JEAN-PIERRE SERRE

Galois Cohomology

Galois Cohomology

Springer Monographs in Mathematics

Springer

Springer Monographs in Mathematics

Springer-Verlag Berlin Heidelberg GmbH

Jean-Pierre Serre

Galois Cohomology

Translated from the French by Patrick Ion

Springer

Jean-Pierre Serre
Collège de France
3 rue d'Ulm
75005 Paris
France
e-mail: serre@dmi.ens.fr

Patrick Ion (Translator)
Mathematical Reviews
P. O. Box 8604
Ann Arbor, MI 48017-8604
USA

Library of Congress Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme
Serre, Jean-Pierre:
Galois cohomology / Jean-Pierre Serre. Transl. from the French by Patrick Ion. -
Corr. 2. printing. - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ;
London ; Milan ; Paris ; Tokyo : Springer, 2002
(Springer monographs in mathematics)
Einheitssacht.: Cohomologie galoisienne <engl.>
ISBN 978-3-642-63866-4 ISBN 978-3-642-59141-9 (eBook)
DOI 10.1007/978-3-642-59141-9

Corrected Second Printing 2002 of the First English Edition of 1997

Mathematics Subject Classification (2000): 12B20

ISSN 1439-7382

ISBN 978-3-642-63866-4

http://www.springer.de

Originally published by Springer-Verlag Berlin Heidelberg New York in 1997

SPIN: 10841416 41/3142LK - 5 4 3 2 1 0 – Printed on acid-free paper

Foreword

This volume is an English translation of "Cohomologie Galoisienne". The original edition (Springer LN5, 1964) was based on the notes, written with the help of Michel Raynaud, of a course I gave at the Collège de France in 1962–1963. In the present edition there are numerous additions and one suppression: Verdier's text on the duality of profinite groups. The most important addition is the photographic reproduction of R. Steinberg's "Regular elements of semisimple algebraic groups", Publ. Math. I.H.E.S., 1965. I am very grateful to him, and to I.H.E.S., for having authorized this reproduction.

Other additions include:

- A proof of the Golod-Shafarevich inequality (Chap. I, App. 2).
- The "résumé de cours" of my 1991–1992 lectures at the Collège de France on Galois cohomology of $k(T)$ (Chap. II, App.).
- The "résumé de cours" of my 1990–1991 lectures at the Collège de France on Galois cohomology of semisimple groups, and its relation with abelian cohomology, especially in dimension 3 (Chap. III, App. 2).

The bibliography has been extended, open questions have been updated (as far as possible) and several exercises have been added.

In order to facilitate references, the numbering of propositions, lemmas and theorems has been kept as in the original 1964 text.

Jean-Pierre Serre
Harvard, Fall 1996

Table of Contents

Chapter I

Cohomology of profinite groups

§1. Profinite groups

1.1 Definition

A topological group which is the projective limit of finite groups, each given the discrete topology, is called a *profinite group*. Such a group is compact and totally disconnected.

Conversely:

Proposition 0. *A compact totally disconnected topological group is profinite.*

Let G be such a group. Since G is totally disconnected and locally compact, the open subgroups of G form a base of neighbourhoods of 1, cf. e.g. Bourbaki TG III, §4, n°6. Such a subgroup U has finite index in G since G is compact; hence its conjugates gUg^{-1} ($g \in G$) are finite in number and their intersection V is both normal and open in G. Such V's are thus a base of neighbourhoods of 1; the map $G \to \varprojlim G/V$ is injective, continuous, and its image is dense; a compactness argument then shows that it is an isomorphism. Hence G is profinite.

The profinite groups form a category (the morphisms being continuous homomorphisms) in which infinite products and projective limits exist.

Examples.

1) Let L/K be a Galois extension of commutative fields. The Galois group $\mathrm{Gal}(L/K)$ of this extension is, by construction, the projective limit of the Galois groups $\mathrm{Gal}(L_i/K)$ of the finite Galois extensions L_i/K which are contained in L/K; thus it is a profinite group.

