1(\mathcal{G}, G) \rightarrow H^1(\mathcal{G}, X)$. \square*

Proposition 2.1.3 (Shapiro's Lemma). *Let \mathcal{H} be a subgroup of \mathcal{G} . Let G be a \mathcal{H} -group and let G' be the set of maps $\phi : \mathcal{G} \rightarrow G$ such that $\phi(\sigma\lambda) = \phi(\sigma)^\lambda$ for all $\lambda \in \mathcal{H}$. Then $H^1(\mathcal{G}, G') \cong H^1(\mathcal{H}, G)$.*

Corollary 2.1.3.1. *In the notations of lemma 2.1.2 $H^1(\mathcal{G}, X) = \{1\}$. \square*

The following result follows from lemma 2.1.2 and corollary 2.1.3.1

Proposition 2.1.4 ([13], p. 44). *The set of principal homogeneous G -spaces up to isomorphism is in one-to-one correspondence with the elements of the cohomology set $H^1(\mathcal{G}, G)$. \square*

In most applications of the results in this chapter \mathcal{G} is the Galois group $\mathcal{G}_{K/k}$ of a possibly infinite Galois extension K/k , where k is a local or number field. The subgroups A, B, \dots are usually groups of algebraic or arithmetical nature.

Chapter 3

The generalized Hilbert theorem 90

3.1 Rings, units and cohomology

In this section, A is a ring provided with a \mathcal{G} action. A left (A, \mathcal{G}) -module is an A -module B provided with a \mathcal{G} -action, and satisfying $(ab)^\sigma = a^\sigma b^\sigma$ for all $a \in A$, $b \in B$, and $\sigma \in \mathcal{G}$.

An element $b \in B$ is a generator if $Ab = B$. It is a regular generator if $ab = 0$ implies $a = 0$. In particular, if $b \in B$ is a regular generator, the map $a \mapsto ab$ is an isomorphism of A -modules between A and B . Assume that b is a regular generator of B . Then an element $ab \in B$ is a regular generator if and only if $a \in A^*$. We say that the (A, \mathcal{G}) -module is principal if it has a regular generator.

Proposition 3.1.1. *The cohomology set $H^1(\mathcal{G}, A^*)$ classifies the set of principal left (A, \mathcal{G}) -modules. The distinguished point of $H^1(\mathcal{G}, A^*)$ corresponds to the modules that have an invariant regular generator.*

Proof. Let X be the group of all maps from \mathcal{G} to A^* . As in §2.1, we define a twisted semi-action as a map $\rho : \mathcal{G} \times A \rightarrow A$ satisfying:

- a) $\rho(aa', \sigma) = a^\sigma \rho(a', \sigma)$.
- b) $\rho(1, \sigma)$ is a unit for all $\sigma \in \mathcal{G}$.

A twisted action as a twisted semi-action that is an action. Any principal left (A, \mathcal{G}) -module is isomorphic to A with a twisted action. The group X acts transitively on the set of twisted semi-action by $(\alpha \cdot \rho)(a, \sigma) = \rho(a\alpha(\sigma), \sigma)\alpha(1)^{-1}$, and the stabilizer of ρ_0 , where $\rho_0(a, \sigma) = a^\sigma$, is the set of maps satisfying $\alpha(\sigma)^\sigma = \alpha(1)$ for all $\sigma \in \mathcal{G}$. Now the proof follows as in §2.1. \square

Example 3.1.2. Let $A = \mathbb{Z}$ with the trivial \mathcal{G} -action. Then $H^1(\mathcal{G}, \mathbb{Z}^*) = \text{Hom}(\mathcal{G}, \{1, -1\})$, hence there exists a free left $(\mathcal{G}, \mathbb{Z})$ -module with no invariant generator if and only if \mathcal{G} has a normal subgroup of index 2. The reader can easily check this result independently.

Example 3.1.3. More generally, if A has the trivial \mathcal{G} -action. Then $H^1(\mathcal{G}, \mathbb{Z}^*) = \text{Hom}(\mathcal{G}, A^*) / \cong$, where \cong denotes the conjugacy relation. The module associated to the homomorphism $\alpha : \mathcal{G} \rightarrow A^*$ has the action $(ab)^\sigma = a\alpha(\sigma)b$.

Example 3.1.4. Let K/k be a finite extension of local or number fields with Galois group \mathcal{G} . Let \mathcal{O}_K and \mathcal{O}_k be the respective rings of integers. Then the exact sequence $\mathcal{O}_K^* \hookrightarrow K^* \twoheadrightarrow P_K$, where P_K is the group of principal fractional ideals of K , shows that the kernel of $H^1(\mathcal{G}, \mathcal{O}_K^*) \rightarrow H^1(\mathcal{G}, K^*)$ corresponds to invariant ideals in P_K modulo ideals in P_k (up to a suitable identification). Since we prove later in this chapter that $H^1(\mathcal{G}, K^*) = 1$, then all free left $(\mathcal{O}_K, \mathcal{G})$ -module of rank 1 are of this form. If the extension K/k is unramified, one can prove that $P_K^{\mathcal{G}}$ is the set of fractional ideals in k that become principal over K . It follows that $H^1(\mathcal{G}, \mathcal{O}_K^*)$ is in correspondence with a subgroup of the ideal group of k .

Example 3.1.5. Let R be a ring with a \mathcal{G} -action. Then there is a natural action of \mathcal{G} on $A = \mathbb{M}_n(R)$ such that the matrices $E_{i,j}$ with a 1 in the intersection of the i -th row and the j -th column and 0 everywhere else are invariant.

Any A -module B has a decomposition of the form $B = \bigoplus_{i=1}^n E_{i,i}B$. Furthermore, we claim that $E_{i,j}(E_{k,k}B) = \delta_{j,k}E_{i,i}B$. In fact, the case $j \neq k$ is trivial and the case $j = k$ follows from the contentions $E_{i,j}B = E_{i,i}(E_{j,j}B) \subseteq E_{i,i}B$ and $E_{i,i}B = E_{i,j}(E_{j,i}B) \subseteq E_{i,j}B$. Conversely, if B' is an R -module of rank n , then $B = \bigoplus_{i=1}^n B_i$ where $B_i \cong B'$ has a natural A -module structure satisfying $E_{i,j}B_k = \delta_{j,k}B_i$. It follows that The cohomology set $H^1(\mathcal{G}, GL_n(R))$ classifies free left (R, \mathcal{G}) -modules of rank n .

3.2 Invariant generators of vector spaces

In this section, K/k is a finite Galois field extension. Also, V_K denotes a finite dimensional vector space. We assume that the Galois group \mathcal{G} acts on V_K in such a way that $(\lambda v)^\sigma = \lambda^\sigma v^\sigma$ for any $\sigma \in \mathcal{G}$, $v \in V_K$, and $\lambda \in K$.

Lemma 3.2.1. *The maps $h \mapsto h^\sigma$, are linearly independent.*

Proof. Assume $\sum_{\sigma \in \mathcal{G}} \alpha_\sigma h^\sigma = 0$ for all $h \in K$. Since any finite separable extension is simple, we can assume $K = k(\omega)$. In particular, $\sum_{\sigma \in \mathcal{G}} \alpha_\sigma \omega^{k\sigma} = 0$. However, the matrix with entries $\omega^{k\sigma}$ is a Vandermonde matrix with non-zero determinant, whence $\alpha_\sigma = 0$ for all σ . \square

Proposition 3.2.2. *The space V_K has a basis of \mathcal{G} -invariant vectors.*

Proof. Let V_k be the subspace of invariant vectors. It suffices to prove that $\dim_k(V_k) = \dim_K(V_K)$. Let $b : V_K \rightarrow V_k$ be the map $b(v) = \sum_{\sigma \in \mathcal{G}} v^\sigma$. If $\dim_k(V_k) < \dim_K(V_K)$, there exists a non-trivial linear form u such that $u(b(v)) = 0$ for all v . For any $h \in K$ we have

$$0 = u(b(hv)) = \sum_{\sigma \in \mathcal{G}} h^\sigma u(v^\sigma).$$

Since the functions $h \mapsto h\sigma$ are linearly independent, it follows that $u(v^\sigma) = 0$ for all v and all σ . In particular $u = 0$. \square

Corollary 3.2.2.1. *There exists a k -subspace V_k of V_K , such that $V_K \cong K \otimes_k V_k$.* \square

Corollary 3.2.2.2 (Hilbert's Theorem 90). $H^1(\mathcal{G}, \text{GL}_n(\mathbb{K})) = \{1\}$. \square

3.3 Cohomology of the group of units of an algebra

In this section, K/k is a finite Galois extension over an infinite field k .

