Universidade de Brasília

Group schemes and Fields of dimension at most one

Alberto Tavares Duarte Neto

Orientador: Dr. Theo Allan Darn Zapata

Departamento de Matemática
Universidade de Brasília

Dissertação apresentada como requisito parcial para obtenção do grau de
Mestre em Matemática

Brasília, 31 de julho de 2025

Agradecimentos

> You walk in the footsteps of those who came before you, and your path guides those who will follow you later.
>
> Outer Wilds

Em primeiro lugar, agradeço a toda minha família por sempre acreditar em mim, em especial minha mãe Soraia, meu irmão Daniel e minhas irmãs Natália e Taynara por todo amor e paciência.

Aos meus amigos matemáticos João, Gabriel, Leonardo, Tyzz, Rômulo, Eduardo, Paulo, Clara, e vários outros, que trocaram comigo experiências, vivências e matemática. Essa jornada não valeria a pena estando sozinho.

Aos meus amigos da UnBalloon, que fizeram parte do prelúdio dessa parte da jornada, mas que me acompanharam não só em viagens e competições, mas também em momentos difíceis da minha vida: agradeço em primeiro lugar meu grande amigo Tiago, que compartilhou comigo desde as viagens mais malucas até as derrotas mais duras, meus outros companheiros de time Lucas Sala, Leonardo Riether e Anderson, a todos os outros que fizeram parte desse grupo incrível. Agradeço também meus técnicos de equipe e professores José Leite, Vinicius Borges e Guilherme Ramos, sempre apoiando meu desenvolvimento. Que a UnBalloon prospere por muitos anos!

A todos os professores que fizeram parte da minha vida, minhas sinceras gratidões, foi um privilégio conhecê-los. Aos professores Diogo e Fernanda, do CEM 04, que fizeram o possível para motivar meu gosto pela matemática, meus mais profundos agradecimentos.

E é claro, este trabalho não seria possível sem o apoio do meu orientador, Theo Zapata. Obrigado por todos os conselhos e ensinamentos e, o mais importante, obrigado por me tratar com toda a humanidade do mundo, paciência e disposição. Nos momentos mais difíceis eu sempre pude contar contigo, e por isso eu serei eternamente

grato. Obrigado por me mostrar que a matemática pode ser tão divertida e interessante, e me direcionar nessa longa jornada que tivemos juntos.

Por fim, agradeço aos membros da banca, Amilcar Pacheco, Eduardo Tengan, Alexandre Zalesski e Theo Zapata, pelas críticas e sugestões feitas ao trabalho.

Abstract

In this work we investigate J.-P. Serre's conjecture I on the Galois cohomology of algebraic groups, later known as the theorem of Serre-Springer-Steinberg. The cases of finite fields (a theorem of S. Lang) and soluble groups (due to Serre) are treated in details.

Resumo

Neste trabalho, cujo título em português seria Esquemas em grupos e Corpos de dimensão no máximo um, investigamos a conjectura I de J.-P. Serre sobre a cohomologia de Galois de grupos algébricos, posteriormente conhecida como o teorema de Serre-Springer-Steinberg. Os casos de corpos finitos (um teorema de S. Lang) e grupos solúveis (devido a Serre) são tratados com detalhes.

Table of contents

Introduction

Much of the early theory of profinite groups and their cohomology was done towards arithmetical applications by the minds of J. Tate, I. Shafarevich and J.-P. Serre and a few other mathematicians (cf. Serre [Ser02, p.60] and [NSW15, Part II]).

In the present work we consider a famous conjecture by Serre of the early years of the 1960s on Galois cohomology of algebric groups.

One should remark that back then those three named mathematicians were also interested in Algebraic Geometry, which was being profoundly renovated in its concepts and methods. In fact, A. Grothendieck introduced schemes and topologies after considerable advances in Algebraic and Differential Topology and in the theory of analytic spaces due to three notions invented by J. Leray: sheaves; cohomology with coefficients in a sheaf; and spectral sequences.

As expected the theory of algebraic groups did not absorb those ideas immediately. For instance, neither the standard trinity of books called *Linear Algebraic Groups*, by A. Borel, J. Humphreys or T. Springer, nor the more recent book *Algebraic Groups and Number Theory*, by V. Platonov and A. Rapinchuk, were based in the modern algebraic geometry. This had to wait, for instance, for W. Waterhouse's *Introduction to affine group schemes* [Wat79] and J. Milne's *Algebraic Groups* [Mil22].

There is no need for much algebraic geometry in the present work, though. What is needed for our purposes and conveniences is presented in Chapter I.

Our Chapter II contains the basics of Galois cohomology; in particular, the notions of cohomology and cohomological dimension are explained. It allows us to formally understand Serre's conjecture, as we do now shortly.

Let k be field. In this work, we say that it has dimension at most one if the Brauer group of each algebraic extension of k is trivial. If k_s denotes the separable closure of k and G is its Galois group over k, then the profinite group G has cohomological dimension at most one provided k has dimension at most one. The converse holds if k is a perfect field.

A so-called Conjecture II of Serre deals with deals G of cohomological dimension at most 2; it does not concern us in the present work. The conjecture of Serre that we are interested in is the following:

Conjecture I. If k is a perfect field of dimension at most one, and if L is a connected linear algebraic group defined over k, then $H^1(G, L(k_s)) = 0$.

When stated by Serre this conjecture was already proved in some cases, notably: if L is G_m (by E. Noether); if k is a finite field (by S. Lang); and if L is soluble (by Serre). The goal of our Chapter III is to provide reformulations of the conjecture, known nowadays as a theorem of Serre-Springer-Steinberg ([Ste65] and [Ser02]), and details of those cases.

Chapter 1

Algebraic groups

In this chapter, we study algebraic groups, which are in the heart of this work. In a few words, fixing a base field k, they are group objects in the category of algebraic schemes over k. One valuable property of algebraic groups is that, if K is a field extension of k, then we can extend G to an algebraic group G_K over K. Galois theory will come into play when we consider the action of $\mathrm{Gal}(K/k)$ over G_K, and later in this work we shall see that the cohomology sets associated to them are naturally related to our main results.

Since most of the examples of algebraic groups that we care about are affine, we will focus on them. For instance, in Section 1.3 we prove that an algebraic group is affine if, and only if, it is an algebraic group of GL_n for some n.

On later sections, we shall study solvable and semisimple algebraic groups, which are essential to our main results.

1.1 Basic facts

1.1.1 Algebraic schemes

We begin by defining and stating some facts about algebraic schemes.

Let A be a finitely generated k-algebra. Let $\mathrm{Spm}(A)$ be the set of maximal ideals in A. If $\mathfrak{a}$ is an ideal in A, we define

$$Z(\mathfrak{a}) = \{\mathfrak{m} \in \mathrm{Spm}(A) \mid \mathfrak{m} \supset \mathfrak{a}\} .$$

The **Zariski topology** on $\mathrm{Spm}(A)$ is the topology in which the sets $Z(\mathfrak{a})$ are the closed sets. It is well-defined since

(i) $Z(0) = \mathrm{Spm}(A)$, $Z(A) = \varnothing$,

(ii) $Z(\mathfrak{a}\mathfrak{b}) = Z(\mathfrak{a} \cap \mathfrak{b}) = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$ for every pair of ideals $\mathfrak{a}$ and $\mathfrak{b}$,

(iii) $Z(\sum_i \mathfrak{a}_i) = \cap_i Z(\mathfrak{a}_i)$ for every family of ideals (a_i).

Let $\alpha : A \to B$ be a homomorphism of k-algebras. We define

$$\begin{aligned} \alpha^* : \mathrm{Spm}(B) &\to \mathrm{Spm}(A) \\ m &\mapsto \alpha^{-1}(\mathfrak{m}) \,. \end{aligned}$$

It is a well-defined continuous function with respect to the Zariski topology, and it makes Spm(−) into a functor from k-algebras to topological spaces [Mil22, A.4].

Definition 1.1 ([Mil22, A.7])**.** A **k-ringed space** is a topological space X equipped with a sheaf $\mathcal{O}_X$ of k-algebras. An affine algebraic scheme over k is a k-ringed space isomorphic to $\mathrm{Spm}(A)$ for some k-algebra A.

Let $(X, \mathcal{O}_X)$ be a k-ringed space. An open subset U of X is said to be affine if the k-ringed space $(U, \mathcal{O}_X|_U)$ is an affine algebraic scheme over k.

Definition 1.2 ([Mil22, A.11])**.** An **algebraic scheme** over k is a k-ringed space $(X, \mathcal{O}_X)$ which admits a finite covering by open affine subsets. A **morphism of algebraic k-schemes** is a morphism of k-ringed spaces.

We shall denote a k-ringed space $(X, \mathcal{O}_X)$ by X, and its underlying topological space by $|X|$. The **local ring** at a point $x \in X$ shall be denoted by $\mathcal{O}_{X,x}$, and its residue field at x by $\kappa(x)$.

Examples 1.3. Let R be a finitely generated k-algebra.

(i) The space $\mathrm{Spm}(R)$ is an (affine) algebraic scheme over k.

(ii) The projective space $\mathbb{P}^n_R$, which can be obtained by gluing $n+1$ copies of $\mathrm{Spm}(R^n)$ along the open sets.

Proposition 1.4 ([Mil22, A.44])**.** An algebraic scheme over k is an algebraic variety over k if, and only if, it is separated and geometrically reduced.

Let X be an algebraic scheme over k. We define $\pi(X)$ as the largest étale subalgebra of $\mathcal{O}_X$. We say that X is **connected** if $\pi(X) = k$, and **geometrically connected** if $X_{k'}$ is connected for every field extension k'/k.

Definition 1.5. The group of **connected components** of X is defined as $\pi_0(X) = \mathrm{Spm}(\pi(X))$.

Proposition 1.6 ([Mil22, Prop. 1.30, 1.31])**.** (i) For all fields k' containing k,

$$\pi_0(X_{k'}) = \pi_0(X)_{k'} .$$

(ii) The fibers of the map $X \to \pi_0(X)$ are the connected components of X.

Now, if we consider an algebraic group G, we can say a little bit more. The connected component G^0 of the identity is an algebraic subgroup of G. It is geometrically connected, and its formation commutes with base extension [Mil22, Prop. 1.34]:

$$(G_{k'})^0 = (G^0)_{k'} .$$

Irreducibility and connectedness are the same in this context, and being connected implies geometrically connected.

Proposition 1.7 ([Mil22, Sec. 1.b])**.** Let G be an algebraic group over k. The following are equivalent:

(i) G is irreducible.

(ii) G is connected.

(iii) G is geometrically connected. And, when G is affine, these are equivalent to:

(iv) The ring $\mathcal{O}_G$ is an integral domain.

As expected, the sequence

$$1 \to G^0 \to G \to \pi_0(G) \to 1$$

is exact (in the sense of Definition 1.37).

Proposition 1.8 ([Mil22, A.68])**.** A morphism $\varphi : Y \to X$ is faithfuly flat if, and only if, it is surjective when viewed as a map $|\varphi| : |Y| \to |X|$ of the underlying topological spaces and, for all $y \in |Y|$, the map $\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$ is a flat homomorphism.

Let S be a subset of $X(k)$ for a algebraic scheme X. We say that S is **schematically dense** in X if the only closed subscheme Z of X such that $S \subset Z(k)$ is X. The following properties are equivalent ([Mil22, Prop. 1.10]):

(i) S is schematically dense in X.

(ii) X is reduced as a scheme and S is dense in the underlying topological space $|X|$.

Definition 1.9. Let F be a functor from k-algebras to sets. A subfunctor D of F is **fat** if, for every R and $x \in F(R)$, there exists a faithfully flat R-algebra R_0 such that the image of x' of x in $F(R_0)$ lies in $D(R_0)$.

We state the next propositions related to fat subfunctors, as they shall be useful later.

Proposition 1.10 ([Mil22, Prop. 5.7])**.** Let $\varphi : X \to Y$ be a faithfully flat morphism of algebraic schemes over k. The subfunctor $R \rightsquigarrow \varphi(X(R))$ is fat in $\tilde{Y}$.

Proposition 1.11 ([Mil22, Prop. 5.10])**.** Let X and Y be algebraic schemes over k, and let D be a fat subfunctor of $\tilde{X}$. Every map of functors $D \to \tilde{Y}$ extends uniquely to a map of functors $\tilde{X} \to \tilde{Y}$.

To finish this section, we state Yoneda's Lemma. Although we state it generally, we will use it on two specific contexts in the next two sections.

Proposition 1.12 (Yoneda's Lemma, [Mil22, A.33], [Mac10, Chap. III, Sec. 2])**.** Let F be a contravariant functor from a locally small category C to the category of sets. Then for each object X of C, the natural transformations

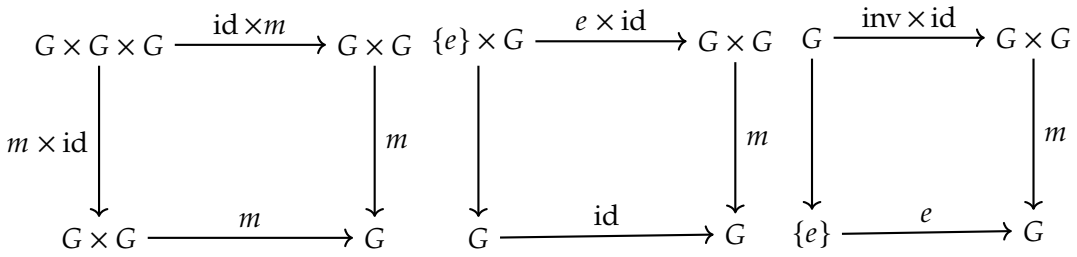
$$\mathrm{Nat}(h_X, F) = \mathrm{Hom}(\mathrm{Hom}(-, X), F)$$

are in one-to-one correspondence with $F(A)$.

1.1.2 Algebraic groups

The main object that we discuss in this chapter is the concept of an *algebraic group* over a field k. We can view it through some different lenses: as certain functors from the category of k-algebras to the category of groups, as group objects in the category of algebraic schemes, and, when they are affine and some conditions are met, as closed subgroups, with respect to the Zariski topology, of some matrix group $\mathrm{GL}_n(k)$.

Definition 1.13. Let G be an algebraic scheme over k, and let $m : G \times G \to G$ be a morphism. The pair (G, m) is an **algebraic group** if there exist morphisms $e : * \to G$ and $\mathrm{inv} : G \to G$ such that the following diagrams commute:



A **homomorphism** $\varphi : (G, m) \to (G', m')$ is a morphism $\varphi : G \to G'$ of algebraic schemes such that $\varphi \circ m = m' \circ \varphi$. An algebraic group (H, m_H) is said to be an **algebraic subgroup** of (G, m) if H is a subscheme of G and the inclusion is an homomorphism.

As usual, we shall denote (G, m) just by G, and the map m will be implied in the context. We often omit the word "algebraic" when the context is clear.

Let X be an affine scheme over k, and define the functor $\tilde{X}$ from k-algebras to sets that leads R to the set $\tilde{X}(R)$ of R-points of X. By the Yoneda Lemma (Proposition 1.12), we have a bijection

$$\tilde{X}(A) \cong \mathrm{Nat}(h_A, \tilde{X}) .$$

This implies that the functor $X \rightsquigarrow \tilde{X}$ is fully faithful (see [Mac10, Chap. I, Sec. 3]). We shall use X to denote both the algebraic scheme and its corresponding functor.

Examples 1.14. (i) Consider the algebraic scheme $\mathrm{G}_a = \mathrm{Spm}(k[X])$. The operation induced by addition makes it into a algebraic group. If $\mathrm{char}\, k = p$, the algebraic scheme $\alpha_p = \mathrm{Spm}(k[X]/(X^p))$ is well defined as an algebraic group with addition. The canonical map $k[X] \to k[X]/(X^p)$ induces an injective homomorphism $\alpha_p \to \mathrm{G}_a$, so α_p is an algebraic subgroup of G_a.

(ii) The algebraic scheme $\mathrm{G}_m = \mathrm{Spm}(k[X, 1/X]) = \mathrm{Spm}(k[X, Y]/(XY - 1))$ is an algebraic group with operation induced by multiplication. The algebraic group $\mu_n = \mathrm{Spm}(k[X]/(X^n - 1))$ is a subgroup of G_m.

(iii) One of the most notable algebraic groups is $\mathrm{GL}_n = \mathrm{Spm}(k[X_{11}, X_{12}, \ldots, X_{nn}, 1/\det]$ and its algebraic subgroups. We shall say more about it later.

Proposition 1.15. Let H be an algebraic subscheme of an algebraic group (G, m_G). The pair (H, m_H) is an algebraic subgroup of (G, m_G) if, and only if, $H(R)$ is a subgroup of $G(R)$ for every k-algebra R.

Proof. If (H, m_H) is an algebraic subgroup, then by definition the inclusion is an homomorphism. Conversely, if $H(R)$ is a subgroup of $G(R)$ for every R, Yoneda's

Lemma allows us to lift it to a map

$$h_H : H \times H \to H \ ,$$

and it satisfies the group axioms because it does on each $H(R)$. It is immediate that the inclusion is an homomorphism. □

Examples 1.16. (i) The functor associated to G_a sends R to its additive group, and the functor associated to its subgroup α_p sends R to the additive group

$$\alpha_p(R) = \{x \in R \mid x^p = 0\} \ .$$

It is clear that $\alpha_p(R)$ is a subgroup of R.

(ii) The functor associated to G_m sends R to its multiplicative group R^*, and the functor associated to its subgroup μ_n sends R to the multiplicative group

$$\mu_n(R) = \{x \in R^* \mid x^n = 1\} \ .$$

We shall often denote the multiplicative group R^* by $\mathrm{G}_m(R)$.

We say that G is **commutative** if $m \circ t = t \circ m$, where t is the transposition defined by

$$\begin{aligned} t : G \times G &\to G \times G \\ (g_1, g_2) &\mapsto (g_2, g_1) \ . \end{aligned}$$

Proposition 1.17. The algebraic group G is commutative if, and only if, $G(R)$ is commutative as an abstract group for every k-algebra R.

Definition 1.18. The **center** $Z(G)$ of an algebraic group G is defined as the functor

$$R \rightsquigarrow \{x \in G(R) \mid \varphi(x)y = y\varphi(x) \text{ for every } \varphi : R \to S \text{ and } y \in G(S)\}$$

Let H be an algebraic subgroup of G. The **normalizer** of H in G, denoted by $N_G(H)$, is the functor $N = N_G(H)$ such that

$$N(R) = \{g \in G(R) \mid gH(R')g^{-1} = H(R') \text{ for all } R\text{-algebras } R'\} \ .$$

The center $Z(G)$ is an algebraic subgroup of G, and it is commutative by definition. The normalizer $N_G(H)$ is also an algebraic subgroup of G ([Mil22, Prop. 1.83]).

Definition 1.19. An algebraic subgroup H of G is **normal** if $H(R)$ is normal in $G(R)$ for all k-algebras R.

1.1.3 The affine case

Let X be an affine algebraic scheme over k, i.e., $X = \mathrm{Spm}(A)$ for some k-algebra A. Then its ring of functions $\mathcal{O}_X$ is just A, and since X is algebraic, it is finitely generated as a k-algebra, so we have the isomorphism $A \cong k[X_1, \ldots, X_n]/I$. A k-algebra homomorphism $f : k[X_1, \ldots, X_n] \to R$ factors through A if, and only if, the images of the indeterminates $X_1, \ldots, X_n$ is a solution to the polynomial equations of I. Therefore, we have a correspondence between elements of $X(R) = \mathrm{Hom}_k(A, R)$ and solutions in R of the equations in I. If $\varphi : R \to S$ is another k-algebra homomorphism, then the composition $\varphi \circ f$ corresponds to the solution $\{(\varphi \circ f)(X_1), \ldots, (\varphi \circ f)(X_n)\}$ in S of I, making the correspondence natural.

In this context, we say that the k-algebra A **represents** G. If we translate the Yoneda Lemma to this context, we obtain the following:

Theorem 1.20 ("Yoneda's Lemma")**.** Let E and F be affine group schemes represented by A and B, respectively. Natural maps $E \to F$ correspond to k-algebra homomorphisms $A \leftarrow B$.

We note that if $\Phi : E \to F$ and $\Psi : F \to E$ are natural maps such that $\Psi \circ \Phi = \mathrm{id}_E$ and $\Phi \circ \Psi = \mathrm{id}_F$, then the homomorphisms that correspond to them are id_A and id_B, respectively. Thus:

Corollary 1.21. The map $E \to F$ is a natural correspondence if, and only if, the corresponding homomorphism $A \leftarrow B$ is an isomorphism.

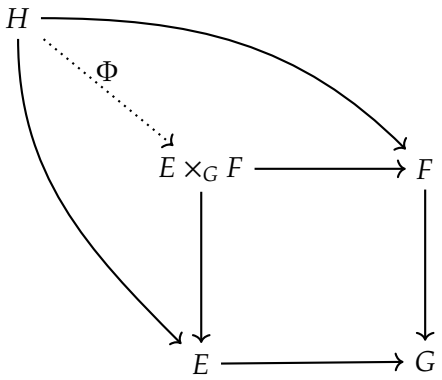
If $X = \mathrm{Spm}(A)$, we say that A **represents** X. It is clear that k represents the trivial algebraic scheme $\{e\} = 1$. Let E and F be algebraic groups. The k-algebra that represents the product $E \times F$ is $A \otimes_k B$. More generally, we can prove the following:

Proposition 1.22. Let E, F, G be algebraic schemes represented by A, B, C respectively, and $\varphi : E \to G$, $\psi : F \to G$ be natural maps. The fiber product $E \times_G F$ defined by

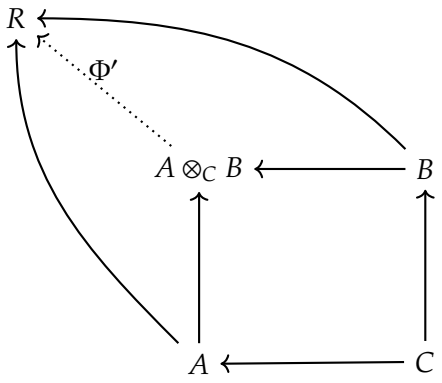
$$(E \times_G F)(R) = \{(e, f) \in E(R) \times F(R) \mid \varphi(e) = \psi(f)\}$$

is represented by $A \otimes_C B$.

Proof. The fiber product is, by definition, the algebraic group that satisfies the pullback:



By Yoneda's lemma, the algebra that represents the fiber product must be the algebra that satisfies the following pushout, and that is exactly $A \otimes_C B$:

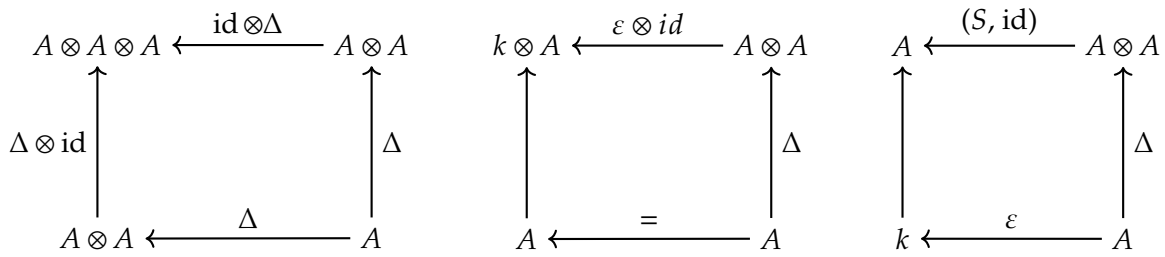


□

Now, let G be an affine algebraic group. The maps on Definition 1.13 that make G into an algebraic group, along with its diagrams, translate to maps between the algebras that represents G and $G \times G$ by Yoneda's Lemma; thus, we obtain homomorphisms

$$\begin{aligned} \Delta &: A \longrightarrow A \otimes A \text{ , called comultiplication,} \\ \varepsilon &: A \longrightarrow k \text{ , called counit,} \\ S &: A \longrightarrow A \text{ , called antipode,} \end{aligned}$$

such that the following diagrams commute:



This motivates the following definition.

Definition 1.23. We say that A is a (commutative) **Hopf algebra** if A is a k-algebra together with homomorphisms Δ, ε and S such that the diagrams above commute.