2) A compact analytic group over the p-adic field $\mathbf{Q}_p$ is profinite, when viewed as a topological group. In particular, $\mathbf{SL}_n(\mathbf{Z}_p), \mathbf{Sp}_{2n}(\mathbf{Z}_p), \ldots$ are profinite groups.

3) Let G be a discrete topological group, and let $\hat{G}$ be the projective limit of the finite quotients of G. The group $\hat{G}$ is called the profinite group *associated to* G; it is the separated completion of G for the topology defined by the subgroups of G which are of finite index; the kernel of $G \to \hat{G}$ is the intersection of all subgroups of finite index in G.

4) If M is a torsion abelian group, its dual $M^* = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$, given the topology of pointwise convergence, is a commutative profinite group. Thus one obtains the anti-equivalence (Pontryagin duality):

$$\text{torsion abelian groups} \iff \text{commutative profinite groups}$$

Exercises.

1) Show that a torsion-free commutative profinite group is isomorphic to a product (in general, an infinite one) of the groups $\mathbf{Z}_p$. [Use Pontryagin duality to reduce this to the theorem which says that every divisible abelian group is a direct sum of groups isomorphic to $\mathbf{Q}$ or to some $\mathbf{Q}_p/\mathbf{Z}_p$, cf. Bourbaki A VII.53, Exerc. 3.]

2) Let $G = \mathbf{SL}_n(\mathbf{Z})$, and let f be the canonical homomorphism

$$\hat{G} \longrightarrow \prod_p \mathbf{SL}_n(\mathbf{Z}_p).$$

(a) Show that f is surjective.

(b) Show the equivalence of the following two properties:

(b_1) f is an isomorphism;

(b_2) Each subgroup of finite index in $\mathbf{SL}_n(\mathbf{Z})$ is a congruence subgroup.

[These properties are known to be true for $n \neq 2$ and false for $n = 2$.]

1.2 Subgroups

Every closed subgroup H of a profinite group G is profinite. Moreover, the homogeneous space G/H is compact and totally disconnected.

Proposition 1. *If H and K are two closed subgroups of the profinite group G, with $H \supset K$, there exists a continuous section $s : G/H \to G/K$.*

(By "section" one means a map $s : G/H \to G/K$ whose composition with the projection $G/K \to G/H$ is the identity.)

We use two lemmas:

Lemma 1. *Let G be a compact group G, and let (S_i) be a decreasing filtration of G by closed subgroups. Let $S = \bigcap S_i$. The canonical map*

$$G/S \longrightarrow \varprojlim G/S_i$$

is a homeomorphism.

Indeed, this map is injective, and its image is dense; since the source space is compact, the lemma follows. (One could also invoke Bourbaki, TG III.59, cor. 3 to prop. 1.)

Lemma 2. *Proposition 1 holds if H/K is finite. If, moreover, H and K are normal in G, the extension*

$$1 \longrightarrow H/K \longrightarrow G/K \longrightarrow G/H \longrightarrow 1$$

splits (cf. §3.4) *over an open subgroup of G/H.*

Let U be an open normal subgroup of G such that $U \cap H \subset K$. The restriction of the projection $G/K \to G/H$ to the image of U is injective (and is a homomorphism whenever H and K are normal). Its inverse map is therefore a section over the image of U (which is open); one extends it to a section over the whole of G/H by translation.

