2001

On K-Conjugacy Classes of Maximal Tori in Semi-Simple Algebraic Groups.

Uroyoan Ramon-emeterio Walker
Louisiana State University and Agricultural & Mechanical College

ON k-CONJUGACY CLASSES OF MAXIMAL TORI IN SEMI-SIMPLE ALGEBRAIC GROUPS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Uroyoán R. Walker
B.S., University of Puerto Rico at Mayagüez, 1996
M.S., Louisiana State University, 1998
August 2001

Acknowledgments

On one occasion Luis Nieves Falcón told me: "La patria también necesita buenos matemáticos". Thank you for your comment. I hope to be counted among these.

I would like to thank several people that helped me along the way. First I would like to thank my mother and father for having me, for all their sacrifice, and for giving me a good upbringing.

I would like to thank my wife, Morayma, my daughter, Genesis DelMar, and my son, Vladimir Guarionex for all their patience and support. I thank the faculty of the Department of Mathematics at Louisiana State University for providing me with a pleasant working environment. I also thank the staff of the Department of Mathematics at Louisiana State University, especially Mr. Anthony Picado. I thank Dr. Luis Fernando Cáceres-Duque, after a rocky start as an undergraduate I was able to identify with him and from there everything changed . I thank Dr. Julio Vidaurrazaga for introducing me to the beauty of the Theory of Numbers. Dr. Julio Barety, thank you for being a source of inspiration. I thank Dr. Wilfredo Quiñones who gave me confidence, focus and determination. I would also like to thank Dr. Jurgen Hurrelbrink, who made everything nice.

A special thanks to Dr. Jorge Morales for believing in me, taking me under his wing, and being a guiding light. Without his guidance none of this would have been possible. I thank him for helping me mature mathematically.

I dedicate this dissertation to my father, Miguel Angel J. Walker Salamán, the best man I know. Always leading by example. Thank you for passing on to me your values and convictions. Thank you for always being there for me.

Table of Contents

Abstract

An attempt was made to make this a self-contained reading. The first three chapters are intended to provide the necessary background. Chapter one develops the tools needed from Galois Cohomology. Chapter two is a brief description of involutions, and in chapter three we define the notion of (linear) algebraic group, we give some examples and discuss some of their properties.

In chapter four, we discuss some variants of the classical Skolem-Noether theorem, requiring only that the subalgebra have a unique faithful representation of full degree over a separable closure. We verify that we can extend every isomorphism to the whole algebra by means of inner automorphisms, just as in the classical case. Examples of algebras that satisfy this condition are simple algebras and commutative Frobenius algebras. In chapter five, we attach involutions to our algebras. We show that Skolem-Noether type results hold over a separable closure and we discuss some descent problems. Chapter six is a study of k-conjugacy classes of maximal k-tori, the main goal of this dissertation. We are able to give explicit descriptions of k-conjugacy classes in particular cases. This was done by applying the general formalism developed in the chapter.

Introduction

The main objective of this dissertation is to study the k-conjugacy class of a (fixed) maximal k-torus T in a semi-simple linear algebraic group G. It is well known that, over a separable closure, all maximal tori of a semi-simple algebraic group G are conjugate. The interesting question is, what happens over the ground field? When are two maximal tori T and T' conjugate by an element of $G(k) = G^{\Gamma}$? To see that this is not a trivial question consider the following examples.

Example 0.1. If $G = \mathbf{SL}_2$ and $k = \mathbb{R}$, take

$$T_1 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2 + b^2 = 1 \right\}$$

and

$$T_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : ab = 1 \right\}$$

then $T_1(\mathbb{R}) \cong S^1$ compact, but $T_2(\mathbb{R}) \cong \mathbb{R}^{\times}$ not compact. So T_1 and T_2 cannot be conjugate over $\mathbb{R}$.

Example 0.2. If $G = \mathbf{SL}_2 \times \mathbf{SL}_2$ and we take

$$T = T_1 \times T_2$$

and

$$T' = T_2 \times T_1$$

then T and T' are not conjugate over $\mathbb{R}$. This example is of particular interest because even though T and T' are abstractly $\mathbb{R}$-isomorphic, they are not conjugate (over $\mathbb{R}$) because an inner automorphism must preserve the factors, and the factors are not conjugate as shown in example 0.1.

Since all maximal tori are conjugate over a separable closure, the set of all maximal tori is parameterized by the homogeneous space G/N, where $N = N_G(T)$ is the normalizer of T in G. We have

$$G/N \longleftrightarrow \text{set of maximal tori in } G$$

It is readily seen that this bijection commutes with the action of Γ, so if we want the set of maximal k-tori, we let Γ act on G and look at the fixed points. We have

$$(G/N)^\Gamma \longleftrightarrow \text{set of maximal } k\text{-tori in } G$$

If in addition we want the k-conjugacy classes of maximal k-tori then we look at the action of Γ on G/N modulo G^Γ, we have

$$(G/N)^\Gamma / G^\Gamma \longleftrightarrow \text{set of } k\text{-conjugacy classes of maximal } k\text{-tori in } G$$

If we consider

$$1 \longrightarrow N \xrightarrow{i_N} G \longrightarrow G/N \longrightarrow 1 \tag{1}$$

we can associate to it a sequence in cohomology,

$$G^\Gamma \longrightarrow (G/N)^\Gamma \longrightarrow \mathbf{H^1}(k, N) \xrightarrow{(i_N)^\sharp} \mathbf{H^1}(k, G) \tag{2}$$

By the general theory of Galois cohomology, there is a natural bijection between the orbit set of the group $G(k) = G^\Gamma$ in $(G/N)^\Gamma$ and $\ker(i_N)^\sharp$. Thus the set of k-conjugacy classes of maximal k-tori is in one-to-one correspondence with $\ker(i_N)^\sharp \subset \mathbf{H^1}(k, N)$.

In chapter 6, we define invariants on the set $\ker(i_N)^\sharp$. We show that these characterize completely the elements of $\ker(i_N)^\sharp$ in low cohomological dimension.

1. Galois Cohomology

1.1 Profinite Groups. Definition and Examples

Definition 1.3. Let I be a partially ordered set, denote this partial order by $\leqslant$. We say that I is a *directed set* if for all $i_1, i_2 \in I$ there is a $j \in I$ such that $i_1, i_2 \leqslant j$.

Example 1.4. Let X be any set and $Y \subseteq X$ a subset. Let $I = \{U \subset X : U \supseteq Y\}$. Define $U \leqslant V$ if $U \supseteq V$, then given U and V in I take $U \cap V$.

Example 1.5. Let $I = \mathbb{Z} \setminus \{0\}$ and for $i, j \in I$ say that $i \leqslant j$ if $i \mid j$. If $i_1, i_2 \in I$ then take $j = \mathrm{LCD}\,(i_1, i_2)$.

Definition 1.6. Let I be a directed set, $\{G_i : i \in I\}$ topological groups. We say that the triple $\left(I, G_i, \pi_i^j : G_j \longrightarrow G_i\right)$ is an *inverse system of topological groups* if

1. $\pi_i^i = \mathrm{id}_{G_i}$ for all i

2. $i \leqslant j \leqslant m \Longrightarrow \pi_i^j \circ \pi_j^m = \pi_i^m$

Definition 1.7. In the situation of definition 1.6 we define the *inverse limit* of the G_i's to be

$$\varprojlim G_i = \left\{(g_i) \in \prod G_i : \pi_i^j(g_j) = g_i\right\}$$

We call $\pi_i^j(g_j) = g_i$ the *coherence* condition.

Definition 1.8. A group G is said to be a *profinite group* if it is isomorphic (as topological groups) to some $\varprojlim G_i$, where all of the G_i's are finite and they all carry the discrete topology.

Theorem 1.9 ([R], p.40). *The following conditions are equivalent:*

1. *G is a profinite group;*

2. *G is a compact, Hausdorff group in which the family of open normal subgroups forms a fundamental system of neighborhoods of 1;*

3. *G is a compact, totally disconnected, Hausdorff group.*

Example 1.10. Any finite group is trivially profinite.

Example 1.11. The p-adic integers $\widehat{\mathbb{Z}}_p \cong \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ are profinite by construction.

For any field k we denote a (fixed) separable closure by k_{sep}. Recall that $k_{sep} = \bigcup_{i\in I} L_i$ where $\{L_i : i \in I\}$ is the partially ordered set of all finite Galois extensions of k. If $L_j \supset L_i$, then we have the restriction maps

$$\pi_i^j : \mathrm{Gal}(L_j/k) \longrightarrow \mathrm{Gal}(L_i/k)$$

so we can form the profinite group $\varprojlim \mathrm{Gal}(L_i/k)$.

Theorem 1.12 (Krull, [Wi] 6.11.1). *With the notation as above,*

$$\mathrm{Gal}(k_{sep}/k) \cong \varprojlim \mathrm{Gal}(L_i/k)$$

This is actually not so hard to see.

Sketch of Proof. If $\sigma \in \mathrm{Gal}(k_{sep}/k)$, just send it to $(\sigma|_{L_i})$ this is "coherent", by the transitivity of the reduction map. Hence it yields a group homomorphism,

$$f : \mathrm{Gal}(k_{sep}/k) \longrightarrow \varprojlim \mathrm{Gal}(L_i/k)$$

To see that f is injective, take $1 \neq \sigma \in \mathrm{Gal}(k_{sep}/k)$, then $\sigma(x) \neq x$ for some $x \in k_{sep} = \bigcup_{i\in I} L_i$. If $x \in L_i$, then $\sigma_i(x) = \sigma(x) \neq x$. So $f(x) \neq 1$, *i.e.* f is injective. On the other hand, given $(\sigma_i) \in \varprojlim \mathrm{Gal}(L_i/k)$ we want to produce a $\sigma \in \mathrm{Gal}(k_{sep}/k)$. Choose $\alpha \in k_{sep}$, so $\alpha \in L_i$ for some i. Is $\sigma(\alpha) = \sigma_i(\alpha)$? Yes! This is unambiguous because of the coherence condition, $\pi_i^j(\sigma_j) = \sigma_i$, its image under π_i^j does not change. Thus, f is an isomorphism.

In this section, Γ will denote a *profinite group*, *i.e.* a group that is the inverse limit of a system of finite groups. For the most part, we'll be dealing with $\Gamma = \mathrm{Gal}(k_{sep}/k)$. An action of Γ on the left on a discrete topological space is called *continuous* if the stabilizer of each point is an open subgroup of Γ. Discrete topological spaces with continuous left action of Γ are called Γ-*sets*. A group A which is also a Γ-set is called a Γ-*group* if Γ acts by group homomorphisms, that is,

$$\sigma(a_1 \cdot a_2) = \sigma(a_1) \cdot \sigma(a_2) \qquad \text{for } \sigma \in \Gamma,\ a_1,\ a_2 \in A.$$

A Γ-group which is commutative is called a Γ-*module*. In what follows we will construct the cohomology sets $\mathbf{H}^i(\Gamma, A)$ for $i = 0, 1, 2$.

1.2 Cohomology Sets

For any Γ-set A, we set $\mathbf{H}^0(\Gamma, A)$ to be the elements in A fixed by Γ, that is

$$\mathbf{H}^0(\Gamma, A) = A^\Gamma = \{a \in A \colon \sigma a = a \ \text{ for } \sigma \in \Gamma\}$$

If A is a Γ-group, $\mathbf{H}^0(\Gamma, A)$ is a subgroup of A.

Let A be a Γ-group. A 1-*cocycle* of Γ with values in A is a continuous map

$$\alpha \colon \Gamma \longrightarrow A$$

satisfying

$$\alpha_{\sigma\tau} = \alpha_\sigma \cdot \sigma\alpha_\tau$$

where α_σ denotes the image in A of σ under α. The set of all 1-cocycles of Γ with values in A is denoted $Z^1(\Gamma, A)$. We define an equivalence relation, $\sim_1$, on the 1-cocycles as follows

Definition 1.13. Let $\alpha, \beta \in Z^1(\Gamma, A)$,

$$\alpha \sim_1 \beta \iff \exists\, a \in A^\times \text{ such that } \alpha_\sigma = a \cdot \beta_\sigma \cdot \sigma a^{-1} \quad \forall \sigma \in \Gamma$$

Definition 1.14. $\mathbf{H}^1(\Gamma, A) = Z^1(\Gamma, A)/\sim_1$

$\mathbf{H^1}(\Gamma, A)$ is a based set with neutral element, id_A, the identity on A. If $\alpha \sim_1 \beta$, we say that α and β are *equivalent* or *cohomologous*. If A is a Γ-module, $Z^1(\Gamma, A)$ is an abelian group for the natural operation $(\alpha\beta)_\sigma = \alpha_\sigma \beta_\sigma$, and $\mathbf{H^1}(\Gamma, A)$ inherits the structure of an abelian group.

If A is a Γ-module, a 2-cocycle of Γ with values in A is a continuous map

$$\alpha \colon \Gamma \times \Gamma \longrightarrow A$$

such that

$$\sigma\alpha_{\tau,\rho} \cdot \alpha_{\sigma,\tau\rho} = \alpha_{\sigma\tau,\rho}\alpha_{\sigma,\tau} \qquad \text{for } \sigma,\ \tau,\ \rho \in \Gamma$$

The set of all 2-cocycles of Γ with values in A is denoted by $Z^2(\Gamma, A)$. This set is an abelian group for the operation $(\alpha\beta)_{\sigma,\tau} = \alpha_{\sigma,\tau} \cdot \beta_{\sigma,\tau}$. We define an equivalence relation, $\sim_2$, on the group of 2-cocycles as follows:

Definition 1.15. Let $\alpha,\ \alpha' \in Z^2(\Gamma, A)$, $\alpha \sim_2 \alpha'$ if and only if there exists a map $\varphi \colon \Gamma \longrightarrow A$ such that

$$\alpha'_{\sigma,\tau} = \sigma\varphi_\tau \cdot \varphi_{\sigma\tau}^{-1} \cdot \varphi_\sigma \cdot \alpha_{\sigma\tau} \qquad \text{for all } \sigma,\ \tau \in \Gamma$$

α and α' are said to be *equivalent* or *cohomologous*.

Equivalence classes of 2-cocycles form an abelian group denoted by $\mathbf{H^2}(\Gamma, A)$.

1.3 Functoriality

Let $f \colon A \longrightarrow B$ be a homomorphism of Γ-sets, that is, a map such that $f(\sigma a) = \sigma f(a)$ for all $\sigma \in \Gamma$ and $a \in A$. Note that if $a \in A^\Gamma$, then

$$f(a) = f(\sigma a) = \sigma f(a)$$

and thus $f(a) \in B^\Gamma$. Hence f restricts to a map

$$f^0 \colon \mathbf{H^0}(\Gamma, A) \longrightarrow \mathbf{H^0}(\Gamma, B)$$

Now if A, B are Γ-groups and if f is a group homomorphism, then f^0 is also a group homomorphism. Furthermore, there is an induced map

$$f^1 \colon \mathbf{H^1}(\Gamma, A) \longrightarrow \mathbf{H^1}(\Gamma, B)$$

given by $f^1(\alpha)_\sigma = f(\alpha_\sigma)$. One important property of f^1 is that it takes the distinguished element of $\mathbf{H^1}(\Gamma, A)$ to the distinguished element of $\mathbf{H^1}(\Gamma, B)$.

The cohomology sets have functorial properties in Γ as well. If $\Gamma_0 \subset \Gamma$ is a closed subgroup and A is a Γ-group, the action of Γ restricts to a continuous action of Γ_0, and we have the restriction map

$$\text{res} \colon \mathbf{H^i}(\Gamma, A) \longrightarrow \mathbf{H^i}(\Gamma_0, A)$$

for $i = 0, 1, 2$. Recall that for $\mathbf{H^2}(\Gamma, A)$ to make sense A has to be a Γ-module.

1.4 Cohomology Sequences

For a broader discussion on cohomology sequences the reader may want to see [KMRT, section 28.B].

Let B be a Γ-group, A a normal Γ-subgroup of B, *i.e.* a normal subgroup of B invariant under Γ. Set $C = B/A$, note that it is a Γ-group. We have the inclusion map, $i \colon A \longrightarrow B$ and the projection map $\pi \colon B \longrightarrow B/A$. These two give rise to the exact sequence

$$1 \longrightarrow A \xrightarrow{i} B \xrightarrow{\pi} C \longrightarrow 1 \tag{1.3}$$

Now the projection, $\pi \colon B \longrightarrow B/A$, induces a map of pointed sets $B^\Gamma \longrightarrow (B/A)^\Gamma$. Let $b \cdot A \in (B/A)^\Gamma$, *i.e.* $\sigma b \cdot A = b \cdot A \quad \forall \sigma \in \Gamma$. The map $\alpha \colon \Gamma \longrightarrow A$ given by $\alpha_\sigma = b^{-1} \cdot \sigma b \in A$ is a 1-cocycle with values in A, whose class $[\alpha]$ in $\mathbf{H^1}(\Gamma, A)$ is

independent of the choice of b in $b \cdot A$, for

$$\begin{aligned} b \cdot A = b' \cdot A &\implies b^{-1}\sigma(b) = b'^{-1}\sigma(b') \\ &\implies b'b^{-1} = \sigma(b'b^{-1}) \\ &\implies b'b^{-1} \in B^{\Gamma} \end{aligned}$$

so we have a (connecting) map of pointed sets $\delta^0 \colon \mathbf{H^0}(\Gamma, C) \longrightarrow \mathbf{H^1}(\Gamma, A)$ given by $\delta^0(b \cdot A) = [\alpha]$, where $\alpha_\sigma = b^{-1} \cdot \sigma(b)$.

Proposition 1.16. *The sequence*

$$1 \longrightarrow A^{\Gamma} \xrightarrow{i^0} B^{\Gamma} \xrightarrow{\pi^0} C^{\Gamma} \xrightarrow{\delta^0} \mathbf{H^1}(\Gamma, A) \xrightarrow{i^1} \mathbf{H^1}(\Gamma, B) \xrightarrow{\pi^1} \mathbf{H^1}(\Gamma, C)$$

is exact.

Proof. Exactness at A^{Γ} and at B^{Γ} follow readily from the exactness of sequence (1.3).

Exactness at C^{Γ}: Suppose the 1-cocycle $\alpha_\sigma = b^{-1} \cdot \sigma(b) \in A$ is trivial in $\mathbf{H^1}(\Gamma, A)$, that is, suppose $\alpha_\sigma = a^{-1} \cdot \sigma(a)$ for some $a \in A$. Then $b^{-1} \cdot \sigma(b) = a^{-1} \cdot \sigma(a)$, so $\sigma(ba^{-1}) = ba^{-1}$. Hence $ba^{-1} \in B^{\Gamma}$ and the coset $bA = ba^{-1}A \in B/A$ is equal to the image of $ba^{-1} \in B^{\Gamma}$ under π^0.

Exactness at $\mathbf{H^1}(\Gamma, A)$: If $\alpha \in \mathbf{H^1}(\Gamma, A)$ is in $\ker i^1$, then $i \circ \alpha_\sigma = b^{-1}\sigma b$ for some $b \in B$. Hence $\alpha_\sigma = i^{-1}(b^{-1}\sigma b)\ \forall \sigma \in \Gamma$ and $\alpha = \delta^0(c)$ where $c = \pi(b)$. On the other hand, if $\alpha \in \mathrm{Im}\delta^0$ then there is a $b \in B$ such that $\alpha_\sigma = i^{-1}(b^{-1}\sigma b)$ so $i^1\alpha_\sigma = i\alpha_\sigma = b^{-1}\sigma b$, *i.e.* $i^1\alpha \equiv \mathrm{id}_A$. Thus, $\alpha \in \ker i^1$.

Exactness at $\mathbf{H^1}(\Gamma, B)$: Let $\beta \in Z^1(\Gamma, B)$, where $[\beta] \in \ker \pi^1$. Then

$$\begin{aligned} \beta_\sigma \cdot A &= b^{-1}\sigma bA \qquad \text{for some } b \in B \\ &= b^{-1}A\sigma b \qquad \text{as } A \text{ is normal.} \end{aligned}$$

so $\beta_\sigma = b^{-1}\alpha_\sigma \sigma b$ for some $\alpha_\sigma \in Z^1(\Gamma, A)$. Hence β is in the same class as the image of $[\alpha]$ under i^1. So $\ker \pi^1 \subset \operatorname{Im} i^1$. But clearly $\operatorname{Im} i^1 \subset \ker \pi^1$. So, we have exactness at $\mathbf{H^1}(\Gamma, B)$. □

Corollary 1.17. *There is a natural bijection between* $\ker i^1$ *and the orbit set of the group* B^Γ *in* $C^\Gamma = (B/A)^\Gamma$.

Proof. A coset $b \cdot A \in C^\Gamma$ determines the element $\delta^0(b \cdot A) = [b^{-1} \cdot \sigma(b)] \in \ker i^1$. It is readily seen that $\delta^0(b \cdot A) = \delta^0(b' \cdot A)$ if and only if the cosets $b \cdot A$ and $b' \cdot A$ lie in the same B^Γ-orbit in C^Γ. □

Corollary 1.18. *There is a natural bijection between* $\ker \pi^1$ *and the orbit set of the group* C^Γ *in* $\mathbf{H^1}(\Gamma, A)$.