Note that, if A is such an algebra, it represents the functor $R \rightsquigarrow \mathrm{Hom}_k(A, R)$. Applying Yoneda's Lemma on the maps above gives $\mathrm{Hom}_k(A, -)$ a group structure, or, equivalently, gives $\mathrm{Spm}(A)$ a group structure, thus making $\mathrm{Spm}(A)$ into an (affine) algebraic group. The product on $\mathrm{Spm}(A)$ corresponds, of course, to the comultiplication Δ. Passing from $\mathrm{Spm}(A)$ to A, we get:

Proposition 1.24. Let $g, h \in G = \mathrm{Spm}(A)$. If g and h correspond to homomorphisms $\tilde{g}, \tilde{h} : A \to R$, respectively, then the product gh corresponds to the homomorphism

$$(g, h)\Delta : A \xrightarrow{\Delta} A \otimes A \xrightarrow{(g,h)} R \otimes R \xrightarrow{\text{mult}} R \, .$$

From now on, we shall denote $\tilde{g}$ by just g. Let G and H be affine algebraic groups represented by A and B, respectively. If H is an affine algebraic subgroup of G, then the homomorphism that injects H into A corresponds to a surjective homomorphism $A \to B$, so $B \cong A/I$ for some ideal of I. Since H is a subgroup of G, its product is the restriction of the product on G; thus, we must have

$$\begin{aligned} \Delta(A/I) &\subset A/I \otimes A/I \, , \\ \varepsilon(I) &= 0 \, , \\ S(I) &\subset I \, . \end{aligned}$$

Ideals I satisfying these conditions are called **Hopf ideals**. Equivalently, A/I is a Hopf ideal if A/I represents an affine algebraic subgroup H of G. Indeed, if so, the product on $\mathrm{Spm}(A/I)$ would be well-defined. A natural map $G \to H$ is a homomorphism if, and only if, the corresponding homomorphism $A \leftarrow B$ preserves Δ, ε and S. Such an homomorphism $A \leftarrow B$ is called a **Hopf algebra homomorphism**.

Examples 1.25. (i) The algebraic groups G_a and α_p (the second being well-defined when $\mathrm{char}\, k = p$), represented by $k[X]$ and $k[X]/(X^p)$, respectively, have maps Δ, ε and S defined by

$$\begin{aligned}\Delta(X) &= 1 \otimes X + X \otimes 1 \,,\\ \varepsilon(X) &= 0 \,,\\ S(X) &= -X \,.\end{aligned}$$

The groups G_m and μ_n, represented by $k[X, 1/X]$ and $k[X, 1/X]/(X^n - 1)$, respectively, have maps defined by

$$\begin{aligned}\Delta(X) &= X \otimes X \,,\\ \varepsilon(X) &= 1 \,,\\ S(X) &= 1/X \,.\end{aligned}$$

(ii) Consider the algebraic group GL_n. The algebra that represents it is

$$A = k[X_{11}, X_{12}, \ldots, X_{nn}, 1/\det] \,.$$

The comultiplication mirrors the usual matrix multiplication law:

$$\Delta(X_{ij}) = \sum_{k=1}^{n} X_{ik} \otimes X_{kj} \,,$$

the counit ε must satisfy $(g, \varepsilon)\Delta = g$; then,

$$\varepsilon(X_{ij}) = \delta_{ij} \,,$$

and, finally, the antipode must satisfy $(g, S(g))\Delta = \varepsilon$, so $S(X_{ij})$ is the element at row i and column j of the inverse of the matrix (X_{ij}) multiplied by $1/\det$. For example, if $n = 2$, we have

$$\begin{aligned}S(X_{11}) &= (1/\det)X_{22} \,,\\ S(X_{12}) &= -(1/\det)X_{12} \,,\\ S(X_{21}) &= -(1/\det)X_{21} \,,\\ S(X_{22}) &= (1/\det)X_{11} \,.\end{aligned}$$

By the discussion above, the algebras representing algebraic subgroups of GL_n must also have the same maps Δ, ε and S, although it may be easier to write those maps in those cases. Some of those subgroups are:

(a) The algebraic group SL_n consisting of matrices with det = 1. The algebra that represents it is

$$k[X_{11}, X_{12}, \ldots, X_{nn}]/(\det - 1) .$$

(b) Consider the algebraic group of n-by-n orthogonal matrices O_n. Its Hopf algebra is A/I, where I is the ideal generated by the relations given by $XX^T = I$. It has a subgroup SO_n, consisting of orthogonal matrices with det = 1.

(c) The group of n-by-n triangular matrices T_n is a subgroup of GL_n, and its Hopf algebra is obtained by taking the quotient of A by the ideal generated by elements X_{ij} for $i > j$. Similarly, we have the group U_n of n-by-n unitriangular matrices, and D_n, the group of n-by-n diagonal matrices. Both are subgroups of T_n.

In Section 1.3, we will prove that every affine algebraic group is an algebraic subgroup of GL_n for some n, so understanding GL_n is essential.

(iii) Let Γ be a finite nontrivial group and let $n = |\Gamma|$. There is no k-algebra A such that $\mathrm{Hom}(A, R)$ has exactly n elements for every k-algebra R. Indeed, if $|\mathrm{Hom}(A, R)| = n$, then $\mathrm{Hom}(A, R \times R) = \mathrm{Hom}(A, R) \times \mathrm{Hom}(A, R)$ has cardinality $2n$.

Let $A = k^\Gamma$ be the ring of functions $\Gamma \to k$. For each $\sigma \in \Gamma$, consider the map $e_\sigma \in A$ that takes σ to 1 and all other elements to 0. The set $B = \{e_\sigma\}_{\sigma \in \Gamma}$ is a basis for A as a vector space over k, so it also generates A as a k-algebra. For $\sigma, \tau \in \Gamma$, we have

$$\begin{aligned} e_\sigma^2 &= e_\sigma , \\ \sum e_\sigma &= 1 , \\ e_\sigma e_\tau &= 0 . \end{aligned}$$

Now, let R be a k-algebra such that its only idempotent elements are 0 and 1 (such as a field extension of k). A homomorphism $A \to R$ is defined by its image

on its basis B, and the equations above imply that exactly one element of B is mapped into 1 and all others are mapped into 0. Thus, $\mathrm{Hom}(A, R)$ is isomorphic to Γ as an abstract group. The affine algebraic group $\mathrm{Hom}(A, -)$ is the **constant algebraic group**. The Hopf algebra structure on A is defined by

$$\begin{aligned}\Delta(e_\rho) &= \sum_{\rho=\sigma\tau} e_\sigma e_\tau \ , \\ \varepsilon(e_\sigma) &= 1 \text{ if } \sigma \text{ is the unit, and 0 otherwise} \ , \\ S(e_\sigma) &= e_{\sigma^{-1}} \ .\end{aligned}$$

We take a moment to remark on the power of Yoneda's Lemma to translate the language of affine algebraic groups into that of Hopf algebras. We can further play with properties of those groups to derive Hopf algebra identities, and vice-versa. We offer the following easy examples:

Examples 1.26. (i) Let G be a commutative algebraic group. By definition, this means that $\mathrm{mult} \circ t = \mathrm{mult}$, so by the Yoneda Lemma, we have $T \circ \Delta = \Delta$, where T corresponds to the transposition t and sends each $a_i \otimes b_i$ to $b_i \otimes a_i$. If $\Delta(a) = \sum a_i \otimes b_i$, then

$$\sum a_i \otimes b_i = T\left(\sum a_i \otimes b_i\right) = \sum b_i \otimes a_i \ .$$

(ii) ([Wat79, Sec. 1, Exer. 10]) We know that $\mathrm{inv} \circ \mathrm{mult} = \mathrm{mult} \circ (\mathrm{inv}, \mathrm{inv})$, so the equality

$$\Delta \circ S = (S \otimes S) \circ \Delta$$

must hold.

1.1.4 Scalar extension and restriction

Let K/k be a field extension.

Definition 1.27. (i) If G is an algebraic group over k, the algebraic scheme G_K extending G such that

$$G_K(R) = G(R)$$

for every K-algebra R is an algebraic group over K, said to have been obtained from G by extension of scalars.

(ii) If G is an algebraic group over K, we define the **Weil restriction** of G to k as the algebraic group $G_{K/k}$ defined by the functor.

$$(G)_{K/k}(R) = G(K \otimes_k R) .$$

By definition, it is clear that $G_{K/k}(k) = G(K)$. The elements of $G_{K/k}(K)$ are the elements of $G(K \otimes_k K)$, but note that $K \otimes_k \otimes K$ is not K; in fact, it may not even be a field: consider the non-zero element $x = (i \otimes i)$ in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Its square is $x^2 = (-1 \otimes -1) = 1$, so we have

$$(x + 1)(x - 1) = x^2 - 1 = 0 .$$

Proposition 1.28 ([Mil22, p. 2.61])**.** Let K be a finite Galois extension of k and G be an algebraic group over K. We have

$$(R_{K/k}(G))_K \cong \prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma G ,$$

where σG corresponds to the algebraic group G twisted by σ.

Proof. Let R be a K-algebra. We have

$$\begin{aligned} R_{K/k}(G)_K(R) &= G(K \otimes_k R) \\ &= G(K \otimes_k K \otimes_K R) = R_{K\otimes K/K}(G_K)(R) , \end{aligned}$$

since $K \otimes_k R = K \otimes_k K \otimes_K R$, so

$$R_{K/k}(G) = R_{K\otimes K/K}(G_K) .$$

Writing $K \otimes_k K = \prod_{\sigma \in Gal(K/k)} K$ (as will be done in Subsection 2.4.1), we have

$$\begin{aligned} G_{K\otimes K/K}(R) &= G(K \otimes K \otimes_K R) \\ &= G((\prod_{\sigma \in \mathrm{Gal}(K/k)} K) \otimes_K R) \\ &= G(\prod_{\sigma \in \mathrm{Gal}(K/k)} (K \otimes_K R)) \\ &= \prod_{\sigma \in \mathrm{Gal}(K/k)} G(K \otimes_K R) \\ &= \prod_{\sigma \in \mathrm{Gal}(K/k)} (\sigma G)(R) . \end{aligned}$$

Note that $K \otimes_K R$ is not just R; it is R with the K-action "twisted" by the automorphism $\sigma : K \to K$. We conclude that

$$R_{K\otimes K/K}(G_K) = \prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma G \ ,$$

and the proposition follows. □

The previous proposition gives us a way to recover the k-structure of a restriction $R_{K/k}(G)$. Since its extension to K is equal to $\prod_{\sigma\in\mathrm{Gal}(K/k)} \sigma G$, the invariant elements under the Galois action of $\mathrm{Gal}(K/k)$ are just G.

Corollary 1.29. The k-structure of $R_{K/k}(G)$ is recovered by the invariant elements under the action of the Galois group $\mathrm{Gal}(K/k)$.

1.1.5 Kernels, quotient maps and exact sequences

Definition 1.30. Let $\varphi : G \to H$ be a homomorphism of algebraic groups. We define $\mathrm{Ker}(\varphi)$ as the functor

$$R \rightsquigarrow \mathrm{Ker}(\varphi_R) \ ,$$

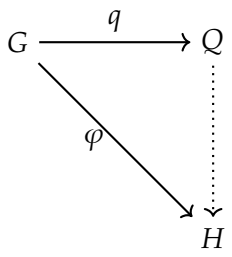
where $\varphi_R : G(R) \to H(R)$ is induced by φ.

Recall that Proposition 1.8 says that a map $G \to Q$ is faithfully flat if, and only if, it is surjective when viewed as a map $|G| \to |Q|$ of the underlying topological spaces, and, for all $y \in |Y|$, the map $\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$ is a flat homomorphism.

Definition 1.31. Let $q : G \to Q$ be a homomorphism of algebraic groups. Then q is called a **quotient map** if it is faithfully flat.

For affine algebraic groups, however, there is a easier way to detect faithfully flatness. If G and Q are represented by A and B, respectively, an homomorphism $G \to Q$ is faithfully flat if, and only if, the corresponding homomorphism $A \leftarrow B$ is injective (see [Wat79, Sec. 15.1]).

Proposition 1.32. Let $q : G \to Q$ be a quotient map of algebraic groups and let N be the kernel. Every homomorphism $\varphi : G \to H$ whose kernel contains N factors uniquely through q:



Proof. Let D be defined as the functor

$$R \rightsquigarrow q(g(R)) = G(R)/N(R) .$$

It is fat in $\tilde{Q}$ and, since N is in the kernel of φ, it factors through D. By Proposition 1.10, it extends to a map $Q \to H$ such that the diagram commutes. □

If $q' : G \to Q'$ is another quotient map with kernel N, then using the universal property of Proposition 1.32 for both q and q', we obtain homomorphisms $Q \to Q'$ and $Q' \to Q$ that are the inverse of one another. So, $Q \cong Q'$. Then, the kernel N uniquely determines (up to isomorphism) the group Q, therefore we define the **quotient** G/N as Q.

Examples 1.33. (i) Let $q : \mathrm{G}_m \to \mathrm{G}_m$ be the map defined by $x \to x^n$ for a positive integer n. Then, $\operatorname{Ker} q = \mu_n$. The corresponding Hopf algebra homomorphism $k[X, 1/X] \to k[X, 1/X]$ is just

$$X \mapsto X^n ,$$

which is injective, so q is faithfully flat. Thus, $\mathrm{G}_m/\mu_n = \mathrm{G}_m$.

We note that the map $q_R : \mathrm{G}_m(R) \to \mathrm{G}_m(R)$ is not always surjective: if $R = \mathbb{R}$ and n is even then the negative numbers are not in the image of q_R.

(iii) Consider the map $\det : \mathrm{GL}_n \to \mathrm{G}_m$. Its corresponding Hopf algebra homomorphism is

$$k[X, 1/X] \to k[X_{11}, \ldots, X_{nn}, 1/\det]$$

defined by $X \mapsto \det(X_{11}, \ldots, X_{nn})$, the polynomial that defines the determinant. Since both X and $1/\det$ are invertible in its respective algebras, the map is well-defined. It is injective, so det is faithfully flat, and thus a quotient map. The kernel of det is exactly SL_n, so $\mathrm{GL}_n/\mathrm{SL}_n = \mathrm{G}_m$.

(ii) Let $\operatorname{char} k \neq 2$. Consider the map $\det : \mathrm{O}_2 \to C_2$, where C_2 is the constant algebraic group associated to the group of two elements. The algebra $A = k \times k$

that represents C_2 is isomorphic to $k[X]/(X^2)$, and we can see from Examples 1.25 that they are actually isomorphic as Hopf algebras. Then, the map corresponding to det is

$$\begin{aligned} k[X]/(X^2-1) &\to k[X_{11}, X_{12}, X_{21}, X_{22}]/I \\ X &\mapsto \det , \end{aligned}$$

where I is the ideal generated by the formulas obtained from $XX^t = I$. Those formulas imply that $\det^2 = 1$, so the Hopf algebra homomorphism is well-defined. The kernel det is SO_n, so $\mathrm{O}_2/\mathrm{SO}_2 = C_2 = \mu_2$.

A natural question is: given a normal subgroup of G, is there a group Q and a quotient map $G \to Q$ such that N is its kernel? In other words, does the group G/N exists for any normal subgroup N of G? The answer is affirmative:

Proposition 1.34 ([Mil22, Appendix B])**.** Let N be a normal subgroup of G. There exists an algebraic group Q together with a quotient map $q : G \to Q$ such that N is the kernel of q.

Example 1.35. Consider $G = \mathrm{GL}_n$. Since the center $Z(G)$ is a normal subgroup of G, then the previous proposition implies that there exists a quotient $G/Z(G)$. We define it as PGL_n.

The **derived subgroup** is defined as the intersection of the normal algebraic subgroups N of G such that G/N is commutative. We will use it in section 1.4 to define solvable algebraic groups and calculate some examples. For now, we will consider some properties of the derived subgroup.

Proposition 1.36. The group G/DG is commutative.

Proof. We know that algebraic groups satisfies the descending chain condition with respect to its algebraic subgroups, so $DG = N_1 \cap \ldots \cap N_m$. The map

$$G \to G/N_1 \times \ldots \times G/N_m$$

has exactly DG as its kernel, and, since each G/N_i is commutative, so is G/DG. □

Definition 1.37. Let N, G and Q be algebraic groups. We say that the sequence

$$1 \to N \xrightarrow{\iota} G \xrightarrow{q} Q$$

is exact if ι is injective and $\operatorname{Ker} q = \operatorname{Im} \iota$. Furthermore, the sequence

$$1 \to N \xrightarrow{\iota} G \xrightarrow{q} Q \to 1$$

is exact if, in addition, q is a faithfully flat map.

Examples 1.38. (i) The map $x \mapsto x^p$ induces the exact sequence

$$1 \to \mu_p \to \mathrm{G}_m \to \mathrm{G}_m \to 1 \,.$$

(ii) Both the sequences

$$1 \to \mathrm{SL}_n \to \mathrm{GL}_n \to \mathrm{G}_m \to 1 \,,$$

and, when $\operatorname{char} k \neq 2$,

$$1 \to \mathrm{SO}_2 \to \mathrm{O}_n \to \mu_2 \to 1 \,,$$

are exact (see the previous examples). When $\operatorname{char} k = 2$, then $\mathrm{SO}_2 = \mathrm{O}_2$.

1.2 Connectedness and smoothness

1.2.1 Connectedness

Let G be an algebraic scheme. We review some facts from algebraic geometry (see Subsection 1.1 and [Mil22, Sec. 1.b]). The algebraic scheme $\pi_0(G)$ was defined as $\operatorname{Spm}(\pi(G))$, where $\pi(G)$ is the largest étale subalgebra of $\mathcal{O}_G$. There is a canonical map

$$G \to \pi_0(G) \,,$$

and its fibers are the connected components of G.

If G is an algebraic group, then G^0, the connected component of the identity, and $\pi_0(G)$ are also groups, and the sequence

$$1 \to G^0 \to G \to \pi_0(G) \to 1$$

is exact. Also, the following conditions are equivalent (Proposition 1.7):

(i) G is irreducible.

(ii) G is connected.

(iii) G is geometrically connected. And, when G is affine, these are equivalent to:

(iv) The ring $\mathcal{O}_G$ modulo is nilradical is an integral domain.

Item (iv) is specially useful to prove the connectivity of some examples.

Examples 1.39. (i) The ring of functions of G_a and G_m are $k[X]$ and $k[X, 1/X]$, respectively, and both are integral domains since k is a field. Thus, both are connected.

(ii) Let $\operatorname{char} k = p$. The algebraic group α_p is represented by $A = k[X]/(X^p)$. Although A is not an integral domain, the quotient of A by its nilradical is just the field k, so α_p is connected.

(iii) Let $\operatorname{char} k = 2$. The algebraic group μ_2 is not connected. Indeed, its Hopf algebra is $A = k[X]/(X^2 - 1)$, and we have

$$(X + 1)(X - 1) = X^2 - 1 = 0 \,,$$

So A modulo its nilradical, which is A, is not an integral domain.

(iv) The algebraic group D_n of diagonal matrices is isomorphic to $\mathrm{G}_m \times \cdots \times \mathrm{G}_m$, and its Hopf algebra is

$$k[X_1, \ldots, X_n, 1/X_1, \ldots, 1/X_n] \,,$$

which is clearly an integral domain. Thus, D_n is connected.

(v) The algebraic group SL_n is connected.

Proposition 1.40 ([Mil22, 1.b])**.** Let

$$1 \to N \to G \to Q \to 1$$

be an exact sequence of algebraic groups. The sequence

$$\pi_0(N) \to \pi_0(G) \to \pi_0(Q) \to 1$$

of algebraic groups is exact.

The following corollary is immediate:

Corollary 1.41. Let

$$1 \to N \to G \to Q \to 1$$

be an exact sequence of algebraic groups.

(i) If N and Q are connected, then G is connected.

(ii) If G is connected, then Q is connected.

Examples 1.42. (i) O_n is connected if and only if $\mathrm{char}(k) = 2$. Indeed, if $\mathrm{char}(k) = 2$ then $\mathrm{O}_n = \mathrm{SO}_n$, which is connected, and if $\mathrm{char}(k) \neq 2$, we have the exact sequence

$$1 \to \mathrm{SO}_n \to \mathrm{O}_n \to \mu_2 \to 1 \,.$$

The fact that μ_2 is not connected implies that O_n is not connected.

(ii) In the exact sequence

$$1 \to \mathrm{SL}_n \to \mathrm{GL}_n \to \mathrm{G}_m \to 1 \,,$$

both SL_n and G_m are connected, so GL_n is connected. This means that its Hopf algebra A is an integral domain. The Hopf algebra representing the algebraic group of triangular matrices T_n is A/I, where I is the ideal generated by X_{ij} for $i > j$. The algebra A/I is also an integral domain, and that implies that T_n is also connected.

1.2.2 Smoothness

Definition 1.43. Let X be an algebraic scheme over k and let $x \in |X|$. The tangent space at x is defined as $T_x = \mathrm{Hom}_k(m_x/m_x^2, k)$, where m_x is the maximal ideal of the local ring $\mathcal{O}_{X,x}$. When $\dim T_x(X)$ is equal to the **Krull dimension** of $\mathcal{O}_{X,x}$ (see [Mil22, A.g]), we say that X is at x. If X is smooth at every point x, then we say that X is smooth.

An algebraic scheme X is **reduced** if the local rings $\mathcal{O}_{X,x}$ are reduced as k-algebras for every $x \in |X|$, and it is **geometrically reduced** if the extension $X_{\overline{k}}$ is reduced. If X is affine, then $X = \mathrm{Spm}(A)$ is reduced if, and only if, A is reduced.

We say that an algebraic scheme X defined over k is **homogeneous** if its group of automorphisms is transitive on $|X|$. One notable characteristic of algebraic groups is that, over an algebraically closed field $\overline{k}$, it is always homogeneous. Indeed, the left translation map $L_g : x \mapsto gx$ is an isomorphism, since its inverse is $L_{g^{-1}}$, and it acts transitively on $G(\overline{k})$, which is equal to $|X|$ if the field is algebraically closed. This has a striking implication on the smoothness of an algebraic group:

Proposition 1.44. Let G be an algebraic group over a field k. The following are equivalent:

(i) G is smooth.

(ii) G is smooth at the identity e.

(iii) G is geometrically reduced.

Proof. (i) $\Leftrightarrow$ (ii): If e is smooth on G, then it is smooth on $G_{\overline{k}}$. By homogeneity, for any point x in $G_{\overline{k}}$ we have an isomorphism that sends e to x, thus x is smooth on $G_{\overline{k}}$. We conclude that G is smooth.

(i) $\Leftrightarrow$ (iii): Smooth algebraic groups are always geometrically reduced. On the other hand, if G is geometrically reduced, then $G_{\overline{k}}$ is an algebraic variety, and thus G is smooth in at least some point (see [Mil22, A.55]). The previous equivalence shows that G is smooth. □

If k is a perfect field, then every reduced algebraic scheme over k is geometrically reduced (see [Mil22, A.43]). This implies the following proposition:

Proposition 1.45. Let G be an algebraic group over a perfect field k. If G is reduced, then it is geometrically reduced.

The above proposition shows that a connected affine algebraic group over a perfect field k is smooth if, and only if, it is reduced.

Example 1.46. Let us consider α_p with $\mathrm{char}(k) = p$, represented by $k[X]/(X^p)$. It is not reduced since X is nilpotent, so it is not smooth.

A theorem by Cartier says that Hopf algebras over fields of characteristic 0 are reduced ([Wat79, Sec. 11.4]). Thus, we have:

Proposition 1.47. Affine algebraic groups over a field of characteristic 0 are smooth.

Examples 1.48. (i) The algebraic groups G_a and G_m are reduced, since their ring of functions, $k[X]$ and $k[X, 1/X]$, respectively, are reduced as k-algebras.

(ii) The algebraic group SL_n is smooth.

(iii) When $\mathrm{char}\, k \neq 2$, the algebraic group SO_n is smooth.

An important fact is that extensions of smooth algebraic groups are smooth.

Proposition 1.49 ([Mil22, Prop. 1.62])**.** Let

$$1 \to N \to G \to Q \to 1$$

be an exact sequence of algebraic groups. We have:

(i) If N and Q are smooth, then G is smooth.

(ii) If G is smooth, then Q is smooth.

Example 1.50. Consider the exact sequence

$$1 \to \mathrm{SL}_n \to \mathrm{GL}_n \to \mathrm{G}_m \to 1 \,.$$

Since SL_n and G_m are smooth, then GL_n is smooth by the previous proposition.

Definition 1.51. Let G be a smooth algebraic group. We define the **dimension** of G as the dimension of the tangent space $T_1(G)$, denoted by $\dim G$.

We can use the tangent space to test if a smooth algebraic subgroup is proper:

Proposition 1.52 ([Mil22, Prop. 10.15])**.** Let $H \subset G$ be algebraic groups such that $\mathrm{T}_1(H) = \mathrm{T}_1(G)$. If H is smooth and G is connected, then $H = G$.

Consequently, if H is a proper smooth algebraic subgroup of G, then $\dim H < \dim G$.

1.3 Actions, comodules and linear algebraic groups

In this section, we aim to prove two main results: first, a correspondence between comodules and linear representations; and, second, that every affine algebraic group is a subgroup of GL_n. We begin with some basic definitions.

Definition 1.53. Let G be an algebraic group and X be a functor. An **action** of G on X is a natural map $G \times X \to X$ such that the maps $G(R) \times X(R) \to X(R)$ are group actions for every k-algebra R.

Let V be a vector space over k. If X is the functor that assigns to each k-algebra R the R-module $X(R) = V \otimes R$, then the functor GL_V defined by

$$R \rightsquigarrow \mathrm{Aut}_R(V \otimes R)$$

acts naturally on X. If $\dim V = n$, then $\mathrm{GL}_V = \mathrm{GL}_n$. In this case, a **linear representation** of an algebraic group G is a homomorphism $G \to \mathrm{GL}_V$ for some V. If $G(R) \to \mathrm{GL}_V(R)$ is injective for every k-algebra R, then we say that the representation is **faithful**, and that G is a **linear algebraic group**.