Proposition 3.3.1. *For any finite dimensional algebra A , defined over k , and any algebraic extension K/k , it holds that $H^1(\mathcal{G}_{K/k}, A_K^*) = \{1\}$.*

Proof. Assume first that K/k is finite. Let B_K be a free left (A_K, \mathcal{G}) -module of rank 1. Then B_K is a finite dimensional vector space over K satisfying the hypotheses of proposition 3.2.2. It follows that B_K has a basis of invariant vectors $\{v_1, \dots, v_n\}$. In particular, $B_K \cong K \otimes_k B_k$ for some k -vector space B_k . The set of generators of B_K is a Zariski open set and therefore it must contain an element of B_k (see some reference). In the general case, if $\{L\}$ is the set of finite subextensions of K/k , then

$$H^1(\mathcal{G}, A_K^*) = H^1(\varprojlim \mathcal{G}_{L/k}, \varinjlim A_L^*) = \varinjlim H^1(\mathcal{G}_{L/k}, A_L^*) = \{1\}. \quad \square$$

Corollary 3.3.1.1. *If A_k is a k -algebra which is the direct limit of a family $\{B_k\}$ of finite dimensional algebras then $H^1(\mathcal{G}_{K/k}, A_K^*) = \{1\}$.*

Proof. In fact,

$$H^1(\mathcal{G}, A_K^*) = H^1(\mathcal{G}, \varinjlim B_K^*) = \varinjlim H^1(\mathcal{G}, B_K^*) = \{1\}. \quad \square$$

Corollary 3.3.1.2. *If A_k is a k -algebra such that every finite subset of A_k generates a finite dimensional subalgebra then $H^1(\mathcal{G}_{K/k}, A_K^*) = \{1\}$.*

Proof. In this case, A_k is the direct limit of its finite dimensional subalgebras. \square

Since $GL_K(V) \cong (\text{End}_K(V))^*$, Hilbert's theorem 90 is a particular case of proposition 3.3.1. However, proposition 3.3.1 has many other applications, as can be seen in these notes.

Let K/k be any field, then we have an exact sequence:

$$0 \longrightarrow SL_K(V) \longrightarrow GL_K(V) \longrightarrow K^* \longrightarrow 0$$

which gives a long exact sequence in cohomology:

$$GL_k(V) \rightarrow k^* \rightarrow H^1(\mathcal{G}_{K/k}, SL_K(V)) \rightarrow H^1(\mathcal{G}_{K/k}, GL_K(V)) = 1.$$

as the determinant map is always surjective, this proves:

Proposition 3.3.2. *for any field extension K/k we have:*

$$H^1(\mathcal{G}_{K/k}, SL_K(V)) = \{1\}.$$

More generally, if A is a finite dimensional central simple algebra split by K/k and $N_E : A_E \rightarrow E^*$ is the reduced norm, we have a sequence:

$$A_k^* \xrightarrow{N_k} k^* \rightarrow H^1(\mathcal{G}, SA_K^*) \rightarrow H^1(\mathcal{G}, A_K^*) = \{1\},$$

where $SA_K^* = \ker(N_K)$, therefore:

$$H^1(\mathcal{G}, SA_K^*) = k^*/N_k(A_K^*).$$

Example 3.3.3. $A_E = \left(\frac{-1, -1}{E}\right)$, $A_{\mathbb{R}} = \mathbb{H}$, $N(A_{\mathbb{R}}) = \mathbb{R}^+$, and $A_{\mathbb{C}} = \mathbb{M}_2(\mathbb{C})$, hence $H^1(\mathcal{G}, SA_{\mathbb{C}}^*) = \{[1], [-1]\}$. Same result applies to any matrix algebra over \mathbb{H} .

Proposition 3.3.4. *The multiplicative and additive groups \mathbb{G}_m and \mathbb{G}_a have trivial H^1 .*

Proof. It is an immediate application of proposition 3.3.1 that $H^1(\mathcal{G}, \mathbb{G}_m) = \{1\}$.

Let $A_k = k[x]/(x^2)$. A is a local algebra with maximal ideal $I = (x)$. Let $\mathcal{U} = \{1 + y|y \in I\}$. Then, $\mathcal{U} \cong \mathbb{G}_a$. Therefore, there exists an exact sequence

$$\{1\} \rightarrow \mathbb{G}_a \rightarrow A^* \rightarrow \mathbb{G}_m \rightarrow \{1\}.$$

It follows that $H^1(\mathcal{G}, \mathbb{G}_a) \cong \text{coker}(A_k^* \rightarrow k^*) = \{1\}$. \square

In fact, it holds that $H^i(\mathcal{G}, \mathbb{G}_a) = \{1\}$ for all $i > 0$. One way to prove this is to see that K is an induced \mathcal{G} -module so that Shapiro's lemma applies ([6], p.73). If k has characteristic 0, an alternative proof follows from the fact that $H^i(\mathcal{G}, A)$ is annihilated by $|\mathcal{G}|$ for all \mathcal{G} -module A , while the map $\lambda \rightarrow n\lambda$ is an isomorphism for all n ([6], p. 84).

Proposition 3.3.5. *If V_K is a finite dimensional vector space over K provided with a Galois action, then $H^1(\mathcal{G}, V_K) = \{1\}$.*

Proof. Let $\{v_1, \dots, v_n\}$ be a basis of invariant vectors of V_K , and let $W = \text{span}\{v_1, \dots, v_{n-1}\}$. There exists an exact sequence

$$\{1\} \rightarrow W \rightarrow V \rightarrow \mathbb{G}_a \rightarrow \{1\}.$$

Hence, the result follows by induction.

Proposition 3.3.6. *If V_k is an arbitrary vector space over k , then $H^1(\mathcal{G}, V_K) = \{1\}$.*

Proof. This follows from the previous result since V_k is a direct limit of its finite dimensional subspaces $\{W_k\}$ and therefore

$$H^1(\mathcal{G}, V_K) = H^1(\mathcal{G}, \varinjlim W_K) = \varinjlim H^1(\mathcal{G}, W_K) = \{1\}. \quad \square$$

Example 3.3.7. Let G be a \mathcal{G} -group and let K be a field with a faithful \mathcal{G} -action. Let $F = K^{\mathcal{G}}$. It follows from Galois theory that the extension K/F is Galois and $\text{Gal}(K/F) \cong \mathcal{G}$. Let $A_K = K[G]$ be the group algebra. Let $A_F = A_K^{\mathcal{G}}$. It follows from proposition 3.2.2 that $\dim_F(A_F) = \dim_K(A_K)$. In particular, A_K is actually obtained from A_F by extension of scalars and proposition 3.3.1 applies. A basis S of A_K satisfying both $S = S^\sigma$ for $\sigma \in \mathcal{G}$, and $GS = S$, is a principal homogeneous G -space. If a principal homogeneous G -space is isomorphic to some basis S as above we say that it is represented in A_K . Let T be the set of bases S of A_K satisfying $GS = S$. then A_K^* acts on T by $S \mapsto Sa$ for $a \in A_K^*$. Invariants elements of T are principal homogeneous G -spaces represented in A_K^* . By propositions 2.1.1 and 3.3.1, it follows that $T^{\mathcal{G}}/A_F^*$ is in correspondence with $H^1(\mathcal{G}, G)$. It follows that every principal homogeneous G -space is represented in A_K and if two bases S and S' that are principal homogeneous G -spaces are isomorphic as such, then there exists $a \in A_F^*$ such that $S' = Sa$.