Proof. The group C^Γ acts on $\mathbf{H^1}(\Gamma, A)$ as follows: For $c = b \cdot A \in C^\Gamma$ and $\alpha \in Z^1(\Gamma, A)$, set $c[\alpha] = [\beta]$ where $\beta_\sigma = b \cdot \alpha_\sigma \cdot \sigma b^{-1}$. □

In general, this is as far as we can go with non-abelian cohomology. However if we have a central extension, *i.e.* $i(A) \subset Z(B)$, then we can go a seventh term, $\mathbf{H^2}(\Gamma, A)$. Since $i(A) \subset Z(B)$, A is an abelian group. We can define a (connecting) map $\delta^1 \colon \mathbf{H^1}(\Gamma, C) \longrightarrow \mathbf{H^2}(\Gamma, A)$ of pointed sets as follows:
Given $\gamma \in \mathbf{H^1}(\Gamma, C)$, choose a map $\beta \colon \Gamma \longrightarrow B$ such that β_σ is mapped to $\gamma_\sigma \quad \forall \sigma \in \Gamma$ and consider the function $\alpha \colon \Gamma \times \Gamma \longrightarrow A$ given by

$$\alpha_{\sigma,\tau} = \beta_\sigma \cdot \sigma\beta_\tau \cdot \beta_{\sigma\tau}^{-1}$$

We need to prove that $\alpha \in Z^2(\Gamma, A)$ and that $[\alpha]$ does not depend on the choices of $\gamma \in [\gamma]$ and β. To see that $\alpha \in Z^2(\Gamma, A)$ we need to check that

$$\sigma\alpha_{\tau,\rho} \cdot \alpha_{\sigma,\tau\rho} = \alpha_{\sigma\tau,\rho} \cdot \alpha_{\sigma,\tau}$$

so it is enough to see that

$$\alpha_{\sigma,\tau}^{-1}\sigma\alpha_{\tau,\rho}\cdot\alpha_{\sigma,\tau\rho}\alpha_{\sigma\tau,\rho}^{-1}=1$$

this is equivalent to

$$\alpha_{\sigma,\tau}^{-1}\cdot\beta_\sigma\sigma\alpha_{\tau,\rho}\beta_\sigma^{-1}\cdot\alpha_{\sigma,\tau\rho}\cdot\alpha_{\sigma\tau,\rho}^{-1}=1$$

which is clear since we have cancellation all over, just substituting we get

$$(\beta_{\sigma\tau}\cdot\sigma\beta_\tau^{-1}\cdot\beta_\sigma^{-1})\beta_\sigma(\sigma\beta_\tau\cdot\sigma\tau(\beta_\rho)\cdot\sigma\beta_{\tau\rho}^{-1})$$
$$\beta_\sigma^{-1}\left(\beta_\sigma\cdot\sigma\beta_{\tau\rho}\cdot\beta_{\sigma\tau\rho}^{-1}\right)\left(\beta_{\sigma\tau\rho}\cdot\sigma\tau(\beta_\rho)^{-1}\beta_{\sigma\tau}^{-1}\right)=1$$

Now if we replace β_σ by $\alpha'_\sigma\beta_\sigma$ the 2-cocycle $\alpha_{\sigma,\rho}$ is replaced by the cohomologous 2-cocycle $\alpha'_{\sigma,\tau}\cdot\alpha_{\sigma,\tau}$ with

$$\alpha'_{\sigma,\tau}=\alpha'_\sigma\cdot\beta_\sigma\sigma\alpha'_\tau\beta_\sigma^{-1}\cdot{\alpha'_{\sigma,\tau}}^{-1}$$

Thus, we can define $\delta^1([\gamma])=[\alpha]$, and we have:

Proposition 1.19. *The sequence*

$$1\longrightarrow A^\Gamma\xrightarrow{i^0}B^\Gamma\xrightarrow{\pi^0}C^\Gamma\xrightarrow{\delta^0}\mathbf{H^1}(\Gamma,A)$$
$$\xrightarrow{i^1}\mathbf{H^1}(\Gamma,B)\xrightarrow{\pi^1}\mathbf{H^1}(\Gamma,C)\xrightarrow{\delta^1}\mathbf{H^2}(\Gamma,A)$$

is exact.

Proof. We need only check exactness at $\mathbf{H^1}(\Gamma,C)$. Suppose that for some $\gamma\in Z^1(\Gamma,C)$ and some $\beta\,,\alpha$ as above we have

$$\alpha_{\sigma,\tau}=\beta_\sigma\sigma\beta_\tau\cdot\beta_{\sigma\tau}^{-1}=a_\sigma\sigma a_\tau\cdot a_{\sigma\tau}^{-1}$$

for some $a_\sigma\in A$, that is, $\gamma\in\ker\delta^1$, then $\beta_\sigma a_\sigma^{-1}\in Z^1(\Gamma,B)$, call it β'_σ. But then $\gamma=\pi^1([\beta'])$. □

Corollary 1.20. *There is a natural bijection between* $\ker \delta^1$ *and the orbit set of the group* $\mathbf{H^1}(\Gamma, A)$ *in* $\mathbf{H^1}(\Gamma, B)$.

Proof. Two elements of $\mathbf{H^1}(\Gamma, B)$ have the same image in $\mathbf{H^1}(\Gamma, C)$ if and only if they are in the same orbit under the action of $\mathbf{H^1}(\Gamma, A)$. □

Remark 1.21. The group $\mathbf{H^1}(\Gamma, A)$ acts naturally on $\mathbf{H^1}(\Gamma, B)$ by

$$(\alpha \cdot \beta)_\sigma = \alpha_\sigma \cdot \beta_\sigma$$

1.5 Some Applications

Let's see some applications of Galois Cohomology. Let L/k be a finite field extension, and set $G_L = \mathrm{Gal}(L/k)$, in particular we'll use Γ for $\mathrm{Gal}(\mathrm{k_{sep}/k})$.

Lemma 1.22. $\mathbf{H^1}(G_L, L) = \{1\}$.

Proof. By the normal basis theorem, L is a free kG_L-module. □

Theorem 1.23 (Linear Independence of Characters). *Let* Γ *be a monoid,* L *a field, and let* $f_1, \ldots, f_n$ *be distinct homomorphisms* $\Gamma \longrightarrow L^\times$. *Then the homomorphisms* $f_1, \ldots, f_n$ *are linearly independent over* L.

Proof. Suppose that $f_1, \ldots, f_n$ are linearly dependent over L. Take a linear combination

$$c_1 f_1 + c_2 f_2 + \cdots + c_k f_k = 0 \tag{1.4}$$

of minimal length k (after renumbering if necessary) where $c_i \neq 0$ for all $i = 1, \ldots, k$. Let $\sigma, \tau \in \Gamma$ and evaluate (1.4) at σ. We get

$$c_1 f_1(\sigma) + c_2 f_2(\sigma) + \cdots + c_k f_k(\sigma) = 0$$

and multiplying this by $f_1(\tau)$ we have

$$c_1 f_1(\sigma\tau) + c_2 f_2(\sigma) f_1(\tau) + \cdots + c_k f_k(\sigma) f_1(\tau) = 0$$

so

$$c_2(f_1(\tau) - f_2(\tau))f_2(\sigma) + \cdots + c_k(f_1(\tau) - f_k(\tau))f_k(\sigma) = 0$$

and since k was minimal and all the c_i's where non-zero we must have

$$f_1(\tau) - f_2(\tau) = f_1(\tau) - f_3(\tau) = \cdots = f_1(\tau) - f_k(\tau) = 0$$

hence all the homomorphisms agree on τ, which was arbitrary, *i.e.*

$$f_1(\tau) = f_2(\tau) = f_3(\tau) = \cdots = f_k(\tau) = 0$$

but this is impossible since the f_i's were distinct. □

Lemma 1.24. $\mathbf{H}^1(G_L, L^\times) = \{1\}$.

Proof. Choose a 1-cocycle α: $G_L \longrightarrow L^\times$. By theorem 1.23 the elements of G_L, regarded as characters $L^\times = \Gamma \longrightarrow L^\times$, are linearly independent. Hence we may pick $c \in L$ such that $b \neq 0$ where

$$b = \sum_{\sigma \in G_L} \alpha_\sigma \sigma(c)$$

Apply $\tau \in G_L$ to get

$$\begin{aligned} \tau(b) = \sum_{\sigma \in G_L} \tau\alpha_\sigma\tau\sigma(c) &= \sum_{\sigma \in G_L} \alpha_\tau^{-1}(\alpha_\tau\tau\alpha_\sigma)\tau\sigma(c) \\ &= \sum_{\sigma \in G_L} \alpha_\tau^{-1}\alpha_{\tau\sigma}\tau\sigma(c) \\ &= \alpha_\tau^{-1}\sum_{\sigma \in G_L} \alpha_{\tau\sigma}\tau\sigma(c) = \alpha_\tau^{-1}b \end{aligned}$$

so $\alpha_\tau = b\tau(b)^{-1}$, hence α is cohomologous to the trivial 1-cocycle. □

Let V be a finite dimensional k-vector space, so $V^* = \mathrm{Hom}_k(V, k)$.

Let $V^{(p,q)} = \underbrace{V \otimes_k \cdots \otimes_k V}_{p\text{–times}} \otimes_k \underbrace{V^* \otimes_k \cdots \otimes_k V^*}_{q\text{–times}} = V^{\otimes p} \otimes_k V^{*\otimes q}$. Elements of $V^{(p,q)}$

are called (p, q)- tensors. Suppose that W is also a finite dimensional k-vector space, and $f\colon V \xrightarrow{\sim} W$ is an isomorphism. We want to construct a map $V^{(p,q)} \longrightarrow W^{(p,q)}$. We have $f^p\colon V^{\otimes p} \longrightarrow W^{\otimes p}$, $f^*\colon W^* \xrightarrow{\sim} V^*$, and so $\left(f^{*\otimes q}\right)^{-1} = f^q\colon V^{*\otimes q} \longrightarrow W^{*\otimes q}$. Hence we get a map $f^{(p,q)}\colon V^{(p,q)} \longrightarrow W^{(p,q)}$ which, by abuse of notation, we will also call f.

Definition 1.25. A (p, q) k-object is a pair (V, x), where $x \in V^{(p,q)}$.

Definition 1.26. An isomorphism of (p, q)-objects $(V, x) \longrightarrow (W, y)$ is an isomorphism of vector spaces $f\colon V \longrightarrow W$ such that $f(x) = y$.

Example 1.27. If $(p, q) = (0, 0)$, then $V^{(0,0)} = k$. Take $x = 1 \in k$. Our object $(k, 1)$ is just a vector space.

Example 1.28. Suppose V is endowed with a k-bilinear form $b\colon V \times V \longrightarrow k$. From this we get $b\colon V \otimes V \longrightarrow k$, so (V, b) is an object of type $(0, 2)$.

Suppose $f\colon (V, b) \longrightarrow (W, b')$, to be an isomorphism of such $(0, 2)$-objects means that for any v, $v' \in V$ we must have $b(v, v') = b'(fv, fv')$.

Example 1.29. Suppose V is a k-algebra, and $\mu\colon V \times V \longrightarrow V$ gives multiplication in V. We get $\mu\colon V \otimes V \longrightarrow V$ so $\mu \in \mathrm{Hom}_k(V \otimes V, V) = V \otimes V^{*\otimes 2}$. Hence to get an algebra we need $(1, 2)$-tensors.

Now fix two k-objects (V, x) and (W, y). For any $\sigma \in G_L$, we have $\sigma(v \otimes \ell) = v \otimes {}^\sigma\ell$. Hence $(V_L)^{G_L} = V \otimes_k k = V$, similarly for W.
Now take $x \in V^{(p,q)} \subset V_L^{(p,q)}$ and $y \in W^{(p,q)} \subset W_L^{(p,q)}$, and suppose that we have an isomorphism of L-objects $f\colon V_L \xrightarrow{\sim} W_L$ such that $f(x) = y$. Can we get an isomorphism of k-objects? If not, can we measure the obstruction?
Set ${}^\sigma f = \sigma \circ f \circ \sigma^{-1}$, $A = \mathrm{Aut}\,(V_L, x)$, and $\alpha_\sigma = f^{-1} \circ {}^\sigma f$. Note that $\alpha_\sigma \in A$ and

$\alpha\colon G_L \longrightarrow A$ is a 1-cocycle, since

$$\alpha_{\sigma\tau} = f^{-1} \circ {}^{\sigma\tau}f = f^{-1} \circ {}^{\sigma}f \circ {}^{\sigma}(f^{-1} \circ {}^{\tau}f) = \alpha_{\sigma} \circ {}^{\sigma}\alpha_{\tau}$$

Remark 1.30. Replacing f by $f \circ g$ for any $g \in A$ yields a cohomologous 1-cocycle. α_σ changes to $g^{-1} \circ f^{-1} \circ {}^{\sigma}f \circ {}^{\sigma}g$.

If α is the trivial 1-cocycle, then $\alpha_\sigma = c^{-1} \circ {}^{\sigma}c$ for all $\sigma \in G_L$, so $c^{-1} \circ {}^{\sigma}c = f^{-1} \circ {}^{\sigma}f$, *i.e.* $f \circ c^{-1}$ is a G_L-equivariant isomorphism, so $(f \circ c^{-1})^{G_L} : V \xrightarrow{\sim} W$.

Let $E(L/k)$ denote the set of isomorphism classes of k-objects which become isomorphic to (V, x) over L. The above argument gives an injective map

$$\theta\colon E(L/k) \longrightarrow \mathbf{H}^1(G_L, A) \text{ where } A = \mathrm{Aut}\,(V_L, x).$$

Theorem 1.31. *θ is a bijection.*

Sketch of Proof. Choose $\alpha \in \mathbf{H}^1(G_L, A)$. As $A \subset \mathrm{GL}\,(V_L)$, by 1.24 we can find $f \in \mathrm{GL}\,(V_L)$ such that $\alpha_\sigma = f^{-1} \circ {}^{\sigma}f$. Extend f to $V_L^{(p,q)}$ as before and set $y = f(x)$. To show that (V, y) is a k-object, we want to show that $y \in V^{(p,q)}$ (not just $V_L^{(p,q)}$). It is easily seen that ${}^{\sigma}y = y$, thus $f\colon (V_L, x) \longrightarrow (V_L, y)$ is an isomorphism of L-objects and its associated 1-cocycle is given by $\alpha_\sigma = f^{-1} \circ {}^{\sigma}f$.

For a broader discussion on this see [KMRT, p.392] or [Se2, p.152].

If $\mathrm{char}\, k \neq 2$, and b is a non-degenerate skew-form on a k-vector space V, we define the symplectic group as

$$\mathrm{Sp}(V, b) = \{\gamma \in \mathrm{GL}(V)\colon b(v, v') = b(\gamma v, \gamma v')\}$$

Theorem 1.32. $\mathbf{H}^1(G_L, \mathrm{Sp}(V_L, b)) = \{1\}$.

Proof. This set classifies skew-forms on V which become isomorphic on V_L. But it is well-known that all non-degenerate skew-forms on V are isomorphic. Thus $\mathbf{H}^1(G_L, \mathrm{Sp}(V_L, b)) = \{1\}$. □

Theorem 1.33. $\mathbf{H}^1(G_L, \mathbf{GL}_n L) = \{1\}$ *for all* $n \geqslant 1$.

Proof. This set classifies vector space structures of V which become isomorphic on L, there is only one such. □

Theorem 1.34. $\mathbf{H}^1(G_L, \mathbf{SL}_n L) = \{1\}$.

Proof. Consider the exact sequence

$$1 \longrightarrow \mathbf{SL}_n L \longrightarrow \mathbf{GL}_n L \xrightarrow{\det} L^\times \longrightarrow 1$$

Looking at its associated exact sequence in cohomology we have

$$1 \longrightarrow \mathbf{SL}_n k \longrightarrow \mathbf{GL}_n k \longrightarrow k^\times \xrightarrow{\delta^0} \mathbf{H}^1(G_L, \mathbf{SL}_n L) \longrightarrow \underbrace{\mathbf{H}^1(G_L, \mathbf{GL}_n L)}_{=\{1\} \text{ by } 1.24}$$

so the sequence becomes

$$1 \longrightarrow \mathbf{SL}_n k \longrightarrow \mathbf{GL}_n k \xrightarrow{\det^0} k^\times \xrightarrow{\delta^0} \mathbf{H}^1(G_L, \mathbf{SL}_n L) \longrightarrow 1$$

and so applying the first isomorphism theorem we have

$$k^\times / \ker \delta^0 \cong \mathrm{Im}\delta^0$$

But $\ker \delta^0 = \mathrm{Im}\det^0 \cong k^\times$ and δ^0 is also surjective since the sequence is exact. Hence $\mathrm{Im}\delta^0$ is isomorphic to $\mathbf{H}^1(G_L, \mathbf{SL}_n L)$ and so $\mathbf{H}^1(G_L, \mathbf{SL}_n L) = \{1\}$. □

1.6 Kummer Theory

Let k be a field, and let $k \supset \mu_n$ be the set of n^{th} roots of unity, where $\gcd(n, \mathrm{char}\, k) = 1$, and $\Gamma = \mathrm{Gal}(k_{sep}/k)$. We have an exact sequence of discrete Γ-modules

$$1 \longrightarrow \mu_n \longrightarrow k_{sep}^\times \xrightarrow{n} k_{sep}^\times \longrightarrow 1$$

where the map n takes $x \in k_{sep}^{\times}$ to x^n. Looking at the associated sequence in cohomology we get:

$$1 \longrightarrow \mu_n \longrightarrow k^{\times} \xrightarrow{n} k^{\times} \longrightarrow \mathbf{H}^1(\Gamma, \mu_n) \longrightarrow \underbrace{\mathbf{H}^1(\Gamma, k_{sep}^{\times})}_{= \varinjlim \underbrace{\mathbf{H}^1(G_L, L^{\times})}_{=\{1\} \text{ by } 1.24}}$$

Thus we have

Theorem 1.35 (Kummer, [KMRT] 30.1). $\mathbf{H}^1(\Gamma, \mu_n) \cong k^{\times}/k^{\times n}$.

Proof. Just apply the first isomorphism theorem to the above sequence in cohomology. □

1.7 Central Simple Algebras

A finite dimensional k-algebra A is called a *central simple k-algebra* or a *central simple algebra over k* (sometimes denoted CSA over k) provided:

1. $k = Z(A)$
2. A has no proper 2-sided ideals.

Theorem 1.36 (Wedderburn). *Let A be a central simple algebra over k, and M be a simple (irreducible) left A-module. Then*

1. $D = \mathrm{End}_A(M)$ *is a division algebra with* $Z(D) = k$.
2. $A \cong \mathrm{M}_n(D)$ *for some* n.

Proof. See, for example, [Sc, Theorem 1.11] on p. 284. □

Example 1.37. $A = \mathbf{M}_n k$ is a CSA over k.

Example 1.38. Let D be a skew field. Set $k = Z(D)$. Then D is a CSA over k.

Example 1.39. Let $\mathbb{H} \subset \mathbf{M}_2\mathbb{C}$ be the algebra of Hamilton quaternions

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & -\bar{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$$

Then $\mathbb{H}$ is a CSA over $\mathbb{R}$, and $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbf{M}_2\mathbb{C}$.

Theorem 1.40 (Skolem-Noether, [KMRT] 1.4). *Let A be a central simple algebra over k, and B be a simple k-algebra. Suppose that $f, g\colon B \longrightarrow A$ are any two k-algebra embeddings. Then there is an $a \in A^\times$ such that $f(b) = ag(b)a^{-1}\ \forall\, b \in B$.*

Before proving this result we state the following immediate corollary:

Corollary 1.41. *Let A be a central simple algebra over k, and let* $\mathrm{Aut}(A)$ *denote the group of all k-algebra automorphisms of A, then*

$$\mathrm{Aut}(A) \cong A^\times / k^\times$$

Proof. Define a homomorphism

$$\begin{aligned} \mathrm{Inn} &: A^\times / k^\times \longrightarrow \mathrm{Aut}(A) \\ &: a \mapsto (x \mapsto axa^{-1}) \end{aligned}$$

Since A is central over k, Inn is injective. To see that Inn is surjective, let $\varphi\colon A \longrightarrow A$ be an automorphism, and apply the Skolem-Noether theorem with $B = A$, $f = \varphi$, and $g = \mathrm{id}_A$. We get $\varphi(x) = axa^{-1}$ for some $a \in A^\times$ and all $x \in A$, so $\varphi = \mathrm{Inn}(a)$. □

In particular, $\mathrm{Aut}(\mathbf{M}_n k) \cong (\mathbf{GL}_n k)/k^\times = \mathbf{PGL}_n k$, where $k^\times$ is isomorphic to the diagonal matrices.

Proof. (of 1.40) Let us break the proof up into two cases.

Case 1: Suppose A is split, *i.e.* $A = \mathrm{End}_k(D)$ for some skew-field D.