Examples 1.54. (i) Let V be a vector space of dimension n. A **flag** F_0 of V is a sequence of vector spaces

$$F_0 : V = V_r \supset V_{r-1} \supset \cdots \supset V_1 \supset V_0 = 0$$

in which $\dim V_i = i$. Now, extending a k-algebra R, each factor $V_i \otimes R$ is a free R-module of rank i. Consider the functor F that assigns to each k-algebra R the set $F(R)$ of sequences of (free) R-modules

$$V \otimes R = F_r \supset F_{r-1} \supset \cdots \supset F_1 \supset F_0 = 0$$

such that $\operatorname{rank} F_i = i$. The algebraic group GL_V acts naturally on F. In fact, F is a variety represented by GL_V/B, where B is the subgroup of GL_V that fixes F; this holds because the functor $R \rightsquigarrow (\mathrm{GL}_V)(R)/B(R)$ is a fat (Proposition 1.10) subfunctor of both F and GL_V/B. Such varieties are called **flag varieties**.

(ii) Consider the map $\mathrm{G}_a \to \mathrm{GL}_2$ defined by

$$x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

It is a faithful representation of G_a. It corresponds to a k-algebra homomorphism

$$k[X_{11}, X_{12}, X_{21}, X_{22}, 1/\det] \to k[X]$$

that sends X_{11} and X_{22} to 1, X_{21} to 0 and X_{12} to X.

(iii) The map $(G_m)^n \to \mathrm{GL}_n$ that sends $(x_1, \ldots, x_n)$ to a diagonal matrix A such that $a_{ii} = x_i$ is a faithful representation of $(G_m)^n$, and this map corresponds to a k-algebra homomorphism

$$k[X_{11}, \ldots, x_{nn}, 1/\det] \to k[Y_1, \ldots, Y_n, 1/Y_1, \ldots, 1/Y_n]$$

that sends X_{ij} to Y_i if $i = j$ and to 0 otherwise.

Let G be an affine algebraic group represented by A.

Definition 1.55. An A-comodule is a k-vector space V together with a linear map $\rho : V \to V \otimes A$ such that the diagrams

$$\begin{array}{ccc} V & \xrightarrow{\rho} & V \otimes A \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle \mathrm{id}\otimes\Delta} \\ V \otimes A & \xrightarrow{\rho\otimes\mathrm{id}} & V \otimes A \otimes A \end{array} \qquad \begin{array}{ccc} V & \xrightarrow{\rho} & V \otimes A \\ {\scriptstyle\mathrm{id}}\downarrow & & \downarrow{\scriptstyle \mathrm{id}\otimes\varepsilon} \\ V & \longrightarrow & V \otimes k \end{array}$$

commute. If W is a submodule of V such that $\rho(W) \subset W \otimes A$, then we say W is a **subcomodule** of V.

Let us shed some light on this definition. An abstract group action is a map $\Phi : G \times X \to X$ satisfying the following conditions:

$$\begin{aligned} \Phi(g_1 g_2, x) &= \Phi(g1, \Phi(g2, x)) \,, \\ \Phi(1, x) &= x \,. \end{aligned}$$

Looking at the above diagrams, we see that they express exactly that, though with arrows reversed. Our comodules are simply the Hopf algebraic analogues of linear representations. Of course, the conditions above are for group actions, but the fact that the maps ρ and Δ in the definition are k-linear will suffice to establish the correspondence we need. Thus, we arrive at the following theorem:

Theorem 1.56 ([Wat79, Sec. 3.2])**.** Let G be an affine algebraic group represented by A. Then the linear representations of G on V correspond to comodules $\rho : V \to V \otimes A$.

Proof. Let (V, r) be a linear representation of G. The image in $\mathrm{GL}_V(A)$ of the identity element of $G(A)$ is an A-linear map $V \otimes A \to \otimes V \otimes A$. We define $\rho : V \to V \otimes A$ as its restriction to $V \otimes k \cong V$. Since the action is a natural map, the diagram

$$\begin{array}{ccc} V \otimes A & \xrightarrow{r(\mathrm{id})} & V \otimes A \\ {\scriptstyle\mathrm{id}\otimes g}\downarrow & & \downarrow{\scriptstyle \mathrm{id}\otimes g} \\ V \otimes R & \xrightarrow{r(g)} & V \otimes R \end{array}$$

commutes for $g \in G(R)$ corresponding to a homomorphism $A \to R$. If $v \otimes 1 \in V \otimes R$, we have $(r(g))(v) = ((\mathrm{id} \otimes g) \circ r(\mathrm{id}))(v) = ((\mathrm{id} \otimes g) \circ \rho)(v)$, so r is determined by ρ.

Now let (V, ρ) be a comodule. If $g \in G(R)$, we define $r_R(g) : V \otimes R \to V \otimes R$ as following: on V, we have the map

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{\mathrm{id} \otimes g} V \otimes R \ ,$$

and we extend it to a R-linear map $V \otimes R \to V \otimes R$. Thus, the map $\Phi : G \times X \to X$ defined by

$$\begin{aligned} \Phi_R : (G \times X)(R) &\to X(R) \\ (g, v) &\mapsto (r(g))(v) \end{aligned}$$

is a natural transformation. We want to prove that Φ is a linear action, that is, we still need to prove that $r_R(\mathrm{id}) = \mathrm{id}$ and that $r_R(gh) = r_R(g)r(h)$.

The element $r_R(\mathrm{id})$ is defined by the composition

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{id \otimes \varepsilon} V \otimes k \subset V \otimes R \ ,$$

but the second diagram in the comodule definition says that this composition is just the identity.

Let g, h correspond to maps $A \to R$. The map corresponding to the product is $(g, h)\Delta : A \to R$, so $r(gh)$ is defined by the map

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{\mathrm{id} \otimes \Delta} V \otimes A \otimes A \xrightarrow{\mathrm{id} \otimes g \otimes h} V \otimes R \otimes R \ ,$$

and $r(g)r(h)$, after some ordering of the compositions, is defined by

$$V \xrightarrow{\rho} V \otimes A \xrightarrow{\rho \otimes \mathrm{id}} V \otimes A \otimes A \xrightarrow{\mathrm{id} \otimes g \otimes h} V \otimes R \otimes R \ .$$

Since the first diagram in the comodule definition commutes, those two maps are the same. □

A subspace W of an A-comodule V is a **subcomodule** if $\rho(W) \subset W \otimes R$ for every k-algebra R.

Proposition 1.57. Let (U, ρ) and (V, σ) be A-comodules. The following holds:

(i) $U \oplus V$ is an A-comodule.

(ii) $U \otimes V$ is an A-comodule.

(iii) Let $\{v_j\}$ be a basis for V and suppose $\dim V = n$. Write $\rho(v_j) = \sum_i v_j \otimes a_{ij}$. Then

$$\Delta(a_{ij}) = \sum_k a_{ik} \otimes a_{kj} \ .$$

Proof. The map

$$U \oplus V \xrightarrow{(\rho,\sigma)} (U \otimes A) \oplus (V \otimes A) \cong (U \oplus V) \otimes A$$

turns $(U \oplus V)$ into an A-comodule, and the map

$$U \otimes V \xrightarrow{\rho\otimes\sigma} U \otimes A \otimes V \otimes A \cong U \otimes V \otimes A \otimes A \xrightarrow{id\otimes id\otimes \mathrm{mult}} U \otimes V \otimes A$$

turns $(U \otimes V)$ into an A-comodule, thus (i) and (ii) hold.

Now, if (V, r) is a linear representation of G, then we have a map $\Psi : B \to A$, where A represents G and B represents $\mathrm{GL}_V \cong \mathrm{GL}_n$. The action of G on V comes from an action of GL_V on V, so the comodule (V, ρ) corresponding to (V, r) comes from a comodule (V, λ) associated with GL_n. Thus, ρ is decomposed as

$$V \xrightarrow{\lambda} V \otimes B \xrightarrow{\mathrm{id}\otimes\Psi} V \otimes A \ .$$

Thus, the elements a_{ij} are the image of $X_{ij} \in B$, and (iii) follows from the equality

$$\Delta(X_{ij}) = \sum_k X_{ij} \otimes X_{jk} \ .$$

□

Examples 1.58. (i) The space $V = A$ with $\rho = \Delta$ clearly satisfies the comodule definition. It is called the **regular representation** of G.

(ii) Consider the example (ii) of Examples 1.54. Fixing the canonical basis $\{e_1, e_2\}$, the map $\rho : V \to V \otimes A$ satisfies

$$\rho(e_1) = e_1 \otimes 1, \ \rho(e_2) = e_1 \otimes X + e_2 \otimes 1 \ ,$$

and so, by the previous proposition,

$$\Delta(1) = \Delta(a_{11}) = 1 \otimes 1 + X \otimes 0 = 1 \ ,$$

and

$$\Delta(X) = \Delta(a_{12}) = a_{11} \otimes a_{12} + a_{12} \otimes a_{22} = 1 \otimes X + X \otimes 1 \ ,$$

as expected.

(iii) Looking now at example (iii) of Examples 1.54, and fixing the canonical basis $\{e_1, \dots, e_n\}$, we have

$$\rho(e_i) = e_i \otimes a_{ii} = e_i \otimes Y_i \ ,$$

and by the previous proposition, the fact that $a_{ij} = 0$ for $i \neq j$ implies

$$\Delta(X_i) = \Delta(a_{ii}) = \sum_k a_{ik} \otimes a_{kj} = X_i \otimes X_i \ ,$$

as expected.

We prove now that every affine algebraic group G admits a faithful representation.

Theorem 1.59 ([Wat79, Sec. 3.4])**.** Every affine algebraic group G is an algebraic subgroup of some GL_n.

Proof. Let V be a finite dimensional comodule contaning generators $v_1, \dots, v_n$ of A, with $\rho = \Delta$. If $\Delta(v_j) = \sum_i b_i \otimes c_i$, we can write every b_i as a linear combination of this basis and, after some reindexing, write

$$\Delta(v_j) = \sum_i v_i \otimes a_{ij} \ .$$

Now consider $\mathrm{GL}(V) = \mathrm{GL}_n$. The action $G \to \mathrm{GL}_n$ corresponds (by Theorem 1.56) to the homomorphism $k[X_{11}, \dots, X_{nn}] \to A$, and the elements a_{ij} are in the image. By definition, we know that

$$v_j = (\varepsilon \otimes \mathrm{id})(\rho(v_j)) = \sum_i \varepsilon(v_j) a_{ij} \ ,$$

that is, all v_j are linear combination of the a_{ij}. But that implies that all of V is in the image, thus G is embedded in GL_n. □

We remind ourselves of a basic group theory fact: every finite group is a subgroup of some permutation group S_n, and S_n can be embedded in $\mathrm{GL}_n(k)$. In a sense, the previous theorem is the analogue for algebraic groups.

We end the present section stating another useful theorem.

Theorem 1.60 ([Mil22, Th. 4.14])**.** Let (V, ρ) be a faithful representation of G. Then every finite-dimensional representation W of G can be constructed from V by forming tensor products, direct sums, duals, and subquotients.

1.4 Solvable and unipotent algebraic groups

1.4.1 Solvable groups

Let G be an algebraic group. Recall the definition of the derived subgroup DG from Subsection 1.2: it is the intersection of all the normal subgroups N such that G/N is commutative. We say that G is **solvable** if it satisfies the following equivalent conditions:

Proposition 1.61. (i) There exists a **subnormal series**

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$$

such that each quotient G_i/G_{i+1} is commutative. Such a series is called a **solvable series** for G.

(ii) There exists an integer n such that $D^n G = 1$.

Proof. If (i) holds, G_i/G_{i+1} being commutative means that $D^{i+1}G \subset G_{i+1}$, so $D^n G = 1$. On the other hand, if (ii) holds, the derived groups forms a subnormal series such that each $D^i G/D^{i+1}G$ is commutative. □

Proposition 1.62. Consider the exact sequence

$$1 \to N \to G \to Q \to 1\,.$$

The following holds:

(i) If G is solvable, then N and Q are solvable.

(ii) If N and Q are solvable, then G is solvable.

Proof. The obvious argument works here too. Suppose G solvable and consider a solvable series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$$

for G. Its intersection with N is a solvable series for N, since $(N \cap G_i)/(N \cap G_{i+1})$ is isomorphic to a subgroup of G_i/G_{i+1}, and its image in Q is also a solvable series for Q.

Now suppose N and Q are solvable, and take a solvable series for each:

$$N = N_0 \supset N_1 \supset \cdots \supset N_m = 1 \,,$$
$$Q = Q_0 \supset Q_1 \supset \cdots \supset Q_k = 1 \,.$$

Letting Q_i' be the inverse image of Q_i in G (see Subsection 1.2), we construct a solvable series for G:

$$G = Q_0' \supset Q_1 \supset \cdots \supset Q_k' = N_0 \supset N_1 \supset \cdots \supset N_m = 1 \,.$$

□

Examples 1.63. (i) All commutative algebraic groups, such as G_a, G_m, μ_n and α_p, are solvable.

(ii) Let T_n be the group of matrices of the form

$$\begin{pmatrix} * & * & * & \cdots & * \\ 0 & * & * & \cdots & * \\ 0 & 0 & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & * \end{pmatrix}.$$

The map $\mathrm{T}_n \to \mathrm{D}_n = \mathrm{G}_m \times \cdots \mathrm{G}_m$ that projects the diagonal is a homomorphism of algebraic groups such that its kernel is the group of unipotent matrices U_n (see Example 1.68). Since both U_n and D_n are solvable (see Examples 1.66) and D_n is normal, then T_n also is.

The two following propositions give us conditions on the solvability of G.

Proposition 1.64. Let G be affine or smooth and K be a field extension of k. Then G is solvable if, and only if, G_K is solvable.

Proof. A subnormal series of G is a solvable series if, and only if, the subnormal series of G_K consisting of the extension of its terms is also a solvable series 1.61. □

Proposition 1.65. Let G be a smooth connected group over $\overline{k}$. Then G is solvable if, and only if, $G(\overline{k})$ is solvable.

Proof. If G is solvable, then it is clear that $G(\overline{k})$ is solvable. The converse holds since the hypothesis implies that $G(\overline{k})$ is schematically dense in G. □

Examples 1.66. (i) We know that the abstract group $\mathrm{SL}_n(\overline{k})$ is not solvable for $n \geq 2$, thus SL_n is not solvable as an algebraic group.

(ii) A **torus** is an algebraic group over k such that it becomes isomorphic to a product of G_m over a finite separable extension of k. Thus, Proposition 1.64 implies that a torus is solvable.

(iii) Consider the abstract group $\mathrm{U}_n(\overline{k})$ of n-by-n unitriangular matrices (i.e. upper triangular matrices with 1 on the main diagonal). The corresponding algebraic group U_n is smooth and connected over $\overline{k}$, so Proposition 1.65 says that it is solvable.

Remark. Let H_1 and H_2 be algebraic subgroups of G. It is possible to define the commutator subgroup $[H_1, H_2]$ of G ([Mil22, Sec. 6.d]). We say that G is **nilpotent** if it admits a subnormal series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$$

such that $[G, G_i] \subset G_{i+1}$. It is immediate that a nilpotent algebraic group is also solvable.

1.4.2 Unipotent groups

We motivate the definition of unipotent algebraic groups by first considering the abstract case. Let $G \subset \mathrm{GL}(V)$ be an abstract group where V is a finite dimensional k-vector space. We say that G is **unipotent** if one of the following equivalent conditions holds:

(i) For every $g \in G$, $(g - 1)$ is nilpotent.

(ii) For every $g \in G$, every eigenvalue of $(g - 1)$ is 0.

(ii') For every $g \in G$, every eigenvalue of g is 1.

(iii) There exists a basis for V such that $G \subset \mathrm{U}_n(k)$.

(iv) Every linear representation of G is unipotent.

Our most important example is the algebraic group U_n such that $\mathrm{U}_n(R)$ is the multiplicative group of upper triangular matrices with entries in R and 1s on the diagonal, that is, matrices of the form

$$\begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

we shall say more about it after the next proposition. Let G be an affine algebraic group. If (V, ρ) is a linear representation of G, we say that ρ is **unipotent** if there exists a basis for V such that $\rho(G)$ is an algebraic subgroup of U_n.

Proposition 1.67. A linear representation (V, r) of G is unipotent if, and only if, there exists a flag

$$V = V_n \supset V_{n-1} \supset \cdots \supset V_1 \supset V_0 = 0\,.$$

such that $(g-1)V_{i+1} \subset V_i$ for all $g \in G$.

Proof. If (V, r) is unipotent, the proposition follows from the fact that such a flag exists for U_n (see example below) and that $r(G)$ is isomorphic to an subgroup of it.

For the converse, we choose a basis for every V_i such that the basis for V_{i+1} is contained in the basis for V_i. It is clear that, in this basis, $\rho(G)$ is an algebraic subgroup of U_n. □

Example 1.68. Let us consider again U_n. Let $V = k^n$ be a k-vector space and denote by e_i the vector with 1 on the i-th position and 0 everywhere else. Let G act on V by matrix multiplication and consider $V_i = \langle e_1, e_2, \ldots, e_i \rangle$. It forms a flag

$$V = V_n \supset V_{n-1} \supset \cdots \supset V_1 \supset V_0 \ = 0$$

and, if U_n acts on V by matrix multiplication, then we have $(g-1)e_1 = 0$, $(g-1)e_2 = \lambda e_1$ and, more generally,

$$(g-1)e_{i+1} \subset V_i\,.$$

Then, the representation (V, ι), in which ι is the inclusion of U_n in GL_n, satisfies Proposition 1.67. Now, let us consider the subgroups B_i defined by

$$B_i(R) = \{g \in G(R) \mid (g-1)(V_j \otimes R) \subset V_{i+j} \otimes R\}\,.$$

By definition, $B_1 = \mathrm{U}_n$ and $B_n = 1$. The elements of $B_i(R)$ are exactly the matrices $g \in \mathrm{U}_n(R)$ such that the columns $1, \ldots, i-1$ of $g-1$ are all zeroes. To prove that U_n is nilpotent, it suffices to prove that $[B_1, B_j] \subset B_{j+1}$, but it can be proven with some

simple calculations (see [Mil22, p. 6.49]). In fact, we can refine the series

$$B_1 \supset \cdots \supset B_n$$

into another series such that each quotient B_i/B_{i+1} is isomorphic to G_a.

The previous example is, in a sense, almost our only example, as we see that every unipotent group is isomorphic to a subgroup of U_n:

Proposition 1.69. The following are equivalent:

(i) G admits a faithful unipotent representation.

(ii) Every linear representation of G is unipotent.

(iii) G is isomorphic to a subgroup of U_n.

Proof. (i) $\Rightarrow$ (ii): Let (V, r) be a faithful unipotent representation of G. We know from Theorem 1.60 that every linear representation can be constructed from (V, r) by forming tensor products, direct sums, subquotients and duals, and those constructions on unipotent representations are also unipotent.

(ii) $\Rightarrow$ (iii): By Theorem 1.59, there's always a faithful representation of G, and it is unipotent by hypothesis.

(iii) $\Rightarrow$ (i): The injective map $G \to \mathrm{U}_n \to \mathrm{GL}_n$ is a faithful unipotent representation. □

We say that G is **unipotent** if it satisfies the equivalent conditions of the previous proposition. We saw that U_n is nilpotent; every subgroup of U_n (that is, every unipotent group) is also nilpotent. The fact that the quotients B_i/B_{i+1} on Example 1.68 are isomorphic to G_a will come in play in the following corollary. It will be important later on to calculate the cohomology group of unipotent groups.

Corollary 1.70. If G is a unipotent algebraic group, then it has a central normal series whose quotients are isomorphic to algebraic subgroups of G_a. In particular, G is nilpotent. In particular, if k is perfect then the quotients are isomorphic to G_a.

Proof. Every unipotent group is isomorphic to a subgroup of U_n. We know from Example 1.68 that U_n has a central normal series whose quotients are isomorphic G_a. Intersecting every group of one such series with G makes a central normal series for G whose quotients are isomorphic to subgroups of G_a.

If k is perfect, the fact that $\dim \mathrm{G}_a = 1$ implies that it has no nontrivial proper smooth subgroups, so we obtain the second part. □

Proposition 1.71. Let

$$1 \to N \to G \to Q \to 1$$

be an exact sequence of algebraic groups. The following holds:

(i) If G is unipotent, then N and Q are also so.

(ii) If N and Q are unipotent, then G is also so.

Proof. (i) By item (iii) of the Proposition 1.67 , it is clear that N is unipotent. If $Q \to \mathrm{GL}_n$ is a linear representation of Q, then $G \to Q \to \mathrm{GL}_n$ is linear representation of G, which must be unipotent. Thus, Q is unipotent.

(ii) Consider any representation (V, r) of G. It is also a representation of N, and it is unipotent by item (ii) of the previous proposition. The space V^N of elements fixed by N is nontrivial by Proposition 1.67 (the subspace V_1 of a flag). The action of G/N on V^N is, then, well defined, and the space $(V^N)^{G/N}$ is also nontrivial. Then, there is a nonzero element v of V fixed by G. We can construct a flag satisfying 1.67 by induction: the case $V = 1$ is clear, and if $\dim(V) > 1$, we apply the induction hypothesis on the orthogonal complement of v in V, which is stable under G because v is a fixed point. □

Proposition 1.72. Let G be an unipotent algebraic group. Then all elements of $G(k)$ are unipotent, and the converse holds if $G(k)$ is schematically dense in G.

Proof. If G is unipotent, then $G(k)$ is isomorphic to a subgroup of $\mathrm{U}_n(k)$, and all its elements are unipotent. Conversely, the elements of $G(k)$ being all unipotent implies $G(k) \subset \mathrm{U}_n(k)$, and as $G(k)$ is schematically dense in G, we have $G \subset \mathrm{U}_n$. □

Corollary 1.73. A smooth algebraic group G is unipotent if, and only if, every element of $G(\overline{k})$ is unipotent.

Proof. If G is smooth, then $G(\overline{k})$ is schematically dense in G. The rest follows from the previous proposition. □

The next theorem will be very useful later on: we will be able to prove the triviality of the Galois cohomology set of connected linear solvable algebraic groups by reducing it to the unipotent and torus cases. We will assume it without proof.

Theorem 1.74 ([Mil22, Th. 16.33])**.** Let G be a smooth connected solvable algebraic group over a perfect field k. Then:

(i) There exists a normal unipotent subgroup G_u such that G/G_u is of multiplicative type.

(ii) The subgroup in (i) contains all unipotent subgroups of G and its formation commutes with base extension.

(iii) The subgroup G_u in (i) is connected and smooth, and G/G_u is a torus.

(iv) Suppose that k is algebraically closed and let T be a maximal torus of G. Then G_u is normal in G and the map $(u,t) \mapsto ut : G_u(R) \times T(R) \to G(R)$ is a bijection of sets for all k-algebra R.

1.4.3 Fixed-point Theorem and Borel subgroups

Let G be a linear algebraic group.

Our objective in this subsection is to define Borel subgroups for connected algebraic groups G defined over a perfect field k. Two of its properties will be essential in the proof of the main theorem of this work: Borel subgroups are conjugated by elements of $G(k)$, and they are self-normalizing. Our main tool to prove those properties is the Borel Fixed-Point Theorem:

Theorem 1.75 (Borel Fixed-Point Theorem, [Mil22, Th. 17.2])**.** If G is a smooth connected solvable algebraic group and X is a separated complete nonempty algebraic scheme (see [Mil22, A.m]), then the scheme of fixed points X^G is nonempty; hence, there's a fixed point in $X(\overline{k})$.

Proof. We sketch the proof. Assume k is algebraically closed and X is reduced. An orbit O_x of $x \in X(k)$ of miminal dimension is closed by the Orbit Lemma (see [Mil22, Prop. 1.66]), so it is complete.

If H is an algebraic subgroup of G and G is solvable, it can be proven that G/H does not contain a complete subscheme of dimension > 0 or, in other words, if G/H is complete then $H = G$. Since G/G_x is isomorphic to O_x as schemes ([Mil22, Prop. 7.12]), in which G_x is the fiber of the orbit map $G \to O_x$, then the fact that O_x is complete implies $G = G_x$, hence, the orbit consists of only one element. □

Let V be a vector space of dimension n. Recall from Example 1.54 (i) that a flag F_0 of V is a sequence of vector spaces

$$F_0 : V = V_r \supset V_{r-1} \supset \cdots \supset V_1 \supset V_0 = 0$$

in which $\dim V_i = i$. If $n = r$, we say that the flag is maximal. An algebraic group G is said to be **trigonalizable** if it stabilizes a maximal flag.

Theorem 1.76 (Lie-Kolchin, [Mil22, Th. 17.4])**.** Let G be a connected solvable algebraic group over k. If k is algebraically closed, then G is trigonalizable.

Proof. Let X be the variety of maximal flags (see Examples 1.54). It is a is projective variety ([Mil22, Sec. 7.g]), hence complete, and G acts on it in a natural way. By the Borel Fixed-point Theorem (Theorem 1.75), there is a maximal flag which is stabilized by G, so G is trigonalizable by definition. □

Now, let us consider G to be a connected affine algebraic group over a perfect field k.