Let us now prove prop. 1. One may assume $K = 1$. Let X be the set of pairs (S, s), where S is a closed subgroup of H and s is a continuous section $G/H \to G/S$. One gives X an ordering by saying that $(S, s) \geq (S', s')$ if $S \subset S'$ and if s' is the composition of s and $G/S \to G/S'$. If (S_i, s_i) is a totally ordered family of elements of X, and if $S = \bigcap S_i$, one has $G/S = \varprojlim G/S_i$ by Lemma 1; the s_i thus define a continuous section $s : G/H \to G/S$; one has $(S, s) \in X$. This shows that X is an inductively ordered set. By Zorn's Lemma, X contains a maximal element (S, s). Let us show that $S = 1$, which will complete the proof. If S were distinct from 1, then there would exist an open subgroup U of G such that $S \cap U \neq S$. Applying Lemma 2 to the triplet $(G, S, S \cap U)$, one would get a continuous section $G/S \to G/(S \cap U)$, and composing this with $s : G/H \to G/S$, would give a continuous section $G/H \to G/(S \cap U)$, in contradiction to the fact that (S, s) is maximal.

Exercises.

1) Let G be a profinite group acting continuously on a totally disconnected compact space X. Assume that G acts freely, i.e., that the stabilizer of each element of X is equal to 1. Show that there is a continuous section $X/G \to X$. [same proof as for prop. 1.]

2) Let H be a closed subgroup of a profinite group G. Show that there exists a closed subgroup G' of G such that $G = H \cdot G'$, which is minimal for this property.

1.3 Indices

A *supernatural number* is a formal product $\prod p^{n_p}$, where p runs over the set of prime numbers, and where n_p is an integer ≥ 0 or $+\infty$. One defines the product in the obvious way, and also the gcd and lcm of any family of supernatural numbers.

Let G be a profinite group, and let H be a closed subgroup of G. The *index* $(G : H)$ of H in G is defined as the lcm of the indices $(G/U : H/(H \cap U))$, where U runs over the set of open normal subgroups of G. It is also the lcm of the indices $(G : V)$ for open V containing H.

Proposition 2. (i) *If $K \subset H \subset G$ are profinite groups, one has*

$$(G : K) = (G : H) \cdot (H : K) \ .$$

(ii) *If (H_i) is a decreasing filtration of closed subgroups of G, and if $H = \bigcap H_i$, one has $(G : H) = \operatorname{lcm} (G : H_i)$.*

(iii) *In order that H be open in G, it is necessary and sufficient that $(G : H)$ be a natural number* (i.e., an element of $\mathbf{N}$).

Let us show (i): if U is an open normal subgroup of G, set $G_U = G/U$, $H_U = H/(H \cap U)$, $K_U = K/(K \cap U)$. One has $G_U \supset H_U \supset K_U$, from which

$$(G_U : K_U) = (G_U : H_U) \cdot (H_U : K_U) .$$

By definition, $\mathrm{lcm}(G_U : K_U) = (G : K)$ and $\mathrm{lcm}(G_U : H_U) = (G : H)$. On the other hand, the $H \cap U$ are cofinal with the set of normal open subgroups of H; it follows that $\mathrm{lcm}(H_U : K_U) = (H : K)$, and from this follows (i).

The other two assertions (ii) and (iii) are obvious.

Note that, in particular, one may speak of the *order* $(G : 1)$ of a profinite group G.

Exercises.

1) Let G be a profinite group, and let n be an integer $\neq 0$. Show the equivalence of the following properties:

(a) n is prime to the order of G.

(b) The map $x \mapsto x^n$ of G to G is surjective.

(b′) The map $x \mapsto x^n$ of G to G is bijective.

2) Let G be a profinite group. Show the equivalence of the three following properties:

(a) The topology of G is metrisable.

(b) One has $G = \varprojlim G_n$, where the G_n $(n \geq 1)$ are finite and the homomorphisms $G_{n+1} \to G_n$ are surjective.

(c) The set of open subgroups of G is denumerable.

Show that these properties imply:

(d) There exists a denumerable dense subset of G.

Construct an example where (d) holds, but not (a), (b) or (c) [take for G the bidual of a vector space over $\mathbf{F}_p$ with denumerably infinite dimension].

3) Let H be a closed subgroup of a profinite group G. Assume $H \neq G$. Show that there exists $x \in G$ so that no conjugate of x belongs to H [reduce to the case where G is finite].