Since A is a CSA over k, write $A = \mathbf{M}_n D$, where D is a skew-field. Let $S = D^n$ $(D = \mathrm{End}_A(S))$. A acts on S by left matrix multiplication, where the elements of S are written as column vectors. We know that S is *the* simple A-module. Let $C = D \otimes_k B$, notice that, in particular, C is a simple algebra. We will define two C-module structures on S. For all $d \in D$, $b \in B$, $x \in S$ we define:

$$S_f \quad : \quad (d \otimes b)(x) = d(f(b)x)$$

$$S_g \quad : \quad (d \otimes b)(x) = d(g(b)x)$$

C being a simple algebra, all C-modules are sums of copies of the simple C-module S. In particular, if S_1 and S_2 are C-modules of the same dimension over k, they are isomorphic. Hence S_f and S_g are isomorphic as C-modules, *i.e.* there exists $\theta\colon S \longrightarrow S$ such that

$$\theta\,(df(b)x) = d\,(g(b)\theta(x)) \tag{1.5}$$

for all $d \in D$, $b \in B$, and $x \in S$. So, taking $b = 1$ in (1.5) above, we have $\theta(dx) = d\theta(x)$, hence θ commutes with d, *i.e.*

$$\theta \in \mathrm{End}_D(S) = \mathrm{End}_D(D^n) \cong \mathbf{M}_n(D) = A$$

so θ is just left multiplication by an element of $A^\times$, say a. Again from (1.5) above we have

$$a\,(df(b)x) = d\,(g(b)ax)$$

for all $d \in D$, $b \in B$, and $x \in S$. Taking $d = 1$, we get $af(b)x = g(b)ax$ for all $x \in S$, hence $af(b) = g(b)a$ for all $b \in B$. Therefore,

$$af(b)a^{-1} = g(b) \quad \text{for all } b \in B$$

Case 2: General Case

Consider the maps

$$f \otimes \mathrm{id},\ g \otimes \mathrm{id}\colon B \otimes A^{op} \longrightarrow A \otimes A^{op} = \mathrm{End}_k(A)$$

Since $B \otimes A^{op}$ is simple (as B is), we may apply corollary 1.41. By the corollary there exists an invertible $\varphi \in A \otimes A^{op}$ such that

$$(gb) \otimes a' = \varphi^{-1}\,(f(b) \otimes a')\,\varphi \quad \text{for all } b \in B,\ a' \in A^{op}$$

Setting $b = 1$, one sees that f commutes elementwise with all elements of $1 \otimes A^{op} \cong A^{op}$. But $\varphi = \psi \otimes 1$ for some $a \in A$. Setting $a' = 1$ yields

$$gb = a^{-1}(fb)a \qquad \forall b \in B$$

□

The Skolem-Noether theorem states that every isomorphism of a simple subalgebra can be extended to the entire algebra in a very particular way, namely by an inner automorphism.

1.8 The Brauer Group

We now define an equivalence relation $\sim$ on central simple algebras over k as follows: Let $A \cong \mathbf{M}_n D$ and $B \cong \mathbf{M}_m D'$, then

$$A \sim B \iff D \cong D' \text{ as } k\text{-algebras and } n = m$$

Denote the equivalence class of A as $[A]$, then we define the product of two equivalence classes to be $[A] \cdot [B] := [A \otimes B]$, later we will write this additively, *i.e.* $[A] + [B] = [A \otimes B]$. Let $\mathrm{Br}(k)$ be the set of equivalence classes of central simple algebras over k. $\mathrm{Br}(k)$ with this operation is actually an abelian group, called the

Brauer group of k, the associativity of the product follows from the associativity of the tensor product. $\mathrm{Br}(k)$ has identity $[k]$, and the inverse of a class $[A]$ is the class of its opposite algebra $[A^{op}]$.

Example 1.42. If k is algebraically closed, then $\mathrm{Br}(k) = \{0\}$.

Proof. Let D be a skew field, central over k. We need to show that $D = k$. Choose $\lambda \in D$, and let $\ell_\lambda \colon D \longrightarrow D$ be left multiplication by λ, a k-linear map. Since k is algebraically closed, ℓ_λ has an eigenvector. Call it v. So $\ell_\lambda(v) = av$ for some $a \in k$. Hence, we have the following

$$\begin{aligned} \lambda v = av &\iff (\lambda - a)v = 0 \qquad (v \neq 0) \\ &\iff \lambda - a = 0 \\ &\iff \lambda = a \in k \end{aligned}$$

□

Theorem 1.43 (Tsen). *If k is a function field in one variable over an algebraically closed field, then* $\mathrm{Br}(k) = \{0\}$.

Proof. See [Sh]. □

If L/k is a finite field extension we define a map

$$\begin{aligned} \_ \otimes_k L \ &: \ \mathrm{Br}(k) \longrightarrow \mathrm{Br}(L) \\ &: \ [A] \longmapsto [A \otimes_k L] \end{aligned}$$

Definition 1.44. We define the relative Brauer group of a finite field extension, $\mathrm{Br}(L/k)$, to be $\ker(\_ \otimes_k L)$.

Note that these are the central simple algebras over k that split over L, *i.e.* $A \otimes_k L \cong \mathrm{M}_n L$. Another way to view $\mathrm{Br}(k)$ is as follows

$$\mathrm{Br}(k) = \bigcup_{L/k} \mathrm{Br}(L/k) = \varinjlim \mathrm{Br}(L/k)$$

where L/k are all the finite separable field extensions of k. In fact one can show

Theorem 1.45. $\mathrm{Br}(L/k) \cong \mathbf{H^2}(G_L, L^\times)$.

Proof. Define a vector space A over L with basis $\{a_\sigma : \sigma \in G_L\}$. Hence the elements of A may be written uniquely in the form $\sum_{\sigma \in G_L} c_\sigma a_\sigma$ with $c_\sigma \in L$. Now, given a 2-cocycle $\psi \in \mathbf{H^2}(G_L, L^\times)$ we define a multiplication in A with relations as follows:

$$a_\sigma a_\tau = \psi_{\sigma,\tau} a_{\sigma\tau} \quad \text{and} \quad a_\sigma c = \sigma(c) a_\sigma \quad \text{for all } c \in L$$

The 2-cocycle condition assures the associativity of this product. Now, denote by $A(\psi)$ the algebra just defined. We will state the following facts without proof. The proofs may be found in [J, section 8.4].

1. The algebra $A(\psi)$ is a central simple algebra over k.
2. $A(\psi) \otimes_k A(\varphi) \cong A(\psi + \varphi) \otimes_k \mathbf{M}_n(k)$.
3. The trivial 2-cocycle yields the matrix algebra $\mathbf{M}_n(k)$, where $n = [L : k]$.
4. $A(\psi) \cong A(\varphi)$ if and only if ψ and φ are cohomologous.
5. Every central simple algebra is isomorphic to an algebra $A(\psi)$ for some 2-cocycle $\psi \in \mathbf{H^2}(G_L, L^\times)$.

From these (non-trivial) facts we conclude that the correspondence $\psi \longmapsto A(\psi)$ defines a group isomorphism

$$\mathbf{H^2}(G_L, L^\times) \xrightarrow{\sim} \mathrm{Br}(L/k)$$

as desired. □

Example 1.46. $\mathrm{Br}(\mathbb{C}/\mathbb{R}) \cong \mathbf{H}^2(C_2, \mathbb{C}^\times) \cong \mathbb{Z}/2\mathbb{Z}$. The non-zero element of $\mathrm{Br}(\mathbb{C}/\mathbb{R})$ corresponds to the 4-dimensional algebra of Hamiltonian quaternions $\mathbb{H}$.

As an immediate consequence of theorem 1.45 we have:

Corollary 1.47. $\mathrm{Br}(k) \cong \mathbf{H}^2(\Gamma, k_{sep}^\times)$.

In particular, $\mathrm{Br}(k)$ is always a torsion group. Hence, one can look at the n-th torsion of $\mathrm{Br}(k)$,

$$ {}_n\mathrm{Br}(k) = \{[A] \in \mathrm{Br}(k) \colon [A^{\otimes n}] = 0\}$$

Around 1980, Suslin and Merkujev proved that ${}_n\mathrm{Br}(k)$ is generated by n-cyclic algebras. The interested reader may want to see [Wi, section 6.11].

1.9 Étale Algebras

Let k be an arbitrary field, k_{sep} denote a (fixed) separable closure of k, and $\Gamma = \mathrm{Gal}\,(k_{sep}/k)$ be the absolute Galois group of k. Let V_0 be a k-vector space. The left action of Γ on $V = V_0 \otimes_k k_{sep}$ defined by

$$\gamma * (u \otimes x) = u \otimes \gamma(x) \qquad \text{for } u \in V_0,\ x \in k_{sep}$$

is semi-linear with respect to Γ, *i.e.*

$$\gamma * (vx) = (\gamma * v)\gamma(x) \qquad \text{for } v \in V,\ x \in k_{sep}$$

Lemma 1.48 (Galois Descent, [KMRT] 18.1). *Let V be a k_{sep}-vector space. If Γ acts continuously on V by semi-linear automorphisms, then*

$$V^\Gamma = \{v \in V \colon \gamma * v = v \quad \forall \gamma \in \Gamma\}$$

is a k-vector space and the map

$$\begin{aligned} V^{\Gamma} \otimes k_{sep} &\longrightarrow V \\ v \otimes x &\longmapsto vx \end{aligned}$$

is an isomorphism of k_{sep}-vector spaces.

Proof. See [KMRT, Lemma 18.1] on p.279. □

Let Alg_k be the category of unital commutative associative k-algebras with k-algebra homomorphisms as morphisms. For every finite dimensional commutative k-algebra L, let

$$X(L) = \mathrm{Hom}_{\mathrm{Alg}_k}(L, k_{sep})$$

For any field extension F/k, let L_F be the F-algebra $L \otimes_k F$. Notice that if $F \subset k_{sep}$, then k_{sep} is also a separable closure of F, and every k-algebra homomorphism $L \longrightarrow k_{sep}$ extends uniquely to an F-algebra homomorphism $L_F \longrightarrow k_{sep}$. Hence we can identify $X(L_F) = X(L)$.

Proposition 1.49. *For a finite dimensional commutative k-algebra L, the following statements are equivalent:*

1. *For every field extension F/k, the F-algebra L_F is reduced, i.e. L_F does not contain any non-zero nilpotent elements;*
2. *$L \cong F_1 \times \cdots \times F_r$ for some finite separable field extensions $F_1, \cdots, F_r$ of k;*
3. *$L_{k_{sep}} \cong k_{sep} \times \cdots \times k_{sep}$;*
4. *The bilinear form $T\colon L \times L \longrightarrow k$ induced by the trace:*

$$T(x, y) = \mathrm{Tr}_{L/k}(xy) \qquad \text{for } x, y \in L$$

is non-singular;

5. $\operatorname{card} X(L) = \dim_k L$;

6. $\operatorname{card} X(L) \geqslant \dim_k L$.

If the field k is infinite, the above statements are also equivalent to:

7. $L \cong k[X]/(f)$ for some polynomial $f \in k[X]$ which has no multiple root in an algebraic closure of k.

Proof. See [KMRT, Proposition 18.3] p.281. □

A finite-dimensional commutative k-algebra satisfying any (and hence all) of the conditions above is called an *étale k-algebra*. Notice from the first (or fourth) statement that étale algebras remain étale under scalar extensions.

We now use Hilbert's theorem 90 to show how étale algebras are classified by an $\mathbf{H^1}$-cohomology set.

The k-algebra $A = k \times \cdots \times k$ (n copies) is étale of dimension n. For if $\{e_i\}_{i=1}^n$ is the set of primitive idempotents of A, any k-algebra automorphism is completely determined by the images of the e_i's. Thus, $\operatorname{Aut}_{alg}(A)$ is the constant symmetric group S_n. Proposition 1.49 shows that the étale k-algebras of dimension n are precisely the twisted forms of $A = k \times \cdots \times k$. Therefore we have a bijection:

$$\mathbf{H^1}(k, S_n)$$

$$\updownarrow$$

k-isomorphism classes of étale k-algebras of degree n

For a more detailed discussion on Étale Algebras the interested reader may refer to [KMRT, section 18.A].

1.10 The p-Cohomological Dimension of a Profinite Group

Let p be a prime number, and let G be a profinite group.

Definition 1.50. A profinite group G is said to be a *pro-p-group* if it is the inverse limit of p-groups, *i.e.* if its order is a power of p.

Definition 1.51. If G is a profinite group, a closed subgroup H of G is said to be a p-Sylow group of G if H is a pro-p-group and $(G\colon H)$ is prime to p.

Example 1.52. $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is a pro-p-group.

Theorem 1.53 (Sylow Theorem for Profinite Groups). *Let G, G_1 and G_2 be profinite groups.*

1. *G possesses p-Sylow subgroups.*
2. *If H is any pro-p-subgroup of G, then H is contained in some p-Sylow subgroup of G.*
3. *Any two p-Sylow subgroups of G are conjugate in G.*
4. *$|G| = \prod_p |G_p|$, where G_p is a p-Sylow group of G.*
5. *If $h\colon G_1 \longrightarrow G_2$ is a continuous surjective homomorphism of profinite groups, then the image of a p-Sylow group is a p-Sylow group.*

Proof. See [R, p.47]. □

For a profinite group G, let $\mathrm{Mod}(G)$ denote the category of G-modules, and let $\mathrm{Mod}_t(G)$ denote the full subcategory of $\mathrm{Mod}\,(G)$ consisting of the torsion modules (torsion as abelian groups). If $A \in \mathrm{Mod}_t(G)$ and p is a prime number, denote by $A(p)$ the p-primary part of A, *i.e.* those elements of A of order p^n for some n. If $A(p) = A$ we say A is p-primary.

Proposition 1.54. *If G is a pro-p-group, every simple p-primary G-module A is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Definition 1.55. The p-cohomological dimension of G, denoted $\mathrm{cd}_p(G)$, is the lower bound of the set of natural numbers n satisfying:

$$\mathbf{H}^q(G, A)(p) = 0 \quad \text{for all } q > n \text{ and all } A \in \mathrm{Mod}_t(G). \tag{1.6}$$

By convention, if there is no integer n satisfying (1.6) $\mathrm{cd}_p(G) = +\infty$. One calls $\mathrm{cd}(G) = \sup \mathrm{cd}_p(G)$ the *cohomological dimension of G.*

Proposition 1.56. *Let G be a profinite group, let p be a prime number, and let n be an integer. The following statements are equivalent:*

a. $\mathrm{cd}_p(G) \leqslant n$;

b. $\mathbf{H}^q(G, A) = 0$ *for all $q > n$ and all p-primary $A \in \mathrm{Mod}_t(G)$;*

c. $\mathbf{H}^{n+1}(G, A) = 0$ *for all simple p-primary G-modules A.*

Proof. See [R, p.200]. □

Proposition 1.57. *Let $H \subset G$ be profinite groups, and p a prime number. Then*

$$\mathrm{cd}_p(H) \leqslant \mathrm{cd}_p(G)$$

Moreover, equality holds in either of the following cases

1. $p \nmid (G : H)$
2. *H is open in G and* $\mathrm{cd}_p(G) < \infty$

Proof. See [R, p.204]. □

Corollary 1.58. *Let G_p be a p-Sylow group of G. Then*

$$\mathrm{cd}_p(G) = \mathrm{cd}_p(G_p) = \mathrm{cd}\,(G_p)$$

Corollary 1.59. $\mathrm{cd}_p(G) = 0 \iff p \nmid |G|$

Corollary 1.60. *If* $\mathrm{cd}_p(G) \neq 0, \infty$, *then* p^∞ *divides* $|G|$.

Corollary 1.61. *If* G *is finite and* $p \nmid |G|$, *then* $\mathrm{cd}_p(G) = \infty$.

Proposition 1.62. *Let* N *be a normal closed subgroup of a profinite group* G, *and let* p *be a prime. Then*

$$\mathrm{cd}_p(G) \leqslant \mathrm{cd}_p(N) + \mathrm{cd}_p(G/N)$$

Proof. [R, p.209]. □

2. Involutions

2.1 Involutions on Rings

Definition 2.63. Let R be a ring. An *involution* on R is a map $\sigma\colon R \longrightarrow R$ such that for all $a, b \in R$

1. $\sigma(a+b) = \sigma(a) + \sigma(b)$
2. $\sigma(ab) = \sigma(b)\sigma(a)$
3. $\sigma^2(a) = a$

The pair (R, σ) is called a *ring with involution.*

Example 2.64. $(\mathbb{C}, \bar{})$ is a ring with involution, where $\bar{}$ denotes complex conjugation.

Example 2.65. Let R be any commutative ring, then the transpose is an involution on $\mathbf{M}_n(R)$.

Definition 2.66. Let k be a field. For $a, b \in k^\times$ define a 4-dimensional k-algebra with basis $1, e_1, e_2, e_3$ by the following multiplication table:

$$e_1e_2 = e_3, \quad e_2e_1 = -e_1e_2, \quad e_1^2 = a \cdot 1\,(= a), \quad e_2^2 = b \cdot 1\,(= b)$$

This algebra is denoted by $(a, b) = (a, b)_k$ and called a *quaternion algebra over k.*

The subspace $e_1k + e_2k + e_3k = \{x \in (a, b)\colon x^2 \in k,\ x \notin k^\times\}$ is denoted by $(a, b)_0$, and is called the subspace of pure quaternions. Hence we have

$$(a, b) = k \cdot 1 \oplus (a, b)_0$$

Thus, if $x \in (a, b)$, then $x = x_0 + x_1$, where $x_0 \in k$ and $x_1 \in (a, b)_0$ are uniquely determined. The map

$$\begin{aligned} \sigma \quad : \quad & (a, b) \longrightarrow (a, b) \\ & x \longmapsto x_0 - x_1 \end{aligned}$$

is a k-linear involution, and it is called the *canonical involution* on the quaternion algebra (a, b).

Example 2.67. The canonical involution on a quaternion algebra.

Example 2.68. Let G be a group, and k be a field. Let $A = k[G]$ be the group algebra of G over k. The canonical involution on A is the k-linear extension of $\sigma\colon\ g \mapsto g^{-1}$.

In the category of rings with involutions, a morphism is a ring homomorphism $f\colon (R, \sigma) \longrightarrow (S, \tau)$ with $\tau(f(x)) = f(\sigma(x))$ for all $x \in B$. If R is a commutative ring, the identity is an involution. If R is not commutative, the identity is *not* an involution. For every involution σ the fixed elements form a subring $R^\sigma = \{\alpha \in R\colon \sigma\alpha = \alpha\}$ of R.

Remark 2.69. Let V be a k-space, where $\operatorname{char} k \neq 2$, then there is a one-to-one correspondence between involutions on V and idempotents on $\operatorname{End}_k(V)$.

Proof. If $e \in \operatorname{End}_k(V)$ is an idempotent, associate to it $2e - \mathrm{id}$ an involution on V. On the other hand, if τ is an involution on V, associate to it the idempotent $\frac{1}{2}(\tau + \mathrm{id})$. □

Definition 2.70. Let R be a ring with involution σ, and M be a right R-module

1. A *sesquilinear mapping* or a *sesquilinear form* on M is a map $s\colon M \times M \longrightarrow R$ such that

a. $s(x+y,z) = s(x,z) + s(y,z)$

b. $s(x,y+z) = s(x,y) + s(x,z)$

c. $s(x,y\alpha) = s(x,y)\alpha$

d. $s(x\alpha,y) = \sigma(\alpha)s(x,y)$

for all x, $y \in M$ and $\alpha \in R$. The transpose σs of a sesquilinear map is defined by $\sigma s(x,y) = \sigma(s(y,x))$.

2. Let $Z = Z(R)$ be the center of R. Let $\lambda \in Z$ satisfy $\lambda\sigma(\lambda) = 1$. Then a sesquilinear form $h\colon M \times M \longrightarrow R$ is called λ-hermitian if $h = \lambda\sigma(h)$, *i.e.* $h(x,y) = \lambda(\sigma h(x,y))$ for all x, $y \in M$. The pair (M,h) is called a *λ-hermitian module* or a λ-hermitian space.

Remark 2.71. If $\lambda = 1$, h is simply called a hermitian form.

An involution σ on a skew field D is called of the first kind if σ is the identity on Z, the center of D. Otherwise the involution is called of the second kind. In this case $\sigma|Z$ is an automorphism of order 2. Define $Z^\sigma = \{\alpha \in Z\colon \sigma\alpha = \alpha\}$. Thus $Z = Z^\sigma$ for involutions of the first kind and Z/Z^σ is a separable quadratic extension for involutions of the second kind. In the case of involutions of the first kind only $\lambda = \pm 1$ appear. We thus have, hermitian forms ($\lambda = 1$), or skew hermitian forms ($\lambda = -1$). In the case of involutions of the second kind, we can assume without loss of generality that $\lambda = 1$, and thus we have only hermitian forms.

2.2 Involutions on Central Simple Algebras

Definition 2.72. An *involution* on a central simple algebra A over an arbitrary field k is a map $\sigma\colon A \longrightarrow A$ such that for all x, $y \in A$

1. $\sigma(x+y) = \sigma(x) + \sigma(y)$

2. $\sigma(xy) = \sigma(y)\sigma(x)$

3. $\sigma^2(x) = x$

Notice that if A is a k-algebra σ is *not* necessarily k-linear. However, k is stable under σ. Hence $\sigma|k$ is an automorphism which is either the identity or of order 2. If the involution σ is such that

1. $\sigma|k = \mathrm{id}$, then σ is said to be an *involution of the first kind.*

2. $\sigma|k \neq \mathrm{id}$, then σ is said to be an *involution of the second kind.*

Involutions of the first kind are divided into two types: the orthogonal type and the symplectic type. Involutions of the second kind are called unitary or of unitary type.