Definition 1.77. A **Borel subgroup** of G defined over $\overline{k}$ is a maximal connected solvable subgroup of $G_{\overline{k}}$. A subgroup of G over k is a Borel subgroup if, after extending it to $\overline{k}$, its image is a Borel subgroup over $\overline{k}$.

Example 1.78. Consider $G = \mathrm{GL}(V)$ for a n-dimensional vector space V and let B be a Borel subgroup of G. By the Lie-Kolchin Theorem we have B trigonalizable, and thus $B \subset \mathrm{T}_n$ for some basis of V. But since T_n is connected and solvable, then $\mathrm{T}_n \subset B$, and thus $B = \mathrm{T}_n$.

Proposition 1.79. (i) The variety G/B is complete.

(ii) Any two Borel subgroups of G are conjugated by an element of $G(k)$.

Proof. We only sketch the proof of (i). Flag varieties are projective, and thus complete, so it suffices to prove that G/B is a flag variety.

Let B be a Borel subgroup of G of maximum dimension. By Chevalley's Theorem ([Mil22, Th. 4.27]), there is a representation (V, r) of G such that B is the stabilizer of a one-dimensional subspace V_1 if V. Since B satisfies the hypothesis of Lie-Kolchin's Theorem, it stabilizes some flag of V/V_1, and thus stabilizes a flag F_0 of some lifting to V, and since B is the stabilizer of V_1, it is the stabilizer of the whole flag. The orbit $G \cdot F_0$ is of minimal dimension since B has the maximal possible dimension, so the Orbit Lemma (see [Mil22, Prop. 1.66]) says that it is a closed subvariety of the variety of maximal flags. Then, $G/B \cong G \cdot F_0$ is a flag variety.

Now we prove (ii). Let B' be another Borel subgroup of G. We can make B act on G/B' by left multiplication and, since B is solvable and G/B' is complete, Borel Fixed-Point Theorem implies that there is $x \in G(k)$ such that $BxB' \subset xB'$. So, we have $x^{-1}Bx \subset B'$. Since $x^{-1}Bx$ is solvable and connected, the maximality of B' implies that $x^{-1}Bx = B'$ □

As a consequence of this proposition, every Borel subgroup contains a maximal tori and they are conjugate (see [Mil22, 17.b]).

Lemma 1.80. If $\dim G \leq 2$, then G is solvable.

Proof. Let B be a Borel subgroup of G. Theorem 1.74 allows us to write $B = B_u \rtimes T$. If $B \neq G$, then either $B = B_u$ or $B = T$, and in either case B is nilpotent, but this implies that G is nilpotent ([Mil22, Prop. 17.23]), and thus $B = G$, a contradiction. □

Theorem 1.81 (Normalizer Theorem, [Mil22, Th. 17.48], [Bor91, Th 11.16])**.** If B is a Borel subgroup of G, then $N_G(B) = B$.

Proof. We sketch the proof. We can suppose that k is algebraically closed. If $\dim G \leq 2$ then G is solvable by the previous lemma, so $G = B = N_G(B)$. We proceed by induction on $\dim G$.

The group $N_G(B)$ is smooth (see [Mil22, Lemma 17.47]), so we only need to prove that $(N_G(B))(k) \subset B(k)$. Let $x \in (N_G(B))(k)$ and T be a maximal torus contained in B. The torus $x^{-1}Tx$ is also maximal and it is contained in B, so there exists some $b \in B(k)$ such that $x^{-1}Tx = b^{-1}Tb$. Replacing x with bx, we may assume that T is $x^{-1}Tx$. This implies that the homomorphism

$$\begin{aligned} \varphi : T &\to T \\ t &\mapsto [x, t] , \end{aligned}$$

where $[x, t]$ is the commutator if x and t, is well-defined. We need to consider the following two cases.

If $\varphi(T) \neq T$, then $\operatorname{Ker} \varphi$ is nontrivial, and so it contains a torus S. The key here is that Borel subgroups of the centralizer $C_G(S)$ are of the form $C_G(S) \cap B$ (see [Mil22, Th. 17.46]). Thus, if $C_G(S) \neq G$, the theorem follows from the induction hypothesis applied to $C_G(S)$. Otherwise, S is normal in G, so we apply the induction hypothesis on G/S.

Now let $\varphi(T) = T$. By Chevalley's Theorem we can take a representation (V, r) of G such that $N_G(B)$ is the stabilizer of a line $V_1 = \langle v \rangle$. Both B_u and T fixes v so, writing $B = B_u \rtimes T$ (see 1.74), then B also fixes v. The rest of the proof follows a similar argument used in Proposition 1.79: G/B is complete, so it fixes v, but then $G = N_G(B)$; but this implies $G = B$ (see [Mil22, Th. 17.33]). □

1.5 Semisimple algebraic groups

Let G be a connected smooth affine algebraic group over a perfect field k.

We know that extensions of algebraic groups that are connected or smooth also inherit these properties. Since G is smooth and of finite dimension, there exists a maximal connected solvable normal group. We call it the **radical** of G, and denote it by $r(G)$. We have:

Proposition 1.82. If H is a smooth connected solvable normal subgroup of G, then $H \subset r(G)$.

Definition 1.83. We say G, defined over k, is **semisimple** if it is smooth, connected and $G_{\overline{k}}$ has radical $r(G_{\overline{k}}) = 1$.

Proposition 1.84. The radical $r(G)$ commutes with separable algebraic field extensions.

Proof. Let K/k be a finite extension. We want to prove that $r(G_K) = r(G)_K$. Since $r(G)_K$ is a connected solvable normal subgroup of G_K, then $r(G)_K$ is a subgroup of $r(G_K)$. Now, consider the action of the Galois group $\mathrm{Gal}(K/k)$ on $r(G_K)$. For $s \in \mathrm{Gal}(K/k)$, the subgroup ${}^s r(G_K)$ is connected, solvable and normal, so by uniqueness, it is $r(G_K)$ itself. Thus, since $r(G_K)$ is stable by the Galois action, Proposition 1.29 shows us that it is defined over k. As it is a connected and solvable normal subgroup of G, it is a subgroup of $r(G)$ and, passing to K, this implies that $r(G_K)$ is a subgroup of $r(G)_K$. □

Proposition 1.85. (i) If $r(G) = 1$, then G is semisimple.

(ii) The quotient $G/r(G)$ is semisimple.

Proof. By the previous proposition, $r(G_{\overline{k}}) = r(G)_{\overline{k}} = 1$, so G is semisimple.

Let H be the inverse image of $r(G/r(G))$ in G. Consider the exact sequence

$$1 \to r(G) \to H \to r(G/r(G)) \to 1\,.$$

Since H is an extension of connected solvable smooth normal subgroups, then it also has all those properties. Since $r(G)$ is contained in H, we have $H = r(G)$ by maximality, but $H/r(G)$ is isomorphic to $r(G/r(G))$, so $r(G/r(G)) = 1$. □

In particular, G is semisimple if, and only if, $G_{\overline{k}}$ is semisimple.

Examples 1.86. (i) Every nontrivial connected commutative smooth group G is not semisimple, since $r(G)$ would be simply G. Examples of this are G_a, G_m and tori.

(ii) Products of semisimple groups are also semisimple, since a product is an extension.

(iii) The algebraic group GL_n is not semisimple. Its center, which is isomorphic to G_m, is a connected smooth commutative normal subgroup of GL_n, thus $1 \neq \mathrm{G}_m \subset r(\mathrm{GL}_n)$.

(iii) The algebraic groups SL_n and PGL_n are semisimple.

Proposition 1.87. Let K/k be a separable extension. If G is a semisimple group over K, then the Weil restriction $R_{K/k}(G)$ is also semisimple

Proof. Proposition 1.28 implies that

$$(R_{K/k}(G))_K = \prod \sigma G$$

is a product of semisimple groups, so it is semisimple. By Proposition 1.84, we conclude that $R_{K/k}(G)$ is also semisimple. □

Chapter 2

Cohomology

Let G be a profinite group and let A be a discrete group such that G acts continuously on it. If A is abelian, we can define cohomology groups $H^q(G, A)$ for every $q \geq 0$. It extends the notion of cohomology groups in the finite case and, in fact, we can calculate $H^q(G, A)$ using the cohomology groups $H^q(G/U, A^U)$ with U ranging over the normal open subgroups of G (in which case, G/U is finite). It makes sense, then, to also define cohomological dimension for profinite groups. For A non-abelian things get more complicated: we can still define $H^0(G, A)$ and $H^1(G, A)$, but they are only sets, and they will be useful in Chapter 3.

We are interested in the case where G is a Galois group $\mathrm{Gal}(K/k)$, and we note that every Galois group is profinite. If k is a perfect field, we say that k has dimension at most one if $\mathrm{Gal}(\overline{k}/k)$ has cohomological dimension at most one. We immediately have some equivalent conditions, like the Brauer group $\mathrm{Br}(K)$ being trivial for every algebraic extension K/k, or, for finite extension L/K with K/k algebraic, the $\mathrm{Gal}(L/K)$-module L^* being cohomologically trivial.

This notion of a field having dimension at most one will come into play again in the last chapter. Most of the results in the present chapter can be found in [Ser02]. Its first 9 pages on profinite groups are assumed as basic knowledge.

2.1 Abelian cohomology

Let G be a profinite group. We say that a discrete abelian group A is a G**-module** if G acts continuously on A by automorphisms. For an integer $q \geq 0$, we denote by G^q the cartesian product $G \times \cdots \times G$ of q factors equal to G.

Definition 2.1. Let $C^q(G, A)$ be the group of continuous maps $G^q \to A$ with maps

$$\begin{aligned} d_q : C^q(G, A) &\to G^{q+1}(G, A) \\ f &\mapsto df : (g_1, \dots, g_q, g_{q+1}) \mapsto g_1 \cdot f(g_2, \dots, g_{q+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_q) \\ &\quad + (-1)^{q+1} f(g_1, \dots, g_q) \end{aligned}$$

for every $q \geq 0$. Let $Z^q(G, A) = \operatorname{Ker} d_q$ be the group of **q-cocycles** and $B^q(G, A) = \operatorname{Im} d_{q-1}$ be the group of **q-coboundaries**. The quotient $H^q(G, A) = Z^q(G, A)/B^q(G, A)$ is the q-th **cohomology group** of G with coefficients in A.

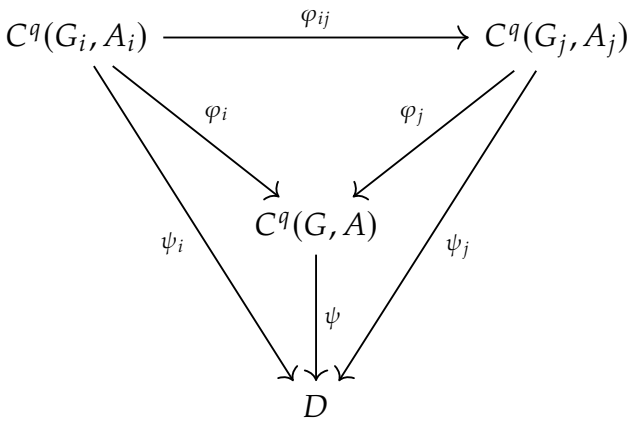
This definition makes sense because $d_{q-1} \circ d_q = 0$. For simplicity, we shall denote the maps d_q by d. The following results show us that the cohomology groups of profinite groups can be calculated from the cohomology groups of its finite quotients.

Proposition 2.2. Let $G = \varprojlim G_i$ and $A = \varinjlim A_i$. Then

$$H^q(G, A) = \varinjlim H^q(G_i, A_i)$$

for every $q \geq 0$.

Proof. We will prove that $C^q(G, A)$ possesses the universal property of the direct system $\{C^q(G_i, A_i)\}$, that is, given $\psi_i : C^q(G_i, A_i) \to D$ there exists $\psi : C^q(G, A) \to D$ such that the diagram



commutes.

Since A is discrete, a continuous function $\sigma : G^q \to A$ factors through some G_i, which is finite. Since A is the direct system of A_i, the image of an element of G_i has

a representative contained in some A_j and, because G_i is finite, there exists some A_k which contains representatives for all of them. We take some l such that $l \geq k$; this means that there exist maps $G_l \to G_k$ and $A_k \to A_l$, and composing with σ, we obtain

$$\overline{\sigma} : G_i^n \to A_k \ .$$

We define $\psi(\sigma) = \psi_l(\overline{\sigma})$. It is clear that the map ψ is well-defined and the diagram commutes, as required. □

Corollary 2.3. Let A be a G-module. Then

$$H^q(G, A) = \varinjlim H^q(G/U, A^U)$$

for every $q \geq 0$, in which U ranges over all open subgroups of G.

Proof. Let $a \in A$. Since the action of G on A is continuous and A, the inverse image of a by this action must be open. As A is discrete, this open set is of the form

$$\bigcup_i U_i \times \{a_i\} \ ,$$

in which case the set $U_i \times \{a_i\}$ with $a_i = a$ must be open in $G \times A$. In other words, U_i is the stabilizer of a and it is an open subgroup of G. We conclude that $A = \varinjlim A^U$. □

Examples 2.4. (i) Let $a \in Z^0(G, A)$. We have

$$0 = da(x) = x \cdot a - a \ ,$$

so $x \cdot a = a$. Then, $H^0(G, A) = A^G$.

(ii) Let $f(s) \in Z^1(G, A)$. We have

$$0 = df(s, t) = s \cdot f(t) - f(st) + f(s) \ ,$$

so

$$f(st) = f(s) + s \cdot f(t) \ .$$

Such functions are called **crossed homomorphisms**. We note that, if the action of s on $f(t)$ is trivial, then f is a group homomorphism.

(iii) Let $G = 1$. We have:

$$H^q(G, A) = \begin{cases} A, \text{ if } q = 0 \,, \\ 0, \text{ if } q \geq 1 \,. \end{cases}$$

Indeed, we identify the group of functions $1 \to A$ with A. Then, the formula for d is just an alternating sum of a and $-a$, thus, $da = 0$ if q is even and $da = a$ if q is odd. We get,

$$Z^q(G, A) = \begin{cases} A, \text{ if } q \text{ is even,} \\ 0, \text{ if } q \text{ is odd,} \end{cases}$$

and

$$B^q(G, A) = \begin{cases} A, \text{ if } q \text{ is even and nonzero,} \\ 0, \text{ if } q \text{ is odd or zero,} \end{cases}$$

so $H^n(G, A) = Z^q(G, A)/B^q(G, A)$ is only nonzero if $q = 0$.

(iv) Let $G = \mathbb{Z}/p^n\mathbb{Z}, A = \mathbb{Z}/p\mathbb{Z}$. Since the only homomorphism $\mathbb{Z}/p^n\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/(p-1)\mathbb{Z}$ is the trivial one, the only action of G on A that makes A a G-module is the trivial action. Then, by (i) and (ii), we have $H^0(G, A) = A$ and $H^1(G, A) = \mathrm{Hom}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$.

(v) Let $G = \mathbb{Z}_p$ and $A = \mathbb{Z}/p\mathbb{Z}$. Let us consider the trivial action of G on A. We have $H^0(G, A) = A = \mathbb{Z}/p\mathbb{Z}$. Since $G = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, by the previous corollary we have

$$H^1(G, A) = \varinjlim H^1(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \,.$$

Let G and G' be profinite groups, A' a G'-module and A a G-module. If $\varphi : G \to G'$ is a homomorphism of profinite groups and $\psi : A' \to A$ is a homomorphism of abelian groups such that $g \cdot \psi(a') = \psi(\phi(g) \cdot a')$, then we have a natural map $C^q(G', A') \to C^q(G, A)$ by composing with φ and ψ. Passing to cohomology, we have a map

$$H^q(G', A') \to H^q(G, A) \,.$$

For example, the inclusion $H \to G$ gives us the map

$$\mathrm{res} : H^q(G, A) \to H^q(H, A)$$

for every $q \geq 0$. The map res is called the **restriction**.

Definition 2.5. Let H be a closed subgroup of G and let A be an H-module. The **coinduced module** $A^* = M_G^H(A)$ is defined as the module of continuous functions $a^* : G \to A$ such that $a^*(hg) = h \cdot a^*(g)$. The action of G on $M_G^H(A)$ is given by

$$(ga^*)(x) = a^*(xg) \, .$$

If A is a H-module, there is a natural homomorphism $M_G^H(A) \to A$ defined by $a^* \to a^*(1)$.

Proposition 2.6 (Shapiro's lemma, [Ser02, Chap. 1, Sec. 2, Prop. 10], [NSW15, Prop. 1.6.4])**.** The homomorphism

$$H^q(G, M_G^H(A)) \to H^q(H, A)$$

induced by the inclusion $H \to G$ and the natural map $M_G^H(A) \to A$ is an isomorphism.

Proof. This proposition can be proven in a number of ways. We sketch the proof found in [NSW15].

Consider the groups $X^q(G, A)$ of continuous maps $G^{q+1} \to A$, with $d : X^q(G, A) \to X^{q+1}(G, A)$ given by

$$df(g_0, \ldots, g_n, g_{n+1}) = \sum_{i=0}^{q+1} (-1)^i f(g_0, \ldots, \hat{g_i}, \ldots g_{n+1}) \, ,$$

where $\hat{g_i}$ denotes the omission of g_i. Since H is a closed subgroup of G, we denote by $X^q(G, A)^H$ the subgroup of $X^q(G, A)$ of elements that satisfies

$$f(gg_0, \ldots, gg_n) = g \cdot f(g_0, \ldots, g_n) \, .$$

It can be proven that there is an isomorphism $\Phi : X^q(G, A)^G \to C^q(G, A)$ such that $\Phi \circ d = d \circ \Phi$, so that the cohomology groups induced by them are isomorphic.

Thus, the proposition follows from the isomorphism

$$X^q(G, M_G^H(A))^G \to X^q(G, A)^H$$

by passing to cohomology, and from the fact that the cohomology group induced by $X^q(G, A)^H$ is $H^q(H, A)$. □

If $H = 1$, then $H^q(G, M_G^H(A)) = H^q(1, A)$, which, by Example 2.4 (iii), is A when $q = 0$ and 0 otherwise. In this case, we shall denote $M_G^H(A)$ by simply $M_G(A)$.

Let H be an open subgroup of G. If A is a G-module, we have a map $\pi : M_G^H(A) \to A$ defined by

$$\pi(a^*) = \sum_{x \in G/H} x \cdot a^*(x^{-1}) .$$

This map does not depend on the choice of representatives of right cosets of H; if $hx \in Hx$, then

$$(hx) \cdot a^*((hx)^{-1}) = (h^{-1}hx) \cdot a^*(x^{-1}) = x \cdot a^*(x^{-1}) .$$

For every $a \in A$, the map a^* defined by $a^*(1) = a$, $a^*(h) = h \cdot a$ and $a^*(g) = 0$ for $g \in G \setminus H$ is such that $\pi(a^*) = a$, so π is surjective. The map π induces a map $H^q(G, M_G^H(A)) \to H^q(G, A)$, and the composition

$$\mathrm{cor} : H^q(H, A) \cong H^q(G, M_G^H(A)) \to H^q(G, A) ,$$

called the **corestriction**.

The following proposition describes the long exact sequence of cohomology groups associated to a short exact sequence of G-modules. It is a wonderfully useful tool that allows us to calculate cohomology groups, lift some properties to extensions, and more.

Proposition 2.7. Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence of G-modules. There exists $\delta : H^q(G, C) \to H^{q+1}(G, A)$ such that the sequence

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to \cdots$$
$$\cdots \to H^q(G, C) \xrightarrow{\delta} H^{q+1}(G, A) \to H^{q+1}(G, B) \to H^{q+1}(G, C) \to \dots$$

is exact.

Proof. Consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C^q(G,A) & \longrightarrow & C^q(G,B) & \longrightarrow & C^q(G,C) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C^{q+1}(G,A) & \longrightarrow & C^{q+1}(G,B) & \longrightarrow & C^{q+1}(G,C) & \longrightarrow & 0 \end{array}$$

Take an element $\overline{f} \in H^q(G,C)$, and let f denote a representative for it. There is an element $g \in C^q(G,B)$ such that its image is f, and because $df = 0$, the image of dg in $C^{q+1}(G,C)$ is also 0, hence it is also in $C^{q+1}(G,A)$; $\delta(\overline{f})$ is mapped to the class of this element, which is, of course, a cocycle. By the construction of δ and the commutativeness of the diagram, the equality

$$\delta \circ d = d \circ \delta$$

holds.

Exactness at $H^q(G,C)$: if $\delta(\overline{f}) = \overline{0}$ if, and only if, $dg = 0$, that is to say, g is a cocycle and f is its image.

Exactness at $H^{q+1}(G,A)$: Let $h \in C^{q+1}(G,A)$ be a cocycle. If its image in $C^{q+1}(G,B)$ is a coboundary dg, then the image f of g in $C^q(G,C)$ is such that $\delta(\overline{f}) = \overline{h}$ by construction. The converse is clear. □

Now, let us consider the exact sequence

$$1 \to A \xrightarrow{i} M_G \to A/M_G \to 1$$

associated to the coinduced module M_G, where $i(a)(x) = x \cdot a$. Looking at the long exact sequence associated to it, we are able to prove some properties for the cohomology groups $H^q(G,A)$ by proving directly for $q = 0$ and lifting it to a long exact sequence. Indeed, we have

$$H^q(G, A/M_G) \to H^{q+1}(G,A) \to H^{q+1}(G,M_G) = 0\ ,$$

so the map $H^q(G, A/M_G) \to H^{q+1}(G,A)$ is surjective, and goes to a higher dimensional cohomology group. We shall use it to prove the next proposition.

Proposition 2.8. If $(G : H) = n$, then $\mathrm{cor} \circ \mathrm{res} = n\,\mathrm{id}$

Proof. Let $q = 0$. We have

$$(\mathrm{cor} \circ \mathrm{res})(a) = \sum_{g \in G/H} g^{-1} \cdot a = na\ ,$$

We prove for $q > 0$ by dimension shifting. By induction we have $\mathrm{cor} \circ \mathrm{res} = n\,\mathrm{id}$ for A/M_G and, since the map $H^{q-1}(G, A/M_G) \to H^q(G, A)$ is surjective, the equality must also hold for $H^q(G, A)$. □

Corollary 2.9. The kernel of res is killed by n. In particular, if $(G : H)$ is prime to p, then res is injective on the p-primary component of $H^q(G, A)$.

Suppose G is a finite group. We define the norm map $N_G : A \to A$ by

$$N(a) = \sum_{g \in G} ga \ .$$

The **modified cohomology groups** $\hat{H}$ are defined as

$$\begin{aligned} \hat{H}^0(G, A) &= A^G/NA \ , \\ \hat{H}^q(G, A) &= H^q(G, A), \text{ for } q > 0 \ . \end{aligned}$$

Now, if G is a profinite group, then we define $\hat{H}^q(G, A)$ as $\varinjlim \hat{H}^q(G/U, A^U)$, where U runs through the open normal subgroups of G ([NSW15, p. 1.9.3]). For $n > 1$, this definition agrees with our definition of $H^q(G, A)$ by Proposition 2.2.

Definition 2.10. A G-module A is **cohomologically trivial** if $\hat{H}^q(H, A) = 0$ for every closed subgroup H of G and every $n \geq 0$.

There is a useful condition for a G-module A to be cohomologically trivial [NSW15, Prop. 1.8.2, 1.8.14]: if for every prime p there exists $n \geq 0$ such that

$$\hat{H}^q(G_p, A) = \hat{H}^{q+1}(G_p, A) = 0 \ ,$$

where we shall use this result in Section 2.5, and also to calculate the Galois cohomology of tori.

2.2 Cohomological dimension

Let A be a discrete G-module. If an element $a \in A$ has order p^n, then $p(g \cdot a) = g \cdot (p^n a) = 0$, so the order of $g \cdot a$ divides p^n. Thus, the subgroup $A_p = \{a \in A \mid p^n a = 0 \text{ for some } n \geq 0\}$ of A is a G-submodule of A, and it is called the **p-primary component** of A. A submodule B of A is **p-annihilated** if $pB = 0$.

Definition 2.11. Let G be a profinite group and p be a prime number. The **p-cohomological dimension** of G, denoted by $\mathrm{cd}_p(G)$, is the least of the integers n which satisfy the following condition: For every discrete torsion G-module A, and for every $q > n$, the p-primary component of $H^q(G, A)$ is null.

The **cohomological dimension** of G, denoted by $\mathrm{cd}(G)$, is defined as $\sup \mathrm{cd}_p(G)$, ranging over all primes.

The following proposition gives us a nice equivalence for the p-cohomological dimension to be $\leq n$. Let A be a torsion discrete G-module. We can decompose A into its p-primary components, obtaining $A = \bigoplus_p A_p$. By Corollary 2.3, we have

$$H^q(G, A) = \varinjlim H^q(G/U, A^U) .$$

Since each G/U is a finite group and A is a torsion group, the cohomology groups $H^q(G/U, A^U)$ are torsion groups, thus so is $H^q(G, A)$.