Chapter 4

Algebraic applications of cohomology

4.1 Tensors and K/k -forms

By a tensor of type (l, m) on V , we mean an Ω -linear map $\tau : V^{\otimes l} \rightarrow V^{\otimes m}$, where

$$V^{\otimes r} = \bigotimes_{i=1}^r V \text{ for } r \geq 1, \quad V^{\otimes 0} = \Omega.$$

τ is said to be defined over k , if $\tau(V_k^{\otimes l}) \subseteq V_k^{\otimes m}$. All tensors mentioned in this work are assumed to be defined over k . $GL(V)$ acts on the set of tensors of type (l, m) by $g(\tau) = g^{\otimes m} \circ \tau \circ (g^{\otimes l})^{-1}$. It makes sense, therefore, to speak about the stabilizer of a tensor.

Let I be any set. By an I -family of tensors, we mean a map that associates, to each element $i \in I$, a tensor t_i of type (n_i, m_i) . $GL(V)$ acts on the set of all I -families by acting in each coordinate. In all that follows, we say a family instead of an I -family unless the set of indices needs to be made explicit. Let \mathfrak{T} be a family of tensors and $H = \text{Stab}_{GL(V)}(\mathfrak{T})$. Then, H is a linear algebraic group.

If K/k is a Galois extension with Galois group \mathcal{G} , we get an exact sequence

$$\{1\} \rightarrow H_K \rightarrow GL_K(V) \rightarrow X_K \rightarrow \{1\},$$

where X_K is the $GL_K(V)$ -orbit of \mathfrak{T} . It follows from (2.1), and example 3.2.2.2, that $X_K^{\mathcal{G}}/GL_k(V) \cong H^1(\mathcal{G}, H_K)$. The elements of $X_K^{\mathcal{G}}/GL_k(V)$ can be thought of as isomorphism classes of pairs (V'_k, \mathfrak{T}') that become isomorphic to (V_k, \mathfrak{T}) when extended to K . These classes are usually called K/k -forms of (V, \mathfrak{T}) , or just k -forms if $K = \bar{k}$. Observe that two vector spaces of the same dimension are isomorphic, so we can always assume that the vector space V , in which all tensors are defined, is fixed.

Definition 4.1.1. We call a pair (V, \mathfrak{T}) , where \mathfrak{T} is a family of tensors on V , a *space with tensors*, or simply a *space*. By abuse of language, we identify (V, \mathfrak{T}) and (V, \mathfrak{T}') whenever $\mathfrak{T}, \mathfrak{T}'$ are in the same $GL_k(V)$ -orbit, i.e., if they correspond to the same K/k -form. We say that (V, \mathfrak{T}') is a K/k -form of (V, \mathfrak{T}) , if \mathfrak{T} and \mathfrak{T}' are in the same $GL_K(V)$ orbit.

Example 4.1.2. Let Q be a non-singular quadratic form on the space V . Then, $\mathcal{O}_n(Q) = Stab_{GL(V)}(Q)$. Equivalence classes of non-singular quadratic forms on V_k are classified by $H^1(\mathcal{G}, \mathcal{O}_{n, \bar{k}}(Q))$. A space, in this case, is what is usually called a quadratic space.

4.2 Semi-simple abelian algebras

An abelian algebra is semisimple if it has no nontrivial nilpotent elements. In this section, let L be an abelian semi-simple algebra defined over a number field k . Then L is a k -form of the trivial semi-simple algebra

$$A^{(m)} = \underbrace{k \oplus k \oplus \dots \oplus k}_{m \text{ times}}$$

whose group of automorphisms equals S_m , the symmetric group on m symbols. It follows that the set of isomorphism classes of semi-simple abelian algebras of dimension m over k is in one-to-one correspondence with the cohomological set $H^1(\mathcal{G}, S_m) \cong Hom(\mathcal{G}, S_m) / \sim$, where $\phi \sim \psi$ means that there exists $\sigma \in S_m$ such that $\psi(g) = \sigma \phi(g) \sigma^{-1}$ for any $g \in \mathcal{G}$.

Let $\psi : \mathcal{G} \rightarrow S_m$ be one map in the conjugacy class corresponding to L . Then some properties of the algebra L can be translated into properties of the map ψ .

According to the general theory, the algebra L can be defined as the set of invariant points of the corresponding twisted action, i.e.,

$$L = \{l \in \bar{k}^m \mid \psi(\sigma)l^\sigma = l \ \forall \sigma \in \mathcal{G}\}.$$

Next we describe some properties of L in terms of $\Psi = \text{im}(\psi)$.

Proposition 4.2.1. *L is a field iff and only if Ψ acts transitively on the set $\{1, \dots, m\}$.*

Proof. The algebra L is a field if it contains a non-trivial projection P . Let $P_t \in \bar{k}^m$ be the projection in the t -th factor. If $S \subseteq \{1, \dots, m\}$, define $P_S = \sum_{t \in S} P_t$. Any projection $P \in \bar{k}^m$ is of the form P_S for some subset S . Since all projections are fixed by the non-twisted action, $P_S \in L$ if and only if $\psi(\sigma)P_S = P_S$ for all $\sigma \in \mathcal{G}$. We have $\psi(\sigma)P_m = P_{\psi(\sigma)(m)}$. Therefore, a non-trivial projection exists if and only if Ψ is not transitive. \square

More precisely, if $O \subseteq \{1, \dots, m\}$, then $P_O \in L$ if and only if O is invariant under Ψ , i.e., is a union of orbits. Any element l of L has the form $l = (l_1, \dots, l_m)$ where the elements in l_1, \dots, l_m corresponding to elements in the same orbit form a complete set of conjugates under the action of the Galois group, which

acts on them by $l_j^\sigma = l_{\psi^{-1}(j)}$. In particular, if L is a field, $\{l_1, \dots, l_m\}$ is a complete set of conjugates.

Proposition 4.2.2. *Let \mathcal{H} be the subset of \mathcal{G} that fixes a subfield L' of \bar{k} isomorphic to L . Then*

$$\ker(\psi) = \bigcap_{\sigma \in \mathcal{G}} \sigma \mathcal{H} \sigma^{-1}.$$

The description of L given earlier, implies that L' can be assumed to be the image of L under the projection on the first factor. the group $\ker(\psi)$ is the subgroup of \mathcal{G} that fixes L pointwise (in the non-twisted action). Every conjugate of \mathcal{H} is the stabilizer of the image of L under some projection. \square

Corollary 4.2.2.1. *If L is a Galois extension of k , then $\text{Gal}(L/k) \cong \Psi$. \square*

Corollary 4.2.2.2. *L is a cyclic extension of k if and only if $\text{im}\psi$ is generated by an m -cycle.*

Proof. If L/k is a cyclic extension, then $\text{im}(\psi)$ is cyclic and transitive. \square

Example 4.2.3. The exact sequence

$$\{1\} \longrightarrow A_m \longrightarrow S_m \longrightarrow \mu_2 \longrightarrow \{1\}$$

defines a cohomology map $d : H^1(\mathcal{G}, S_m) \longrightarrow H^1(\mathcal{G}, \mu_2) \cong k^*/(k^*)^2$, called the *discriminant*, whose kernel is $H^1(\mathcal{G}, A_m)$. In other words, L has discriminant 1 if and only if $\Psi \subseteq A_m$. It follows that if L is Galois and n is odd then the discriminant of L is 1. The converse is true for $n = 3$.

4.3 finite dimensional abelian algebras with nilpotent elements

Let L_k be an arbitrary finite dimensional abelian algebra over k , and let K be an algebraic closure of k .

Proposition 4.3.1. *There are no non-trivial K/k -forms of $k[x]/(x^n)$.*

Proof. Set $A_k = k[x]/(x^n)$. Then $A_K = K \oplus I_K$, where I_K is the ideal generated by x . Similarly $A_k = k \oplus I_k$. Observe that $I_K^{n-1} \neq 0$ and $I_K^n = 0$. We use induction on n . If $n = 1$ there is nothing to prove. If $n \geq 2$, then $G_n = \text{Aut}(A)$ acts on A/I^{n-1} . Let G' be the kernel of this action. Then $G_n/G' \cong G_{n-1}$, so that by induction hypothesis $H^1(\mathcal{G}, G/G') = \{1\}$.