Example 2.73. For any field k, take $A = \mathbf{M}_n(k)$ together with the transposition.

Example 2.74. There could be different involutions on $\mathbf{M}_n(k)$, for example if $n = 2$, we have the involution

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

which is clearly different from the transposition.

Example 2.75. Let (R, σ) be any ring with involution, then

$$(a_{ij}) \longmapsto {}^t(\sigma(a_{ij}))$$

is an involution on $\mathbf{M}_n(R)$.

There is also the concept of adjoint involution which we will find particularly useful so we will define it here.

Let k be an arbitrary field of characteristic different from 2. Let (V, q) be a

quadratic space of dimension $2n$ over k, where q is a non-degenerate form, and b is the symmetric bilinear form associated to q. We can define an (adjoint) involution σ_b from the bilinear form b as follows

Definition 2.76. For any $f \in \mathrm{End}_k(V)$ define $\sigma_b(f) \in \mathrm{End}_k(V)$ by

$$\sigma_b(f) = \hat{b}^{-1} \circ f^t \circ \hat{b}$$

where $\hat{b}\colon V \xrightarrow{\sim} V^*$ is the isomorphism induced by b, and $f^t \in \mathrm{End}_k(V^*)$ denotes the transpose of f defined by mapping $\varphi \in V^*$ to $\varphi \circ f$.

Equivalently,

Definition 2.77. With the notation as above, σ_b is defined by the condition

$$b(\sigma_b(f)(x), y) = b(x, f(y))$$

for $x, y \in V$

In particular σ_b is k-linear.

We can also define the adjoint involution σ_h of a hermitian form $h\colon V \times V \longrightarrow k$ defined on a vector space V over quadratic field extension L/k.

Definition 2.78. σ_h is defined by the condition

$$h(\sigma_h(f)(x), y) = h(x, f(y))$$

for any $x, y \in V$ and any $f \in \mathrm{End}_k(V)$.

3. Linear Algebraic Groups

3.1 Definition and Examples

Let k be an algebraically closed field.

Definition 3.79. An *algebraic group* over k is an algebraic variety G, endowed with the structure of a group, with distinguished element $e \in G$, and such that the maps defining the group structure

$$\mu\colon G \times G \longrightarrow G \quad \text{with} \quad \mu(x, y) = xy$$
$$i\colon G \longrightarrow G \quad \text{with} \quad i(x) = x^{-1}$$

are morphisms of varieties.

If the underlying variety is affine, then G is called a *linear algebraic group*. A *morphism* of algebraic groups is a morphism of varieties which is also a homomorphism of groups.

Let G be a linear algebraic group, and set $A = k[G]$. The group structure of G is defined by algebra homomorphisms

$$\mu^*\colon A \longrightarrow A \otimes_k A$$
$$i^*\colon A \longrightarrow A$$

and the identity element e is a homomorphism $A \longrightarrow k$.

Example 3.80. Let $G = \mathbf{A}^1$ with $e = 0$, group law given by $\mu(x, y) = x + y$, and $i(x) = -x$. We denote this algebraic group by $\mathbf{G}_a$: it is the additive group.

Example 3.81. $G = \mathbf{A}^1 \setminus \{0\}$ with $e = 1$ and group law given by $\mu(x, y) = xy$ and $i(x) = x^{-1}$. We denote this algebraic group by $\mathbf{G_m}$ or $\mathbf{GL}_1$: it is the multiplicative group.

If n is a non-zero integer, then $\varphi\colon \mathbf{G_m} \longrightarrow \mathbf{G_m}$ given by $\varphi(x) = x^n$ defines a homomorphism of algebraic groups. If $\operatorname{char} k = p > 0$, and $n = p^m$ for some m, then φ is an isomorphism of abstract groups but *not* of algebraic groups, since $\varphi^*\colon k[\mathbf{G_m}] \longrightarrow k[\mathbf{G_m}]$ is not surjective.

Example 3.82. View the space $\mathbf{M}_n$ of all $n \times n$-matrices as $k^{n^2}_{sep}$. The *general linear group* $\mathbf{GL}_n$ consists of all $n \times n$-matrices with non-zero determinant, together with matrix multiplication as group operation. We have

$$k[\mathbf{GL}_n] = k[T_{ij}, D^{-1}]_{1 \leqslant i,j \leqslant n}$$

where $D = \det T_{ij}$. Here μ^* is given by

$$\mu^* T_{ij} = \sum_{h=1}^{n} (T_{ih} \otimes T_{hj})$$

and $i^* T_{ij}$ is the (i,j)-entry of the matrix of $(T_{ij})^{-1}$. The identity e sends T_{ij} to δ_{ij}. Since $\mathbf{M}_n$ is an irreducible variety, so is $\mathbf{GL}_n$. It has dimension n^2.

Example 3.83. Any closed subgroup of $\mathbf{GL}_n$ in the Zariski topology is a linear algebraic group. Here are some of them:

a. Any finite subgroup of $\mathbf{GL}_n$;

b. $\mathbf{D}_n = \{X = (x_{ij}) \in \mathbf{GL}_n\colon x_{ij} = 0 \text{ if } i \neq j\}$, the group of non-singular diagonal matrices;

c. $\mathbf{T}_n = \{X = (x_{ij}) \in \mathbf{GL}_n\colon x_{ij} = 0 \text{ if } i > j\}$, the group of non-singular upper triangular matrices;

d. $\mathbf{U}_n = \{X = (x_{ij}) \in \mathbf{GL}_n\colon x_{ij} = 0 \text{ if } i > j \text{ and } x_{ii} = 1\}$, the group of non-singular unipotent upper triangular matrices;

e. $\mathbf{SL}_n = \{X \in \mathbf{GL}_n\colon \det X = 1\}$, the special linear group;

f. $\mathbf{O}_n = \{X \in \mathbf{GL}_n : X \cdot X^t = 1\}$, the orthogonal group;

g. $\mathbf{SO}_n = \mathbf{O}_n \cap \mathbf{SL}_n$, the special orthogonal group;

h. $\mathbf{Sp}_{2n} = \{X \in \mathbf{GL}_{2n} : X^t \cdot J \cdot X = J\}$, where $J = \begin{pmatrix} 0 & \mathrm{Id}_n \\ -\mathrm{Id}_n & 0 \end{pmatrix}$, the symplectic group.

Example 3.84. Let Q be a quadratic form of rank n over k, where $\operatorname{char} k \neq 2$. If B is a symmetric matrix representing Q, then

$$\mathbf{SO}(Q) = \{X \in \mathbf{SL}_n : X^t \cdot B \cdot X = B\}$$

is called the *special orthogonal group of* Q. When Q is the unitary form $(\langle 1, \ldots, 1 \rangle)$, we denote $\mathbf{SO}(Q)$ by $\mathbf{SO}_n$.

Remark 3.85. $\mathbf{SL}_n$, $\mathbf{Sp}_{2n}$, and $\mathbf{SO}(Q)$ are examples of the so-called classical groups. $\mathbf{SL}_n$ is of type A_{n-1}. $\mathbf{Sp}_{2n}$ is of type C_n for $n \geqslant 2$. $\mathbf{SO}_{2n}$ is of type D_n for $n \geqslant 3$, and $\mathbf{SO}_{2n+1}$ is of type B_n for $n \geqslant 2$. Knowing the type of group gives a lot of data about it. For example, the dimension of a maximal torus in a group G of type T_n is n, where $T = A, B, C, \ldots$.

Example 3.86. Let k be a field, V an n-dimensional k-vector space, and let h be a positive definite hermitian form on V. Hence for some $M \in \mathbf{M}_n$ we can write

$$h(v, w) = {}^t\bar{v} \cdot M \cdot w \qquad \text{for all } v, w \in k^n$$

We define the group of k-linear automorphisms of V preserving the positive definite hermitian form h, called the unitary group of h, as

$$\mathrm{U}(h) = \{A \in \mathbf{M}_n : {}^t\bar{A} \cdot M \cdot A = M\}$$

In particular, if h is the standard inner product, then

$$\mathrm{U}(h) = \{A \in \mathbf{M}_n : {}^t\bar{A} = A^{-1}\}$$

We define the special unitary group of h as the subgroup of $\mathrm{U}(h)$ of automorphisms of determinant 1, *i.e*

$$\mathrm{SU}(h) = \{A \in \mathrm{U}(h) \colon \det A = 1\}$$

Now we exhibit an example of a non-linear algebraic group

Example 3.87. Elliptic curves. These are closed subsets of the projective plane $\mathbb{P}^2$. If char $k \neq 2, 3$ such a group G can be defined as the set of all $\mathbf{x} = (x_0, x_1, x_2) \in \mathbb{P}^2$ such that

$$x_0 x_2^2 = x_1^3 + a x_1 x_0^2 + b x_0^3$$

where $a, b \in k$ are such that the polynomial $T^3 + aT + b$ has no multiple roots. The neutral element e is $(0, 0, 1)$, the point at infinity. The group operation of G is abelian, and is often written additively. It is such that if three distinct points are colinear, then their sum is e. If $\mathbf{x} = (x_0, x_1, x_2) \in G$, then $-\mathbf{x} = (x_0, x_1, -x_2)$.

3.2 Diagonalizable Groups and Tori

Definition 3.88. Let G be a linear algebraic group. A homomorphism of algebraic groups $\chi \colon G \longrightarrow \mathbf{G_m}$ is called a *rational character* of G.

The set of rational characters of G is denoted by $X^*(G)$, it has the natural structure of abelian group, and the operation is often written additively. One can think of the group of rational characters as sitting inside the group algebra $k_{sep}[G]$, *i.e.* $X^*(G) \subset k_{sep}[G]$.

We define $X_*(G)$ to be the set of homomorphisms of algebraic groups $\lambda \colon \mathbf{G_m} \longrightarrow G$. Such a λ is called a *multiplicative 1-parameter subgroup of* G ($\mathbf{1-psg}$ of G). If G is commutative, then $X_*(G)$ has also a natural structure of abelian group. For $t \in \mathbf{G_m}$, and $\lambda, \mu \in X_*(G)$ we define

$$(\lambda + \mu)(t) = \lambda(t)\mu(t), \qquad (-\lambda)(t) = \lambda(t)^{-1}$$

Definition 3.89. A linear algebraic group G which is isomorphic over k_{sep} to a closed subgroup of some group of diagonal matrices $\mathbf{D}_n$ is called *diagonalizable*. G is an *algebraic torus* (or simply a torus) if it is isomorphic over k_{sep} to some $\mathbf{D}_n$.

Remark 3.90. In case G is diagonalizable, G is necessarily commutative and consists of semisimple elements.

Example 3.91. Let $T = \mathbf{G_m}$. If $\chi \in X^*(T)$, then $\chi(t) = t^m$ for some $m \in \mathbb{Z}$. Hence

$$X^*(\mathbf{G_m}) \cong \mathbb{Z}$$

Lemma 3.92. *If G is a connected algebraic group, then $X^*(G)$ is torsion-free. In particular if T is an n-dimensional torus, then $X^*(T) \cong \mathbb{Z}^n$.*

Proof. If $\chi \in X^*(G)$, then $\chi(G) \subset \mathbf{G_m}$ is a connected subgroup. But the only connected subgroups of $\mathbf{G_m}$ are $\{0\}$ and $\mathbf{G_m}$ itself. Thus for $n > 0$, $n\chi \neq 0$ unless $\chi = 0$. Thus, $X^*(G)$ is torsion-free.

Now, if T is an n-dimensional torus,

$$T \cong \underbrace{\mathbf{G_m} \times \cdots \times \mathbf{G_m}}_{n \text{ times}}$$

so we have, $X^*(T) \cong X^*(\mathbf{G_m})^n \cong \mathbb{Z}^n$. □

Theorem 3.93. *Let G be a linear algebraic group. The following are equivalent:*

a. *G is diagonalizable.*

b. *$X^*(G)$ is an abelian group of finite type, its elements generate $k_{sep}[G]$.*

c. *Any rational representation of G is a direct sum of 1-dimensional ones.*

Proof. See [TS, Theorem 2.5.2] p.52. □

Corollary 3.94. *Let H be a closed subgroup of the diagonalizable group G. Then H is diagonalizable, and it is the intersection of the kernels of finitely many rational characters of G.*

Proof. See [TS, Corollary 2.5.3] p.53. □

Proposition 3.95. *If T is a torus, then $X^*(T) \times X_*(T) \longrightarrow \mathbb{Z}$ is a dual pairing over $\mathbb{Z}$.*

Proof. If $\chi \in X^*(T)$ and $\lambda \in X_*(T)$ define $\langle \chi, \lambda \rangle \in \mathbb{Z}$ by

$$\chi(\lambda(x)) = x^{\langle \chi, \lambda \rangle}$$

then $\langle\ ,\ \rangle$ defines a perfect pairing between $X^*(T)$ and $X_*(T)$, *i.e.* any homomorphism $X^*(T) \longrightarrow \mathbb{Z}$ is of the form $\chi \longmapsto \langle \chi, \lambda \rangle$, where $\chi \in X^*(T)$. Similarly for $X_*(T)$. □

3.3 Maximal Tori

Assume G is a connected solvable linear algebraic group. Define $G_u = G \cap \mathbf{U}_n$, where $\mathbf{U}_n$ is the group of unipotent upper triangular matrices. Thus, G_u is a closed normal subgroup which is nilpotent since $\mathbf{U}_n$ is. Moreover, there is an injective homomorphism of algebraic groups $G/G_u \longrightarrow \mathbf{T}_n/\mathbf{U}_n$. Now, since $\mathbf{T}_n/\mathbf{U}_n$ is a torus, all elements of G/G_u must be semisimple. Being connected, this group is a torus.

Definition 3.96. A *maximal torus* of G is a subtorus which has the same dimension as the torus $S = G/G_u$.

A maximal torus is also a maximal torus in the set-theoretical sense, hence we may, equivalently, define a maximal torus of G to be a closed subtorus of G of maximal dimension.

Proposition 3.97. *If G is a semisimple algebraic group over k, then any two maximal tori are conjugate over k_{sep}.*

Proof. See [TS, Theorem 7.2.6] p.159. □

For a k-torus T, we denote by $X_k^*(T)$ the subset of $X^*(T)$ consisting of k-morphisms. We have the following:

Definition 3.98. A maximal torus T is called *k-split* if $X_k^*(T)$ generates $k[T]$, equivalently, if $T \cong_k \mathbf{G_m} \times \cdots \times \mathbf{G_m}$; then $T(k) \cong k^\times \times \cdots \times k^\times$.

We say that an algebraic group G is *split* if it contains a split maximal torus.

4. Skolem-Noether Type Theorems

In this chapter k will always be an arbitrary field, B will be a k-algebra, and A a central simple algebra over k (denoted CSA over k from now on) of degree n. For any k-algebra C and any field extension $\mathbb{F}/k$ we write $C_{\mathbb{F}}$ for the $\mathbb{F}$-algebra obtained from C by extending scalars to $\mathbb{F}$, so $C_{\mathbb{F}} := C \otimes_k \mathbb{F}$. Let k_{sep} denote a (fixed) separable closure of k, and let Γ denote the absolute Galois group of k, *i.e.* $\Gamma = \text{Gal}\,(k_{\text{sep}}/k)$. Recall that if A is a k-algebra and $B \subseteq A$, then the centralizer of B in A, denoted $Z_A(B)$, is the set of elements in A which commute with every element of B, *i.e.* $Z_A(B) = \{x \in A\colon xy = yx \text{ for all } y \in B\}$.

4.1 Main Result

In this section our main goal is to extend the classical Skolem-Noether theorem stated in 1.40 as follows:

Theorem 4.99. *Let n be a fixed (positive) integer. Suppose that B is a k-algebra such that B_{sep} has a unique faithful representation of degree n over k_{sep}. Then all the embeddings of B into a central simple k-algebra A are conjugate, i.e. if $\psi, \varphi\colon B \longrightarrow A$ are two embeddings, then there exists $a \in A^\times$ such that $\psi(b) = a\varphi(b)a^{-1}$ for all $b \in B$.*

Proof. Fix an embedding $B \overset{i}{\hookrightarrow} A$. Now, let $\varphi\colon B \longrightarrow A$ be any other embedding. We need to find an $a \in A^\times$ such that $\varphi(x) = axa^{-1}$ for all $x \in B$.
By hypothesis, we can find such an $a \in A_{k_{sep}}^\times$ since $A_{k_{sep}}^\times \cong M_n(k_{sep})^\times$, and A_{sep} has a unique representation of degree n.

Lemma 4.100. *Let $a, b \in A^\times$. If $axa^{-1} = bxb^{-1}$ for all $x \in B$, then $b = az^{-1}$ for some $z \in Z_A(B)^\times$.*

Proof. Well, this is a straightforward computation.

$$\begin{aligned} axa^{-1} = bxb^{-1} \text{ for all } x \in B &\implies x = (a^{-1}b)x(a^{-1}b)^{-1} \quad \text{for all } x \in B \\ &\implies a^{-1}b \in Z_A(B)^\times, i.e., b = az^{-1} \\ &\quad \text{for some } z \in Z_A(B)^\times \end{aligned}$$

□

What we need to show is that we can choose z in such a way that $\sigma(b) = b$ for all $\sigma \in \Gamma$ where $\Gamma = \mathrm{Gal}(k_{sep}/k)$. For $x \in B$ we have $\varphi(x) = axa^{-1}$ for some $a \in A^\times_{k_{sep}}$. So $\varphi(\sigma(x)) = a\sigma(x)a^{-1}$ where $\sigma \in \Gamma$. But φ is k-linear, so $\varphi(\sigma(x)) = \sigma(\varphi(x))$. Hence

$$a\sigma(x)a^{-1} = \varphi(\sigma(x)) = \sigma(\varphi(x)) = \sigma(axa^{-1}) = \sigma(a)\sigma(x)\sigma(a)^{-1},$$

so $a\sigma(x)a^{-1} = \sigma(a)\sigma(x)\sigma(a)^{-1}$, *i.e.*

$$\sigma(x) = (a^{-1}\sigma(a))\sigma(x)(a^{-1}\sigma(a))^{-1},$$

so $a^{-1}\sigma(a) \in Z_A(B)^\times$.

Now, to each $\sigma \in \Gamma$ associate a continuous map $c\colon \Gamma \to Z_A(B)^\times$ given by $c_\sigma = a^{-1}\sigma(a)$. Note that $c_\sigma \in Z^1(k, Z_A(B)^\times)$ since

$$c_\sigma \sigma c_\tau = (a^{-1}\sigma(a))\sigma(a^{-1}\tau(a)) = a^{-1}\sigma(a)\sigma(a^{-1})\sigma\tau(a) = a^{-1}\sigma\tau(a) = c_{\sigma\tau}$$

What we want to do is show that $c_\sigma = 1 \ \forall \sigma \in \Gamma$ since then all embeddings of B into A would be conjugate. This amounts to showing that $\mathbf{H^1}(k, Z_A(B)^\times) = \{1\}$. To accomplish this we filter the algebra through its radical.

Let $Z = Z_A(B)^\times$ and $R = \mathrm{Rad}(Z_{sep})$. Define

$$U := 1 + R \quad \text{and} \quad U^{(n)} := 1 + R^n \ \text{ for } n \geqslant 1$$

Let's observe the following:

a. $U^{(n)} \subseteq U^{(n-1)}$ for every $n \geqslant 2$.

If $x \in U^{(n)}$ then $x = 1 + r^n$ for some $r \in R$, but $R^n \subseteq R^{n-1}$ so $x = 1 + r^n \in 1 + R^n \subseteq 1 + R^{n-1} = U^{(n-1)}$. Hence $U^{(n)} \subseteq U^{(n-1)}$ for every $n \geqslant 2$. Note that we now have a decreasing sequence:

$$U = U^{(1)} \supseteq U^{(2)} \supseteq \cdots \supseteq U^{(n-1)} \supseteq U^{(n)} \supseteq \cdots$$

b. R is nilpotent, so there exists an $N \in \mathbb{N}$ such that $U^{(n)} = \{1\} \ \forall n \geqslant N$. Hence the sequence in **(a)** above is finite, it becomes

$$U \supseteq U^{(2)} \supseteq \cdots \supseteq U^{(n-1)} \supseteq U^{(n)} \supseteq \cdots \supseteq U^{(N-1)} \supseteq U^{(N)} = \{1\} \qquad (4.7)$$

c. Every $u \in U$ is invertible, *i.e.* if $u \equiv 1 \mod R$, there is a v such that $uv = 1$.