If σ is a q-cocycle of order p^α, then the order of $\sigma(g_1, \ldots, g_q)$ is a power of p, so it is contained in A_p. Conversely, let us suppose that $\sigma(g_1, \ldots, g_q)$ is a power of p for every $g_i \in G$. Since $H^q(G, A)$ is a torsion group, it follows that the order of σ must be a power of p. We obtain

$$H^q(G, A)_p = H^q(G, A_p) .$$

Thus, the p-cohomological dimension can be determined by the cohomology groups with respect to p-primary torsion groups. Item (iii) of the proposition gives us a very economical way of testing the p-cohomological dimension.

Proposition 2.12. The following are equivalent:

(i) $\mathrm{cd}_p(G) \leq n$.

(ii) $H^q(G, A) = 0$ for every $q > n$ and every discrete G-module A that is a p-primary torsion group.

(iii) $H^{n+1}(G, A) = 0$ for every discrete G-module A that is simple (i.e., has exactly two sub-G-modules) and is p-annihilated.

Proof. (i) $\Leftrightarrow$ (ii): We can write a torsion group A as the sum $\bigoplus_p A_p$ where A_p is the p-primary component of A. The equivalence follows from the fact that $H^q(G, A)_p$ can be identified with $H^q(G, A_p)$.

(ii) $\Rightarrow$ (iii): It is clear.

(iii) $\Rightarrow$ (ii): First we prove that $H^{n+1}(G, A) = 0$ for any discrete G-module A which is a p-primary torsion group. Since we can write A as a direct limit of its finitely

generated submodules, which are finite because A is an abelian torsion group, it is enough to prove the case in which A is finite. We have the exact sequence

$$1 \to pA \to A \to A/pA \to 1.$$

If p^α is the lowest power of p that annihilates A then $p^{\alpha-1}$ annihilates A/pA, so induction shows us that $H^{n+1}(G, A/pA) = 0$. As $H^{n+1}(G, pA) = 0$ by (iii), the corresponding exact sequence of cohomology groups implies $H^{n+1}(G, A) = 0$.

For $q > n+1$, we proceed by induction. Since A is p-primary and torsion, $M_G(A)$ also is, and we can inject A into $M_G(A)$ with the map

$$a \mapsto (g \mapsto g \cdot a)\,.$$

This injection induces an exact sequence which, by Proposition 2.7, gives us the exact sequence

$$H^q(G, M_G(A)/A) \to H^{q+1}(G, A) \to H^{q+1}(G, M_G(A)).$$

The first is trivial by the induction hypothesis, and the third is always trivial since, so we conclude that $H^{q+1}(G, A) = 0$. □

The p-cohomological dimension of closed subgroups behaves nicely, as we shall see in the next proposition.

Proposition 2.13. Let H be a closed subgroup of a profinite group G. We have $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$ and, if any of the following holds

(i) $(G : H)$ is prime to p,

(ii) H is open in G and $\mathrm{cd}_p(G) < \infty$,

then $\mathrm{cd}_p(H) = \mathrm{cd}_p(G)$.

Proof. Let A be a H-module. We know from Shapiro's Lemma (2.6) that $H^q(H, A) = H^q(G, M_G^H(A))$, so $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$.

Suppose $(G : H)$ is prime to p. If A is p-primary, then the restriction

$$\mathrm{res} : H^q(G, A) \to H^q(H, A)$$

is injective (Corollary 2.9), and so $\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H)$.

Now, suppose H is open and $\mathrm{cd}_p(G) = n$. The map

$$\begin{aligned} \pi : M_G^H(A) &\to A \\ a^* &\mapsto \sum_{x \in G/H} x \cdot a^*(x^{-1}) \end{aligned}$$

does not depend on the choice of representatives, and is surjective, for if $a \in A$, the map a^* defined as $a^*(h) = h \cdot a$ and $a^*(g) = 0$ for $g \in G \setminus H$ is such that $a^* \in M_G^H(A)$ and $\pi(a^*) = a$. The associated exact sequence gives us the exact sequence

$$H^n(H, A) = H^n(G, M_G^H(A)) \to H^n(G, A) \to H^{n+1}(G, \operatorname{Ker} \pi) ,$$

in which the p-primary component of the latter is trivial, and we conclude that $\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H)$. □

Corollary 2.14. If G_p is a p-Sylow subgroup of G, then

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

Proof. It is always true that G_p is closed in G and $(G : G_p)$ is prime to p, so it follows from item (i) of the previous proposition. □

If H is a closed normal subgroup of G, the Lyndon-Hochschild-Serre spectral sequence ([NSW15, Th. 2.4.1]) gives us a first quadrant spectral sequence

$$E_2^{ij} = H^i(G/H, H^j(H, A)) \Rightarrow H^{i+j}(G, A) .$$

It allows us to give a upper bound to $\mathrm{cd}_p(G)$ in terms of the p-dimension of G/H and H.

Proposition 2.15. Let H be a closed normal subgroup of profinite group G. The following inequality holds:

$$\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H) + \mathrm{cd}_p(G/H) .$$

If $\mathrm{cd}_p(G/H)$ is finite, we have equality if H is in the center of G.

Proof. Let $n = \mathrm{cd}_p(H) + \mathrm{cd}_p(G/H)$. The the Lyndon-Hochschild-Serre spectral sequence gives us the spectral sequence

$$E_2^{ij} = H^i(G/H, H^j(H, A)) \Rightarrow H^{n+1}(G, A) .$$

for i, j such that $i + j = n + 1$. But this implies that either $i > \mathrm{cd}_p(H)$, in which case $H^i(H, A)_p = 0$, or $j > \mathrm{cd}_p(G/H)$, so $H^i(G/H, \cdot)_p = 0$. So, by the spectral sequence, $H^{n+1}(G, A)_p = 0$. □

Examples 2.16. (i) Let p and q be distinct primes. Since the q-Sylow subgroup of $\mathbb{Z}_p$ is trivial, it follows that $\mathrm{cd}_q(\mathbb{Z}_p) = 0$. In general, every profinite group with order prime to q has null q-cohomological dimension.

(ii) ([RZ10, Exer. 7.4.3]) Consider $A = \bigoplus^m \mathbb{Z}_p$. We have $\mathrm{cd}_p(A) = m$. Indeed, we proceed by induction on m. As A is abelian, Proposition 2.15 shows us that $\mathrm{cd}_p(A) = \mathrm{cd}_p(\mathbb{Z}_p) + \mathrm{cd}_p(A/\mathbb{Z}_p)$. The quotient $A/\mathbb{Z}_p$ is isomorphic to $\bigoplus^{m-1} \mathbb{Z}_p$, so the induction hypothesis implies $\mathrm{cd}_p(A/\mathbb{Z}_p) = m - 1$, and we conclude that $\mathrm{cd}_p(A) = m$.

We can use some of the previous results to prove that, for pro-p groups, its cohomological dimension is determined by the cohomology with respect to $\mathbb{Z}/p\mathbb{Z}$.

Proposition 2.17. Let G be a pro-p group and n an integer. Then $\mathrm{cd}(G) \leq n$ if, and only if, $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$.

Proof. By the equivalence of items (i) and (iii) of Proposition 2.12, it suffices to prove that the only simple discrete G-module A that is p-annihilated is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ with trivial G-action.

Our hypothesis shows that A must be finitely generated and, since it is p-annihilated, it must be finite. Since the G-action is continuous, it factors through some G/U where U is a open normal subgroup of G, which is finite, so we only need to prove the case in which G is finite.

If G is finite, the G-action on A must be trivial. Since G and A are finite p-groups, the congruence

$$0 \equiv |A| \equiv |A^G| \pmod{p}$$

holds. Since $0 \in A^G$ then A^G is nontrivial, but A is simple, so $A = A^G$. We conclude that $A = \mathbb{Z}/p\mathbb{Z}$. □

2.2.1 Profinite groups with cohomological dimension ≤ 1

In this subsection, we aim to characterize profinite groups of cohomological dimension ≤ 1: they are precisely the projective profinite groups.

If G is a finite group and A is a finite G-module, it is a known result that the second cohomology group is in a bijective correspondence with extensions of G by A ([Ser16,

Sec. 4.4]). The first step for the characterization is to prove this fact for when G is profinite.

Let

$$1 \to A \to E \to G \to 1$$

be an exact sequence of profinite groups, in which A is finite and abelian. There is a natural G-action on A: the conjugation by elements of E corresponds to a homomorphism $E \to \mathrm{Aut}(A)$, and, since A is abelian, it factors through $E/A \cong G$. Hence, if $h : G \to E$ is any continuous section, the action is described by

$$^{x}a = h(x)ah(x)^{-1} .$$

Another extension E' of A by G is said to be isomorphic to E if there is an isomorphism $\varphi : E' \to E$ such that the diagram

$$\begin{array}{ccccc} A & \longrightarrow & E' & \longrightarrow & G \\ {\scriptstyle \mathrm{id}}\downarrow & & {\scriptstyle \varphi}\downarrow & & {\scriptstyle \mathrm{id}}\downarrow \\ A & \longrightarrow & E & \longrightarrow & G \end{array}$$

commutes.

Theorem 2.18 ([RZ10, Th. 6.8.4])**.** Given a profinite group G and a finite G-module A, there exists a one-to-one correspondence between extensions of G by A and $H^2(G, A)$.

Proof. The operations will be written in multiplicative notation.

Let E be an extension of G by A. Let $\pi : E \to G$ be the projection and choose a continuous section $h : G \to E$. Since $\pi \circ h = \mathrm{id}_G$ and π is a homomorphism, then $\pi(h(x)h(y)) = \pi(h(xy))$ for every $x, y \in G$. Hence, we can define a (continuous) map $f_h : G \times G \to A$ such that

$$h(x)h(y) = f_h(x, y)h(xy) .$$

The map f is a 2-cocycle. Indeed, it is continuous, and we have

$$\begin{aligned} h(x)h(y)h(z) &= h(x)f_h(y, z)h(yz) = {}^{x}f_h(y, z)f_h(x, yz)h(xyz) , \\ h(x)h(y)h(z) &= f_h(x, y)h(xy)h(z) = f_h(x, y)f_h(xy, z)h(xyz) ., \end{aligned}$$

however, since both equations are equal, we obtain

$$f_h(x, y)f_h(xy, z)\,{}^{x}f_h(y, z)f(x, yz) = 1 ,$$

but that is just the formula for $df(x,y,z)$. If h' is another section for π, we have $h'(x) = l(x)h(x)$ for every $x \in G$. We will show that l is a 1-cocycle that makes h and h' cohomologous. On one hand we have

$$h'(x)h'(y) = f_{h'}(x,y)h'(xy) = f_{h'}(x,y)l(xy)h(xy)\ ,$$

but if we use $h'(x) = l(x)h(x)$ first, we obtain

$$\begin{aligned} h'(x)h'(y) &= l(x)h(x)l(y)h(y) \\ &= l(x)h(x)l(y)h(x)^{-1}h(x)h(y) \\ &= l(x)\,{}^{x}l(y)h(x)h(y) \\ &= l(x)\,{}^{x}l(y)f_h(x,y)h(xy)\ . \end{aligned}$$

Since A is abelian, we can conclude that

$$f_{h'}(x,y) = f_h(x,y)\,{}^{x}l(y)l(x)l(xy)^{-1} = f_h(x,y)dl(x,y)\ ,$$

that is, f_h and $f_{h'}$ are indeed cohomologous. Then, if E and E' are two isomorphic extensions, we can choose sections h and h' for them, respectively, coming from the same 2-cocycle; the map $\varphi : ah(x) \mapsto ah'(x)$ is an isomorphism.

Now, if f is a 2-cocycle, it is cohomologous to a normalized 2-cocycle f_0 (i.e. satisfies $f(1,1) = 0$). We can define a group $E = A \times G$ with the following multiplication rule (with A written additively):

$$(a_1,x_1)(a_2,x_2) = (a_1 + a_2x_2 + f_0(x_1,x_2), x_1x_2)\ .$$

It is an extension of A by G, and it corresponds to f_0. □

The p-cohomological dimension of a profinite group G being ≤ 1 already has some implications of certain extensions splitting. We begin with the following technical lemma.

Lemma 2.19. Let H be a closed normal subgroup of a profinite group E, and let H' be an open subgroup of H. Then, there is an open subgroup H'' of H that is contained in H' and is normal in E.

Proof. Let N be the normalizer of H' in E. Consider the map $E \times H' \to H$ that maps (e,h) into $e^{-1}he$. The inverse image of H' by this map is exactly N, which is open

since conjugation is continuous. Thus, there are only finitely many conjugates of H'. Defining H'' as their intersection finishes the proof. □

Proposition 2.20 ([Ser02, Chap. 1, Sec. 3.4, Prop. 16])**.** Let G be a profinite group and p a prime. The following properties are equivalent.

(i) $\mathrm{cd}_p(G) \leq 1$.

(ii) The group G has the lifting property for extension

$$1 \to P \to E \to W \to 1$$

where E is finite and P is a abelian p-group which is p-annihilated.

(ii') Every extension of G by a finite abelian p-group which is p-annihilated splits.

(iii) The group G has the lifting property for extensions.

$$1 \to P \to E \to W \to 1$$

where P is a pro-p group.

(iii') Every extension of G by a pro-p group splits.

Proof. (i) $\Leftrightarrow$ (ii'): If $\mathrm{cd}_p(G) \leq 1$ then $H^2(G, P) = 0$; thus, extensions of G by P split by Theorem 2.18. On the other hand, (ii') implies that extensions of G by $\mathbb{Z}/p\mathbb{Z}$ split, and the same theorem implies $H^2(G, \mathbb{Z}/p\mathbb{Z}) = 0$. By Proposition 2.17, we conclude that $\mathrm{cd}_p(G) \leq 1$.

(iii) $\Leftrightarrow$ (iii'): It is clear that (iii) implies (iii'). Let us suppose (iii'), and consider an extension $1 \to P \to E \xrightarrow{\pi} W$ such that $\varphi : G \to W$ is a surjective homomorphism. We can construct the pullback E_φ of E by φ:

$$E_\varphi = \{(e, g) \in E \times G \mid \pi(e) = \varphi(g)\} .$$

We then have an extension

$$1 \to P \to E_\varphi \to G \to 1 ,$$

and (iii') implies that it splits. If $h : G \to E_\varphi$ is a section that splits the extension, we can define $G \to E$ as the projection of the first coordinate of $h(g)$. It is a homomorphism and its composition with π is exactly φ.

(ii) $\Leftrightarrow$ (ii'): It is analogous to the previous equivalence. We note that (ii) $\Rightarrow$ (ii') is not immediate, because our hypothesis is that E is finite. If $1 \to P \to E \to G \to 1$ is an extension, we can find an open normal subgroup H of E such that $P \cap H = 1$ since P is finite and normal in E, and the image of H in G is also normal. Now, the sequence

$$1 \to P \to E/H \to G/H \to 1$$

has E/H finite and satisfies the hypothesis of (ii). We have, then, a lifting $G/H \to E/H$, which can be lifted to $G \to E$, which splits the extension.

(iii') $\Leftrightarrow$ (ii'): The implication (iii') $\Rightarrow$ (ii') is clear. For the converse, let us consider an extension

$$1 \to P \to E \to G \to 1$$

where P is a pro-p group that is closed and normal in E. Let us consider the set X of pairs (P', h) such that P' is an open subgroup of P and h is a homomorphism $G \to E/P'$ compatible with the extension above. We say that $(P'_1, h_1) \geq (P'_2, h_2)$ if $P'_1 \subset P'_2$ and h_2 is the composition $G \xrightarrow{h_1} E/P'_1 \to E/P'_2$. This set has a maximal element, say (P', h). It suffices to prove that $P' = 1$.

Let us suppose that $P' \neq 1$ and consider the extension

$$1 \to P' \to E' \to G \to 1\ ,$$

where E' is the inverse image of $h(G)$ in E. By the previous lemma, there exists an open subgroup P'' of P' that is normal in E. The quotient P'/P'' is a finite p-group, thus, we can assume that P'/P'' is abelian and p-annihilated. By (ii'), the extension

$$1 \to P'/P'' \to E'/P'' \to G \to 1$$

splits. Thus, there is a lifting $G \to E'/P'' \to E/P''$ which contradicts maximality of (P', h). □

In particular, if G is a pro-p group, we can use the previous result, along with the following lemma, to prove that $\mathrm{cd}_p(G) \leq 1$ is equivalent to G being a projective pro-p group. Furthermore, we can prove that projective pro-p groups are always free as pro-p groups. This is not the case for profinite groups in general.

We recall some facts. The **Frattini subgroup** $\Phi(G)$ of a profinite group G is the intersection of all maximal closed subgroups of G. It is a characteristic subgroup of G, and is coincides with the set of nongenerators of G ([RZ10, Sec. 2.8]). The following

two propositions, which we state without proof, give us nice properties for the Frattini subgroup and the quotient $G/\Phi(G)$.

Proposition 2.21 (cf. [RZ10, Prop. 2.8.2])**.** Let G be a profinite group.

(i) If $N \lhd_c G$ and $N \leq \Phi(G)$, then $\Phi(G/N) = \Phi(G)/N$.

(ii) If $\rho : G \to H$ is a epimorphism of profinite groups, then $\rho(\Phi(G)) \leq \Phi(H)$.

(iii) If H is a closed subgroup of G and $H\Phi(G) = G$, then $H = G$.

Proposition 2.22 (cf. [RZ10, Lemma 2.8.7])**.** Let G be a pro-p group.

(i) Every maximal closed proper subgroup M of G has index p.

(ii) The Frattini quotient $G/\Phi(G)$ is a p-elementary abelian profinite group, and hence a vector space over the field with p elements.

(iii) $\Phi(G) = \overline{G^p[G,G]}$, where $G^p = \{x^p \mid x \in G\}$ and $[G,G]$ denotes the commutator subgroup of G.

The next lemma relates the Frattini subgroup and the first cohomology group of a pro-p group.

Lemma 2.23 ([RZ10, Remark 7.7.1])**.** Let G be a pro-p group.

(i) We have
$$H^1(G, \mathbb{Z}/p\mathbb{Z}) = \bigoplus_X \mathbb{Z}/p\mathbb{Z}\,.$$

(ii) The group $G/\Phi(G)$ is the (Pontryagin) dual of $H^1(G, \mathbb{Z}/p\mathbb{Z})$.

(iii) Let F be the free pro-p group over a set Y converging to 1. Then $H^1(F, \mathbb{Z}/p\mathbb{Z}) = \bigoplus_Y \mathbb{Z}/p\mathbb{Z}$.

Proof. (i) We have $H^1(G, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$, as the G-action on $\mathbb{Z}/p\mathbb{Z}$ must be trivial. Since $\Phi(\mathbb{Z}/p\mathbb{Z}) = 0$ and every nontrivial homomorphism $G \to \mathbb{Z}/p\mathbb{Z}$ is surjective, Proposition 2.21 implies that $\mathrm{Hom}(G/\Phi(G),\ \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Hom}(G,\ \mathbb{Z}/p\mathbb{Z})$, so

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G/\Phi(G), \mathbb{Z}/p\mathbb{Z})\,.$$

It follows from Proposition 2.22 that the above is an elementary abelian p-group, and the proposition follows.

(ii) We have

$$\begin{aligned}\mathrm{Hom}(G/\Phi(G), \mathbb{Q}/\mathbb{Z}) &\cong \mathrm{Hom}(G/\Phi(G), \mathbb{Z}/p\mathbb{Z}) \\ &\cong H^1(G, \mathbb{Z}/p\mathbb{Z})\,.\end{aligned}$$

(iii) Since Y converges to 1,

$$\begin{aligned}\mathrm{Hom}(F, \mathbb{Z}/p\mathbb{Z}) &= \{h : Y \to \mathbb{Z}/p\mathbb{Z} \mid h \text{ converges to } 0\} \\ &= \bigoplus_Y \mathbb{Z}/p\mathbb{Z}\,.\end{aligned}$$

□

Suppose G is a pro-p group. By the previous proposition we have $H^1(G, \mathbb{Z}/p\mathbb{Z}) = \bigoplus_X \mathbb{Z}/p\mathbb{Z}$. If we let F be the free pro-p group over X, then $H^1(G, \mathbb{Z}/p\mathbb{Z}) = H^1(F, \mathbb{Z}/p\mathbb{Z})$ and, by duality, we obtain an isomorphism $G/\Phi(G) = F/\Phi(F)$.

Proposition 2.24. Let G be a pro-p group. The following are equivalent:

(i) $\mathrm{cd}_p(G) \leq 1$.

(ii) G is free in the category of pro-p groups.

(iii) G is projective in the category of pro-p groups.

Proof. (i) $\Leftrightarrow$ (iii): It follows from Proposition 2.20.

(ii) $\Rightarrow$ (iii): Let G be a free pro-p group over X and $\psi : E \to W$ a onto homomorphism. Let $G \to W$ be a homomorphism. For every $x \in X$, let w_x be its image in W. Since $E \to W$ is surjective, we can lift it to an element $e_x \in E$. Thus, we have a (unique) homomorphism $G \to E$ such that the diagram

$$\begin{array}{ccc} & & G \\ & \swarrow & \downarrow \\ E & \longrightarrow & W \end{array}$$

commutes.

(i) $\Rightarrow$ (ii) ([RZ10, Th. 7.7.4]): By Lemma 2.23, $H^1(G, \mathbb{Z}/p\mathbb{Z}) = \bigoplus_X \mathbb{Z}/p\mathbb{Z} = H^1(F, \mathbb{Z}/p\mathbb{Z})$, where F is the free pro-p group over X, and by item (iii) of the lemma, we have the isomorphism

$$\varphi_0 : F/\Phi(F) \to G/\Phi(G)\,.$$

Since F is projective (as (ii) implies (iii)) and φ_0 is surjective, we can lift the homomorphism $F \to F/\Phi(F) \to G/\Phi(G)$ to a homomorphism $\varphi : F \to G$ such that the diagram

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & G \\ \downarrow & & \downarrow \\ F/\Phi(F) & \xrightarrow{\varphi_0} & G/\Phi(G) \end{array}$$

commutes.

Since F is projective (as (ii) implies (iii)) and $F \to G/\Phi(G)$ is surjective, we have $\varphi(F)\Phi(G) = G$ so, by Proposition 2.21, we have $\varphi(F) = G$. Thus, φ is surjective.

Since (i) implies (iii), then G is also projective, which implies that the identity $G \to G$ lifts to a map $\psi : G \to F$ such that $\varphi \circ \psi = \mathrm{id}_G$. This shows that ψ is injective and $\psi(G)\operatorname{Ker}(\varphi) = F$. The image $\varphi(\Phi(F))$ must be contained in $\Phi(G)$, and φ_0 being injective gives that $\Phi(F)\operatorname{Ker}\varphi \subset \Phi(G)$, so Proposition 2.21 shows that $\psi(G) = F$. Thus, ψ is isomorphic to the free group F. □

At last, we can prove the main result of this subsection.

Corollary 2.25. Let G be a profinite group. The following are equivalent:

(i) $\mathrm{cd}(G) \leq 1$.

(ii) G is projective in the category of profinite groups.

(iii) For every prime p, the p-Sylow subgroups of G are free (in the category of pro-p groups).

Proof. (i) $\Rightarrow$ (ii): ([Ser02, Chap. 1, Sec. 5.9, Exer. 3]) Let us consider extensions

$$1 \to P \to E \to W \to 1$$

where E is finite. We prove by induction on $|P|$ that G has the lifting properties with respect to such extensions. If $|P| = 1$ then $E \cong W$, so we suppose $|P| > 1$. Let p be a prime divisor of $|P|$ and consider a p-Sylow subgroup S of P. We have two cases:

If S is normal in P, then it is the unique p-Sylow of P, so it must be normal in E. We have the exact sequence

$$1 \to P/S \to E/S \to W \to 1$$

which splits by the induction hypothesis. We also have the exact sequence

$$1 \to S \to E \to E/S \to 1\,,$$

which splits by Proposition 2.20. Thus, we have a lifting $G \to E$.

If S is not normal in P, we consider $E' = N_E(S)$ and $P' = N_P(S) = E' \cap P$. It suffices to prove that $E' \to W$ is surjective; in this case, the exact sequence

$$1 \to P' \to E' \to W \to 1\,,$$

splits by the induction hypothesis, and since $E' \subset E$, it lifts $G \to W$ to $G \to E$. Let $x \in E$. The group xSx^{-1} is a p-Sylow subgroup of P, and since all p-Sylow subgroups are conjugate, there exists $y \in P$ such that $yxS(yx)^{-1} = S$. Thus $yx \in E'$, that is, $E = E' \cdot P$, and we conclude that $E' \to W$ is surjective.

Now, consider an arbitrary extension

$$1 \to P \to E \to G \to 1\,,$$

where P and E are profinite groups. Let E' be a closed subgroup of E minimal with respect to the following property: the restriction $E' \to G$ splits. If $P' = 1$ then the proposition follows. Let us suppose, then, that $P' \neq 1$. By Lemma 2.19, there exists a proper open subgroup P'' of P' that is normal in E', and the exact sequence

$$1 \to P'/P'' \to E/P'' \to G \to 1$$

splits by the previous paragraph, since P'/P'' is finite. The inverse image E'' of the lifting of G into E/P'' contradicts the minimality of E'.