Let $g \in G'$, and set $g(u) = u + e(u)$ with $e(u) \in I^m$. Then $g(1) = 1$, so that $e(1) = 0$. Also, for $uv \in I^2$, $g(uv) = (u + e(u))(v + e(v)) = uv$, so $e(uv) = 0$. It follows that $G' \cong \text{Hom}(I/I^2, I^m)$. In particular, it is a vector space, so it is acyclic. \square

A similar argument shows the following result:

Proposition 4.3.2. *There are no non-trivial K/k -forms of*

$$k[x_1, \dots, x_n]/(x_1, \dots, x_n)^m.$$

In general, for an algebra A_k without projectors on the algebraic closure \bar{k} it is always true that $A_K = K \oplus I_K$, where I_K is the nilradical of A_K . We can also define $G_n = \text{Aut}(A_k/I_k^{n+1})$. However, in general G_n/G' is only a subgroup of G_{n-1} , and it is not always true that $H^1(\mathcal{G}, \text{Aut}(A_K)) = \{1\}$.

The following example will make this clear:

Let $A_k = k[x, y]/((x, y)^3 + (x^2 - y^2))$. Then if I_k is the image of the ideal (x, y) , then $I^3 = 0$, but $I^2 \neq 0$. Let G be the automorphism group of A and let G' be the subgroup of automorphisms of A that induce the trivial automorphism of A/I^2 . Then G/G' is contained in the group of automorphisms of A/I^2 , i.e., the group $\text{GL}(V)$, where V is the vector space generated by x and y . An element $g \in \text{GL}(V)$ is in G/G' if and only if it fixes the ideal $(x, y)^3 + (x^2 - y^2)$. It follows that there is a short exact sequence

$$K^* \hookrightarrow G_K/G'_K \twoheadrightarrow \mathcal{O}_K(q),$$

where q is the quadratic form $x^2 - y^2$ and $\mathcal{O}(q)$ its orthogonal group. Since K^* is acyclic, it follows that $H^1(\mathcal{G}, G_K)$ equals $H^1(\mathcal{G}, \mathcal{O}_K(q))$. In other words, the K/k -forms of A_k are the algebras of the form $k[x, y]/((x, y)^3 + (q'(x, y)))$, where q' is a quadratic form.

4.4 Skolem-Noether theorem

Let \mathfrak{A} be a central simple algebra defined over k . Let L be a maximal semisimple Abelian subalgebra defined over k . \mathfrak{A}^* acts on the set of maximal semisimple Abelian subalgebras by conjugation. It is a trivial exercise in linear algebra to prove the transitivity of this action over an algebraically closed field. Let G be the stabilizer of L . It follows from (2.1), and proposition 3.3.1, that the set of conjugacy classes of maximal Abelian subalgebras that are defined over k is parametrized by $H^1(\mathcal{G}, G)$. Observe that, over the algebraic closure, any automorphism of L arises from a conjugation. The short exact sequence

$$\{1\} \longrightarrow L^* \longrightarrow G \longrightarrow \text{Aut}(L) \longrightarrow \{1\},$$

where $\text{Aut}(L)$ is the set of automorphisms of L as an Ω -algebra, gives

$$1 = H^1(\mathcal{G}, L^*) \longrightarrow H^1(\mathcal{G}, G) \longrightarrow H^1(\mathcal{G}, \text{Aut}(L)).$$

It follows, since $H^1(\mathcal{G}, \text{Aut}(L))$ classifies isomorphism classes of semisimple Abelian algebras, that any two isomorphic algebras are conjugate.

4.5 Finite subgroups in projective groups of algebras

Let k be a field and let \mathfrak{A}_k be a finite dimensional k -algebra. Let Γ_0 be a finite subgroup of \mathfrak{A}_k^*/k^* . The group Γ_0 can be regarded as a subgroup of \mathfrak{A}_K^*/K^* for any field extension K/k . In this section we describe a cohomology set that classifies finite subgroups Γ of \mathfrak{A}_k^*/k^* that become conjugate to Γ_0 over some separable algebraic extension K/k . Let C_K be the centralizer of Γ_0 in \mathfrak{A}_K^*/K^* and let W be the group of automorphisms of Γ_0 that can be realized as conjugations from elements in \mathfrak{A}_K^*/K^* . In this section we prove the following result:

Proposition 4.5.1. *Let K/k be a Galois extension. There exists a natural action of W on the cohomology set $H^1(C_K) = H^1(K/k, C_K)$. The set of conjugacy classes of finite subgroups of \mathfrak{A}_k^*/k^* that become conjugate over K to Γ_0 is in one-to-one correspondence with the set of orbits $H^1(C_K)/W$.*

Proof. The group \mathfrak{A}_K^* act on the set of finite subgroups by conjugation. The stabilizer of Γ_0 is the preimage $N_K \subseteq \mathfrak{A}_K^*$ of the normalizer of Γ_0 in \mathfrak{A}_K/K^* . It follows from Proposition 2.1.1 that, if X is the set of finite subgroups Γ of \mathfrak{A}_K^*/K^* that are conjugate to Γ_0 , i.e., the \mathfrak{A}_K^* -orbit of Γ_0 , then $X^{\mathcal{G}}/\mathfrak{A}_k^* \cong \ker[H^1(N_K) \rightarrow H^1(\mathfrak{A}_K^*)]$. Since $H^1(\mathfrak{A}_K^*) = \{1\}$ ([5], p. 16), it follows that $H^1(N_K)$ is in correspondence with the set of conjugacy classes under \mathfrak{A}_k^* of \mathcal{G} -invariant finite groups Γ that are \mathfrak{A}_K^* -conjugate to Γ_0 . The initial group Γ_0 corresponds to the distinguished element of $H^1(N_K)$. There exists a short exact sequence $C_K \hookrightarrow N_K \rightarrow W$, where W is a subgroup of $\text{Aut}(\Gamma_0)$. Notice that \mathcal{G} acts trivially on $\text{Aut}(\Gamma_0)$, and hence also on W . It follows from Propositions 38 and 39 in ([13], p. 49), that $H^1(C_K)/W \cong \ker[H^1(N_K) \xrightarrow{\pi} H^1(W)]$. Now, since the action of \mathcal{G} on W is trivial, the set $H^1(W)$ is identified with the set of conjugacy classes of homomorphisms from \mathcal{G} to W . Under this identification, the map π sends a cocycle $\alpha \in H^1(N_K)$ to a map ϕ_α , where $\phi_\alpha(\sigma) \in W$ acts on Γ_0 as conjugation by α_σ . If α is the cocycle corresponding to a group $\Gamma = a\Gamma_0a^{-1}$, then $\alpha_\sigma = a^{-1}a^\sigma$. Now,

$$(a\gamma a^{-1})^\sigma = a\alpha_\sigma\gamma\alpha_\sigma^{-1}a^{-1} \quad \forall \gamma \in \Gamma_0 \subseteq \mathfrak{A}_k.$$

It follows that the kernel of the map ϕ_α is the subgroup of \mathcal{G} corresponding to the Galois extension $k(\Gamma)/k$ generated by the coordinates of the elements of Γ . Hence ϕ_α is trivial if and only if $k(\Gamma) = k$. The result follows. \square

We give two applications of this result:

Corollary 4.5.1.1. *Let k be a field whose characteristic does not divide n . If \mathfrak{A}_k is a central division algebra over k of dimension n^2 , and if Γ_0 contains a subgroup $\Omega \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ that intersects trivially the center $Z(\Gamma_0)$ of Γ_0 , then every finite group Γ of \mathfrak{A}_k^*/k^* that is conjugate to Γ_0 over K is conjugate to Γ_0 over k .*

Proof. Without loss of generality we assume K/k is a Galois extension. we claim that if Ω is a subgroup of \mathfrak{A}_k^*/k^* isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, then Ω is its own centralizer in \mathfrak{A}_K^*/K^* . The group Ω is generated by $\rho(x)$ and $\rho(y)$, where $\rho : \mathfrak{A}_K^* \rightarrow \mathfrak{A}_K^*/K^*$ is the canonical projection, and the elements x and y satisfy the identities $x^n = a$, $y^n = b$, and $xy = \eta yx$ for some $a, b, \eta \in k$. By Kummer's Theory, $y^t \in k(x)$ implies that n divides t . In particular, η is a primitive n -th root of unity. By considering the eigenvectors of $u \mapsto xux^{-1}$, it follows that x and y generates \mathfrak{A}_K as a K -algebra. Any element centralizing $\rho(x)$ and $\rho(y)$ must be of the form $\rho(z)$ where $z^{-1}xz = \tau x$ and $z^{-1}yz = \kappa y$. Comparing eigenvalues of the functions $u \mapsto xu$ and $u \mapsto (z^{-1}xz)u$ we see that $\tau = \eta^t$, and similarly $\kappa = \eta^s$. It follows that $zy^{-t}x^{-s}$ centralizes both x and y , so that $\rho(z) = \rho(y)^t \rho(x)^s$. The condition that Ω meets trivially the center of Γ_0 implies that $C_K = K^*$, hence $H^1(C_K) = \{1\}$ ([5], p. 16). The result follows by Theorem 4.5.1. \square

This result applies to groups Γ_0 containing a copy of A_{2n} for $n^2 = \dim_k \mathfrak{A}_k > 1$. If $n = 2$, it applies to groups isomorphic to A_4 , S_4 or A_5 .