Proof. Let $u \in U$, we have

$$\begin{aligned} -1 &= (1-u)\sum_{j=1}^{\infty}(1-u)^j - \sum_{j=1}^{\infty}(1-u)^j \\ &= \sum_{j=1}^{\infty}(1-u)^j - u\sum_{j=1}^{\infty}(1-u)^j - \sum_{j=1}^{\infty}(1-u)^j \end{aligned}$$

hence $-1 = -u\sum_{j=1}^{\infty}(1-u)^j$, *i.e.* $1 = u\sum_{j=1}^{\infty}(1-u)^j$. So take

$$v = \sum_{j=1}^{\infty}(1-u)^j$$

□

Lemma 4.101. $U^{(n)}/U^{(n+1)} \cong R^n/R^{n+1}$ *for every* $n \geqslant 1$

Proof. Define a map $\Phi\colon U^{(n)} \longrightarrow R^n/R^{n+1}$ by $\Phi(u) = \overline{u-1}$. To see that Φ is a homomorphism just note that

$$\begin{aligned}\Phi(uv) &= \overline{uv-1} = \overline{(u-1)+(v-1)-(u-1)(v-1)} \\ &= \overline{(u-1)} + \overline{(v-1)} - \overline{(u-1)(v-1)} \\ &= \Phi(u) + \Phi(v) - \Phi(u)\Phi(v)\end{aligned}$$

and $\Phi(u)\Phi(v) \in R^{2n} \subset R^{n+1}$. Hence $\Phi(uv) = \Phi(u) + \Phi(v)$. Now we ask, what is the kernel of Φ? Well, $\ker\Phi = \left\{u \in U^{(n)}\colon \Phi(u) \in R^{n+1}\right\}$ so

$$\begin{aligned}\ker\Phi &= \left\{u \in U^{(n)}\colon \overline{u-1} \in R^{n+1}\right\} \\ &= \left\{u \in U^{(n)}\colon u \in 1 + R^{n+1}\right\} \\ &= \left\{u \in U^{(n)}\colon u \in U^{(n+1)}\right\} \\ &= U^{(n+1)}\end{aligned}$$

so $\ker\Phi$ is exactly $U^{(n+1)}$.

To see that Φ is a surjection, for any $0 \neq \bar{r} \in R^n/R^{n+1}$ pick $\overline{1+r} \in U^{(n)}$ and we have $\Phi(1+r) = \overline{(1+r)-1} = \bar{r}$. Hence Φ induces an isomorphism $U^{(n)}/U^{(n+1)} \cong R^n/R^{n+1}$. □

Lemma 4.102. *With the same notation as above,* $\mathbf{H}^1(k, U) = 0$.

Proof. From lemma 4.101 we get the exact sequence

$$U^{(m+1)} \rightarrowtail U^{(m)} \twoheadrightarrow R^m/R^{m+1}$$

Now R^m/R^{m+1} is just a vector space over k_{sep}, so it is isomorphic to k_{sep}^M where $M = \dim_{k_{sep}}(R^m/R^{m+1})$. In terms of linear algebraic groups this is just the additive group $\mathbf{G}_a$, which by the additive version of Hilbert's Theorem 90, is cohomologically trivial, *i.e.* $\mathbf{H}^1(k, \mathbf{G}_a) = 0$. So looking at the $\mathbf{H}^1$ part of the associated sequence

in cohomology we see:

$$\mathbf{H}^1(k, U^{(m+1)}) \longrightarrow \mathbf{H}^1(k, U^{(m)}) \longrightarrow \mathbf{H}^1(k, R^m/R^{m+1}) = \mathbf{H}^1(k, \mathbf{G}_a) = 0$$

Also note that $\mathbf{H}^1(k, U^{(N)}) = 0$, since $U^{(N)} = \{1\}$, so from 4.7 we have

$$0 = \mathbf{H}^1(k, U^{(N)}) \twoheadrightarrow \mathbf{H}^1(k, U^{(N-1)}) \twoheadrightarrow \cdots \twoheadrightarrow \mathbf{H}^1(k, U^{(2)}) \twoheadrightarrow \mathbf{H}^1(k, U)$$

which gives $\mathbf{H}^1(k, U^{(n)}) = 0 \ \forall n \geqslant 1$. Hence, in particular, when $n = 1$ we have $\mathbf{H}^1(k, U) = 0$. □

Now we put together all the information we have gathered so far. What we have is

$$U \rightarrowtail \mathbf{G}_{\mathbf{m},Z} \twoheadrightarrow \mathbf{G}_{\mathbf{m},Z}/R$$

and we look at the $\mathbf{H}^1$ part of the associated sequence in cohomology

$$\mathbf{H}^1(k, U) \to \mathbf{H}^1(k, \mathbf{G}_{\mathbf{m},Z}) \twoheadrightarrow \mathbf{H}^1(k, \mathbf{G}_{\mathbf{m},Z}/R)$$

by lemma 4.102, $\mathbf{H}^1(k, U) = 0$ and we also have $\mathbf{H}^1(k, \mathbf{G}_{\mathbf{m},Z}/R) = 0$. Hence we have succeeded in "pinching" $\mathbf{H}^1(k, \mathbf{G}_{\mathbf{m},Z})$ in between two cohomologically trivial objects, so $\mathbf{H}^1(k, \mathbf{G}_{\mathbf{m},Z})$ is trivial. We have shown that $c_\sigma = 1$ for all $\sigma \in \Gamma$. So all embeddings of B into A must be conjugate, and this proves theorem 4.99. □

4.2 Examples

To effectively illustrate the result obtained above let us consider a couple of examples.

Example 4.103. If B is simple, then we are in the situation of the Skolem-Noether theorem.

Example 4.104. We can take B to be an étale algebra of degree n.

Before we see some more examples let's define the term Frobenius algebra. A very detailed discussion on Frobenius Algebras may be found in [CR, Chapter IX].

Definition 4.105. A finite dimensional algebra A over a field k is called a *Frobenius algebra* if the left A-modules ${}_AA$ and $(A_A)^*$ are isomorphic.

Definition 4.106. Let S be a subset of a finite dimensional algebra A over k. The *left annihilator* $\ell(S)$ of S is defined as

$$\ell(S) = \{a \in A \colon aS = 0\}$$

whereas the *right annihilator* $r(S)$ of S is defined as

$$r(S) = \{a \in A \colon Sa = 0\}$$

The following theorem establishes the equivalence of several characterizations of Frobenius algebras.

Theorem 4.107. *Let A be a finite-dimensional k-algebra. Then the following statements are equivalent:*

1. *A is a Frobenius algebra.*
2. *There exists a non-degenerate bilinear form $f \colon A \times A \longrightarrow k$ which is associative, in the sense that $f(ab, c) = f(a, bc)$ for all $a, b, c \in A$.*
3. *There exists a linear function $\lambda \in A^*$ whose kernel contains no left or right ideals different from zero.*
4. *For all left ideals L and right ideals R in A we have*

$$\ell(r(L)) = L, \quad \text{and} \quad (r(L) \colon k) + (L \colon k) = (A \colon k);$$

$$r(\ell(R)) = R, \quad \text{and} \quad (\ell(R) \colon k) + (R \colon k) = (A \colon k)$$

Proof. See [CR, p.415]. □

Lemma 4.108. *Let A/k be a Frobenius algebra with associative bilinear form f. Let $0 \neq I \subsetneq A$ be an ideal. Then $I^{\perp} = \{x \in A \colon f(b, x) = 0 \, \forall \, b \in I\}$ is also an ideal.*

Proof. Let $a \in A$, $b \in I^{\perp}$. We need to show that $ab \in I^{\perp}$. Let $c \in I$, then note that $ca \in I$, since I is an ideal. Thus, we have

$$f(c, ab) = f(ca, b) = 0$$

Hence $ab \in I^{\perp}$. □

Proposition 4.109. *If B has a unique faithful representation of degree n over k_{sep}, then B is a Frobenius algebra.*

Proof. Suppose B has a unique faithful representation of degree n over k_{sep}. Then B^* also has a unique faithful representation of degree n over k_{sep}. Take a basis for B^*, $B^* = \lambda B$. If there is a non-trivial ideal $I \in \ker \lambda$, then $(B/I)^* \subset B^*$. A contradiction. So $\lambda \equiv 0$. Thus, B is a Frobenius algebra. □

The converse is not true in general, but we have

Proposition 4.110. *If B is a commutative Frobenius algebra, then B has a unique faithful representation of degree* $\deg B$ *over k_{sep}.*

Proof. Suppose first that B is a commutative Frobenius algebra, equipped with form f, which is local. Let $\mathcal{M}$ be its maximal ideal. Let V be a faithful B-module with $\dim V = \dim B$, then $V \cong B$. For $v \in V$, define

$$I_v = \mathrm{Ann}_B(v) = \{x \in B : xv = 0\}$$

We need to check that there exists a non-zero vector $v \in V$ for which $I_v = 0$. So, let $0 \neq v \in V$ be such that $\dim I_v$ is minimal. We want to show that this dimension, in fact, has to be zero. Suppose $I_v \neq 0$, then $0 \neq I_v^{\perp} \subsetneq B$ is an ideal and hence $I_v^{\perp} \subset \mathcal{M}$, which in turn implies that $\mathcal{M}^{\perp} \subset \left(I_v^{\perp}\right)^{\perp} = I_v$. Now, let n denote the

nilpotency index of $\mathcal{M}$. Notice that $\mathcal{M}^{n-1} \cdot \mathcal{M} = 0$, so $\mathcal{M}^{n-1} \subset \mathcal{M}^{\perp}$. This follows since if $x \in \mathcal{M}^{n-1}$, and $y \in \mathcal{M}$, then

$$f(x, y) = f(1, xy) = f(1, 0) = 0$$

Thus, $0 \neq \mathcal{M}^{n-1} \subset \mathcal{M}^{\perp} \subset I_v$ for all v. So, $0 \neq \mathcal{M}^{n-1} \subset \bigcap_v I_v = \ker(B \longrightarrow \mathrm{End}_k V)$ which is a contradiction since V is a faithful B-module. Therefore, if B is a (commutative) Frobenius algebra which is local, then B has a unique faithful representation. Moreover, if B is any commutative Frobenius algebra, we can write

$$B = B_1 \times \cdots \times B_r$$

where each B_i is a local algebra. Let $e_i \in B_i$ $(i = 1, \ldots, r)$ be the corresponding idempotents. If V is a faithful B-module with $\dim V = \dim B$, we can decompose $V = \bigoplus_{i=1}^{r} V_i$ where $V_i = e_i V$ for each $i = 1, \ldots, r$. Hence each V_i contains a faithful B_i-module, and so $\dim V_i \geqslant \dim B_i$ for each $i = 1, \ldots, r$. But,

$$\sum_{i=1}^{r} \dim V_i = \dim V = \dim B = \sum_{i=1}^{r} \dim B_i$$

so $\dim V_i = \dim B_i$ for each i. Hence V is the regular representation. This finishes the proof of the proposition. □

This proposition provides us with a vast array of examples since:

a. Every semi-simple algebra over a field is a Frobenius algebra.

Just take $f(a, b) = \mathrm{Tr}(ab)$, a non-degenerate associative form.

b. For any finite group G, its group algebra $A = k[G]$ over any field k is a Frobenius algebra.

Define a linear function λ on A by

$$\lambda\left(\sum_{g \in G} \alpha_g g\right) = \alpha_1$$

where 1 is the identity element of G. Suppose that for some $a \in A$, Aa is in $\ker \lambda$. In particular we have

$$\lambda(g^{-1}a) = 0 \; \forall g \in G$$

But since $\lambda(g^{-1}a)$ is the coefficient of g in a, we must have $a = 0$. Similarly, we can show that $aA \in \ker \lambda$ implies $a = 0$. Thus, A is a Frobenius algebra.

Example 4.111. The group algebra of any abelian group.

Example 4.112. Let B be a local non-commutative Frobenius algebra. Let $\mathcal{M}$ be its maximal ideal. If $B/\mathcal{M}$ is a field, then B has a unique faithful representation of degree $\deg B$.

Proof. Let V be a faithful B-module of degree $\deg B$. For $v \in V$ define $I_v = \mathrm{Ann}_B(v)$. Since V is a faithful B-module, $\bigcap_v I_v = 0$. Hence

$$\sum_v I_v^{\perp} = B$$

i.e we can write $1 = \sum_v a_v$ for some $a_v \in I_v^{\perp}$. Thus, there is a $v \in V$ such that $a_v \notin \mathcal{M}$. Hence a_v is an invertible element, since $B/\mathcal{M}$ is a field. We also have $a_v \in I_v^{\perp}$, which together with a_v being invertible implies that $1 \in I_v^{\perp}$, thus $B = I_v^{\perp}$ and $I_v = 0$. Therefore, V is the regular representation. □

Remark 4.113. Unlike in the proposition, there is no hope to generalize from the local non-commutative case. Commutativity is required in the proposition.

If we look at the representations of S_3: $6 = 2(1)^2 + 1(2)^2$, so we have two 1-dimensional representations, $\mathbb{C}_+$ and the signature $\mathbb{C}_-$, and we have a 2-dimensional representation, which we will call V. We have

$$\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times \mathrm{M}_2\mathbb{C} \longrightarrow \mathbb{C}_+ \oplus \mathbb{C}_- \oplus V \oplus V$$

But note that $\chi = 2\mathbb{C}_+ \oplus 2\mathbb{C}_- \oplus V$ is a faithful representation different from the regular representation.

Remark 4.114. If B is an algebra with no central idempotents other than 0 and 1, just take, for example, $B = k$.

Just take, for example, $B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in k \right\}$. Then note that B is not local. In fact, $B/\operatorname{Rad} B \cong k \times k$ and B has two maximal ideals,

$$C = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in k \right\}$$

and

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in k \right\}$$

hence not local.

4.3 Embedding Simple Algebras

There is an underlying problem in theorem 4.99.

Question: What are the conditions for the existence of an embedding of B in A?

If B is a commutative Frobenius algebra, then the answer is given in [KM, Proposition 3.4]. Here we will consider the case where B is a simple k-algebra.

Let k be a field, let B be a simple k-algebra of degree d, and let A be a CSA over k of degree n. Denote by E the centralizer of B, $Z(B)$. It is evident that a necessary condition for the existence of an embedding $B \hookrightarrow A$ is that there exist an embedding $B \supset Z(B) = E \hookrightarrow A$. If $E \hookrightarrow A$, then $E \subset Z_A(E) = A' \subset A$ and $Z_A(E)$ is a CSA over E.

Case 1: $E = k$, *i.e.* B is a CSA over k.

Recall that if B is a CSA over k and $B \hookrightarrow A$, then $B \otimes Z_A(B) \cong A$, and so $[Z_A(B)] = [A] - [B] \in \mathrm{Br}(k)$ (See Chapter 2, Cor 8.4 in [Ke]).

Proposition 4.115. *There is an embedding $B \hookrightarrow A$ if and only if $[A]-[B] \in \mathrm{Br}(k)$ is representable by an algebra of degree $r = n/d$.*

Proof. If there is an embedding $B \hookrightarrow A$, then $B \otimes Z_A(B) = A$, and so $[Z_A(B)] = [A] - [B] \in \mathrm{Br}(k)$ of degree n/d. On the other hand, if $[A] - [B] \in \mathrm{Br}(k)$ is represented by an algebra $[T]$ of degree n/d, then $[A] - [B] = [T] \in \mathrm{Br}(k)$ and so $A \cong B \otimes T$, *i.e.* B is a subalgebra of A. □

Case 2: General Case, *i.e.* B a simple k-algebra (with center possibly larger than k).

We have $E \longrightarrow \mathrm{End}_k(L) \cong \mathbf{M}_n(k)$, for any maximal k-algebra L satisfying $k \subset E \subset L \subset A$. Hence $Z_{\mathbf{M}_n}(E)$ is a matrix algebra over E, in fact, a central simple algebra over E. Set $C = \mathbf{G}_{\mathbf{m},Z_{\mathbf{M}_n}(E)}/\mathbf{G}_{\mathbf{m}}$ and $\bar{C} = \mathbf{G}_{\mathbf{m},Z_{\mathbf{M}_n}(E)}/\mathbf{G}_{\mathbf{m},E}$. Consider

$$0 \longrightarrow C \longrightarrow \mathrm{Aut}(\mathbf{M}_n, E) \xrightarrow{\text{res}} \mathrm{Aut}(E) \longrightarrow 0 \tag{4.8}$$

We also have the exact sequences,

$$0 \longrightarrow \mathbf{G}_{\mathbf{m}} \longrightarrow \mathbf{G}_{\mathbf{m},Z_{\mathbf{M}_n}(E)} \longrightarrow C \longrightarrow 0 \tag{4.9}$$

$$\mathbf{G}_{\mathbf{m},E}/\mathbf{G}_{\mathbf{m}} \overset{g}{\rightarrowtail} C \overset{f}{\twoheadrightarrow} \bar{C} \tag{4.10}$$

From 4.9 we get an induced map in cohomology

$$\mathbf{H}^1(k, C) \xrightarrow{\delta^1} \mathbf{H}^2(k, \mathbf{G}_{\mathbf{m}})$$

The set $\mathbf{H^1}(k, C)$ classifies embeddings $E \overset{\varphi}{\hookrightarrow} A$, and the image of δ^1 consists of algebras containing E. If we extend scalars to E we have another exact sequence of pointed sets,

$$0 \longrightarrow \mathbf{G_m} \xrightarrow{i} \mathbf{G}_{\mathbf{m},E} \longrightarrow \mathbf{G}_{\mathbf{m},E}/\mathbf{G_m} \longrightarrow 0 \tag{4.11}$$

From (4.10) we get an associated sequence in cohomology;

If $\beta \in Z^1(k, C)$, let $\gamma \in Z^1\left(k, \bar{C}\right)$ be the image of β. Then there is a natural bijection between the fiber of

$$\mathbf{H^1}(k, C) \xrightarrow{f^1} \mathbf{H^1}(k, \bar{C})$$

over $[\gamma]$ and the orbit set of the group

$$\left(\bar{C}_\gamma\right)^\Gamma \text{ acting on } \mathbf{H^1}(k, \mathbf{G}_{\mathbf{m},E}/\mathbf{G_m})$$

From sequences (4.10) and (4.11) we get a commutative diagram

$$\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
\mathbf{H^1}(k, \mathbf{G}_{\mathbf{m},E}/\mathbf{G_m}) & = & \mathrm{Br}\,(E/k) \\
{\scriptstyle g^1}\downarrow & & \downarrow \\
\mathbf{H^1}(k, C) & \xrightarrow{\delta^1} & \mathbf{H^2}(k, \mathbf{G_m}) \\
{\scriptstyle f^1}\downarrow & & \downarrow{\scriptstyle i^2} \\
\mathbf{H^1}(k, \bar{C}) & \xrightarrow{\delta^1_E} & \mathbf{H^2}(k, \mathbf{G}_{\mathbf{m},E}) \\
\downarrow & & \downarrow \\
\mathbf{H^2}(k, \mathbf{G}_{\mathbf{m},E}/\mathbf{G_m}) & = & \mathbf{H^2}(k, \mathbf{G}_{\mathbf{m},E}/\mathbf{G_m})
\end{array}$$

The maps $f^\sharp$ and $i^\sharp$ are defined by

$$f^\sharp\left([E \overset{\varphi}{\hookrightarrow} A]\right) = [Z_A(\varphi E)]$$

$$i^\sharp([A]) = [A \otimes E]$$

Theorem 4.116. *There exists an embedding $E \hookrightarrow A$ if and only if the class of $A \otimes E$ in* $\mathrm{Br}(E)$ *is represented by the class of a central simple algebra N of degree* $\deg A/[E : k]$.

Proof. The only if part is clear. To prove the other direction, choose $[T] \in \mathbf{H^2}(k, \mathbf{G_m})$, then $[T \otimes E] \in \mathbf{H^2}(k, \mathbf{G}_{\mathbf{m},E})$. Now $T \otimes E$ contains E, so it comes from $\mathbf{H^1}(k, \bar{C})$. On the other hand, it goes to zero in $\mathbf{H^2}(k, \mathbf{G}_{\mathbf{m},E}/\mathbf{G_m})$ so it is in the image under $f^\sharp$ of some $[c] \in \mathbf{H^1}(k, C)$. Hence $\delta^1([c]) = [T] + [d]$ for some $[d] \in \mathrm{Br}(E/k)$. But the action

$$\mathbf{H^1}(k, C) \xrightarrow{f^\sharp} \mathbf{H^1}(k, \bar{C})$$

is transitive so, if we take a representative $\alpha \in Z^1(k, C)$ of $[c]$, and $\beta \in Z^1(k, \mathbf{G}_{\mathbf{m},E}/\mathbf{G_m})$ a representative of $[d]$, then $\alpha\beta^{-1} \in Z^1(k, C)$ since (4.10) is a central extension. Now, since δ^1 is a homomorphism,

$$\delta^1([\alpha\beta^{-1}]) = \delta^1([\alpha]) - \delta^1([\beta]) = [T] + [d] - [d] = [T]$$

Thus we obtain our original class. □

5. Algebras with Involutions

In this chapter B will always be a k-algebra with involution σ, and A a CSA over k of degree n with involution τ central over k or over a quadratic extension of k if τ is of type II (unitary). Given two embeddings $f,\ g\colon (B,\sigma) \longrightarrow (A,\tau)$ we wish to know whether there exists a $\varphi \in \mathrm{Aut}(A,\tau)$ such that the diagram,

$$\begin{array}{ccc} (B,\sigma) & \xrightarrow{f} & (A,\tau) \\ \| & & \downarrow \varphi \\ (B,\sigma) & \xrightarrow[g]{} & (A,\tau) \end{array}$$

commutes, *i.e.* we want to classify embeddings which are in the same conjugacy class.