(ii) $\Rightarrow$ (i): If G is projective, then it has the lifting property for extensions

$$1 \to P \to E \to W \to 1$$

where P is a pro-p group, for any prime p. Thus, $\mathrm{cd}_p(G) \leq 1$ for every p, that is, $\mathrm{cd}(G) \leq 1$.

(i) $\Leftrightarrow$ (iii): We have $\mathrm{cd}(G) \leq 1$ if, and only if, $\mathrm{cd}_p(G) = \mathrm{cd}_p(G_p) \leq 1$ for every prime p, where G_p is the p-Sylow subgroup of G. Proposition 2.24 shows us that G_p is free if, and only if, $\mathrm{cd}_p(G_p) \leq 1$. □

Using the cohomological dimension, it is easy to prove results such as this:

Corollary 2.26 ([Ser02, Chap. 1, Sec. 5, 9, Exer. 5])**.** A closed subgroup H of a projective profinite group G is projective.

Proof. By Proposition 2.13, we have $\mathrm{cd}(H) \leq \mathrm{cd}(G) \leq 1$, so H is projective. □

Examples 2.27. (i) The pro-p group $\mathbb{Z}_p$ is free of rank 1.

(ii) For any prime p, the p-Sylow subgroup of $\hat{\mathbb{Z}}$ is $\mathbb{Z}_p$. By item (iii) of Corollary 2.25, it follows that $\hat{\mathbb{Z}}$ is projective. In general, any product $\prod_p F_p$, in which F_p is a free pro-p group, is projective.

2.3 Galois cohomology

Let K/k be a Galois extension. If A is a commutative algebraic group over k, the Galois group $\mathrm{Gal}(K/k)$ acts naturally (and continuously) on $A(K)$. Since the Galois group, equipped with the Krull topology, is profinite, it makes sense to consider the cohomology groups $H^1(\mathrm{Gal}(K/k), A(K))$. We shall denote them by $H^1(K/k, A)$. When K is the separable closure of k, we shall denote it by $H^1(k, A)$.

Proposition 2.28. Let K/k be a Galois extension. It can be written as $K = \varinjlim K_i$, where the K_i ranges over the finite Galois subextensions of K. Furthermore, $\mathrm{Gal}(K/k) = \varprojlim \mathrm{Gal}(K_i/k)$.

Proof. If $x \in K$, the splitting field of k with respect to the minimal polynomial of x is a finite Galois extension of k that contains x and is contained in K, so $K = \varinjlim K_i$.

The group $G = \mathrm{Gal}(K/k)$ satisfies the universal property of the inverse system $\{\mathrm{Gal}(K_i/k)\}$. Indeed, if we have homomorphisms $\varphi_i : H \to \mathrm{Gal}(K_i/k)$ compatible with the system, we construct a homomorphism $H \to G$ that maps $h \in H$ to the following map σ_h: if $x \in K$ then it is contained in some K_i; define $\sigma(x) = \varphi(x)$. By compatibility this map is well defined, and it is also an isomorphism. The map $h \mapsto \sigma_h$ makes the necessary diagrams commute. □

Corollary 2.29. If K/k is Galois, then

$$H^q(\mathrm{Gal}(K/k), A(K)) = \varinjlim H^q(\mathrm{Gal}(K_i/k), A(K_i))$$

for every $q \geq 0$.

Proof. We just apply the previous proposition and Proposition 2.2. □

Examples 2.30. (i) Let K/k be a Galois extension. If K' is a finite Galois subextension of K, the normal basis theorem (see [Mor96, p. 61]) shows us that there exists $\beta \in K'$ such that $\{g(\beta)\}_{g\in G}$ is a k-basis for K'. We construct the map

$$\begin{aligned} K' &\to M_G^1(k) \\ \sum_{g\in G} \alpha_g g(\beta) &\mapsto (g \mapsto \alpha_g)\,. \end{aligned}$$

It is clearly an isomorphism. Then, for $q \geq 1$,

$$H^q(\mathrm{Gal}(K'/k), K') = H^q(\mathrm{Gal}(K'/k), M_G^1(K)) = 0$$

(Section 2.1), and, by the previous corollary, we pass to the limit and obtain

$$H^q(\mathrm{Gal}(K/k), K) = 0\,.$$

In particular, $H^q(k, \mathrm{G}_a) = 0$.

(ii) Suppose $\mathrm{char}(k) = p$. Let us consider the exact sequence

$$1 \to \alpha_p \to G_a \to G_a \to 1\,.$$

Passing to cohomology, the sequence

$$0 = H^{q-1}(k, \mathrm{G}_a) \to H^q(k, \alpha_p) \to H^q(k, \mathrm{G}_a) = 0$$

is exact for $q > 1$, so $H^q(k, \alpha_p) = 0$ for all $q > 1$. For $q = 1$, we have

$$0 \to \alpha_p(k) \to k \to k^p \to H^1(k, \alpha_p) \to 0\,,$$

and since $k \to k^p$ is injective, then $H^q(k, \alpha_p) = k^p/k$.

(iii) The equality $H^1(k, \mathrm{G}_m) = 0$ holds. This fact, proved by E. Noether, is known as Hilbert's Theorem 90 ([Ser79, Chap. X, Sec. 1, Prop. 2]). We reproduce the argument (also using multiplicative notation).

Let K/k be a finite extension. Let $t \mapsto a_t$ be a 1-cocycle, $c \in K$ and consider $b = \sum_{t\in\mathrm{Gal}(K/k)} a_t \cdot t(c)$. Since automorphisms are linearly independent, there is

some c such that b is not zero. We have

$$\begin{aligned} s(b) &= \sum s(a_t) \cdot st(c) \\ &= \sum a_s^{-1} a_{st} \cdot st(c) = a_s^{-1} b \ . \end{aligned}$$

Thus, $b^{-1} a_s s(b) = 1$, so a_s is a 1-coboundary by definition.

(iv) Item (iii) and the exact sequence

$$1 \to \mu_n \to \mathrm{G}_m \xrightarrow{n} \mathrm{G}_m \to 1$$

give us $H^1(k, \mu_k) = \mathrm{G}_m(k)/\mathrm{G}_m(k)^n$.

Proposition 2.31. Let K' be a Galois extension of k contained in K and let A be algebraic group defined over K. Then

$$M^{\mathrm{Gal}(K'/k)}_{\mathrm{Gal}(K/k)}(A(K)) = (R_{K/K'}(A))(K') \ .$$

Proof. The group $M^{\mathrm{Gal}(K'/k)}_{\mathrm{Gal}(K/k)}(A(K))$ is formed by the elements $A(K)$ invariant to the Galois action of $\mathrm{Gal}(K'/k)$; thus, the proposition follows from Corollary 1.29. □

When $K' = k$, the module $R_{K/k}(A)$ is cohomologically trivial.

We proceed with some results concerning the cohomological dimension of Galois groups. We denote the Galois group $\mathrm{Gal}(k_s/k)$ by G_k.

Proposition 2.32. Let k be a field of characteristic p. Then $\mathrm{cd}_p(G_k) \leq 1$ and $\mathrm{cd}(G_k(p)) \leq 1$.

Proof. Let $f(x) = x^p - x$. We have the exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathrm{G}_a \xrightarrow{f} \mathrm{G}_a \to 0 \ ,$$

which, passing to cohomology, gives us the exact sequence

$$H^1(k, G_a) \to H^2(k, \mathbb{Z}/p\mathbb{Z}) \to H^2(k, \mathrm{G}_a) \ .$$

We know that $H^q(k, \mathrm{G}_a) = 0$ for $q \geq 1$ by the previous example, which implies $H^2(k, \mathbb{Z}/p\mathbb{Z}) = 0$. By Proposition 2.17, we obtain $\mathrm{cd}_p(G_k) \leq 1$.

Let $G_k(p) = G_k/N$ be the largest quotient of G_k which is a pro-p group. If N has a map into a pro-p group, then its kernel K is such that G_k/K is pro-p, so $K = N$ and the

map is trivial. In particular, $H^1(N, \mathbb{Z}/p\mathbb{Z}) = 0$, and it follows that $\mathrm{cd}_p(N) \leq 1$. From the Hochschild-Serre Spectral Sequence ([NSW15, Th. 2.4.1]), we have

$$H^q(G/N, \mathbb{Z}/p\mathbb{Z}) \cong H^q(G, \mathbb{Z}/p\mathbb{Z}) \,,$$

so $\mathrm{cd}_p(G(p)) \leq \mathrm{cd}_p(G) \leq 1$. □

Let $G_k(p)$ be the largest quotient of G_k which is a pro-p group.

Corollary 2.33. The pro-p group $G_k(p)$ is free.

Proof. It follows from the previous proposition since a pro-p group is free if, and only if, its cohomological dimension is at most 1. □

Proposition 2.34. Let k be a field of characteristic $\neq p$, and n be an integer ≥ 1. The following are equivalent:

(i) $\mathrm{cd}_p(G_k) \leq n$.

(ii) For any algebraic extension K of k, we have $H^{n+1}(K, G_m)_p = 0$ and the group $H^n(K, \mathrm{G}_m)$ is p-divisible.

(iii) The same as (ii), but restricted to extensions K/k which are separable, finite and with degree prime to p.

Proof. Consider the exact sequence (at Examples 1.38 item (iv))

$$0 \to \mu_p \to G_m \xrightarrow{p} G_m \to 0 \,.$$

Then, (ii) (resp. (iii)) is equivalent to $H^{n+1}(K, \mu_p) = 0$ for algebraic extensions K/k (resp. for separable finite extensions K/k of degree prime to p). Indeed, the sequence above induces the two following exact sequences:

$$H^n(K, \mathrm{G}_m) \xrightarrow{p} H^n(K, \mathrm{G}_m) \to H^{n+1}(K, \mu_p) = 0 \,,$$

so the map $H^n(K, \mathrm{G}_m) \xrightarrow{p} H^n(K, \mathrm{G}_m)$ is surjective, and that means that $H^n(K, \mathrm{G}_m)$ is p-divisible; and

$$0 = H^{n+1}(K, \mu_p) \to H^{n+1}(K, \mathrm{G}_m) \to H^{n+1}(K, \mathrm{G}_m)$$

means that the map induced by p multiplication is injective, so it has to send the p-primary component to 0. On the other hand, those maps being injective and surjectively, respectively, imply (ii) (resp. (iii)).

(i) $\Rightarrow$ (ii): If $\mathrm{cd}_p(G_k) \leq n$, then its quotient G_K satisfies $\mathrm{cd}_p(G_K) \leq n$, so $H^{n+1}(K, \mu_p) = 0$. The proof follows as above.

(ii) $\Rightarrow$ (iii): It is clear.

(iii) $\Rightarrow$ (i): Let H be a p-Sylow subgroup in G_k. If K/k is its corresponding extension, then K can be written as the direct limit of its finite separable subextensions with degrees prime to p. By our hypothesis, $H^{n+1}(K_i, \mu_p) = 0$, so passing to the limit (Proposition 2.2), we obtain

$$H^{n+1}(K, \mu_p) = 0 \, .$$

Since H is a pro-p group, it acts trivially on $\mathbb{Z}/p\mathbb{Z}$. Since the polynomial $X^p - 1$ is separable then $\mu_p(K_s)$ has all p-roots of the unity, so we can identify μ_p with $\mathbb{Z}/p\mathbb{Z}$. Proposition 2.17 shows us that $\mathrm{cd}_p(H) \leq n$, so $\mathrm{cd}_p(G) \leq n$ since H is a p-Sylow subgroup of G. □

2.4 Non-abelian cohomology

Definition 2.35. A G-set E is a discrete topological space in which G acts continuously on. A G-group A is a group that is a G-set such that, for any $s \in G$, $x, y \in A$, it holds

$$^s(xy) = {}^s x \, {}^s y \, .$$

If E is a G-set, we define $H^0(G, E) = E^G$. If A is a G-group, we define the 1**-cocycles** as functions $a : G \to A$ such that

$$a(st) = a(s) \, {}^s a(t) \, .$$

We shall denote $a(s)$ as just a_s. We say that two cocycles a and a' are **cohomologous** if there exists $b \in A$ such that

$$a'_s = b^{-1} a_s \, {}^s b \, .$$

Since $(b_1 b_2)^{-1} = b_2^{-1} b_1^{-1}$ and ${}^s(b_1 b_2) = {}^s b_1 \, {}^s b_2$, this is an equivalence relation. The set $H^1(G, A)$ is then defined as the set of 1-cocycles modulo this equivalence relation. We shall consider $H^q(G, A)$, for $q = 0, 1$, as a **pointed set**, with the distinguished element being the class of the identity when $q = 0$, and the class of the map $G \to A$ that sends

all elements to the identity in A when $q = 1$. If X, Y, Z are pointed sets, the sequence

$$X \to Y \to Z$$

is called **exact** if the image of $X \to Y$ is exactly the preimage of the distinguished element in Z.

It is clear from the definition that, if A is abelian, the sets $H^0(G, A)$ and $H^1(G, A)$ coincide with the cohomology groups defined in Section 2.1.

Example 2.36 ([Ser02, Chap. 1, Sec. 5.1, Exer. 2])**.** Let σ be the canonical generator of $\hat{\mathbb{Z}}$. If E is a $\hat{\mathbb{Z}}$-set, then σ defines a permutation of E all of whose orbits are finite; conversely, such a permutation defines a $\hat{\mathbb{Z}}$-set structure.

Indeed, let $x \in E$. The action $\hat{\mathbb{Z}} \times E \to E$ being continuous implies that there exists an open subgroup U of G such that the orbit $U \cdot x$ has cardinality 1. The fact that the open subgroup U has finite index implies that the orbit of x is finite.

On the other hand, consider the function

$$\begin{aligned} f : \mathbb{Z} \times E &\to E \\ (n, e_i) &\mapsto \sigma^n(e_i) \, . \end{aligned}$$

If $\mathbb{Z}$ has the profinite topology and E is discrete, then f is continuous. Indeed, if $e \in E$ and $|G \cdot e| = n$, then

$$\begin{aligned} f^{-1}(e) &= \{(\sigma^{n+k}, e_k) \mid e_k \in G \cdot e, \sigma^k(e_k) = e\} \\ &= \bigcup_k (k + n\mathbb{Z}) \times \{e_k\} \, , \end{aligned}$$

which is open in $\mathbb{Z} \times E$. It gives that the map lifts to a continuous map $\hat{\mathbb{Z}} \times E \to E$, which defines a $\hat{\mathbb{Z}}$-set structure on E.

Example 2.37. ([Ser79, Chap. X, Sec. 1, Prop. 3]) The cohomology set $H^1(k, \mathrm{GL}_n)$ is trivial for every field k. The proof is analogous to that of Hilbert's Theorem 90 (see Examples 2.30 item (iii)).

2.4.1 Cohomology as elements of $G(K \otimes K)$

Let G be an affine group scheme and let S be a k-algebra. We define maps

$$d^i : \bigotimes_{j=1}^{n-1} S \to \bigotimes_{k=1}^{n} S$$

that inserts 1 after the i-th coordinate. We shall also denote the induced maps $G(d^i)$ as d^i. We say that $\varphi \in G(S \otimes S)$ is a 1**-cocycle** if $d^1\varphi = (d^0\varphi)(d^2\varphi)$. Elements $\varphi, \psi \in G(S \otimes S)$ are **cohomologous** if $\psi = (d^0\lambda)^{-1}\varphi(d^1\lambda)$ for some $\lambda \in G(S)$. The set $H^1(S/R, G)$ of equivalence classes of cocycles modulo the equivalence relation is a pointed set.

Now, let K/k be a finite Galois extension with Galois group Γ. The map

$$\begin{aligned} \Phi : K \otimes K &\to \prod_{\sigma\in\Gamma} K \\ a \otimes b &\mapsto (\sigma(a)b)_\sigma \end{aligned}$$

is a homomorphism, since its corresponding map $K \times K \to \prod_{\sigma\in\Gamma} K$ is bilinear. It is, in fact, an isomorphism. We reproduce the proof in [Bou12, Sec. V.4, Prop. 7]. Let $W = \operatorname{Ker}\Phi$, and consider maps $T_\tau : \prod_{\tau\in\Gamma} K \to \prod_{\tau\in\Gamma} K$ that sends $(\sigma(a)b)_\sigma$ to $(\sigma(a)b)_{\tau^{-1}\circ\sigma}$. The equality

$$T_\sigma \circ \Phi = \Phi \circ (T_\sigma \otimes \mathrm{id})$$

is immediate. It implies that W is stable under the action of $(T_\sigma \otimes \mathrm{id})$ for every $\sigma \in \Gamma$. The subset of K that is invariant under the action of K is exactly k, so elements in W have the form $1 \otimes b$. Since $\Phi(1 \otimes b) = (b)_\sigma$, then $1 \otimes b \in W$ if and only if $b = 0$. We conclude that $W = 0$, that is, Φ is injective. Since both the domain and codomain of Φ have dimension $[K : k]^2$, Φ is also surjective.

The isomorphism allow us to write

$$G(K \otimes K) = G(\prod_{\Gamma} K) = \prod_{\Gamma} G(K)\ ,$$

that is, elements of $G(K \otimes K)$ can be identified with functions $\Gamma \to G(S)$. A similar argument provides us with the isomorphism.

$$\begin{aligned} K \otimes K \otimes K &\to \prod_{(\sigma,\tau)\in\Gamma\times\Gamma} K \\ a \otimes b \otimes c &\mapsto (\sigma(a)\tau(b)c)_\sigma\ . \end{aligned}$$

Let $f : \Gamma \to G(S)$ be the function corresponding to $a \otimes b \in G(K \otimes K)$. We have

$$\begin{aligned}(d^0 f)(\sigma, \tau) &= \tau(a)b = f(\tau) \,, \\ (d^1 f)(\sigma, \tau) &= \sigma(a)b = f(\sigma) \,, \\ (d^2 f)(\sigma, \tau) &= \sigma(a)\tau(b) = \tau f(\tau^{-1}\sigma) \,.\end{aligned}$$

Tracing back the definition, f is a 1-cocycle if, and only if,

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

for every $\sigma, \tau \in \Gamma$. Substituting $\rho = \tau^{-1}\sigma$, we have

$$f(\tau\rho) = f(\tau)\tau f(\rho) \,,$$

and we recover our original definition of 1-cocycles. Similarly, if $\lambda \in G(K)$,

$$\begin{aligned}(d^0\lambda)(\sigma) &= a \,, \\ (d^1\lambda)(\sigma) &= \sigma(a) \,,\end{aligned}$$

so the cohomologous condition is $\psi(\sigma) = a^{-1}\varphi(\sigma)\sigma(a)$ for every $\sigma \in \Gamma$, as expected.

Lemma 2.38. Let G be an affine algebraic group G and $S = \varinjlim S_i$ a k-algebra. Then $G(S) = \varinjlim G(S_i)$.

Proof. Let A be the Hopf algebra representing G, and let $\varphi : A \to S$ be an element of $G(S)$. By hypothesis, A is finitely generated, suppose by $x_1, \ldots, x_n$. As $S = \lim S_i$, there exists an index j such that S_j contains all of $\varphi(x_1), \ldots, \varphi(x_n)$. Then, we can corestrict φ to S_j, and it corresponds to an element of $G(S_j)$. □

Proposition 2.39. Let G be an algebraic group and K/k infinite Galois with group Γ. The definition of $H^1(K/k, G)$ at the start of this subsection coincides with the definition at the start of Section 3.

Proof. We know that $K = \lim K_i$ where K_i run over all finite subextensions. By the lemma above, $G(K_i) = \varinjlim G(K_i)$.

Let F and F' be finite subextensions of K with Galois groups $\Gamma_F, \Gamma_{F'}$ respectively, such that $F \subset F'$. We saw in this section that if we interpret $G(F \otimes F)$ and $G(F' \otimes F')$ as functions from the corresponding (finite) Galois groups, then morphisms $G(F \otimes F) \to G(F' \otimes F')$ corresponds to

$$\{\Gamma/\Gamma_F \to G(F)\} \to \{\Gamma/\Gamma_{F'} \to G(F')\} \,.$$

By the lemma, $G(K \otimes K) = \varinjlim G(K_i \otimes K_i)$. The correspondence above applied to this equality shows us that $G(K \otimes K)$ corresponds to the set

$$\{f : \Gamma \to G(K) \mid \text{f constant on some } \Gamma_{K_i} \text{ with finite index})\} .$$

That is exactly the set of 1-cochains. □

2.5 Fields with dimension ≤ 1

Let k be a field and $G_k = \mathrm{Gal}(k_s/k)$. For now, we define the **Brauer group** of K as $\mathrm{Br}(K) = H^2(K, \mathrm{G}_m)$. In Section 3.2, we shall see the classical definition of the Brauer group and prove that both definitions are equivalent. If L/K is a finite extension, we define the **norm** $N_{L/K} : L^* \to K^*$ as the determinant of the matrix with coefficients in K corresponding to the linear transformation $x \mapsto lx$ for $l \in L^*$. Since $x \mapsto lx$ is invertible, its determinant is nonzero. Both the Brauer group and the norm are closely related to the cohomological dimension of G_k, as we shall see in this subsection.

Lemma 2.40. Let k' be a purely inseparable extension of a field k of characteristic p. Then the map $\mathrm{Br}(k') \to \mathrm{Br}(k)$ is surjective.

Proof. Since k'/k is purely inseparable then $G_k = \mathrm{Gal}(k_s/k)$ can be identified with the Galois group of k'_s/k'. The extension k'_s is purely inseparable over k_s, so for every element $x \in k'_s$ there exists a power q of p such that $x^q \in k_s$. Thus, $\mathrm{G}_m(k'_s)/\mathrm{G}_m(k_s)$ is a p-primary torsion group. Corollary 2.33 shows that $\mathrm{cd}_p(G_k) \leq 1$, so $H^2(G_k, \mathrm{G}_m(k'_s)/\mathrm{G}_m(k_s)) = 0$. Consider the exact sequence

$$1 \to \mathrm{G}_m(k_s) \to \mathrm{G}_m(k'_s) \to \mathrm{G}_m(k'_s)/\mathrm{G}_m(k_s) \to 1 .$$

Passing to cohomology, the map $H^2(G_k, \mathrm{G}_m(k_s)) \to H^2(G_k, \mathrm{G}_m(k'_s))$ is surjective. □

Theorem 2.41. The following properties are equivalent.

(i) One has $\mathrm{cd}(G_k) \leq 1$. Furthermore, if $\mathrm{char}(k) = p \neq 0$, then $\mathrm{Br}(K)_p = 0$ for every algebraic extension K/k.

(ii) One has $\mathrm{Br}(K) = 0$ for every algebraic extension K/k.

(iii) If L/K is a finite Galois extension with K algebraic over k, the $\mathrm{Gal}(L/K)$-module L^* is cohomologically trivial.

(iv) Under the hypothesis of (iii), the norm $N_{L/K} : L^* \to K^*$ is surjective.

(i'), (ii'), (iii'), (iv'): the same assertions, but assuming K/k is a finite separable extension.

Proof. The equivalences (i) ⇔ (i') and (ii) ⇔ (ii') follow from Lemma 2.40.

(i) ⇒ (ii): Since G_K is a closed subgroup of G_k, we have $\mathrm{cd}(G_K) \leq \mathrm{cd}(G_k) \leq 1$ (Proposition 2.13). It is immediate that $\mathrm{Br}(K) = H^2(G_K, K^*) = 0$.

(ii) ⇒ (i): It follows from Propositions 2.32 and 2.34.

(iii') ⇒ (iv'): Since L^* is cohomologically trivial, then

$$\hat{H}^0(\mathrm{Gal}(L/K), L^*) = (L^*)^G / N_{L/K}(L^*) = 0\ ,$$

that is, $K^* = N_{L/K}(L^*)$.

(iii') ⇒ (ii'): Since L^* is cohomologically trivial, we have $H^2(\mathrm{Gal}(L/K), \mathrm{G}_m) = 0$. It remains to prove for subextensions of K, which holds by passage to the limit.

(ii') ⇒ (iii'): Let H be a subgroup of $\mathrm{Gal}(L/K)$. We know from Examples 2.30 that $H^1(H, L^*) = 0$, and $H^2(H, L^*) = 0$ holds by hypothesis, so L^* is cohomologically trivial (see Section 2.1).

(iv') ⇒ (iii') It follows just as above, except that here our hypothesis is $\hat{H}^0(H, L^*) = 0$.

We have that (iii) implies (iii') and (iv) implies (iv') trivially. It remains to show the converses, but it suffices to show that (ii) implies (iii) and (iv). If k satisfies (ii) then every algebraic extension of K/k also satisfies (ii). Thus, every such K/k also satisfies (iii') and (iv'), hence k satisfies (iii) and (iv). □

Definition 2.42. A field satisfying the equivalent conditions of Proposition 2.41 is said to have dimension ≤ 1. We shall also write $\dim(k) \leq 1$.

If we look at, say, item (ii), it is clear that any algebraic extension of a field of dim ≤ 1 also has dim ≤ 1.

We have an important class of fields with this property.

Definition 2.43. We say that a field k satisfy (C_1) if every homogeneous polynomial $f(x_1, \ldots, x_n)$ of degree $1 \leq d < n$ with coefficients in k has a nontrivial solution in k^n.

Proposition 2.44. Let k be a field satisfying (C_1).