Corollary 4.5.1.2. *Let k be a field of characteristic not equal to p , where p is a prime. If \mathfrak{A}_k is a central division algebra over k of dimension p^2 , and if Γ_0 is isomorphic to $\mathbb{Z}/m\mathbb{Z}$ with $m \neq p$, then every finite group Γ of \mathfrak{A}_k^*/k^* that is conjugate to Γ_0 over K is conjugate to Γ_0 over k .*

Proof. Without loss of generality we assume K/k is a Galois extension. The group Γ_0 is generated by an element $\rho(x)$, where $x \in \mathfrak{A}_k$ satisfies $x^m \in k$ and ρ is as in the proof of Corollary 4.5.1.1. Since \mathfrak{A}_k is a division algebra, for any $d < m$ the subalgebra $k(x^d)$ is maximal abelian in \mathfrak{A}_k , i.e., $[k(x^d) : k] = p$. In particular, $k(x^d) = k(x)$. Furthermore, we have $K(x)^* \subseteq C_K$. Then any element $z \in \mathfrak{A}_K$ such that $\rho(z)$ centralizes $\rho(x)$ must satisfy $z^{-1}xz = \tau x$ where τ is an m -th root of unity. Since τx and x have the same eigenvalues, multiplication by τ must permute the eigenvalues of x . It follows that the order of τ must divide $p!$. Assume first that m is not a power of p . Replacing x by some power if needed we might assume that m is a prime. Since $[k(x) : k] = p$, we must have $m > p$. We conclude that $z \in K(x)^*$. Assume next $m = p^r$ with $r > 1$. The same argument as above shows that τ must be a p -th root of unity. Hence z commutes with x^p . Since $k(x^p) = k(x)$, we still have $z \in K(x)^*$. As $H^1(K(x)^*) = 1$ ([5], p. 16), the result follows. \square

Chapter 5

Lattices and cohomology

5.1 Basic results

Let k be a local or number field, K/k a Galois extension, $G \subseteq GL(V)$ an algebraic group defined over k , Λ_k a lattice on V_k , L_K a \mathcal{G} -invariant lattice on V_K . Let $\mathcal{G} = \mathcal{G}_{K/k}$.

Proposition 5.1.1. *If there is an element $\varphi \in G_K$ such that $\varphi(L_K) = \Lambda_K$, then $a_\sigma = \varphi^\sigma \varphi^{-1}$ is a well defined element of $H^1(\mathcal{G}, G_K^\Lambda)$. It is independent of the choice of φ and depends only on the orbit of L_K under G_k . The correspondence assigning, to every such G_k -orbit of \mathcal{O}_K -lattices, an equivalence class of cocycles, is an injection. The image of this map is*

$$\ker(H^1(\mathcal{G}, G_K^\Lambda) \xrightarrow{i_*} H^1(\mathcal{G}, G_K)),$$

where i is the inclusion.

Proof. G_K acts on the set of \mathcal{O}_K -lattices in V_K . Let X be the orbit of Λ_K . We have an exact sequence

$$\{1\} \longrightarrow G_K^\Lambda \longrightarrow G_K \longrightarrow X \longrightarrow \{1\}.$$

Hence, by (2.1), we get $X^{\mathcal{G}}/G_k \cong \ker(H^1(\mathcal{G}, G_K^\Lambda) \longrightarrow H^1(\mathcal{G}, G_K))$. \square

Example 5.1.2. Using the fact that $H^1(\mathcal{G}, GL_K(V)) = \{1\}$, we obtain that the set of $GL_k(V)$ -orbits of \mathcal{G} -invariant \mathcal{O}_K -lattices isomorphic to Λ_K is in correspondence with $H^1(\mathcal{G}, GL_K^\Lambda(V))$.

If G is defined as the stabilizer of a family of tensors, e.g., the unitary group of a hermitian form or the automorphism group of an algebra, we get a more precise result.

Recall that in section 4.1 we identified K/k -forms of (V, \mathfrak{T}) with the corresponding $GL_k(V)$ -orbits of families of tensors.

Definition 5.1.3. Let (V, \mathfrak{T}) be a space. A lattice in (V_K, \mathfrak{T}) is a pair $(\Lambda_K, \mathfrak{T})$, where Λ_K is a lattice in V_K . $GL_K(V)$ acts on the set of pairs $(\Lambda_K, \mathfrak{T}')$, for all families of tensors \mathfrak{T}' , by acting on each component. Two lattices $(\Lambda_K, \mathfrak{T})$, (L_K, \mathfrak{T}') are said to be *in the same space* if $\mathfrak{T}, \mathfrak{T}'$ are in the same $GL_k(V)$ -orbit.

Proposition 5.1.4. *Assume that G is the stabilizer of a family of tensors \mathfrak{T} on V . The set $H^1(\mathcal{G}, G_K^\Lambda)$ is in one-to-one correspondence with the set of G_k -orbits of \mathcal{G} -invariant \mathcal{O}_K -lattices in the same G_K -orbit, in all spaces that are K/k -forms of (V, \mathfrak{T}) . The kernel of the map*

$$H^1(\mathcal{G}, G_K^\Lambda) \xrightarrow{i_*} H^1(\mathcal{G}, G_K),$$

where i is the inclusion, corresponds to the subset of orbits of lattices that are in the same space as Λ_K .

Proof. We have an action of $GL_K(V)$ on the set of all pairs (L_K, \mathfrak{T}') , where L_K is a lattice and \mathfrak{T}' a family of tensors with a fixed index set. If T is the orbit of $(\Lambda_K, \mathfrak{T})$, we have a sequence

$$\{1\} \longrightarrow G_K^\Lambda \longrightarrow GL_K(V) \longrightarrow T \longrightarrow \{1\},$$

and the same argument as before applies. Last statement follows from the fact that spaces (V_K, \mathfrak{T}') are classified by $H^1(\mathcal{G}_{K/k}, G_K)$, (see section 4.1 or [5], p. 15). \square

Remark 5.1.5. Recall that $\Lambda_K = \Lambda_k \otimes_{\mathcal{O}_k} \mathcal{O}_K$. If L_K is in the same G_k -orbit as Λ_K , $L_K = L_k \otimes_{\mathcal{O}_k} \mathcal{O}_K$, since G_k also acts on V_k . Recall that we defined the cocycle corresponding to L by the formula $a_\sigma = \phi^\sigma \phi^{-1}$ (see prop. 5.1.1). This definition does not depend on G , as long as $\phi \in G$. It follows that the set of G_k -orbits of lattices in V_k that are isomorphic as \mathcal{O}_k -modules, and whose extensions to K are in the same G_K orbit, corresponds to

$$\ker(H^1(\mathcal{G}, G_K^\Lambda) \longrightarrow H^1(\mathcal{G}, G_K) \times H^1(\mathcal{G}, GL_K^\Lambda(V))). \quad (5.1)$$

In the case that G is the stabilizer of a family of tensors,

$$\ker(H^1(\mathcal{G}, G_K^\Lambda) \longrightarrow H^1(\mathcal{G}, GL_K^\Lambda(V)))$$

corresponds to the set of G_k -orbits of such lattices in all spaces that are K/k -forms of (V, \mathfrak{T}) .