Let $\mathcal{X}$ be the set of all embeddings of (B,σ) into (A,τ). So, if $f \in \mathcal{X}$, then f is a homomorphism of B into A with $f \circ \sigma = \tau \circ f$. The automorphism group of (A,τ) is the group scheme over k given by

$$\mathrm{Aut}(A,\tau)(R) = \{\alpha \in \mathrm{Aut}(A \otimes R)\colon \alpha \circ \tau = \tau \circ \alpha\}$$

for any commutative k-algebra R. For any algebra with involution (A,τ) we define

$$U_{(A,\tau)} = \left\{u \in \mathbf{G}_{\mathbf{m},A}\colon u\tau(u) = 1\right\}$$

Using the Skolem-Noether theorem, one sees that there is an exact sequence

$$0 \longrightarrow U_{(A,\tau)} \cap \mathbf{G}_{\mathbf{m}} \longrightarrow U_{(A,\tau)} \longrightarrow \mathrm{Aut}\,(A,\tau) \longrightarrow 0 \qquad (5.12)$$

To shorten the notation let us set $G = \mathrm{Aut}(A,\tau)$. Hence G acts on $\mathcal{X}$ naturally, by composition. Let $\Gamma = \mathrm{Gal}(k_{sep}/k)$. Let's fix $f \in \mathcal{X}^{\Gamma}$, *i.e.* f is a k-embedding of (B,σ) into (A,τ). We will adopt the notation Gf for the G-orbit of f and G_f for

the stabilizer of f in G. Hence

$$\begin{aligned} G_f = \mathrm{Stab}_G f &= \{\varphi \in G \colon \varphi \circ f = f\} \\ &= \{u \in Z_A(f(B)) \colon u\tau(u) = 1\} \,/\, \left(\mathbf{G_m} \cap U_{(A,\tau)}\right) \\ &= \{u \in Z_A(B) \colon u\tau(u) = 1\} \,/\, \left(\mathbf{G_m} \cap U_{(A,\tau)}\right) \end{aligned}$$

the latter by identifying B with its image under f. We also have,

$$Gf = \mathrm{Orbit}_G(f) = \{\varphi \circ f \mid \varphi \in G\}$$

It is well-known that if two elements are in the same G-orbit, then their respective stabilizers are conjugate. We have the exact sequence of pointed sets

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_f & \hookrightarrow & G & \xrightarrow{\circ f} & Gf & \longrightarrow & 1 \\ & & \psi & \longmapsto & \psi & & & & \\ & & & & \varphi & \longmapsto & \varphi \circ f & & \end{array}$$

And we look at its associated sequence in cohomology

$$\cdots \longrightarrow G^\Gamma = G(k) \longrightarrow (Gf)^\Gamma \longrightarrow \mathbf{H^1}(k, G_f) \longrightarrow \mathbf{H^1}(k, G) \tag{5.13}$$

Recall from 1.17 that the orbit set of $G(k)$ in $(Gf)^\Gamma$, *i.e.* the k-conjugacy classes of elements of $(Gf)^\Gamma$ are in a natural bijection with $\ker\left(\mathbf{H^1}(k, G_f) \xrightarrow{i^\sharp} \mathbf{H^1}(k, G)\right)$. So what we will do is study $\ker i^\sharp$ in order to better understand the k-conjugacy classes of elements of $(Gf)^\Gamma$.

Let us assume for now that τ is an involution of the first kind on A. Set $U = U_{(A,\tau)} = \left\{u \in \mathbf{G}_{\mathbf{m},A} \colon u\tau(u) = 1\right\}$ and $G = \mathrm{Aut}\,(A, \tau)$, which we shall identify with $U/\{\pm 1\}$. Then $G_f = U_{(Z,\tau)}/\{\pm 1\}$, where $Z = Z_A(B)$ and we have the sequences of pointed sets,

$$1 \longrightarrow \{\pm 1\} \longrightarrow U \longrightarrow G \longrightarrow 1$$

and

$$1 \longrightarrow \{\pm 1\} \longrightarrow U_{(Z,\tau)} \longrightarrow G_f \longrightarrow 1$$

From these we get

$$\begin{array}{ccccc}
\mathbf{H}^1(k, U_{(Z,\tau)}) & \longrightarrow & \mathbf{H}^1(k, U) & \longrightarrow & \mathbf{H}^1(k, \mathbf{G}_{\mathbf{m},A}) \\
\downarrow & & \downarrow & & \downarrow \\
\mathbf{H}^1(k, G_f) & \xrightarrow{i^\sharp} & \mathbf{H}^1(k, G) & \longrightarrow & \mathbf{H}^1(k, \operatorname{Aut} A) \\
\downarrow & & \downarrow{\scriptstyle \delta^1} & & \downarrow \\
\mathbf{H}^2(k, \{\pm 1\}) & = & \mathbf{H}^2(k, \{\pm 1\}) & \longrightarrow & \mathbf{H}^2(k, \mathbf{G}_{\mathbf{m}})
\end{array}$$

In particular, note that we must have $\ker i^\sharp \subseteq \mathbf{H}^1(k, U_{(Z,\tau)})$. So, if $\mathbf{H}^1(k, U_{(Z,\tau)}) = \{1\}$, then $\ker i^\sharp = \{1\}$ and hence all the embeddings of (B, σ) into (A, τ) must be conjugate.

Lemma 5.117. *The connecting homomorphism*

$$\delta^1 \colon \mathbf{H}^1(k, G) \longrightarrow \mathbf{H}^2(k, \{\pm 1\})$$

sends the class of (A', τ') *to the class of* $[A'] - [A]$ *in* $\operatorname{Br}(k)$.

Proof. This follows from the well-known fact that

$$\mathbf{H}^1(k, \operatorname{Aut}(A)) \xrightarrow{\delta^1} \mathbf{H}^2(k, \mathbf{G}_{\mathbf{m}})$$

is given by $[A'] \longmapsto [A'] - [A]$. □

Lemma 5.118. *Let* k *be a field of characteristic different from 2. Let* Z *be a* k*-algebra with involution* τ*. If* $a \in Z_{sep}^{\times}$ *is fixed by the involution, then* $a = \tau(b)b$ *for some* $b \in Z_{sep}$.

Proof. Let's break the proof up into two cases.

Case 1: Z is semisimple.

We can decompose Z_{sep} as

$$(\mathbf{M}_{n_1} \times \mathbf{M}_{n_2}) \times \cdots \times (\mathbf{M}_{n_{q-1}} \times \mathbf{M}_{n_q}) \times \mathbf{M}_{m_1} \times \cdots \mathbf{M}_{m_r}$$

Note that the involution could come from a hyperbolic, symplectic, or an orthogonal form. In case the involution comes from a hyperbolic form, there is no problem since there is only one such. If the involution comes from a symplectic form, it is well known that there is only one symplectic form over any given degree. The only problem would be an orthogonal involution, but over a (fixed) separable closure, again, there is only one. Now on the "pairs" above what we have is essentially the exchange involution, so an element is fixed if and only if it has the form (x, x^t) for some x. But we can write this as

$$(x, x^t) = (1, x^t)(x, 1) = \tau\left((x, 1)\right)(x, 1)$$

and clearly $(x, 1) \in Z_{sep}$.

Case 2: Z any k-algebra.

We know that $Z_{sep}/\mathrm{Rad}\, Z_{sep}$ is semisimple. By the first case, there is a $b_1 \in Z_{sep}$ such that $a \equiv \tau(b_1)b_1 \pmod{\mathrm{Rad}\, Z_{sep}}$. We need to show that we can "lift" this partial approximation from the radical all the way up to Z_{sep}. We proceed à la Hensel. Suppose that $a \equiv \tau(b_n)b_n \pmod{(\mathrm{Rad}\, Z_{sep})^n}$ and we'll show it for $n+1$. Suppose $b_{n+1} = b_n + c$ for some $c \in (\mathrm{Rad}\, Z_{sep})^n$ yet to be determined. Now, we need $a \equiv \tau(b_{n+1})b_{n+1} \pmod{(\mathrm{Rad}\, Z_{sep})^{n+1}}$. Thus, let us see what we need:

$$\begin{aligned}
\tau(b_{n+1})b_{n+1} &= \tau(b_n + c)(b_n + c) \\
&= (\tau b_n + \tau c)(b_n + c) \\
&= \tau(b_n)b_n + \tau(b_n)c + \tau(c)b_n + \tau(c)c \\
&= a - r + \tau(b_n)c + \tau(c)b_n + \tau(c)c
\end{aligned}$$

The latter equality is for some $r \in (\text{Rad}\, Z_{sep})^n$ since $a \equiv \tau(b_n)b_n \pmod{(\text{Rad}\, Z_{sep})^n}$. Note that $\tau(c)c \in (\text{Rad}\, Z_{sep})^{2n}$, so for $n \geqslant 1$, $\tau(c)c \equiv 0 \pmod{(\text{Rad}\, Z_{sep})^{n+1}}$. Hence, what we need is to be able to solve the congruency

$$\tau(b_n)c + \tau(c)b_n \equiv r \pmod{(\text{Rad}\, Z_{sep})^{n+1}}$$

for c. Note that

1. $\tau(b_n)c + \tau(c)b_n$ is fixed by τ.

2. Since b_n is invertible,

$$\ell_{b_n} : (\text{Rad}\, Z_{sep})^n \longrightarrow (\text{Rad}\, Z_{sep})^n$$

(left multiplication by b_n) is an isomorphism.

Thus, it is enough to see that

$$r \equiv s + \tau(s) \pmod{(\text{Rad}\, Z_{sep})^{n+1}}$$

for some $s \in (\text{Rad}\, Z_{sep})^n$. But, since $\text{char}\, k \neq 2$, we can just take $s = \frac{r}{2}$ to solve the latter. □

Proposition 5.119. *Let (B, σ) and (A, τ) be as above. Suppose that B has a unique faithful representation of degree* $\deg A$ *over k_{sep}. Then any two embeddings of (B, σ) into (A, τ) are conjugate over k_{sep}, i.e the action of G on $\mathcal{X}$ is transitive.*

Proof. Let $f, g : (B, \sigma) \longrightarrow (A, \tau)$ be two embeddings. If we "forget" about the involutions we know that by theorem 4.99 there exists an $a \in A^\times$ such that $f(x) = ag(x)a^{-1}$ for all $x \in B$. Is this compatible with the involutions? There's only one

way to find out. For $x \in B$ we have

$$\begin{aligned} ag(\sigma x)a^{-1} &= f(\sigma x) \\ &= \tau(fx) \\ &= \tau(ag(x)a^{-1}) \\ &= \tau(a^{-1})\tau(gx)\tau(a) \\ &= \tau(a^{-1})g(\sigma x)\tau(a) \end{aligned}$$

so $ag(\sigma x)a^{-1} = \tau(a^{-1})g(\sigma x)\tau(a)$, hence $g(\sigma x) = a^{-1}\tau(a^{-1})g(\sigma x)\tau(a)a$ so $z = \tau(a)a \in Z_A(B) = Z$. Now write $\tau(a)a = \tau(b)b$ with $b \in Z_{sep}^{\times}$ (in general b is not rational over k). Then $u = ab^{-1} \in G$ and $ug(x)u^{-1} = f(x)$ for all x. □

Corollary 5.120. *Let $f\colon (B,\sigma) \longrightarrow (A,\tau)$ be a fixed embedding, and let*

$$G_f = \{\varphi \in \mathrm{Aut}\,(A,\tau)\colon \varphi \circ f = f\}$$

then 5.119 tells us that the cohomology set $\mathbf{H^1}(k, G_f)$ classifies the embeddings $\varphi\colon (B,\sigma) \longrightarrow (A',\tau')$ where (A',τ') are algebras with involution isomorphic to (A,τ) over k_{sep}. The embeddings $\varphi\colon (B,\sigma) \longrightarrow (A,\tau)$ are classified by

$$\ker\left(i^*\colon \mathbf{H^1}(k,G_f) \longrightarrow \mathbf{H^1}(k,\mathrm{Aut}\,(A,\tau))\right)$$

where $i\colon G_f \longrightarrow \mathrm{Aut}\,(A,\tau)$ is the inclusion map.

Lemma 5.121. *Let (A,τ) be a CSA over k with involution, and $e \in A$ an idempotent such that $e + \tau(e) = 1$. Set $B = ke + k\tau(e)$. Then $U_{(B,\tau)} = \mathbf{G_m}$ and $Z_A(B) = Ze + Z\tau(e)$.*

Proof. (i) Recall that $U_B = \left\{u \in \mathbf{G}_{\mathbf{m},B}\colon u\tau(u) = 1\right\}$. Let $u \in U_{(B,\tau)}$ and write $u = ve + w\tau(e)$, where $v, w \in k_{sep}$. The condition $u\tau(u) = 1$ is equivalent to $vw = 1$, so $U_{(B,\tau)} = \mathbf{G_m}$.

(ii) Certainly, e and $\tau(e)$ belong to $Z_A(B)$, hence $Z_A(B) \supseteq Ze + Z\tau(e)$. So, in particular $Z_A(B) \cong (W \times W^{op}, \tau)$ for some W. Now, take any element $z_1e+z_2\tau(e) \in Ze+Z\tau(e)$, we must show that it commutes with every element of $B = ke+k\tau(e)$, but this is clear since e and $\tau(e)$ commute with each other. □

Example 5.122. Let (A, τ) be a CSA over k of even degree $2n$ with involution τ. Then there is at most one $U_{(A,\tau)}(k)$-conjugacy class of idempotents $e \in A$ such that $e + \tau(e) = 1$.

Proof. Let $B = ke + k\tau(e)$. Note that B_{sep} has only one representation of degree $2n$ that is self-dual; this is enough to guarantee that G acts transitively on $\mathcal{X}$. So we can use corollary 5.120. Now $Z = Z_A(B)$ decomposes as $Y \times Y'$ with the two factors interchanged by the involution, so $U_{(A,\tau)} \cong \mathbf{G}_{\mathbf{m},Z}$. We have

$$\begin{array}{ccc}
\mathbf{H^1}(k, U_{(Z,\tau)}) & \longrightarrow & \mathbf{H^1}(k, \mathbf{G}_{\mathbf{m},A}) \\
\downarrow & & \downarrow \\
\mathbf{H^1}(k, G_f) & \xrightarrow{i^1} & \mathbf{H^1}(k, \mathrm{Aut}\,(A,\tau)) \\
\downarrow & & \downarrow{\scriptstyle \delta^1} \\
\mathbf{H^2}(k, \{\pm 1\}) & = & \mathbf{H^2}(k, \{\pm 1\})
\end{array}$$

If an element lies in $\ker(i^1)$, then it is also in $\ker \delta^1$. Since we have equality in the bottom row, this element must come from $\mathbf{H^1}(k, U_{(Z,\tau)})$ which is trivial. □

6. Conjugacy Classes of Maximal k-Tori

6.1 General Results

Let G be a semi-simple (linear) algebraic group defined over a field k. Let $\widetilde{G}$ be its universal cover, and let $T \subset G$ be a fixed maximal k-torus.

It is well-known that over a separable closure of k all maximal tori are conjugate. We are interested in determining which maximal k-tori of G are k-conjugate to a fixed maximal torus T. To this effect, we will develop a general set-up to enable us to study k-conjugacy classes. We will mainly use the tools provided by Galois Cohomology. In the case where $G = U_{(A,\sigma)}$, where (A, σ) is a central simple algebra with involution, we can make this general set-up more explicit. This case is essentially the general case when G is a classical simple group, by virtue of a theorem of André Weil in [We, p.597].

Let $N = N_G(T) = \{x \in G\colon xTx^{-1} \subset T\}$ denote the normalizer of T in G, let $Z = Z_G(T)$ denote the centralizer of T in G, and let $W = W(T) = N/T$ denote the Weyl group of G relative to T, a finite group.

Since all maximal tori are conjugate over a separable closure, the set of all maximal tori is parametrized by the homogeneous space G/N. So we have

$$G/N \longleftrightarrow \text{set of maximal tori in } G$$

It is readily seen that this bijection commutes with the action of Γ, so if we want the set of maximal k-tori, then we let Γ act on G and look at the fixed points. We have

$$(G/N)^{\Gamma} \longleftrightarrow \text{set of maximal } k\text{-tori in } G$$

If in addition we want the k-conjugacy classes of maximal k-tori then we look at the action of $G^{\Gamma} = G(k)$ on G/N. We have

$$(G/N)^{\Gamma}/G^{\Gamma} \longleftrightarrow \text{set of } k\text{-conjugacy classes of maximal } k\text{-tori in } G$$

It is this latter relation that we want to exploit. We will use Galois Cohomology to understand and give explicit descriptions of these k-conjugacy classes in particular examples. As a starting point, consider the exact sequences

$$1 \longrightarrow T \longrightarrow N \xrightarrow{\pi} W \longrightarrow 1 \tag{6.14}$$

$$1 \longrightarrow T \xrightarrow{i_T} G \longrightarrow G/T \longrightarrow 1 \tag{6.15}$$

$$1 \longrightarrow N \xrightarrow{i_N} G \longrightarrow G/N \longrightarrow 1 \tag{6.16}$$

From sequence 6.16 above we get the associated sequence in cohomology:

$$G^{\Gamma} \longrightarrow (G/N)^{\Gamma} \longrightarrow \mathbf{H^1}(k,N) \xrightarrow{(i_N)^\sharp} \mathbf{H^1}(k,G) \tag{6.17}$$

By the general theory of Galois Cohomology there is a one-to-one correspondence between the orbit set of G^{Γ} in $(G/N)^{\Gamma}$, namely $(G/N)^{\Gamma}/G^{\Gamma}$ and $\ker(i_N)^\sharp$. First note that this kernel sits inside of $\mathbf{H^1}(k,N)$. By the remarks just made, $\ker(i_N)^\sharp$ is in one-to-one correspondence with the k conjugacy classes of maximal k-tori. We thus want to study $\ker(i_N)^\sharp$ to better understand and be able to compute k-conjugacy classes of maximal tori.

One of the invariants we are interested in arises when considering the sequence in cohomology associated to sequence (6.14). We have

$$W^{\Gamma} \longrightarrow \mathbf{H^1}(k,T) \longrightarrow \mathbf{H^1}(k,N) \xrightarrow{\pi^\sharp} \mathbf{H^1}(k,W) \tag{6.18}$$

We will want to study those classes in $\mathbf{H^1}(k,N)$ that are taken by $\pi^\sharp$ to zero in $\mathbf{H^1}(k,W)$. Note that $\ker(i_T)^\sharp$ is contained in these. By abuse of notation, we denote by $\pi^\sharp$: $\ker(i_T)^\sharp \longrightarrow \mathbf{H^1}(k,W)$ the restriction of $\pi^\sharp$ to $\ker(i_T)^\sharp$.

If we consider the covering map ρ: $\widetilde{G} \longrightarrow G$ and its kernel, $\ker\rho$, we have the exact sequence

$$1 \longrightarrow \ker\rho \longrightarrow \widetilde{G} \xrightarrow{\rho} G \longrightarrow 1$$

Recall that $\ker\rho$ is a finite abelian group. Let $\widetilde{T}$ be the inverse image of T under the covering map ρ, *i.e.* $\widetilde{T} = \rho^{-1}(T)$. Note that $\ker\rho \subset \widetilde{T}$, so we have:

$$1 \longrightarrow \ker\rho \longrightarrow \widetilde{T} \xrightarrow{\rho} T \longrightarrow 1$$

and we obtain the commutative diagram

$$\begin{array}{ccc} \ker\rho & = & \ker\rho \\ \downarrow & & \downarrow \\ \widetilde{T} & \longrightarrow & \widetilde{G} \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle q} \\ T & \longrightarrow & G \end{array}$$

and looking at its associated sequence in cohomology we have

$$\begin{array}{ccc} \mathbf{H^1}(k,\widetilde{T}) & \longrightarrow & \mathbf{H^1}(k,\widetilde{G}) \\ \downarrow & & \downarrow \\ \mathbf{H^1}(k,T) & \xrightarrow{i^\sharp} & \mathbf{H^1}(k,G) \\ {\scriptstyle \delta^1}\downarrow & & \downarrow{\scriptstyle \delta^1} \\ \mathbf{H^2}(k,\ker\rho) & = & \mathbf{H^2}(k,\ker\rho) \end{array}$$

We can restrict ourselves to studying $\ker(i^\sharp)$ since $W = N/T$ is finite.

Proposition 6.123. *With notation as above* $\ker(i^\sharp) \subset \ker\delta^1$.

Proof.

$$\begin{aligned} [S] \in \ker(i^\sharp) &\Rightarrow i^\sharp[S] = e \\ &\Rightarrow (\delta^1 \circ i^\sharp)[S] = e \\ &\Rightarrow \delta^1[S] = e \quad \text{since the diagram commutes} \\ &\Rightarrow [S] \in \ker\delta^1 \end{aligned}$$

□

Proposition 6.124. *If in addition we have* $\mathbf{H}^1(k, \widetilde{G}) = 0$, *then equality holds, i.e.* $\ker i^\sharp = \ker \delta^1$.