(i) Every algebraic extension K/k satisfies (C_1).

(ii) If L/K is a finite extension, with K/k algebraic, then $N_{L/K} : L^* \to K^*$ is surjective.

Proof. (i) Let $P(x)$ be a polynomial in $K[X_1, \ldots, X_n]$ of degree $d < n$. There exists a subextension K'/k of K such that K'/k is a finite extension and $P(x) \in K'[X_1, \ldots, X_n]$. Thus, we will assume that K/k is finite. Let $\{b_1, \ldots, b_m\}$ be a k-basis for K, and let us consider $N_{K/k}(P(x))$ written in this basis. We can see it as a polynomial in nm variables of degree $dm < nm$, so, since k satisfy (C_1), it has a nontrivial solution. We know that $N_{K/k}(P(x)) = 0$ if, and only if, $P(x) = 0$, so it is also a nontrivial solution to $P(x)$.

(ii) Let $a \in K^*$ and $d = [L : K]$. Consider equation

$$N(x, x_0) = (ax_0^d) \cdot x \ .$$

It has degree d and $d+1$ variables, so, since K is also (C_1) by (a), it has a nontrivial solution (x, x_0). If $x_0 = 0$ then $N(x, x_0) = 0$, which implies $x = 0$, a contradiction. Thus, there is a nontrivial solution with $x_0 \neq 0$. It follows that the norm N is surjective.

□

Item (ii) of Proposition 2.44 implies item (iv') of Theorem 2.41; it follows that every field that satisfies (C_1) has dim ≤ 1.

Examples 2.45. (i) A finite field $k = F_q$ satisifes (C_1), and so it has dim ≤ 1. Indeed, let us consider the Chevalley-Warning Theorem ([Ser96, Th. 2.2.3]): if $\{f_i\}$ is a set of polynomials in n variables on the finite field k satisfying $\sum_i \deg f_i < n$, then the number of simultaneous solutions to $\{f_i\}$ is congruent to 0 (mod p). If we take h as a homogeneous polynomial such that $0 < \deg h < n$, then it has a trivial solution, so the theorem implies that it must also have a nontrivial solution.

(ii) ([Ser02, Chap. 2, Sec. 3, Exer. 3]) Let k be a perfect field. The following are equivalent:

(a) k is algebraically closed.

(b) $\dim k((t)) \leq 1$.

(c) $\dim k(t) \leq 1$.

Chapter 3

Null cohomology theorems

It is known that, if k is a field of characteristic 0, the following are equivalent ([Sch17, Sec. 5.1]):

(i) Every nonzero semisimple Lie algebra over k contains a nonzero nilpotent element.

(ii) Every semisimple Lie algebra over k contains a Borel subalgebra.

(iii) The field k has dimension at most one.

Serre was interested in analogous properties for algebraic groups, and in [Ser62] he made the following conjecture:

Conjecture I. If k is a perfect field of dimension at most one, and if L is a connected linear algebraic group defined over k, then $H^1(k, L) = 0$.

Some cases were already proved when the conjecture was stated: namely, when k is a finite field, and when L is soluble. We prove them in Sections 3.3 and 3.4, respectively. Since $H^1(k, L)$ being trivial for every connected linear algebraic group L is equivalent to every semisimple algebraic group over k containing a Borel subgroup, we obtain an analogous result to the Lie algebra case.

3.1 Homogeneous spaces and Twist

Let G be a profinite group, and let A be a G-group as defined in Section 2.4.

Definition 3.1. A **principal homogeneous space** over A is a non-empty G-set P on which A acts on the right compatibly with G, satisfying: for every $x, y \in P$ there is a unique $a \in A$ such that

$$y = x \cdot a.$$

An isomorphism between two A-principal spaces is a map that preserves both the left G-action and the right A-action. Thus, it makes sense to talk about classes of A-principal spaces. If we fix an element x_0 of an A-principal space P, the definition implies that the map $a \mapsto x_0 \cdot a$ is a bijection of A onto P. Essentially, P is the set A with a "twisted" G-action. We can prove that the set of classes of A-principal spaces is in a bijective correspondence with the cohomology set $H^1(G, A)$, defining the twisted G-action using cocycles:

Proposition 3.2. There is a bijection between the set of classes of principal homogeneous spaces on A and the set $H^1(G, A)$.

Proof. Let a_s be a cocycle and let $P = A$, with the right A-action on P being the product in A. We define a G-action on P by

$${}^{s'}x = a_s \cdot {}^{s}x \ .$$

where, ${}^{s'}x$ is the notation for s acting on x by this action. This action is compatible with the A-action: we have

$${}^{s'}(x \cdot a) = a_s \, {}^{s}(x \cdot a) = (a_s \, {}^{s}x) \cdot {}^{s}(a) = {}^{s'}x \, {}^{s'}a \ .$$

Since A is a group, for every $x, y \in P$, there is a unique a such that $x = y \cdot a$, namely $a = y^{-1}x$. Thus, the set P, with the given left G-action and right A-action, is a principal homogeneous space over A.

On the other hand, let P be an A-principal homogeneous space. Fixing $x \in P$, for every $s \in G$ we have $a_s \in A$ such that ${}^{s}x = x \cdot a_s$. The map $s \mapsto a_s$ is a cocycle. Indeed,

$${}^{s}({}^{t}x) = {}^{s}(x \cdot a_t) = x \cdot (a_s \, {}^{s}a_t) \ ,$$

however, by definition, we have $a_{st} = (a_s \, {}^{s}a_t)$. □

Definition 3.3. If F is a G-set on which A acts on the left compatibly with G, we denote the quotient of $P \times F$ by the relation $(p, f) \sim (p \cdot a, a^{-1}f)$, $a \in A$, by $P \times^A F$, or ${}_PF$. We say that ${}_PF$ was obtained by **twisting** F **using** P.

Consider ${}_PF$ as in the previous definition. Since the classes of (pa, f), (paa^{-1}, af) and (p, af) coincide, we can denote (p, f) simply as pf. We can also twist such a G-set F using a cocycle a_s by the formula

$$ {}^{s'}f = f \cdot a_s $$

for every $f \in F$. We note that this formula is exactly the action defined in the proof of Proposition 3.2; it follows that twisting F by a principal space P or by a cocycle a in its corresponding cohomology set yields the same object. We can also denote ${}_PF$ as ${}_aF$.

Proposition 3.4. Let F and F' be two G-sets with compatible right A-action. The twisting has the following properties:

(i) ${}_aF$ is functorial over F.

(ii) We have ${}_a(F \times F') = {}_aF \times {}_aF'$.

(iii) If a G-group B acts on the right on F (so that it commutes with the action of A), then B also acts on the right on ${}_aF$.

Proof. It is all basic computations.

(i) If $\varphi : F \to F'$ is a G-morphism, then it induces a morphism ${}_aF \to {}_aF'$ in the obvious way. We have

$$ \begin{aligned} {}^{s'}\varphi(f) &= a_s \cdot {}^s\varphi(f) \\ &= \varphi(a_s\, {}^s f) = \varphi({}^{s'}f)\,. \end{aligned} $$

(ii) The obvious map ${}_a(F \times F') \to {}_aF \times {}_aF'$ is a G-morphism:

$$ \begin{aligned} {}^{s'}(f, f') &= a_s\, {}^s(f, f') \\ &= (a_s\, {}^s f, a_s\, {}^s f') = ({}^{s'}f, {}^{s'}f')\,. \end{aligned} $$

(iii) Since the B-action commutes with the A-action on F, it is compatible with the twisted G-action on ${}_aF$. □

Examples 3.5. (i) Let $F = A$ acting on itself by left translations. Pairs (p, a) are just $(pa, 1)$, and the map $(pa, 1) \mapsto p \cdot a$ is a bijection that preserves the A-action. Therefore, $P \times {}^A A = P$.

(ii) Let $G = 1$. We have $H^1(G, A) = 1$, so Proposition 3.2 tells us that there is only one class of A-principal homogeneous spaces with respect to $G = 1$, namely the class of A itself, so $P \times {}^A A = A$ for any A-principal space P.

Definition 3.6. Let A and A' be G-groups. An (A, A')**-principal space** is a G-set that is a principal left A-space and a principal right A'-space with commuting actions of A and A'.

If P is an (A, A')-principal space and Q is an (A', A'')-principal space, we can define an (A', A'')-principal space $P \circ Q = P \times^{A'} Q$. The A'-action on the left is defined as

$$a'(p, q) = (p \cdot a', q) = (p, a' \cdot q) ,$$

and the A''-action on the right as

$$(p, q) \cdot a'' = (p, q \cdot a'') .$$

If $A = A'$, the composition defined above makes the set of isomorphism classes of (A, A)-principal spaces into a group, and we can determine its structure if A is abelian:

Proposition 3.7 ([Ser02, Chap. 1, Sec. 5.3, Exercise])**.** Let A be a G-group. Let $E(A)$ be the set of classes of (A, A)-principal spaces. The composition makes $E(A)$ into a group, and this group acts on $H^1(G, A)$. If A is abelian, $E(A)$ is the semi-direct product of $\mathrm{Aut}(A)$ by the group $H^1(G, A)$.

Proof. Let P_1, P_2, P_3 be (A, A)-principal spaces. The map

$$\begin{aligned} \Phi : P_1 \circ (P_2 \circ P_3) &\longrightarrow (P_1 \circ P_2) \circ P_3 \\ (p_1, (p_2, p_3) &\mapsto ((p_1, p_2), p_3) \end{aligned}$$

is an isomorphism of (A, A)-principal spaces, so the composition is associative.

The neutral element is A acting on itself by left translations. Indeed, we already saw in Example 3.5 (i) that $P \times^A A = P$ for every principal space P.

Let P be a (A, A)-principal space. We define the principal space $\overline{P}$ as follows: as a G-set it is just P, and the A-action is defined by

$$\begin{aligned} a \cdot p &= p \cdot a^{-1} , \\ p \cdot a &= a^{-1} p . \end{aligned}$$

We claim that $P \circ \overline{P} = A$. Fixing $p_0 \in P$, all pairs can be written in the form $p_0 p$ for some $p \in \overline{P}$. By definition, there is a unique $a \in A$ such that $p = a \cdot p_0$, so we define the

map $f : p_0(a \cdot p_0) \mapsto a$. If $b \in A$, then $b \cdot (p_0, a \cdot p_0) = (p_0, ba \cdot p_0)$, so

$$\begin{aligned} b \cdot f(p_0, a \cdot p_0) &= ba \\ &= f(p_0, ba \cdot p_0) = f(b \cdot (p_0, a \cdot p_0)) \ , \end{aligned}$$

so f preserves the A-action. We conclude that $P \circ \overline{P} = A$.

Consider the sequence

$$1 \to H^1(G, A) \xrightarrow{\varphi} E(A) \xrightarrow{\psi} \mathrm{Aut}(A) \to 1 \ ,$$

in which φ maps an A-principal space into an (A, A)-principal space where the left action is just the right action, and ψ takes an (A, A)-principal space into $\mathrm{Aut}(A)$ in this way: let $P \in E(A)$ and fix $x \in P$. For every $a \in A$ there is exactly one $b \in A$ such that $a \cdot x = x \cdot b$. We send the class of P into the map $a \mapsto b$. It is in fact an automorphism: it is clearly bijective, and it is a homomorphism because, if we have $(a'x = xb')$, then

$$\begin{aligned} (aa') \cdot x &= a \cdot (a' \cdot x) \\ &= a \cdot (x \cdot b') \\ &= (x \cdot b) \cdot b' = x \cdot (bb') \ . \end{aligned}$$

The sequence is exact, because P belongs to $\operatorname{Ker} \psi$ if, and only if, the right and left A-actions coincide, and that means that P comes from a right A-principal space.

If A is abelian, the map $\varphi' : E(A) \to H^1(G, A)$ that sends an (A, A')-principal space into its left A-principal space structure is an homomorphism such that $\varphi' \circ \varphi = \mathrm{id}$, so $E(A) = H^1(G, A) \rtimes \mathrm{Aut}(A)$. □

Proposition 3.8. Let P be a right principal homogeneous space for a G-group A, and let $A' = {}_PA$ be the corresponding group. If we associate to each principal (right)-homogeneous space Q over A' the composition $Q \circ P$, we obtain a bijection of $H^1(G, A')$ onto $H^1(G, A)$ that takes the neutral element of $H^1(G, A')$ into the class of P in $H^1(G, A)$.

Proof. We define $\overline{P}$ similarly to what we did in the previous proposition: it is a set P, and if $a \in A, a' \in A'$, we give it a (A, A')-principal space structure by:

$$\begin{aligned} a \cdot p &= pa^{-1} \ , \\ p \cdot a' &= (a')^{-1} \cdot p \ . \end{aligned}$$

As expected, we have $Q \circ P \circ \overline{P} = Q$. Indeed, fixing $p_0 \in P$, every element can be written in the form (q, p_0, p_0), and we have

$$\begin{aligned}(q, p_0, p_0) \cdot a' &= (q, p_0, p_0 \cdot a') \\ &= (q, p_0, (a')^{-1} \cdot p_0) \\ &= (q, p_0 \cdot (a')^{-1}, p_0) \\ &= (q, a' \cdot p_0, p_0) = (q \cdot a', p_0, p_0)\,.\end{aligned}$$

So, the map $(q, p_0, p_0) \mapsto q$ preserves the right A'-action; it is also bijective, so it is an isomorphism. If Q' is a homogeneous space over A, the equality $Q' \circ \overline{P} \circ P = Q'$ holds and its proof is analogous. Thus, the maps $Q \mapsto Q \circ P$ and $Q' \mapsto Q' \circ \overline{P}$ are the inverses of each other. □

We will now use this tool to prove that some sequences of pointed sets are exact. Let A be a subgroup of B. We have the following proposition:

Proposition 3.9 ([Ser62, Chap. I, Prop. 5.4.36])**.** The sequence of pointed sets

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

is exact.

Proof. We first define δ. If bA is a class of B/A, then $bA \in (B/A)^G$ means that ${}^s b \in bA$ for every $s \in G$; that is, bA is a well-defined G-set. We make it into a right A-principal space by defining the A-action as right multiplication. We define $\delta(bA)$ as this space. In terms of cocycles, $\delta(bA)$ corresponds to $a_s = b^{-1}\,{}^s b = b^{-1}ba = a$, so its image in $H^1(G, B)$ is just the neutral element. In particular, if $b \in B^G$, then $\delta(bA)$ is simply A, with A-action given by right translations.

Exactness at $H^0(G, B)$: if $a \in A^G$, then its image at $H^0(G, B/A)$ is the neutral element represented by A with right translations. Let $b \in B^G$ be an element mapped to the neutral element. Then $s \cdot b = ba$ for some $a \in A$. but also $s \cdot b = b$, so $a = 1$ and $b \in A$, and we conclude that $b \in A^G$.

Exactness at $H^0(G, B/A)$: Let $bA \in (B/A)^G$ be mapped to the neutral element. We have ${}^s(ba) = ({}^s b\,{}^s a)$, but the G-action on bA must the G-action on A, so ${}^s(ba) = b\,{}^s a$, so ${}^s b = b$, that is, $b \in B^G$.

Exactness at $H^1(G, A)$: Let a_s be a cocycle that is trivial in $H^1(G, B)$. Then $a_s = b^{-1}\,{}^s b$ for some $b \in B$, but that is exactly $\delta(bA)$ as a cocycle. □

We can describe the image of $H^1(G, A)$ in the sequence above. This proposition will be needed later on to prove a lemma used in the proof of Theorem 3.30.

Proposition 3.10 ([Ser62, Chap. I, Prop. 5.4.37])**.** Let $\beta \in H^1(G, B)$ and let $b \in Z^1(G, B)$ be a representative for β. Then β belongs to the image of $H^1(G, A)$ if, and only if, the space ${}_b(B/A)$, obtained by twisting B/A by b, has a point fixed under G.

Proof. Let $c \in {}_b(B/A)$. The G-action is defined as ${}^{s'}c = b_s \cdot {}^s c$ for some cocycle b_s. Then, $c \in H^0(G, {}_b(B/A))$ if, and only if

$$c = b_s \, {}^s c \ .$$

if b is a representative of c, then this holds if, and only if, $b = b_s \cdot {}^s c \cdot a$ for some $a \in A$, that is,

$$b^{-1} b_s \, {}^s b \in A \ ,$$

but that means that b_s is cohomologous to a cocycle which has its image contained in A, so the class of b_s belongs in the image of $H^1(G, A)$. □

Now, if A is normal in B, the exact sequence can be extended:

Proposition 3.11 ([Ser62, Chap. I, Prop. 5.5.38])**.** Let A be normal in B and let $C = B/A$. Then, the sequence

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

is exact.

Proof. We only need to prove the exactness at $H^1(G, B)$. If the image of b_s is $c^{-1} \, {}^s c$ for some $c \in C$ then $b_s = b^{-1} \, {}^s b a$ for some $b \in B$. The cocycle b_s is cohomologous to

$${}^s b a \, {}^s(b^{-1}) = {}^s b a ({}^s b)^{-1} \ ,$$

which is in A, so it is the image of the cocycle's class in $H^1(G, A)$. On the other hand, it is clear that a cocycle a_s will have trivial image in $H^1(G, C)$. □

Proposition 3.12 ([Ser62, Chap. I, Prop. 5.7.43])**.** Let A be contained in the center of B and let $C = B/A$. Then, the sequence

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \xrightarrow{\Delta} H^2(G, A)$$

is exact.

Proof. Let c represent a class of $H^1(G, C)$. Lifting it to a continuous map $s \mapsto b_s$ of G into B, we define $\Delta(c) = a_{s,t}$, with

$$a_{s,t} = b_s \, {}^s b_t b_{st}^{-1} .$$

Since C acts on A by conjugation, the twisted group ${}_C A$ obtained by the twisted action

$${}^{s'}a = b_s \, {}^s a b_s^{-1} .$$

The identity

$$a_{s,t} = {}^{s'}a_{t,u} \cdot a_{s,tu} \cdot a_{st,u}^{-1}$$

holds, thus making $a_{s,t}$ a 2-cocycle representing a class of $H^2(G, {}_c A)$. Replacing the lifting b_s with a lifting $a'_s b_s$, we get a 2-cocycle $a'_{s,t} \cdot a_{s,t}$, where

$$a_{s,t} = a'_s \cdot {}^{s'}a'_t \cdot a'^{-1}_{st}$$

that is, $a'_{s,t}$ is a coboundary. We conclude that both liftings define the same class $\Delta(c)$ in $H^1(G, {}_c A)$.

Up to this point, we have not used the fact that A is in the center of B. In this case, the action of C on A is trivial, so we can identify ${}_c A$ with A, and hence identify $H^1(G, {}_c A)$ with $H^1(G, A)$, so $\Delta(c)$ lies in the latter.

It remains to prove that the sequence is exact at $H^1(G, C)$. The definition of Δ implies that $\Delta(c) = a_{s,t}$ is mapped to the trivial class if, and only if, the lifting $s \mapsto b_s$ is a 1-cocycle defining a class $H^1(G, B)$. □

3.2 K/k forms

Let us consider two vector spaces over a field k. If K is a field extension of k, it is clear that the spaces are isomorphic over k if, and only if, they are isomorphic over K. However, if we endow them with additional structure, such as the structure of a k-algebra, it becomes more subtle. We shall see in this section that this problem has a deep relation with cohomology.

Let V be a k-vector space. A **tensor** of type (p, q) is an element $x \in (\bigotimes^p V) \otimes (\bigotimes^q V^*)$.

Proposition 3.13. We have $(\bigotimes^p V) \otimes (\bigotimes^q V^*) \cong \mathrm{Hom}_k(\bigotimes^q V, \bigotimes^p V)$.

Proof. Let $x = (v_1 \otimes \cdots \otimes v_p \otimes f_1 \cdots \otimes f_q)$, and define the homomorphism

$$\Phi : (w_1, \ldots, w_q) \mapsto f_1(w_1) f_2(w_2) \cdots f_q(w_q)(v_1 \otimes \cdots \otimes v_p) \, .$$

If $\Phi(x) = 0$, then either $(v_1 \otimes \cdots \otimes v_p) = 0$ or some $f_i = 0$. In either case, it implies $x = 0$, so Φ is injective. Let us take a basis $\{e_i\}$ and its dual $\{e_i^*\}$. The element $(e_{i_1} \otimes \cdots \otimes e_{i_p} \otimes e_{j_1}^* \otimes \cdot \otimes e_{j_q}^*)$ is mapped to a homomorphism defined by

$$(w_1, \ldots, w_q) \mapsto \begin{cases} (e_{i_1} \otimes \cdots \otimes e_{i_p}) & \text{if } w_k = e_{j_k} \text{ for k} = 1 \ldots, q \, , \\ 0 & \text{otherwise.} \end{cases}$$

The set of these maps spans $\mathrm{Hom}_k(\bigotimes^q V, \bigotimes^p V)$. □

Now, let us consider pairs (V, x) where V is a k-vector space and x is a (p, q) tensor. A **homomorphism** $(V, x) \to (V', x')$ is defined as a homomorphism $V \to V'$ that maps x to x', and an **isomorphism** between such pairs is defined as a invertible homomorphism.

Let V be an k-algebra, that is, a k-vector space equipped with a homomorphism $V \otimes V \to V$. By the previous proposition, this homomorphism corresponds to a tensor x of type $(1, 2)$. Thus, an automorphism $(V, x) \to (V, x)$ is an isomorphism $V \to V$ of k-vector spaces that preserves the product $V \otimes V \to V$, or, in other words, an automorphism of V as a k-algebra. Now, let (V, x) be a pair such that x is of type $(0, 2)$. Since pairs of this type correspond to bilinear forms (i.e. homomorphisms $V \otimes V \to k$), then automorphisms of (V, x) correspond to automorphisms of V that preserve the bilinear form. We shall use tensors in this section to express those additional structure that V may have.

We shall denote the K-vector space $V \otimes K$ as V_K. If x is a tensor with respect to V, the element $x \otimes 1$ of $(\bigotimes^p V) \otimes (\bigotimes^q V^*) \otimes K$ is a tensor with respect to V_K. We denote it by x_K.

Definition 3.14. A K/k **form** of a pair (V, x) is a pair (V', x') such that (V_K, x_K) is isomorphic to (V'_K, x'_K).

We can reformulate the question at the beginning of this section as follows: is there more than one isomorphism class of K/k forms of (V, x)? Strikingly, the set of such isomorphism classes is in a bijective correspondence with a certain cohomology set, as we shall see.

Let Aut_K be the group of K-automorphisms of (V_K, x_K). If $f : (V_K, x_K) \to (V'_k, x'_K)$ is an isomorphism, we define a function $\theta(f) : \mathrm{Gal}(K/k) \to \mathrm{Aut}_k$ by

$$\theta(f) = (s \mapsto f^{-1} \circ {}^s f) ,$$

where ${}^s f$ is the induced Galois action on Aut_k. This map is well-defined. Denoting by f_s the element $\theta(f)(s)$, we have

$$\begin{aligned} f_s \, {}^s f_t &= (f^{-1} \, {}^s f) \, {}^s(f^{-1} \, {}^t f) \\ &= f^{-1} ({}^s f)({}^s f^{-1}) \, {}^{st} f \\ &= f^{-1} \, {}^{st} f = f_{st}. \end{aligned}$$

that is, $\theta(f)$ is a 1-cocycle. If g is another such isomorphism, then $f^{-1}g \in \mathrm{Aut}_K$, and so

$$(f^{-1}g)^{-1} \circ (f^{-1} \, {}^s f) \circ {}^s(f^{-1}g) = g^{-1} \, {}^s g \, .$$

Thus, $\theta(f)$ and $\theta(g)$ are cohomologous, and so θ does not depend on the choice of the isomorphism f.

Proposition 3.15. The map θ from the set of the classes of K/k forms of (V, x) to $H^1(K/k, \mathrm{Aut}_K)$ defined above is bijective.

Proof. First, we prove injectivity. If f and g are isomorphisms from (V_K, x_K) to (V'_K, x'_K) and (V''_K, x''_K), respectively, such that $\theta(f) = \theta(g)$, then

$$\begin{aligned} f^{-1} \, {}^s f &= g^{-1} \, {}^s g \\ g f^{-1} &= {}^s(g f^{-1}) \, . \end{aligned}$$

Let us consider the map $h = g f^{-1} : (V'_K, x'_K) \to (V''_K, x''_K)$. It suffices to show that h restricted to $(V' \otimes 1, x' \otimes 1) \to (V'' \otimes 1, x'' \otimes 1)$ is a k-isomorphism. Identifying V with the subspace spanned by vectors of the form $v \otimes 1$, we restrict h to it. If $h(v \otimes 1) = \sum v_i \otimes \alpha_i$, then

$$\begin{aligned} {}^s h(v \otimes 1) &= \sum v_i \otimes s(\alpha_i) \\ &= \sum v_i \otimes \alpha_i \\ &= h(v \otimes 1) \, . \end{aligned}$$

for every $s \in \mathrm{Gal}(K/k)$. This implies that α_i is fixed by $\mathrm{Gal}(K/k)$, so α_i must be in k by Galois theory. By bilinearity, we can write

$$h(v \otimes 1) = (\sum \alpha_i v_i) \otimes 1 \ ,$$

so $h(V) \subset V''$. The map h is clearly injective, and by an analogous argument to the one above, if $\sum v_j \otimes \alpha_j$ is mapped to $v \otimes 1$, then $\sum v_j \otimes \alpha_j = w \otimes 1$, so h is also surjective.