Example 5.1.6. If Λ_k is free, (5.1) corresponds to the set of G_k -orbits of free lattices on V_k , whose extensions to K are in the same G_K -orbit.

Definition 5.1.7. We say that an \mathcal{O}_K -lattice Λ_K is *defined over k* , if $\Lambda_K \cong \mathcal{O}_K \otimes_{\mathcal{O}_k} \Lambda_k$ for some Λ_k . We say that Λ_K is a *k -free lattice*, if Λ_k is free.

Assume first that G is the stabilizer of a family of tensors.

Definition 5.1.8. Let $a \in H^1(\mathcal{G}, G_K^\Lambda)$. We say that a is defined over k , k -free or in (V, \mathfrak{T}) if some (hence any), lattice in the class corresponding to a has this property. Define

$$\begin{aligned}\mathcal{L}_{\text{def}}(G, K/k, \Lambda) &= \{a \in H^1(\mathcal{G}, G_K^\Lambda) | a \text{ is defined over } k\}, \\ \mathcal{L}_{\text{fr}}(G, K/k, \Lambda) &= \{a \in \mathcal{L}_{\text{def}}(G, K/k, \Lambda) | a \text{ is } k\text{-free}\}, \\ \mathcal{L}^V(G, K/k, \Lambda) &= \{a \in H^1(\mathcal{G}, G_K^\Lambda) | a \text{ is in } (V_K, \mathfrak{T})\}, \\ \mathcal{L}_{\text{def}}^V(G, K/k, \Lambda) &= \mathcal{L}^V(G, K/k, \Lambda) \cap \mathcal{L}_{\text{def}}(G, K/k, \Lambda), \\ \mathcal{L}_{\text{fr}}^V(G, K/k, \Lambda) &= \mathcal{L}^V(G, K/k, \Lambda) \cap \mathcal{L}_{\text{fr}}(G, K/k, \Lambda).\end{aligned}$$

Let

$$F_1 : H^1(\mathcal{G}, G_K^\Lambda) \longrightarrow H^1(\mathcal{G}, G_K), \quad (5.2)$$

$$F_2 : H^1(\mathcal{G}, G_K^\Lambda) \longrightarrow H^1(\mathcal{G}, GL_K^\Lambda(V)), \quad (5.3)$$

be the maps defined by the inclusions. Then, we have the following proposition:

Proposition 5.1.9. *Assume that Λ_k is free. The following identities hold:*

$$\begin{aligned}\mathcal{L}^V(G, K/k, \Lambda) &= \ker F_1, \\ \mathcal{L}_{\text{fr}}(G, K/k, \Lambda) &= \ker F_2, \\ \mathcal{L}_{\text{fr}}^V(G, K/k, \Lambda) &= \ker F_1 \cap \ker F_2. \square\end{aligned}$$

Later, we give a similar interpretation to \mathcal{L}_{def} .

Example 5.1.10.

$$\mathcal{L}_{\text{fr}}(\mathcal{O}_n(Q), \bar{k}/k, \Lambda) = \ker(H^1(\mathcal{G}, \mathcal{O}_{n, \bar{k}}^\Lambda(Q)) \longrightarrow H^1(\mathcal{G}, GL_{\bar{k}}^\Lambda(V)))$$

is in correspondence with the set of isometry classes of free quadratic lattices that become isometric to Λ_k over some extension.

Remark 5.1.11. Notice that $\mathcal{L}^V, \mathcal{L}_{\text{def}}^V, \mathcal{L}_{\text{fr}}^V$ can be defined, even if G is not the stabilizer of a family of tensors, as follows:

$$\begin{aligned}\mathcal{L}^V(G, K/k, \Lambda) &= \ker(H^1(\mathcal{G}, G_K^\Lambda) \longrightarrow H^1(\mathcal{G}, G_K)), \\ \mathcal{L}_{\text{def}}^V(G, K/k, \Lambda) &= \{a \in \mathcal{L}^V(G, K/k, \Lambda) | a \text{ is defined over } k\}, \\ \mathcal{L}_{\text{fr}}^V(G, K/k, \Lambda) &= \{a \in \mathcal{L}^V(G, K/k, \Lambda) | a \text{ is free}\}.\end{aligned}$$

In this case, the first and last identities of proposition 5.1.9 still hold. Notice that we can still interpret \mathcal{L}^V as a set of equivalence classes of lattices, because of proposition 5.1.1.

5.2 $H^1(\mathcal{G}, U_K)$ and the ideal group

Let k be a local or number field, K/k a finite Galois extension. Let $\mathcal{G} = \mathcal{G}_{K/k}$. $U_K = \mathcal{O}_K^*$ denotes the group of units of \mathcal{O}_k .

For any local or number field E , let I_E be its group of fractional ideals, P_E the subgroup of principal fractional ideals. There is a natural map $\alpha : I_k \rightarrow I_K$

defined by $\alpha(\mathcal{A}) = \mathcal{A} \otimes_{\mathcal{O}_k} \mathcal{O}_K$. Clearly $\alpha(P_k) \subseteq P_K$, so we get a map $\alpha' : I_k/P_k \rightarrow I_K/P_K$.

Apply the general theory to $\Lambda_k = \mathcal{O}_k$, $G = \mathbb{G}_m$, $G_K^\Lambda = U_K$. Any $\lambda \in K^*$ acts by $\mathcal{A} \mapsto \lambda\mathcal{A}$, for $\mathcal{A} \in I_K$. It follows that,

$$H^1(\mathcal{G}, U_K) \cong (P_K)^{\mathcal{G}}/\alpha(P_k).$$

Remark 5.2.1. When this is done over the function field extension $L(X)/F(X)$, one obtains $U_K = L^*$. Since $H^1(\mathcal{G}, L^*) = \{1\}$, this implies that every invariant ideal in $L[X]$ has a generator in $F[X]$. In particular, if a polynomial P of $F[X]$ is an n -power in $L[X]$, by taking the principal ideal generated by the n -th root, we obtain that λP is an n -th power in $F[X]$ for some constant λ . Since powers of monic polynomials are monic we conclude that a monic in $F[X]$ is an n -th power in $L[X]$ if and only if it is an n -th power in $F[X]$.

Non-zero prime ideals of \mathcal{O}_K form a set of free generators for I_K (see [7], p. 18). Let $\mathcal{A} \in I_K$. We can write

$$\mathcal{A} = \prod_{\wp \in \Pi(k)} \left(\prod_{\mathcal{P}|\wp} \mathcal{P}^{\beta(\mathcal{P})} \right).$$

If \mathcal{A} is \mathcal{G} -invariant, all the powers $\beta(\mathcal{P})$ corresponding to prime divisors of the same prime of k must be equal. In other words:

$$\mathcal{A} = \prod_{\wp \in \Pi(k)} \left(\prod_{\mathcal{P}|\wp} \mathcal{P} \right)^{\beta(\wp)}, \quad (5.4)$$

where $\beta(\wp)$ is the common value of $\beta(\mathcal{P})$ for all \mathcal{P} dividing \wp . This ideal is in $\alpha(I_k)$ if and only if the ramification degree e_\wp divides $\beta(\wp)$ for all \wp . Hence, we have an exact sequence

$$0 \longrightarrow \ker \alpha' \longrightarrow (P_K)^{\mathcal{G}}/\alpha(P_k) \longrightarrow \prod_{\wp \in \Pi(k)} (\mathbb{Z}/e_\wp),$$

where the image of the last map corresponds to those ideals of the form (5.4) that are principal in K . The image of $\ker \alpha'$ is what we call $\mathcal{L}_{\text{def}}(G, K/k, \Lambda)$. In particular, since all ideals become principal in some extension, we can take a direct limit, to obtain the long exact sequence:

$$0 \longrightarrow I_k/P_k \longrightarrow H^1(\mathcal{G}_{\bar{k}/k}, U_{\bar{k}}) \longrightarrow \prod_{\wp \in \Pi(k)} (\mathbb{Q}/\mathbb{Z}) \longrightarrow 0.$$

A refinement of this argument gives

$$H^1(\mathcal{G}_{\bar{k}/k}, U_{\bar{k}}) \cong (I_k \otimes_{\mathbb{Z}} \mathbb{Q}) / (P_k \otimes_{\mathbb{Z}} \mathbb{Z}), \quad \mathcal{L}_{\text{def}}(G, K/k, \Lambda) = I_k/P_k.$$

5.3 Localization

Recall remarks 1.0.2 and 1.0.3.