Proof. Let $[S] \in \ker \delta^1$, so $\delta^1[S] = e$ and hence $\left(\delta^1 \circ i^\sharp\right)[S] = e$, but there is only one element in each fiber since $\mathbf{H}^1(k, \widetilde{G}) = 0$. Hence $i^\sharp[S] = e$, *i.e.* $[S] \in \ker i^\sharp$. □

We are interested in this relation since δ^1 has the extra structure of being a group homomorphism. It is known that the condition $\mathbf{H}^1(k, \widetilde{G}) = 0$ holds for all classical groups and some exceptional groups when $\operatorname{cd}(k) \leqslant 2$. For this see [BP1] and [BP2]. We will record what we have shown as a theorem for future reference.

Theorem 6.125. $\ker(i_T)^\sharp / W(k)$ *is in one-to-one correspondence with the set of* k*-conjugacy classes of maximal tori* S *with* $\pi^\sharp(S) = e$, *where* $\pi^\sharp$ *is the restriction of* $\pi^\sharp$ *to* $\ker(i_T)^\sharp$.

The preceding formalism can be applied very effectively (to describe k-conjugacy classes) in the case where G is the unitary group of an algebra with involution. Later we will see that in this case we can interpret the map $\pi^\sharp$ in terms of étale algebras.

This generalizes the work of Kariyama in [Ka] for classical groups split over k. We will see that in this situation we can always associate to any torus T a certain class of étale algebras with involution.

Example 6.126. Let k be a field with $\operatorname{char} k \neq 2$, and let $G = \mathbf{SO}(q)$ be the special orthogonal group of a non-degenerate quadratic form q on a vector space V of dimension $2n$ over k. For $G = \mathbf{SO}(q)$ we have $\widetilde{G} = \mathbf{Spin}(q)$ a connected two-sheeted covering and thus $\ker \rho = \mathbb{Z}/2\mathbb{Z}$. These yield the exact sequence

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbf{Spin}(q) \xrightarrow{\rho} \mathbf{SO}(q) \longrightarrow 1$$

Let $T \subset G$ be a (fixed) maximal k-torus. Then, we can associate to T the étale

algebra $E = E_T = Z_{\mathrm{End}_k(V)}(T)$ consisting of k-endomorphisms of V that commute with T equipped with the involution ν, induced by the adjoint involution of q. If $F = E^\nu$, the subalgebra of elements of E fixed by the involution ν, then $\dim F = \frac{1}{2}\dim E$ as we will see in 6.139, and we can write $E = F[X]/(X^2 - D)$ for some $D \in F^\times$. Viewing E this way we realize ν as $X \longmapsto -X$. Also we may recover T as the kernel of the norm map from the multiplicative group of E to the multiplicative group of F.

$$T \cong U_{E/F} = \ker(N_{E/F}\colon \mathbf{G_{m},}_E \longrightarrow \mathbf{G_{m},}_F)$$

Notice that now we have two exact sequences involving T,

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \widetilde{T} \longrightarrow T \longrightarrow 1 \tag{6.19}$$

and

$$1 \longrightarrow T \longrightarrow \mathbf{G_{m},}_E \xrightarrow{N_{E/F}} \mathbf{G_{m},}_F \longrightarrow 1 \tag{6.20}$$

The exact sequence (6.20) induces an isomorphism

$$\mathbf{H^1}(k, T) \cong F^\times/N_{E/F}(E^\times)$$

With this identification it has been shown in [BKM] that

$$\delta^1\colon \mathbf{H^1}(k, T) \longrightarrow \mathrm{Br}(k) \tag{6.21}$$

is given by $\delta^1(a) = \mathrm{Cor}_{F/k}(a, D)$. With all this information we get a commutative diagram

$$\begin{array}{ccc} \mathbf{H^1}(k,T) & \xrightarrow{\delta^1} & \mathbf{H^2}(k, \mathbb{Z}/2\mathbb{Z}) \\ \wr\downarrow & & \downarrow\wr \\ F^\times/N_{E/F}(E^\times) & \longrightarrow & \mathrm{Br}(k) \end{array}$$

Note that here $W^\Gamma = \mathrm{Aut}_k(E,\nu)$, the k-automorphisms of E that commute with ν, and so we get a surjective map

$$\boxed{k\text{-conjugacy classes of maximal } k\text{-tori } S \text{ with } (E_S,\nu) \cong (E_{U_{E/F}},\nu)}$$

$$\downarrow$$

$$\left\{a \in F^\times/N_{E/F}(E^\times)\colon \mathrm{Cor}\,(a,D) = 0\right\}/W^\Gamma$$

For this map to be injective we need $\mathbf{H^1}(k,\mathbf{Spin}(q)) = 0$. We will give necessary conditions for this in theorem 6.140. This takes care of $\mathbf{SO}(q)$ for the moment. We will come back to it in the next section.

Lemma 6.127. *Let L/k be a quadratic field extension, let $E \supseteq L$ be an étale algebra over k equipped with an involution σ (of any kind), such that $\sigma|L$ is non-trivial ($\Longleftrightarrow L \cap E^\sigma = k$), and let $F = E^\sigma$. Consider $V = E$ as a finite dimensional L-vector space. For $b \in F^\times$ define $h_b\colon E \times E \longrightarrow L$ by $h_b(x,y) = \mathrm{Tr}_{E/L}(bx\sigma(y))$. Then h_b is a hermitian form on E (with respect to σ) invariant under $U_{E/F} = \left\{u \in \mathbf{G}_{\mathbf{m},E}\colon u\sigma(u) = 1\right\}$.*

Proof. Let $x, y \in E$, $\alpha, \beta \in L$, and $u \in U_{E/F}$ be arbitrary. To show that h_b is a hermitian form on E we need to show that $\sigma h_b(x,y) = h_b(y,x)$ and that $h_b(\alpha x, \beta y) = \alpha h_b(x,y)\sigma(\beta)$. This is a straightforward computation that we do as follows:

$$\begin{aligned}
\sigma h_b(x,y) &= \sigma \mathrm{Tr}_{E/L}(bx\sigma(y)) \\
&= \mathrm{Tr}_{E/L}(\sigma(bx\sigma(y))) \\
&= \mathrm{Tr}_{E/L}(y\sigma(x)\sigma(b)) \\
&= \mathrm{Tr}_{E/L}(by\sigma(x)) \\
&= h_b(y,x)
\end{aligned}$$

$$\begin{aligned} h_b(\alpha x, \beta y) &= \sigma h_b(\beta y, \sigma x) \\ &= \sigma \mathrm{Tr}_{\mathrm{E/L}}\left(b\beta y \sigma(\alpha x)\right) \\ &= \sigma\left(\beta \mathrm{Tr}_{\mathrm{E/L}}\left(by\sigma(\alpha x)\right)\right) \\ &= \sigma \mathrm{Tr}_{\mathrm{E/L}}\left(by\sigma(\alpha x)\right)\sigma(\beta) \\ &= \mathrm{Tr}_{\mathrm{E/L}}\left(b\alpha x\sigma(y)\right)\sigma(\beta) \\ &= \alpha \mathrm{Tr}_{\mathrm{E/L}}\left(bx\sigma(y)\right)\sigma(\beta) \\ &= \alpha h_b(x,y)\sigma(\beta) \end{aligned}$$

So h_b is a hermitian form. To see that it is invariant under $U_{E/F}$ note

$$\begin{aligned} h_b(ux, uy) &= \mathrm{Tr}_{\mathrm{E/L}}\left(bux\sigma(uy)\right) \\ &= \mathrm{Tr}_{\mathrm{E/L}}\left(bx\sigma(y)u\sigma(u)\right) \\ &= h_b(x,y) \end{aligned}$$

□

Remark 6.128. To talk about $\mathrm{Tr}_{E/L}$ we need E free over L. If L is a field, there is no problem. If $L = k \times k$, then $E = Ee + Ee^*$ and the involution * interchanges the idempotents, so these idempotents have the same rank. This essentially says that E is free over L.

Recall that a non-singular hermitian form h on a finite dimensional vector space V defined over a quadratic field extension L of a field k with non-trivial automorphism i, yields the adjoint involution σ_h on $\mathrm{End}_L V$ defined by the relation

$$h(x, f(y)) = h(\sigma_h(f)(x), y)$$

for $f \in \mathrm{End}_L V$ and $x, y \in V$. In particular, $\sigma_h(\alpha) = i(\alpha)$ for $\alpha \in L$, so σ_h is an involution of the second kind.

Example 6.129. Let $G = \mathrm{SU}(h)$ $(= \mathrm{SU}(V,h))$, the special unitary group of a hermitian form h defined on an L-vector space, where L is a quadratic field extension over k.

Question: What are the maximal k-tori for $G = \mathrm{SU}(h)$?

Well, we would like to use the same machinery as in the previous example, but $\mathrm{SU}(h)$ is simply-connected unlike $\mathrm{SO}(q)$, *i.e.* $\widetilde{\mathrm{SU}}(h) = \mathrm{SU}(h)$ so we take a different approach. If we have an étale algebra E/k as in the lemma above, then

Claim 6.130. *$U_{E/F}$ is a maximal k-torus.*

Proof. We claim that over the algebraic closure of k we must have $\left(\mathbf{G}_{\mathbf{m},E}\right)^n \cong U_{E/F}$. To see this, consider the map

$$\begin{aligned} \varphi\colon \left(\mathbf{G}_{\mathbf{m},E}\right)^n &\longrightarrow U_{E/F} \\ \mathbf{t} = (t_1, t_2, \ldots, t_n) &\longmapsto (t_1, t_1^{-1}, t_2, t_2^{-1}, \ldots, t_n, t_n^{-1}) \end{aligned}$$

The map φ is clearly surjective and

$$\begin{aligned} \ker\varphi &= \left\{\mathbf{t} \in \left(\mathbf{G}_{\mathbf{m},E}\right)^n : \varphi(\mathbf{t}) = (1, \ldots, 1)\right\} \\ &= \left\{\mathbf{t} \in \left(\mathbf{G}_{\mathbf{m},E}\right)^n : t_i = 1 \ \forall i = 1, \ldots, n\right\} \\ &= \{\mathbf{1}\} \end{aligned}$$

To see that it is a homomorphism note that

$$\begin{aligned} \varphi(\mathbf{ts}) = \varphi(t_1 s_1, \ldots, t_n s_n) &= (t_1 s_1, s_1^{-1} t_1^{-1}, \ldots, t_n s_n, s_n^{-1} t_n^{-1}) \\ &= (t_1 s_1, t_1^{-1} s_1^{-1}, \ldots, t_n s_n, t_n^{-1} s_n^{-1}) \\ &= (t_1, t_1^{-1}, \ldots, t_n, t_n^{-1})(s_1, s_1^{-1}, \ldots, s_n, s_n^{-1}) \\ &= \varphi(\mathbf{t})\varphi(\mathbf{s}) \end{aligned}$$

Hence $U_{E/F}$ is a k-torus, and moreover it is maximal for dimensional reasons. □

For the étale algebra E we may take $E = E_T = \mathrm{End}_T\,(V \otimes_k k_{sep})^\Gamma$ and this algebra comes equipped with the adjoint involution σ_h.

It is easy to calculate $\mathbf{H}^1(k, U_{E/F})$ from the exact sequence

$$1 \longrightarrow U_{E/F} \longrightarrow \mathbf{G}_{\mathbf{m},E} \longrightarrow \mathbf{G}_{\mathbf{m},F} \longrightarrow 1$$

Its exact sequence in cohomology yields $\mathbf{H}^1(k, U_{E/F}) \cong F^\times / N_{E/F}(E^\times)$. If h is of rank n, then $W(k) \cong \mathrm{Aut}_k(F, \sigma) \cong \mathrm{Aut}_L(E, \sigma)$, where $\mathrm{Aut}_k(F, \sigma)$ is the group of k-automorphisms of F that commute with the involution σ, *i.e.*

$$\mathrm{Aut}_k(F, \sigma) = \{\alpha \in \mathrm{Aut}_k(F) \colon \alpha \circ \sigma = \sigma \circ \alpha\}$$

and

$$\mathrm{Aut}_L(E, \sigma) = \{\alpha \in \mathrm{Aut}_L(E) \colon \alpha \circ \sigma = \sigma \circ \alpha\}$$

Lemma 6.131. *Keeping the same notation as above. If h is of rank n, then*

$$W^\Gamma \cong \mathrm{Aut}_k(F, \sigma) \cong \mathrm{Aut}_L(E, \sigma)$$

Proof. The first isomorphism is clear. The isomorphism between the automorphism groups is given by the restriction map,

$$\mathrm{Res} \colon \mathrm{Aut}_L(E, \sigma) \longrightarrow \mathrm{Aut}_k(F, \sigma)$$

taking f to $f|F$. This is clearly a homomorphism. To see that it is injective, note that if $\mathrm{Res}(f) = \mathrm{id}_F$, then $\mathrm{Res}(f)$ fixes pointwise both L and F. Hence it fixes $F \otimes_k L$, but $E = F \otimes_k L$ since $\dim_k (F \otimes_k L) = 2n = \dim_k E$ and $F \otimes_k L \subseteq E$. Thus $f = \mathrm{id}_E$. It is also clear that every k-automorphism of F extends uniquely to a unique L-automorphism of E. □

Lemma 6.132. *If $T \subset \mathrm{SU}(h)$ is a maximal k-torus, then $T \cong U_{E/F}$ for some étale algebra E over k, and $h \cong h_{E,b}$ for some $b \in F^\times$.*

Proof. We can associate to T the étale algebra $E_T = \mathrm{End}_T(V \otimes_k k_{sep})^\Gamma$ of endomorphisms fixed by the action of Γ, together with the adjoint involution σ_h, where k_{sep} denotes a fixed separable closure of k and $\Gamma = \mathrm{Gal}\,(k_{sep}/k)$. It is worth noting here that $(E_T, \sigma_h) \subset (\mathrm{End}\, V, \sigma_h)$. We want to show that

$$T \longmapsto E_T$$

induces a set bijection. Thus, giving an explicit correspondence between maximal tori and a class of étale algebras with involution, namely, n-dimensional subalgebras (E, σ_h) of $(\mathrm{End}\, V, \sigma_h)$. If T is a maximal k-torus, then it is preserved by the action of Γ, so we have our $T \subset E_T \otimes_k k_{sep}$. Moreover, $T \subset \mathrm{SU}(h)$, so $T \subset U_{E/F}$. Since T is maximal equality must hold. In the other direction, if (E, σ_h) is a subalgebra of $(\mathrm{End}\, V, \sigma_h)$ just take $T =: U_{E/F}$, which we've already shown to be a maximal k-torus.

Furthermore, we'll say that E_T is "h-admissible" if $h \cong h_{E_T,b}$ for some $b \in F^\times$. Recall that

a $\det h = \det(h(e_i, e_j)) \cdot N_{L/k}(L^\times)$ where $(h(e_i, e_j))_{1 \leqslant i,j \leqslant n}$ is the Gram matrix of h with respect to an arbitrary basis $(e_1, \ldots, e_n)$.

b The determinant of a hermitian form $h\colon L \times L \longrightarrow k$ is an invariant modulo the norms of L over k.

Claim 6.133. $\det h_{E,b} = N_{F/k}(b) \cdot \mathrm{disc}(F/k)$

Proof. Notice that we can decompose E as a tensor product $E = F \otimes_k L$. From F we pick up, basically, $\mathrm{Tr}_{E/L}\,(xy)$ and from L we get H_L where $H_L(x, y) = x\bar{y}$. □

Claim 6.133 finishes up the proof of lemma 6.132. □

We have seen that $\mathbf{H}^1(k, U_{E/F}) \cong F^\times/N_{E/F}(E^\times)$ and so the natural map

$$\mathbf{H}^1(k, U_{E/F}) \longrightarrow \mathbf{H}^1(k, \mathrm{SU}(h))$$

is given by $a \longmapsto h_a(x,y) = h(ax,y)$ where $a \in F^\times/N_{E/F}(E^\times)$.

Remark 6.134. $h_a(x,y)$ and $h(ax,y)$ have the same determinant.

Proposition 6.135. *The set of k-conjugacy classes of maximal tori S with $(E_S, \sigma_h) \cong (E_{U_{E/F}}, \sigma_h)$ is in one-to-one correspondence with*

$$\left\{a \in \mathbf{H}^1(k, U_{E/F})/W^\Gamma \colon h_a \cong h\right\}$$

Proof. Just consider the commutative diagram:

$$\begin{array}{ccc}
W^\Gamma & & \\
\downarrow & & \\
\mathbf{H}^1(k, U_{E/F}) & = & \mathbf{H}^1(k, U_{E/F}) \\
\wr\downarrow & & \downarrow \\
F^\times/N_{E/F}(E^\times) & \longrightarrow & \mathbf{H}^1(k, \mathrm{SU}(h)) \\
\downarrow & & \\
\mathbf{H}^1(k, N) & &
\end{array}$$

□

Example 6.136. Let $G = \mathrm{SU}(h)$ $(= \mathrm{SU}(V,h))$ where h is a hermitian form over a skew-field D/k. Let $T_0 \subset G$ be a fixed maximal k-torus. Associate to T_0 the algebra $E_{T_0} = Z_{\mathrm{End}_D V}(T_0)$. Let F be the algebra consisting of elements fixed by the adjoint involution σ_h. Let $N = N_G(T_0)$ denote the normalizer of T_0 in G and $W = W(T_0) = N/T_0$ denote the Weyl group of T_0.

Claim 6.137. *E_{T_0} is an étale algebra.*

Proof. Let $X^*(T_0)$ denote the character group of T_0. Over a separable closure, we may break up V as

$$V_{sep} = \bigoplus_{\chi \in X^*(T_0)} V_\chi$$

Note that $V_\chi = \emptyset$ for most $\chi \in X(T_0)$ and if $V_\chi \neq \emptyset$, then $\dim V_\chi = 1$. Hence $\dim V = \dim E$, and so we have $E_{sep} = \prod k_{sep}$, an étale algebra. □

Claim 6.138. $U_{E_{T_0}} = T_0$

Proof. Clearly, $T_0 \subset U_{E_{T_0}}$ so by maximality, equality must hold. □

Lemma 6.139. *Let A be any central simple algebra over k of even dimension, equipped with an involution σ, and $E \subset A$ a maximal étale algebra stable under σ. Let F be the subalgebra of E consisting of elements fixed by the involution σ. Then,* $\dim F = \frac{1}{2} \dim E$.

Proof. It is enough to show this over a separable closure of k. Now, an involution can be either of the first kind, *i.e.* orthogonal or symplectic; or of the second kind, *i.e.* unitary. Say $\dim E = m = 2n$. Let $S = \begin{pmatrix} 0 & \mathrm{I_n} \\ -\mathrm{I_n} & 0 \end{pmatrix}$, and $H = \begin{pmatrix} 0 & \mathrm{I_n} \\ \mathrm{I_n} & 0 \end{pmatrix}$ (we use H since it is a hyperbolic quadratic form). Define

$$\sigma_S(x) = S^{-1}x^tS, \quad \sigma_H(x) = H^{-1}x^tH \quad \text{and} \quad \varepsilon(x,y) = (y^t, x^t)$$

Note that over a separable closure k_{sep} of k we have

$$(A \otimes k_s, \sigma) \cong \begin{cases} (M_m, \sigma_S) & \text{if } \sigma \text{ is symplectic} \\ (M_m, \sigma_H) & \text{if } \sigma \text{ is orthogonal} \\ (M_n \times M_n, \varepsilon) & \text{if } \sigma \text{ is unitary} \end{cases}$$

Case 1: σ is of the first kind.

If σ is of the first kind, note that over a separable closure,

$$E = \{\mathrm{diag}(x_1, \ldots, x_n, y_1, \ldots, y_n)\}$$

We can also see that

$$\sigma_H\,(\mathrm{diag}(x_1, \ldots, x_n, y_1, \ldots, y_n)) = \mathrm{diag}(y_1, \ldots, y_n, x_1, \ldots, x_n)$$

and

$$\sigma_S\,(\mathrm{diag}(x_1, \ldots, x_n, y_1, \ldots, y_n)) = \mathrm{diag}(y_1, \ldots, y_n, x_1, \ldots, x_n)$$

Thus if F consists of elements fixed by the involution, then

$$F = \{\mathrm{diag}(x_1, \ldots, x_n, x_1, \ldots, x_n)\}$$

Therefore, $\dim F = \frac{1}{2} \dim E$.

Case 2: σ is of the second kind.