We prove now the surjectivity of θ. Let a_s be a cocycle representing a class of $H^1(\mathrm{Gal}(K/k), \mathrm{Aut}(K))$. Since $H^1(\mathrm{Gal}(K/k), \mathrm{GL}(V)) = 0$ ([Wat79, Sec. 17]), there is a K-automorphism of V_K such that

$$a_s = f^{-1} \circ {}^s f \ .$$

Defining $x'_K = f(x_K)$, the pair (V_K, x'_K) is isomorphic to the pair (V_K, x_K) via f. We have

$$s(x'_K) = s(f)(s(x)) = s(f)(x) = f \circ a_s(x) = f(x) = x' \ ,$$

so x' is defined over k. The element a_s is the image of (V, x') by θ. □

Examples 3.16. (i) Let x be a tensor of type $(0, 2)$ corresponding to a non-degenerate symmetric bilinear form. If $\mathrm{char}\, k \neq 2$, it corresponds to a quadratic form over k, so the automorphism group of (V, x) is the orthogonal group O_n. Thus, K/k forms of quadratic forms correspond to elements of $H^1(K/k, \mathrm{O}_n)$.

Consider $K = \mathbb{C}, k = \mathbb{R}$ and $n = 2$. All nontrivial quadratic forms over $\mathbb{C}$ are equivalent ([Ser96, Chap. IV, Sec. 1]]. Taking x as the tensor corresponding to it, its automorphism group is O_2, that is, the subgroup of GL_n consisting of orthogonal matrices. Thus, $H^1(\mathrm{Gal}(K/k), \mathrm{O}_2(\mathbb{C})) \cong E_{K/k}$ has cardinality 3, corresponding to the quadratic forms I, $-I$ and $(E_{11} - E_{22})$, where E_{ij} is the matrix with 1 in the (i, j)-entry and zeros elsewhere.

(ii) Let x be a tensor of type $(0, 2)$ corresponding to a non-degenerate alternate bilinear form, its automorphism group is Sp_{2n}. Thus, K/k forms of V equipped with an alternate bilinear form correspond to $H^1(K/k, \mathrm{Sp}_{2n})$.

3.2.1 Brauer group: revisited

Let A be a finitely generated k-algebra.

Definition 3.17. We say that A is **central** if the map $\lambda \mapsto \lambda 1$ is a bijection from k to the center of A. We say that it is **simple** if every two-sided ideal of A is equal to 0 or A.

Proposition 3.18 ([Bou12, Sec. 14, Th. 1])**.** Let A be a finitely generated k-algebra. The following properties are equivalent:

(i) The algebra A is central simple.

(ii) There exists an extension K of the field k and an integer $n \geq 1$ such that the K-algebras A_K and $\mathrm{M}_n(K)$ are isomorphic.

(iii) For every separable closure k_s of the field k, there exists an integer $n \geq 1$ such that the k_s-algebras A_{k_s} and $\mathrm{M}_n(k_s)$ are isomorphic.

(iv) There exists a Galois extension K of the field k of finite degree and an integer $n \geq 1$ such that the K-algebras A_K and $\mathrm{M}_n(K)$ are isomorphic.

(v) There exists a division algebra D with center k such that A is isomorphic to $\mathrm{M}_n(D)$.

We say that two central simple algebras A and B are k-**Brauer equivalent** if there exists a division algebra D with center k and positive integers n and m such that $A \cong M_n(D)$ and $B \cong M_m(D)$. The **Brauer group** $\mathrm{Br}(k)$ is the group of Brauer equivalence classes, with addition given by the tensor product of algebras. This product is well defined: the tensor product $A \otimes B$ is central simple since it is isomorphic to $M_n(K) \otimes M_m(K) = M_{nm}(K)$ over some K/k. Furthermore, the Brauer group is abelian, since $A \otimes_k B \cong B \otimes_k A$.

Central simple algebras of dimension n^2 are, by item (iii) of the previous proposition, exactly the k_s/k forms of $\mathrm{M}_n(k)$ of dimension n^2, for a separable closure k_s of k. Let us calculate $\mathrm{Aut}_K(\mathrm{M}_n(K))$. Since all automorphisms of $\mathrm{M}_n(K)$ are inner, then

$$\mathrm{Aut}_K(\mathrm{M}_n(K)) = \mathrm{GL}_n(K)/\mathrm{Z}(\mathrm{GL}_n(K)) = \mathrm{GL}_n(K)/\mathrm{G}_m(K) = \mathrm{PGL}_n(K)\ .$$

Let us denote by $E(n^2, K/k)$ the set of classes of K/k forms of $M_n(k)$ of dimension n^2. Proposition 3.15 shows that there is a bijection $\theta : E(n^2, K/k) \to H^1(K/k, \mathrm{PGL}_n(K))$. Since G_m is the center of GL_n, Proposition 3.12 yields the exact sequence

$$1 = H^1(K/k, \mathrm{GL}_n) \to H^1(K/k, \mathrm{PGL}_n) \xrightarrow{\delta_n} H^2(K/k, \mathrm{G}_m)\ ,$$

so $\delta_n : H^1(K/k, \mathrm{PGL}_n) \to H^2(K/k, \mathrm{G}_m)$ is injective for every n. Thus, we have injective maps

$$E(n^2, K/k) \to H^2(K/k, \mathrm{G}_m)$$

for every positive integer n. If two central simple algebras A and B of dimensions n^2 and m^2, respectively, are Brauer equivalent, then they are in the same class in $H^1(K/k, \mathrm{PGL}_{max\{n,m\}})$. Thus, $\mathrm{Br}(k)$ is directed union of the $H^1(K/k, \mathrm{PGL}_n)$ ranging over n. We define the map

$$\delta : \mathrm{Br}(K) \to H^2(K/k, \mathrm{G}_m)$$

by the rule: if A_n is central simple of dimension n^2, then it corresponds to an element a_s of $H^1(K/k, \mathrm{PGL}_n)$, so we define $\delta(A_n) = \delta_n(a_s)$. In light of Proposition 3.15, we have

$$\delta_{nm}(A_n \otimes A_m) = \delta_{nm}(A_n) + \delta_{nm}(A_m) = \delta_n(A_n)\delta_m(A_m) \ ,$$

so δ is a group homomorphism.

Proposition 3.19. The map

$$\delta : \mathrm{Br}(K) \to H^2(K/k, \mathrm{G}_m)$$

is a bijection.

Proof. If $\delta([A]) = 0$ then $[A]$ must be $[\mathrm{M}_n(k)]$, so δ is injective.

Suppose first that $[K : k] = n < \infty$. The map

$$\delta_n : H^1(K/k, \mathrm{PGL}_n) \to H^2(K/k, \mathrm{G}_m)$$

is surjective. Indeed, let $a_{s,t}$ be a 2-cocycle representing a class in $H^2(K/k, \mathrm{G}_m)$. We need to prove that there is a 1-cocycle b_s in $H^1(K/k, \mathrm{PGL}_n)$ such that $\delta(b_s) = a_{s,t}$.

We know from Proposition 3.12 how δ_n is defined; thus, we have to prove that, for every 2-cocycle $a_{s,t}$, we have

$$a_{s,t} = b_s \, {}^s b_{st}^{-1}$$

for $b_s \in H^1(K/k, \mathrm{GL}_n)$. Let V be a vector space over K with basis e_s for $s \in \mathrm{Gal}(K/k)$. Since $|\mathrm{Gal}(K/k)| = n$, we can identify $\mathrm{GL}_n(K)$ as the automorphism group of V. Let b_s be the endomorphisms of V defined $e_t \mapsto a_{s,t} \cdot e_{st}$. Since $a_{s,t} \in \mathrm{G}_m(K)$ is nonzero, b_s is an automorphism. We have

$$\begin{aligned} b_s \, {}^s b_t(e_u) &= a_{s,tu} \, {}^s a_{t,u} e_{stu} \\ a_{s,t} p_{st}(e_u) &= a_{s,t} a_{st,u} e_{stu} \ , \end{aligned}$$

and using the fact that $a_{s,t}$ is a cocycle, we have $a_{s,t} = b_s \, {}^s b_{st}^{-1}$.

Passing to the limit, δ is surjective for any Galois extension K/k. □

3.3 Finite case

In this section, we prove the finite case of Conjecture I. We need two lemmas.

Lemma 3.20 (Nakayama's Lemma)**.** Let B be a local ring with maximal ideal I, and let M be a finitely generated R-module. If $I \cdot M = 0$, then $M = 0$.

Lemma 3.21 ([Wat79, Sec. 12.4])**.** Let P be a nontrivial prime ideal of a finitely generated integral domain A over a field k. The transcendence degree of the fraction field of A/P is smaller than the transcedente degree of the fraction field of A.

Theorem 3.22 (Lang, [Wat79, Sec. 18.8])**.** Let k be a finite field and G be a connected affine group. Then $H^1(k, G)$ is trivial.

Proof. Let $q = |k|$, and consider the Frobenius automorphism of k, $\sigma(x) = x^q$, generating $\hat{\mathbb{Z}} = \mathrm{Gal}(\overline{k}/k)$. It suffices to prove that the map $\varphi(x) = x^{-1}\sigma(x)$ is surjective. Indeed, since $G(\overline{k})$ is given the discrete topology, continuous maps $\mathrm{Gal}(\overline{k}/k) \to G(\overline{k})$ factors through some finite quotient Q, which will be cyclic. Let Q be generated by σ. If a_s is a cocycle then, since φ is surjective by hypothesis, there is some x such that $a_\sigma = x^{-1}\sigma(x)$. Using the formula $a_{\sigma^2} = a_\sigma \, {}^\sigma a_\sigma$, we obtain

$$a_{\sigma^2} = x^{-1}x^q(x^{-1}x^q)^q = x^{-1}x^{q^2} = x^{-1}\sigma^2(x) \, ,$$

and, by induction, we have

$$a_{\sigma^n} = x^{-1}x^{q^n} = x^{-1}\sigma^n(x) \, .$$

By definition, the class of a_s is trivial.

Now, we will prove that $\varphi(x) = x^{-1}\sigma(x)$ is surjective. By Theorem 1.59 we can embed G into GL_n for some n, so we will assume G is linear. Let A be its Hopf algebra. The map $\mathrm{GL}_n \to \mathrm{GL}_n$ induced by σ just take the q-power of every entry of the matrix, so the correspondent map $A \to A$ is defined by $f \to f^q$. Since $\varphi(x) = x^{-1}\sigma(x)$, the corresponding map $\psi : A \to A$ is defined by

$$\psi = (S, \sigma)\Delta \, ,$$

so $\sigma(x) = x\varphi(x)$ corresponds to $(\mathrm{id}, \psi)\Delta$. Thus, $f^q = (\mathrm{id}, \psi)\Delta(f)$.

Let $B = \psi(A)$, and let us consider A as a B-module. Let V be a comodule containing generators $f_1, \dots, f_m$ of A as a k-algebra. Since $f_i^q = (\mathrm{id}, \psi)\Delta(f)$, we only need finitely many powers of the f_i to generate A as a B-module, so $\dim A \geq \dim B$. Since G is connected, we know from Proposition 1.7 that A modulo its nilradical is a domain, so factoring ψ through $\psi' : A/\mathrm{nil} \to B/\psi(\mathrm{nil})$ implies that $\operatorname{Ker}\psi'$ is a prime ideal. By Lemma 3.21, $\operatorname{Ker}\psi'$ must be trivial, so $\operatorname{Ker}\psi$ is contained in the nilradical of A.

Let y be an element of $G(\overline{k})$. It corresponds to a homomorphism $A \to \overline{k}$, and since $\operatorname{Ker}\psi \subset \mathrm{nil}$, it factors through a homomorphism $B \to \overline{k}$. Its kernel M is a maximal ideal since $\overline{k}$ is a field. Thus, we can see the localization A_M as a finitely generated B_M module. Since M is nontrivial, $M \cdot A_M \neq A_m$ by Nakayama's Lemma, so $M \cdot A \neq A$. Thus, any homomorphism $x : A \to A/MA \to \overline{k}$, which exists because $M \cdot A \neq A$, satisfies $\varphi(x) = y$. □

As a consequence, we have:

Corollary 3.23. All finite division rings are commutative.

Proof. The theorem implies that $\mathrm{Br}(k)$ is trivial for a finite field k (see Section 3.2). □

3.4 Solvable case

In this section, we prove the solvable case of Conjecture I.

Theorem 3.24 ([Ser62, Prop. 3.1.3])**.** Let G be a connected solvable linear algebraic group. Then $H^1(k, G) = 0$.

According to Theorem 1.74, we can express G as an extension

$$1 \to U \to G \to T \to 1$$

where U is unipotent and T is a torus. Passing to the cohomology, we have the exact sequence

$$H^1(k, U) \to H^1(k, G) \to H^1(k, T)\,.$$

Then, to prove the theorem, it is enough to prove that the cohomology sets of unipotent groups and tori are trivial. This is proved in the following two lemmas:

Lemma 3.25. If U is a unipotent connected linear group, then

$$H^1(k, U) = 0\,.$$

Proof. We know from Proposition 1.70 that U has a central series whose quotients are isomorphic to G_a. We know from Example 2.30 (i) that $H^1(k, \mathrm{G}_a) = 0$, so, by induction, we obtain $H^1(k, U) = 0$. □

Lemma 3.26. Let k be a field of dimension ≤ 1. We have:

(i) If T is a torus, then $H^1(k, T) = 0$.

(ii) If R is a solvable algebraic group, then $H^1(k, R) = 0$.

Proof. (i) Since T is a torus, there is a finite Galois extension K/k such that $T_K = \prod \mathrm{G}_m$. If L/k is a Galois extension containing K, its Galois group Γ acts on the group of characters $X = \mathrm{Hom}(T, \mathrm{G}_m)$, and also on $Y = \mathrm{Hom}(X, \mathbb{Z})$. Then, we have the isomorphism

$$T_L = L^* \otimes Y \, .$$

Since $\dim k \leq 1$, we know from Proposition 2.41 that this implies L^* being cohomologically trivial. Thus, $L^* \otimes Y$ is also cohomologically trivial (see [Ser79, Chap. IX, Sec. 3, Cor.]).

We proved that $H^1(K/k, T) = 0$ for an arbitrary extension L/k containing K. Writing $\overline{k}$ as the direct limit of such L, we pass to the limit (Proposition 2.2) and obtain

$$H^1(k, T) = 0 \, .$$

(ii) If R is solvable, then there exists a normal unipotent subgroup G_u such that the sequence

$$1 \to G_u \to R \to R/G_u \to 1$$

is exact and R/G_u is a torus (Theorem 1.74). It induces the exact sequence

$$H^1(k, G_u) \to H^1(k, R) \to H^1(T, R/G_u) \, .$$

The first is trivial by the previous lemma, and the third is trivial by (i), so $H^1(k, R) = 0$. □

3.5 Null cohomology and fields of dimension ≤ 1

Let k be a perfect field. Recall that $H^1(k, A) = H^1(\mathrm{Gal}(\overline{k}/k), A(\overline{k}))$.

Lemma 3.27. Let A be an algebraic group, H be a subgroup of A and $N = N_A(H)$ be the normalizer of H in A. Let $c \in Z^1(\mathrm{Gal}(\overline{k}/k), A(\overline{k}))$ and x be its class in $H^1(k, A)$. Let ${}_cA$ be the algebraic group obtained by twisting A by c, with A acting on itself by inner automorphisms. The following conditions are equivalent:

(i) x belongs to the image of $H^1(k, N) \to H^1(k, A)$.

(ii) The group ${}_cA$ contains a subgroup H' defined over k which is conjugated to H over $\overline{k}$.

Proof. It is clear that elements of ${}_c(A/N)$ correspond to conjugates of H in ${}_cA$. Proposition 3.8 says that x belongs to the image of $H^1(k, N) \to H^1(k, A)$ if, and only if, ${}_c(A/N)$ has a fixed point under G. This condition means that there is an element $a \in A$ such that

$$ {}^{s'}a = a_s \cdot {}^s a = a_s^{-1}({}^s a)a_s = an $$

for every $s \in G$. In other words, an corresponds to a subgroup H' of ${}_cA$ conjugated to H over $\overline{k}$ and ${}^{s'}a = an$ means that H' is a well-defined G-set. □

Theorem 3.28 ([Ser02, Chap. III, Th. 2.2.1])**.** The following properties are equivalent:

(i) $H^1(k, L) = 0$ for any connected linear algebraic group L.

(i') $H^1(k, L) = 0$ for any semisimple algebraic group L.

(ii) Each linear algebraic group L contains a Borel subgroup defined over k.

(ii') Each semisimple algebraic group L contains a Borel subgroup defined over k.

Moreover, these properties implies $\dim(k) \leq 1$.

Proof. (i') $\Rightarrow \dim(k) \leq 1$: Let L be an algebraic group over a finite extension K of k. Let $R = R_{K/k}(L)$ be the Weil restriction of L to k. By Corollary 2.31, we have $R_{K/k}(L) = M_G^H$, where $H = \mathrm{Gal}(\overline{k}/K)$. Thus,

$$ H^1(K, L) = H^1(k, R) \, . $$

If L is semisimple, then R is also semisimple, and, since (i') implies $H^1(k, R) = 0$, the equality above implies $H^1(K, L) = 0$. If $L = \mathrm{PGL}_n$, then $H^1(K, L) = 0$ implies that the Brauer group of K vanishes (see Section 3.2), so we conclude that $\dim(k) \leq 1$.

(ii′) $\Rightarrow \dim(k) \leq 1$: Suppose $\dim(k) \not\leq 1$. Then, there exists a division ring D such that its center is a finite extension K of k and $[D : K] = n^2$, with $n \geq 2$. Consider the algebraic group G defined by $G(S) = (S \otimes_K D)^*$ over K. The reduced norm

$$N : G \to \mathrm{G}_m$$

is a homomorphism, and its kernel is defined as SL_D. Since D is a central simple algebra, it is isomorphic to $M_n(F)$ for some suitable Galois extension F/K (Proposition 3.18), so, over F, the algebraic groups SL_D and SL_n are the same. Thus, SL_D is semisimple, and so is the restriction $R = R_{K/k}(\mathrm{SL}_D)$. We have $R(k) = \mathrm{SL}_D(K)$, but they do not have nontrivial unipotent elements. Thus, (ii′) does not hold, since Borel subgroups are trigonalizable over $\overline{k}$ (Theorem 1.76), and so contains nontrivial unipotent elements.

(ii) $\Leftrightarrow$ (ii′): It is clear that (ii) implies (ii′). Let us suppose (ii′) and let L be a linear group. By Proposition 1.85, $L/r(G)$ is semisimple, so it contains a Borel subgroup $\overline{B}$ over k. If B_0 is any Borel subgroup, its image in $L/r(G)$ is also a Borel subgroup and, because Borel subgroups are conjugate (Proposition 1.79), there is a $x \in L$ such that $B = B_0^x$ has $\overline{B}$ as its image.

(i) $\Leftrightarrow$ (i′): Semisimple groups are connected and linear by definition, so the first implication is immediate. Let us prove the converse. The exact sequence

$$1 \to r(L) \to L \to L/r(L) \to 1$$

induces the exact sequence

$$H^1(k, r(L)) \to H^1(k, L) \to H^1(k, L/r(L)) \,.$$

By definition, $r(L)$ is solvable, and since (i′) implies $\dim k \leq 1$, we obtain $H^1(k, r(L)) = 0$ by Lemma 3.26. The algebraic group $L/r(L)$ is semisimple, so (i′) implies $H^1(k, L/r(L)) = 0$. We conclude that $H^1(k, L) = 0$.

(ii′) $\Rightarrow$ (i′): Let B be a Borel subgroup of L. We know that $N_L(B) = B$ and Borel subgroups always exist over algebraically closed fields, so, by Lemma 3.27, the map $H^1(k, B) \to H^1(k, L)$ is surjective. We know B is soluble and that (ii′) implies $\dim k \leq 1$, so Lemma 3.26 implies $H^1(k, B) = 0$, hence $H^1(k, L) = 0$.

(i′) $\Rightarrow$ (ii′): Let L be a semisimple group. We may assume, by taking the quotient, that the center of L is trivial. It is known ([Mil22, Cor. 23.57]) that there exists a split reductive group L' such that $L_{\overline{k}} = L'_{\overline{k}}$. It is semisimple because it is so over $\overline{k}$ (by

Proposition 1.64). In other words, L' is a $\overline{k}/k$-form of L, so there exists an element $x \in H^1(k, \mathrm{Aut}(L'))$ such that the twist of L' by x is L.

We have the isomorphism

$$\mathrm{Aut}(L') \cong \mathrm{Inn}(G) \rtimes \mathrm{Out}(G) \cong L' \rtimes F \ ,$$

where F is a finite group, isomorphic to the automorphism group of the corresponding Dynkin diagram (see [Mil22, Sec. 23.e]). The exact sequence associated to this expression gives us the exact sequence of cohomology sets

$$H^1(k, L') \to H^1(k, \mathrm{Aut}(L')) \to H^1(k, F) \ .$$

By (i') we know that $H^1(k, L')$ is trivial, so the map $H^1(k, \mathrm{Aut}(L')) \to H^1(k, F)$ is injective, hence it is bijective. The group F (identified with a subgroup of $\mathrm{Aut}(L')$) must leave invariant a Borel subgroup B of L', so F is a subgroup of $N = N_{\mathrm{Aut}(L')}(B)$. Thus, the map

$$H^1(k, N) \to H^1(k, \mathrm{Aut}(L'))$$

has to be surjective. Since L' can be identified with a subgroup of $\mathrm{Aut}(L')$, the result follows from Lemma 3.27. □

Example 3.29. We can show, in another way, that $\mathbb{R}$ is not of dimension ≤ 1. The determinant $\det : \mathrm{O}_2(\mathbb{C}) \to \{\pm 1\}$ has kernel $\mathrm{SO}_2(\mathbb{C})$. Thus, we have the exact sequence

$$H^1(\mathbb{R}, \mathrm{SO}_2) \to H^1(\mathbb{R}, \mathrm{O}_2) \to H^1(\mathbb{R}, \{\pm 1\}) \ .$$

As $\{\pm 1\}$ is a $\mathbb{Z}/2\mathbb{Z}$-module with trivial action, the cohomology group $H^1(\mathbb{R}, \{\pm 1\}) = \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ has cardinality 2. We also know from Example 3.16 that $H^1(\mathbb{R}, \mathrm{O}_2)$ has cardinality 3. If $H^1(\mathbb{R}, \mathrm{SO}_2)$ were trivial then the map $H^1(\mathbb{R}, \mathrm{O}_2) \to H^1(\mathbb{R}, \{\pm 1\})$ would be injective, a contradiction. Since SO_2 is connected, Theorems 3.28 and 3.30 show that $\mathbb{R}$ cannot have dimension ≤ 1, otherwise $H^1(\mathbb{R}, \mathrm{SO}_2)$ would be trivial.

Although we do not prove it in this work, the theorems in sections 3.2 and 3.3 can be generalized for any perfect field k with dimension at most one:

Theorem 3.30 (Serre-Springer-Steinberg, [Ser02, Chap. 3, Sec. 2.3] and [Ste65])**.** If k is a perfect field and $\dim(k) \leq 1$, then the equivalent conditions of Theorem 3.28 holds.

References

[Bor91] A. Borel. *Linear Algebraic Groups*. Springer, 1991.

[Bou12] N. Bourbaki. *Algebra Chapter 8*. Springer, 2012.

[Mac10] S. Mac Lane. *Categories for the working mathematician*. Springer, 2010.

[Mil22] J. Milne. *Algebraic Groups The Theory of Group Schemes of Finite Type over a Field*. CUP, 2022.

[Mor96] P. Morandi. *Field and Galois Theory*. Springer, 1996.

[NSW15] K. Wingberg J. Neukirch A. Schmidt. *Cohomology of Number Fields*. Springer-Verlag, 2015.

[RZ10] L. Ribes P. Zalesskii. *Profinite Groups*. Springer-Verlag, 2010.

[Sch17] T. Schoeneberg. *Semisimple Lie algebras and their classification over p-adic fields*. Société mathématique de France, 2017.

[Ser02] J-P. Serre. *Galois Cohomology*. Springer-Verlag, 2002.

[Ser16] J-P. Serre. *Finite Groups*. International Press, 2016.

[Ser62] J-P. Serre. "Cohomologie galoisienne des groupes algebriques lineaires". In: *Colloque de Bruxelles* (1962), pp. 53–67.

[Ser79] J-P. Serre. *Local Fields*. Springer New York, 1979.

[Ser96] J-P. Serre. *A Course in Arithmetic*. Springer-Verlag, 1996.

[Ste65] R. Steinberg. "Regular elements of semisimple algebraic groups". In: *Publ. Math. I.H.E.S.* 25 (1965), pp. 281–312.

[Wat79] W. Waterhouse. *Introduction to Affine Group Schemes*. Springer, 1979.

Index