Assume k is a number field. There exist natural localization maps

$$F_v : H^1(\mathcal{G}, G_K^\Lambda) \rightarrow H^1(\mathcal{G}_w, G_{K_w}^\Lambda),$$

defined by inclusion and restriction. We define $G_{K_w}^\Lambda = G_{K_w}$ if w is Archimedean.

Lemma 5.3.1. *Let $F_1 : H^1(\mathcal{G}, G_K^\Lambda) \rightarrow H^1(\mathcal{G}, G_K)$ be the map induced by the inclusion. If the natural map*

$$\tau : H^1(\mathcal{G}, G_K) \rightarrow \prod_{v \in \Pi(k)} H^1(\mathcal{G}_w, G_{K_w})$$

is injective, then $\ker F_1 \supseteq \bigcap_v \ker F_v$.

Proof of lemma. Immediate from the following commutative diagram:

$$\begin{array}{ccc} H^1(\mathcal{G}, G_K^\Lambda) & \xrightarrow{F_1} & H^1(\mathcal{G}, G_K) \\ \downarrow \prod_v F_v & & \downarrow \tau \\ \prod_v H^1(\mathcal{G}_w, G_{K_w}^\Lambda) & \longrightarrow & \prod_v H^1(\mathcal{G}_w, G_{K_w}). \square \end{array}$$

Remark 5.3.2. If the hypothesis of this lemma is satisfied, one says that G satisfies the Hasse principle over k .

Characterisation of \mathcal{L}_{def} . $\mathcal{L}_{\text{def}}(G, K/k, \Lambda)$ is the set of equivalence classes of lattices defined over k that become isomorphic over K . A lattice L_K is defined over k if and only if it is generated by its k -points, i.e.,

$$L_K = \mathcal{O}_K(L_K \cap V_k).$$

This is a local property. On the other hand, for any local place v , all lattices defined over k_v are k_v -free, i.e.,

$$\mathcal{L}_{\text{def}}(GL(V), K_w/k_v, \Lambda) = \mathcal{L}_{\text{fr}}(GL(V), K_w/k_v, \Lambda).$$

The following result is immediate from this observation.

Proposition 5.3.3.

$$\mathcal{L}_{\text{def}}(G, K/k, \Lambda) = \ker \left(H^1(\mathcal{G}, G_K^\Lambda) \longrightarrow \prod_v H^1(\mathcal{G}_w, GL_{K_w}^\Lambda(V)) \right). \square$$

5.4 Genus and cohomology

Assume that In all of section 5.4, k is a number field.

Definition 5.4.1. Let F_v be the localization map. Define

$$C_{\text{gen}}(G, K/k, \Lambda) = \ker\left(\prod_v F_v\right).$$

We call this set the *cohomological genus* of Λ with respect to G .

Proposition 5.4.2. For any linear algebraic group G , it holds that

$$C_{\text{gen}}(G, K/k, \Lambda) \subseteq \mathcal{L}_{\text{def}}(G, K/k, \Lambda).$$

Proof. This follows from proposition 5.3.3 and the commutative diagram

$$\begin{array}{ccc} H^1(\mathcal{G}, G_K^\Lambda) & & \\ \downarrow & \searrow & \\ \prod_{v \in \Pi(k)} H^1(\mathcal{G}_w, G_{K_w}^\Lambda) & \longrightarrow & \prod_{v \in \Pi(k)} H^1(\mathcal{G}_w, GL_{K_w}^\Lambda(V)). \square \end{array}$$

Remark 5.4.3. Assume G is the stabilizer of a family of tensors. This result tells us that the cohomological genus corresponds to a set of equivalence classes of lattices defined over k . In fact, $a \in C_{\text{gen}}(G, K/k, \Lambda)$ if and only if a corresponds to a lattice, in some K/k -form of (V, \mathfrak{T}) , that is in the same G_{k_v} -orbit, at every place v .

Definition 5.4.4. We define the VC -genus of Λ_k by the formula

$$VC_{\text{gen}}(G, K/k, \Lambda) = C_{\text{gen}}(G, K/k, \Lambda) \cap \mathcal{L}^V(G, K/k, \Lambda).$$

In other words, it is the kernel of the map

$$H^1(\mathcal{G}, G_K^\Lambda) \longrightarrow H^1(\mathcal{G}, G_K) \times \prod_{v \in \Pi(k)} H^1(\mathcal{G}_w, G_{K_w}^\Lambda). \quad (5.5)$$

Let G be an arbitrary linear algebraic group. The VC -genus corresponds to a set of G_k -orbits of lattices in V_k . In fact, it corresponds to a subset of the set of double cosets $G_k \backslash G_{\mathbb{A}_k} / G_{\mathbb{A}_k}^\Lambda$, i.e., the *genus* of G (see [10], p. 440). In particular, the following proposition holds.

Proposition 5.4.5. If G has class number 1 with respect to a lattice Λ_k , then (5.5) has trivial kernel for every Galois extension K/k (compare with corollary 4 on p. 491 of [10]). \square

This, in particular, applies to a group having absolute strong approximation (see [10]). However, we have a stronger result.

Proposition 5.4.6. If G has absolute strong approximation over k , the map (5.5) is injective.

Proof. Recall remark 1.0.2.

Let M_K, L_K be two \mathcal{G} -invariant \mathcal{O}_K -lattices in V_K , that are locally in the same G_{k_v} -orbit for all v . Then, we can choose elements $\sigma_v \in G_{k_v}$, such that $\sigma_v M_{K_w} = L_{K_w}$ for every place v , and $\sigma_v = 1$ at all but finite places. Now, any global element σ , close enough to σ_v at all finite places where $\sigma_v \neq 1$, and stabilizing $M_{K_w} = L_{K_w}$ at the remaining finite places, satisfies $\sigma M_K = L_K$, as claimed. \square

The following result is just a restatement of lemma 5.3.1.

Proposition 5.4.7. *If G satisfies the Hasse principle over k , then*

$$VC_{\text{gen}}(G, K/k, \Lambda) = C_{\text{gen}}(G, K/k, \Lambda). \square$$

This result tells us that, in the presence of Hasse principle, the cohomological genus corresponds to a subset of the genus (compare with [11], thm 3.3, p. 198).

5.5 Spinor norm and genera

Let $G \subseteq GL(V)$ be a semi-simple group with universal cover \tilde{G} and fundamental group μ_n . Let $K = \bar{k}$.

The short exact sequence

$$\{1\} \longrightarrow \mu_n \longrightarrow \tilde{G}_K \longrightarrow G_K \longrightarrow \{1\},$$

defines a map $\theta : G_k \longrightarrow H^1(\mathcal{G}, F) = k^*/(k^*)^n$.

Let Λ_k be any lattice in V_k . The following proposition holds.

Proposition 5.5.1. *With the above notations, $VC_{\text{gen}}(G, K/k, \Lambda)$ is in one-to-one correspondence with the genus of G (compare with theorem 8.13 in [10], p. 490).*

Proof. It suffices to show that any two G_k -orbits in the same genus are identified over some extension. Without loss of generality, we assume k is non-real. It suffices to check that they are in the same spinor genus (see [2]). Spinor genera are classified by

$$J_k/J_k^n k^* \Theta_{\mathbb{A}}(G_{\mathbb{A}_k}^{\Lambda}),$$

where $\Theta_{\mathbb{A}}(G_{\mathbb{A}_k}^{\Lambda})$ is the kernel of the local spinor norm (see¹ [1] or [2]). This is a finite set, and the representing adèles can be chosen to have trivial coordinates at almost all places. Therefore, it suffices to take an extension that contains the n -roots of unity, and n roots of a finite set of local elements. \square

This result allows us to use cohomology to study the genus of any Semisimple group.

¹ The case of an orthogonal group is already considered in [3].