If σ is of the second kind, note that over a separable closure, $E = B \times B$, and since $\varepsilon(x, y) = (y^t, x^t)$ if an element is to be fixed by the exchange involution, then it must have the form (x, x^t), so $F = \{(x, x^t) \colon x \in B\}$, but this is isomorphic to one copy of B, and hence $\dim F = \frac{1}{2} \dim E$. □

Note that we have two exact sequences:

$$1 \longrightarrow T_0 \longrightarrow \mathbf{G_{m,}}_E \overset{N_{E/F}}{\longrightarrow} \mathbf{G_{m,}}_F \longrightarrow 1$$

From this we get the sequence in cohomology

$$\cdots \longrightarrow E^\times \longrightarrow F^\times \longrightarrow \mathbf{H^1}(k, T_0) \longrightarrow 0$$

the first isomorphism theorem yields $\mathbf{H^1}(k, T_0) \cong F^\times / N_{E/F}(E^\times)$ and the second exact sequence we'll use is

$$1 \longrightarrow \mathbf{G_{m,}}_F \longrightarrow \mathbf{G_{m,}}_E \longrightarrow T_0 \longrightarrow 1$$

The first map is just the inclusion and the second map sends x to $x\sigma_h(x)^{-1}$, where σ_h is the adjoint involution associated to our hermitian form h. The associated sequence in cohomology is

$$\cdots \longrightarrow 0 \longrightarrow \mathbf{H^1}(k, T_0) \longrightarrow \mathbf{H^2}(k, F) \longrightarrow \mathbf{H^2}(k, E)$$

which yields an isomorphism $\mathbf{H^1}(k, T_0) \cong \mathrm{Br}\,(E/F)$. Thus we have found an iso-

morphism $F^\times/N_{E/F}(E^\times) \cong \mathrm{Br}\,(E/F)$. This isomorphism can be given explicitely by

$$a \in F^\times/N_{E/F}(E^\times) \longmapsto \mathrm{Cor}_{E/F}(a, M)$$

where $E = F[t]/(t^2 - M)$ for $M \in F^\times$. Thus we have found two equivalent ways to study the conjugacy class of maximal tori isomorphic to T_0 over the algebraic closure, $\bar{k}$.

6.2 $\mathrm{cd}\,(\Gamma_k) \leqslant 2$

In the previous section we established the commutativity of the diagram:

$$\begin{array}{ccc}
\mathbf{H^1}(k, \widetilde{T}) & \longrightarrow & \mathbf{H^1}(k, \widetilde{G}) \\
\downarrow & & \downarrow \\
\mathbf{H^1}(k, T) & \xrightarrow{i^\sharp} & \mathbf{H^1}(k, G) \\
{\scriptstyle \delta^1}\downarrow & & \downarrow{\scriptstyle \delta^1} \\
\mathbf{H^2}(k, \ker \rho) & = & \mathbf{H^2}(k, \ker \rho)
\end{array}$$

and we proved in proposition 6.123 that $\ker(i^\sharp) \subset \ker \delta^1$. In proposition 6.124 we showed that equality holds provided $\mathbf{H^1}(k, \widetilde{G}) = 0$. This is of interest as δ^1 has the added advantage of being a group homomorphism. For this equality we need:

Theorem 6.140 (E. Bayer-Fluckiger, R. Parimala). *Let k be a perfect field of $\mathrm{cd}(\Gamma_k) \leqslant 2$. Let $\widetilde{G} \neq$ trialitarian form be a semisimple simply connected classical group defined over k. Then $\mathbf{H^1}(k, \widetilde{G}) = 0$.*

Theorem 6.141 (E. Bayer-Fluckiger, R. Parimala). *Let k be a perfect field of virtual cohomological dimension $\leqslant 2$, and let $\widetilde{G}$ be a semisimple, simply connected group of classical type, or of type G_2 or F_4. Then the natural map,*

$$\mathbf{H^1}(k, \widetilde{G}) \longrightarrow \prod_v \mathbf{H^1}(k_v, \widetilde{G})$$

is injective, where v runs over the orderings of k and where k_v denotes the real closure of k at v.

Notice that theorem 6.140 is a special case of theorem 6.141. This is because the product on the right hand side is an empty product and the map being injective is equivalent to $\mathbf{H}^1(k, \widetilde{G})$ collapsing, *i.e.* $\mathbf{H}^1(k, \widetilde{G}) = 0$.

There is one situation worth noting here. If G itself happens to be simply connected then $G = \widetilde{G}$, and we have $\mathbf{H}^1(k, G) = \mathbf{H}^1(k, \widetilde{G}) = 0$ and so $\ker(i^\sharp) = \ker \delta^1 = \mathbf{H}^1(k, T)$. This is the case when, for example, $G = \mathbf{Sp}_{2n}$, $\mathbf{SL}_n$, or $\mathrm{SU}(h)$. If k is a field of cohomological dimension at most 2. We have the following improvements to our results.

In example 6.126 we get a bijection

$$\left\{a \in F^\times / N_{E/F}(E^\times) \colon \mathrm{Cor}\,(a, D) = 0\right\} / W^\Gamma$$

$$\updownarrow$$

$$k\text{-conjugacy classes of maximal } k\text{-tori } S \text{ with } (E_S, \nu) \cong (E_{U_{E/F}}, \nu)$$

In example 6.129 we have

$$\mathbf{H}^1(k, U_{E/F}) / W^\Gamma$$

$$\updownarrow$$

$$k\text{-conjugacy classes of maximal } k\text{-tori } S \text{ with } (E_S, \sigma_{h_{E,b}}) \cong (E_{U_{E/F}}, \sigma_{h_{E,b}})$$

On lemma 6.132, the hermitian forms h are completely determined (classified) by their determinant (which lives in $k^\times / N_{L/k}(L^\times)$). Hence if $\mathrm{cd}(\Gamma_k) \leqslant 2$, the admissible algebras (E, σ) are precisely those with

$$\det h_{E,b} \equiv \operatorname{disc}(F/k) \pmod{N_{L/k}(L^\times)}$$

On proposition 6.135 if $\operatorname{cd}(\Gamma_k) \leqslant 2$, then $\mathbf{H}^1(k, \mathrm{SU}(h)) = 0$, *i.e.* all hermitian forms are isomorphic. Hence the extra condition that $h_a \cong h$ in the proposition disappears, and we have

$$\mathbf{H}^1(k, U_{E/F})/W^\Gamma$$

$$\updownarrow$$

k-conjugacy classes of maximal tori S with $(E_S, \sigma_h) \cong (E_{U_{E/F}}, \sigma_h)$

6.3 Examples

Now we will illustrate our results with some examples, specifically for $k = \mathbb{F}_q$, the finite field of q elements where $q = p^m$ and p is an odd prime number, for k a finite extension of $\mathbb{Q}_p$, the field of p-adic numbers, and for $k = \mathbb{R}$, the field of real numbers.

We shall consider the case where $G = \mathrm{SO}(Q)$, where Q is a non-degenerate quadratic form of rank $2n$ over k.

Example 6.142. Let $k = \mathbb{F}_q$ the finite field of q elements, where $q = p^m$ is a prime power. Let $G = \mathrm{SO}(Q)$, and $T \subset G$ a maximal torus. We want to study $\ker\left(i_T^\sharp \colon \mathbf{H}^1(\mathbb{F}_q, T) \longrightarrow \mathbf{H}^1(\mathbb{F}_q, G)\right)$, but since quadratic forms over finite fields are classified by their determinant, we have $\mathbf{H}^1(\mathbb{F}_q, G) = \{0\}$, and so $\ker i_T^\sharp = \mathbf{H}^1(\mathbb{F}_q, T)$.

We know that we can associate to each maximal torus T an étale algebra E_T with involution σ. We denote by F those elements of E that are fixed by the involution, *i.e.* $F = E^\sigma$. Now with the notation as before, $T = U_{E/F} = \ker\left(N \colon \mathbf{G}_{\mathbf{m},E} \longrightarrow \mathbf{G}_{\mathbf{m},F}\right)$; then $\mathbf{H}^1(\mathbb{F}_q, T) = F^\times/N(E^\times)$. Notice that the norm map of finite field extensions and of étale extensions is surjective, hence, in this case $\mathbf{H}^1(\mathbb{F}_q, T) = \{0\}$, so S and

T are conjugates over $\mathbb{F}_q$ if and only if $(E_S, \sigma) \cong (E_T, \sigma)$. Thus it is enough then to count the isomorphism classes of algebras with involution (E_S, σ) such that there exists an embedding $U_{E/F} \hookrightarrow \mathrm{SO}(Q)$.

To this end, let $P(n)$ be the set of partitions of n. There is a canonical one-to-one correspondence

$$\{ \text{Étale algebras } F \text{ of degree } n\} \longleftrightarrow P(n)$$

This correspondence can be given explicitly by

$$F = \mathbb{F}_{p^{n_1}} \times \cdots \times \mathbb{F}_{p^{n_r}} \longleftrightarrow \{n_1, \ldots, n_r\}$$

For fixed F, we choose $D \in F^\times/F^{\times 2}$ and set $E = F[t]/(t^2 - D)$. Recall that E comes equipped with the involution σ that sends t to $-t$.

If $U_{E/F}$ can be embedded into $\mathrm{SO}(Q)$, then $Q \cong \mathrm{Tr}_{F/k}(ax\sigma(x))$ for some $a \in F^\times$ and conversely.

Notice that if $x = u + tv$

$$\begin{aligned} \det\left(\mathrm{Tr}_{F/k}(ax\sigma(x))\right) &= \det\left(\mathrm{Tr}_{F/k}(a(u^2 - Dv^2))\right) \\ &= N_{F/k}(a)^2 \cdot d_{F/k} \cdot N_{F/k}(-D) \cdot d_{F/k} \\ &\equiv N_{F/k}(-D) \pmod{F^{\times 2}} \end{aligned}$$

so there exists an embedding $U_{E/F} \hookrightarrow \mathrm{SO}(Q)$ if and only if $N_{F/k}(-D) = \det Q$.

Note as well that $F^\times/F^{\times 2} = (\mathbb{Z}/2\mathbb{Z})^r$ and with this identification

$$\begin{aligned} N \;:\; & (\mathbb{Z}/2\mathbb{Z})^r \longrightarrow \mathbb{Z}/2\mathbb{Z} \\ & (D_1, \ldots, D_r) \longmapsto \sum_{i=1}^{r} D_i \pmod 2 \end{aligned}$$

so there are 2^{r-1} choices for D as $|\ker N| = 2^{r-1}$. Thus the total number of k-conjugacy classes is then given by

$$\sum_{\wp \in P(n)} 2^{\ell(\wp)-1},$$

where $\ell(\wp)$ is the length of the partition $\wp$.

Example 6.143. Let k be a finite extension of $\mathbb{Q}_p$, where p is a prime number. We have

$$\begin{array}{ccc} \mathbf{H}^1(k,T) & \xrightarrow{i^1} & \mathbf{H}^1(k,G) \\ {\scriptstyle \delta^1}\downarrow & & \\ \mathrm{Br}(k) & & \end{array}$$

and we have already seen in (6.21) that δ^1 is given by $a \longmapsto \mathrm{Cor}(a, D)$.

If F is a field, the corestriction map induces an isomorphism

$$\mathrm{Cor}\colon \mathrm{Br}(F) \xrightarrow{\sim} \mathrm{Br}(k)$$

and we also have an injection $\mathrm{Br}(E/F) \hookrightarrow \mathrm{Br}(F)$. Thus if $(E_S, \sigma) \cong (E_T, \sigma)$, then S and T are k-conjugates.

If F is not a field, let $F = F_1 \times F_2 \times \cdots \times F_r \times F_{r+1} \times \cdots \times F_{r+s}$ where each F_i is a field for $i = 1, \ldots, r$, and let

$$E = E_1 \times E_2 \times \cdots \times E_r \times (F_{r+1} \times F_{r+1}) \times \cdots \times (F_{r+s} \times F_{r+s})$$

where E_i/F_i is a quadratic field extension for $i = 1, \ldots r$.

We know that

$$F^\times/N_{E/F}(E^\times) \cong \prod_{i=1}^{r} F_i^\times/N_{E_i/F_i}(E_i^\times)$$

and each $F_i^\times/N_{E_i/F_i}(E_i^\times) \cong \mathbb{Z}/2\mathbb{Z}$, so $F^\times/N_{E/F}(E^\times) \cong \prod_{i=1}^{r} \mathbb{Z}/2\mathbb{Z}$. We have the corestriction map

$$\begin{aligned} \mathrm{Cor} \ : \ & (\mathbb{Z}/2\mathbb{Z})^r \longrightarrow \mathbb{Z}/2\mathbb{Z} \\ & (x_1, \ldots, x_r) \longmapsto \sum_{i=1}^{r} x_i \pmod 2 \end{aligned}$$

W^Γ acts on $\ker(\mathrm{Cor})$ by permuting the coordinates. By theorem 6.125, there is a one-to-one correspondence

$$\ker \mathrm{Cor}/W^{\Gamma}$$

$$\updownarrow$$

k-conjugacy classes of maximal k-tori S with $(E_S, \sigma) \cong (E_T, \sigma)$

Example 6.144. Let $k = \mathbb{R}$. In the case where $k = \mathbb{R}$ a torus T must be of the form $T = S^r \times \left(\mathbf{G}_{\mathbf{m},\mathbb{R}}\right)^s$, where S is defined by the equation $x^2 + y^2 = 1$. We call T a torus of type (r, s). Thus the étale algebra corresponding to a torus of type (r, s) is $E = \mathbb{C}^s \times (\mathbb{R} \times \mathbb{R})^s$, and $F = \mathbb{C}^r \times \mathbb{R}^s$. In this case we shall describe directly the kernel of $\mathbf{H}^1(\mathbb{R}, T) \longrightarrow \mathbf{H}^1(\mathbb{R}, \mathrm{SO}(Q))$.

Proposition 6.145. *Let Q be a quadratic form of rank $2n$, and let $\sigma = \frac{1}{2}\mathrm{sgn}(Q)$. A torus T of type (r, s) with $r + s = n$ can be embedded into $\mathrm{SO}(Q)$ if and only if $r \geqslant |\sigma|$ and $r \equiv \sigma \pmod 2$.*

Proof. If T can be embedded into $\mathrm{SO}(Q)$, then there exists

$$a = (\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_{r+1}, \alpha_{r+2}, \ldots, \alpha_{r+s}) \in F,$$

such that Q is of the form

$$\begin{aligned} Q(x) = \mathrm{Tr}_{F/\mathbb{R}}(ax\bar{x}) &= \mathrm{Tr}_{\mathbb{C}^r/\mathbb{R}}(\alpha x\bar{x}) \oplus \langle 1, -1\rangle^s \\ &= \langle \alpha_1, \alpha_2, \ldots, \alpha_r\rangle \otimes \langle 1, 1\rangle \oplus \langle 1, -1\rangle^s \end{aligned}$$

So $\sigma = \mathrm{sgn}\langle \alpha_1, \alpha_2, \ldots, \alpha_r\rangle \leqslant r$ and we also have $r \equiv \sigma \pmod 2$ since the signature and the dimension of a quadratic form always have the same parity. The converse also holds since we can choose $\langle \alpha_1, \alpha_2, \ldots, \alpha_r\rangle$ as above so that it has the needed signature. □

Proposition 6.146. *With the same notation as above. If $r \geqslant |\sigma|$, then the number of conjugacy classes of tori $S \subset \mathrm{SO}(Q)$ with $S \cong T$ is $1 + \frac{r-|\sigma|}{2}$.*

Proof. We may assume without loss of generality that $\sigma \geqslant 0$ since we can always replace Q by $-Q$ without changing $\mathrm{SO}(Q)$. Now we have

$$F^\times/N(E^\times) = \mathbf{H}^1(\mathbb{R}, T) \longrightarrow \mathbf{H}^1(\mathbb{R}, \mathrm{SO}(Q))$$

sending a to $[\mathrm{Tr}(abx\bar{x})]$. But

$$[\mathrm{Tr}(abx\bar{x})] = [\langle \alpha_1\beta_1, \alpha_2\beta_2, \ldots, \alpha_r\beta_r\rangle \otimes \langle 1, 1\rangle \oplus \langle 1, -1\rangle^s] = [Q]$$

if and only if

$$\langle \alpha_1\beta_1, \alpha_2\beta_2, \ldots, \alpha_r\beta_r\rangle \cong \langle \alpha_1, \alpha_2, \ldots, \alpha_r\rangle$$

Now we can always write

$$\langle \alpha_1, \alpha_2, \ldots, \alpha_r\rangle \cong \langle \overbrace{1, \ldots, 1}^{m\text{-times}}, \overbrace{-1, \ldots, -1}^{(r-m)\text{-times}}\rangle$$

If we choose j 1's from the m 1's to form β, we must have $j \leqslant m$, and $m-j \leqslant r-m$. Thus we must have

$$2m - r \leqslant j \leqslant m$$

But notice that $\sigma = 2m - r$, so in terms of σ we have

$$\sigma \leqslant j \leqslant \frac{\sigma + r}{2}$$

and hence the number of conjugation classes of tori of type (r, s) is the number of possible j's which is $\frac{\sigma+r}{2} - \sigma + 1 = \frac{r-\sigma}{2} + 1$. Notice that this is always an integer since r and σ have the same parity. □

Proposition 6.147. *The total number of $\mathbb{R}$-conjugacy classes of $\mathbb{R}$-tori is*

$$\frac{\left(\left[\frac{n-\sigma}{2}\right] + 1\right)\left(\left[\frac{n-\sigma}{2}\right] + 2\right)}{2}$$

Proof. To get all the conjugacy classes we need to sum over all possible r's. These are the ones satisfying $\sigma \leqslant r \leqslant n$ and $r \equiv \sigma \pmod 2$. Now since $r \equiv \sigma \pmod 2$ we must have $r - \sigma = 2k$ for some k, that is, $k = \frac{r-\sigma}{2}$. Let $M = \left[\frac{n-\sigma}{2}\right]$. We have

$$\begin{aligned} \text{Total Number of Conjugacy Classes} &= \sum_{\substack{r \equiv \sigma \pmod 2 \\ \sigma \leqslant r \leqslant n}} 1 + \frac{r-\sigma}{2} \\ &= \sum_{k=0}^{M} (1+k) \\ &= \frac{(M+1)(M+2)}{2} \end{aligned}$$

□

Notice that if $\sigma = n$, then $T(\mathbb{R})$ is compact. If $n = \sigma + 1$, then $r = \sigma$ and so $\frac{(M+1)(M+2)}{2} = 1$. We call this case the Lorentz case.

References

[BKM] R. Brusamarello, P. Koulmann, and J. Morales, *Orthogonal Groups Containing a Given Maximal Torus*, preprint 2000.

[BP1] E. Bayer-Fluckiger and R. Parimala, *Galois cohomology of classical groups over fields of cohomological dimension* $\leqslant 2$, Inventiones mathimaticae 122, 195-229 (1995).

[BP2] E. Bayer-Fluckiger and R. Parimala, *Classical groups and the Hasse principle*, Annals of Mathematics, **147** (1998), 651-693.

[CR] C.W. Curtis, and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, John Wiley & Sons, Inc. **1962**.

[H] J. Humphreys, *Linear Algebraic Groups*, Springer-Verlag GTM 21, New York 1975.

[J] N. Jacobson, *Basic Algebra II*, W.H. Freeman and Company, New York, 1980.

[Ka] K. Kariyama, *On Conjugacy Classes Of Maximal Tori In Classical Groups*, Journal of Algebra **125**, 133-149 (1989).

[Ke] I. Kersten, *Brauergruppen von Körpern*, Aspects of Mathematics, D6, Friedr. Vieweg & Sohn, Braunschweig, 1990.

[KM] P. Koulmann, and J. Morales, *Embedding Commutative Frobenius Algebras Into Central Simple Algebras*, preprint 2000.

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The Book of Involutions*, American Mathematical Society Colloquium Publications, vol. 44.

[QSS] H.-G. Quebbemann, W. Scharlau, and M. Schulte, *Quadratic and hermitian forms in additive and abelian categories*, Journal of Algebra **59** (1979), 264-289.

[R] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology*, Queen's Papers in Pure and Applied Mathematics-no. 24 (1970).

[Sc] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren der mathematischen Wissenschaften 270, Springer-Verlag, 1985.

[Se1] J.-P. Serre, *Cohomologie Galoisienne*, Cinquième édition, révisée et complétée, Lecture Notes in Mathematics, vol. 5 (LNM 5) Springer-Verlag, Berlin 1994.

[Se2] J.-P. Serre, *Local Fields*, GTM 67, Springer-Verlag, 1979.

[Sh] S.S. Shatz, *Profinite groups, Arithmetic, and Geometry*, Annals of Mathematics Studies-no. 67, Princeton University Press (1972).

[TS] T. A. Springer, *Linear Algebraic Groups*, Progress in Mathematics vol. 9, Birkhäuser, Boston 1981.

[W] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Springer-Verlag GTM 66, New York, 1979.

[We] A. Weil, *Algebras With Involution and the Classical Groups*, Journal of the Indian Mathematical Society, **24** 1960 589-623 (1961).

[Wi] C. Wiebel, *An Introduction to Homological Algebra*, Cambridge Studies in Advanced Mathematics 38, Cambridge University Press, New York, 1994.

Vita

Uroyoán R. Walker was born on November 7, 1973, in Brooklyn, N.Y. He finished his undergraduate studies in mathematics at the University of Puerto Rico at Mayagüez in May 1996. In August 1996, he came to Louisiana State University to pursue graduate studies in mathematics. He earned a Master of Science degree in mathematics from Louisiana State University in December 1998. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2001.

DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Uroyoan R. Walker

Major Field: Mathematics

Title of Dissertation: On k-Conjugacy Classes of Maximal Tori in Semi-Simple Algebraic Groups

Approved:

Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

J. Hurelbrink

Robert Perlis

Lawrence Smolinsky

Ian Richardson

Michael McCracken

Date of Examination:

05/01/01