5.6 Determinant class of a lattice

Let $[\mathcal{A}]$ be the k^* -orbit of the \mathcal{O}_K -ideal \mathcal{A} . Assume that

$$\Lambda_k = \underbrace{\mathcal{O}_k \oplus \dots \oplus \mathcal{O}_k}_{n \text{ times}}.$$

The map $\det_* : H^1(\mathcal{G}, GL_K^\Lambda(V)) \rightarrow H^1(\mathcal{G}, U_K)$ is the map induced in cohomology by the determinant. It is surjective, since \det has a right inverse. However, in general it is not injective, as the example below shows.

Definition 5.6.1. Let L_K be a \mathcal{G} -invariant lattice in V_K , and let a be the cocycle class corresponding to the $GL_k(V)$ -orbit of L_K . We define the determinant class of L_K , which we denote $\det_*(L_K)$, by:

$$\det_*(L_K) = \det_*(a) \in H^1(\mathcal{G}, U_K) \cong P_K^{\mathcal{G}}/\alpha(P_k),$$

and we identify it with the corresponding ideal class.

Example 5.6.2. Using the standard embedding $GL(V) \times GL(W) \rightarrow GL(V \oplus W)$, it is easy to prove that $\det_*(\Lambda_K \oplus L_K) = \det_*(\Lambda_K)\det_*(L_K)$. In particular, we obtain that $\det_*(\mathcal{A}_1 \oplus \dots \oplus \mathcal{A}_n) = [\mathcal{A}_1 \dots \mathcal{A}_n]$.

Assume $k \subseteq K$ are local fields with maximal ideals \wp, \mathcal{P} . Assume that $\wp\mathcal{O}_K = \mathcal{P}^e$. Then,

$$\det_*\left(\underbrace{\mathcal{P} \oplus \dots \oplus \mathcal{P}}_e\right) = [\mathcal{P}^e] = 1 = \det_*\left(\underbrace{\mathcal{O}_K \oplus \dots \oplus \mathcal{O}_K}_e\right),$$

but the latter lattice is defined over k and the first one is not.

Let $\mathcal{L}_{\text{def}} = \mathcal{L}_{\text{def}}(GL(V), K/k, \Lambda)$. We have the following result:

Lemma 5.6.3. $\mathcal{L}_{\text{def}} \cap \ker(\det_*) = \{1\}$.

Proof of lemma. This follows from the fact that all k -defined lattices are of the form $\mathcal{A}_k \oplus \mathcal{O}_k \oplus \dots \oplus \mathcal{O}_k$ (see [8], (81:5)). It can also be proved by a diagram chasing argument. \square

Now observe that, for any algebraic group $G \subseteq GL(V)$, we have $\mathcal{L}_{\text{def}}(G, K/k, \Lambda) = i_*^{-1}(\mathcal{L}_{\text{def}})$, where i_* is the cohomology map induced by the inclusion.

Proposition 5.6.4. *If $G \subseteq SL(V)$, then $i_*^{-1}(\mathcal{L}_{\text{def}}) = \ker(i_*)$.*

Proof of proposition. It is immediate from the commutative diagram

$$\begin{array}{ccc} H^1(\mathcal{G}, G_K^\Lambda) & \xrightarrow{\quad} & H^1(\mathcal{G}, SL_K^\Lambda(V)) \\ & \searrow i_* & \swarrow \\ & H^1(\mathcal{G}, GL_K^\Lambda(V)) & \\ & \downarrow \det_* & \\ & H^1(\mathcal{G}, U_K) & \end{array}$$

that $\text{im}(i_*) \subseteq \ker(\det_*)$. Now recall lemma 5.6.3. \square

In particular, such a group cannot identify a free lattice to a non-free k -defined lattice over any extension, although it can identify a free lattice to a non- k -defined lattice.

In this case, a description of \mathcal{L}_{fr} is equivalent to a description of \mathcal{L}_{def} , hence $\mathcal{L}_{\text{def}}(G, K/k, \Lambda)$ can be described without resorting to localization.

5.7 Cohomology and representation

Let M be a sublattice of Λ . Let $G_K^{\Lambda, M}$ be the stabilizer of M in G_K^Λ . There exists a short exact sequence:

$$\{1\} \longrightarrow G_K^{\Lambda, M} \longrightarrow G_K^\Lambda \longrightarrow X \longrightarrow \{1\},$$

where X is the orbit of M in the set of sublattices. Then

$$X^{\mathcal{G}}/G_k^\Lambda \cong \ker(H^1(\mathcal{G}, G_K^{\Lambda, M}) \longrightarrow H^1(\mathcal{G}, G_K^\Lambda))$$

can be identified with the set of G_k^Λ -orbits of \mathcal{G} -invariant sublattices in the same G_K^Λ -orbit.

Let F be the stabilizer in G of the space $W = \Omega M$. Γ its point-wise stabilizer. $H = F/\Gamma$. There is a natural map $G_K^{\Lambda, M} \longrightarrow H_K^M$, which induces a map

$$H^1(\mathcal{G}, G_K^{\Lambda, M}) \longrightarrow H^1(\mathcal{G}, H_K^M)$$

in cohomology. If we are interested in lattices that are in the same H_k -orbit, they will be classified by the kernel of the map

$$H^1(\mathcal{G}, G_K^{\Lambda, M}) \longrightarrow H^1(\mathcal{G}, H_K^M) \times H^1(\mathcal{G}, G_K^\Lambda).$$

In the applications, G is the stabilizer of a tensor τ of type (l, m) , W a subspace satisfying $\tau(W^{\otimes l}) \subseteq W^{\otimes m}$, and $H = \text{Stab}_{GL(W)}(\tau|_W)$, where $\tau|_W$ is the restriction of τ to W . The condition on W is vacuous if $m = 0$.

Example 5.7.1. Let $\tau = q$ is a quadratic form. Inequivalent representations of M_k by Λ_k , that become equivalent over K , are in correspondence with

$$\ker \left(H^1(\mathcal{G}, \mathcal{O}_{K,n}^{\Lambda, M}(q)) \longrightarrow H^1(\mathcal{G}, \mathcal{O}_{K,p}^M(q|_W)) \times H^1(\mathcal{G}, \mathcal{O}_{K,n}^\Lambda(q)) \right),$$

where $n = \dim V$, $p = \dim W$, and $q|_W$ is the restriction of q to W .

Remark 5.7.2. All result in this paper apply also to lattices over rings of S -integers. Absolute strong approximation must be replaced by strong approximation with respect to S .

Bibliography

- [1] L.E. Arenas-Carmona. “Spinor genera under field extensions for skew-hermitian forms and cohomology.” Ph. D. thesis. Ohio-State University. Columbus. 2000.
- [2] L.E. Arenas-Carmona. “Spinor class fields and representation.” Preprint.
- [3] J. S. Hsia, Arithmetic of indefinite quadratic forms, *Contemporary Math.* **249** (1999), 1-15.
- [4] Martin Kneser, Strong approximation, in “Algebraic groups and discrete subgroups,” *Proc. Symp. Pure Math., Amer. Math. Soc.*, **9** (1966), 187-197.
- [5] Martin Kneser “Lectures on Galois cohomology of classical groups.” Tata institute of fundamental research. Bombay. 1969.
- [6] Kenneth Brown. “Cohomology of Groups.” Springer Verlag. New York. 1982.
- [7] Serge Lang. “Algebraic Number Theory.” 2nd Ed. Springer Verlag. New York. 1994.
- [8] O.T.O’meara. “Introduction to quadratic forms.” Academic press. New York. 1963.
- [9] V. P. Platonov, A. A. Bondarenko, and A. S. Rapinchuk, Class numbers and groups of algebraic groups, *Math. USSR Izv.*, **14**(1980), 547-569.
- [10] Platonov and Rapinchuk. “Algebraic groups and number theory.” Academic Press. Boston. 1994.
- [11] J. Rohlfs, Arithmetisch definierte Gruppen mit Galoisoperation, *Inventiones math.* **48** (1978), 185-205.
- [12] Louis H. Rowen. “Ring Theory.” Academic press. San Diego. 1988.
- [13] J. P. Serre. “Cohomologie Galoisienne.” 5th Ed. Springer Verlag. Berlin. 1997.