4) Let g be an element of a profinite group G, and let $C_g = \overline{\langle g \rangle}$ be the smallest closed subgroup of G containing g. Let $\prod p^{n_p}$ be the order of C_g, and let I be the set of p such that $n_p = \infty$. Show that:

$$C_g \simeq \prod_{p \in I} \mathbf{Z}_p \times \prod_{p \notin I} \mathbf{Z}/p^{n_p}\mathbf{Z}.$$

1.4 Pro-p-groups and Sylow p-subgroups

Let p be a prime number. A profinite group H is called a pro-p-group if it is a projective limit of p-groups, or, which amounts to the same thing, if its order is a power of p (finite or infinite, of course). If G is a profinite group, a subgroup H of G is called a Sylow p-subgroup of G if it is a pro-p-group and if $(G : H)$ is prime to p.

Proposition 3. *Every profinite group G has Sylow p-subgroups, and these are conjugate.*

One uses the following lemma (Bourbaki, TG I.64, prop. 8):

Lemma 3. *A projective limit of non-empty finite sets is not empty.*

Let X be the family of open normal subgroups of G. If $U \in X$, let $P(U)$ be the set of Sylow p-subgroups in the finite group G/U. By applying Lemma 3 to the projective system of all $P(U)$, one obtains a coherent family H_U of Sylow p-subgroups in G/U, and one can easily see that $H = \varprojlim H_U$ is a Sylow p-subgroup in G, whence the first part of the proposition. In the same way, if H and H' are two Sylow p-subgroups in G, let $Q(U)$ be the set of $x \in G/U$ which conjugate the image of H into that of H'; by applying Lemma 3 to the $Q(U)$, one sees that $\varprojlim Q(U) \neq \emptyset$, whence there exists an $x \in G$ such that $xHx^{-1} = H'$.

One may show by the same sort of arguments:

Proposition 4. (a) *Every pro-p-subgroup is contained in a Sylow p-subgroup of G.*

(b) *If $G \to G'$ is a surjective morphism, then the image of a Sylow p-subgroup of G is a Sylow p-subgroup of G'.*

Examples.

1) The group $\widehat{\mathbf{Z}}$ has the group $\mathbf{Z}_p$ of p-adic integers as a Sylow p-subgroup.

2) If G is a compact p-adic analytic group, the Sylow p-subgroups of G are open (this follows from the well-known local structure of these groups). The order of G is thus the product of an ordinary integer by a power of p.

3) Let G be discrete group. The projective limit of the quotients of G which are p-groups is a pro-p-group, denoted by $\widehat{G}_p$, which is called the *p-completion* of G; it is the largest quotient of $\widehat{G}$ which is a pro-p-group.

Exercise.

Let G be a discrete group such that $G^{\mathrm{ab}} = G/(G,G)$ is isomorphic to $\mathbf{Z}$ (for example the fundamental group of the complement of a knot in $\mathbf{R}^3$). Show that the p-completion of G is isomorphic to $\mathbf{Z}_p$.

1.5 Pro-p-groups

Let I be a set, and let $L(I)$ be the free discrete group generated by the elements x_i indexed by I. Let X be the family of normal subgroups M of $L(I)$ such that:

a) $L(I)/M$ is a finite p-group,
b) M contains almost all the x_i (i.e., all but a finite number).

Set $F(I) = \varprojlim L(I)/M$. The group $F(I)$ is a pro-p-group which one calls the *free pro-p-group* generated by the x_i. The adjective "free" is justified by the following result:

Proposition 5. *If G is a pro-p-group, the morphisms of $F(I)$ into G are in bijective correspondence with the families $(g_i)_{i\in I}$ of elements of G which tend to zero along the filter made up of the complements of finite subsets.*
[When I is finite, the condition $\lim g_i = 1$ should be dropped; anyway, then the complements of finite subsets don't form a filter ...]

More precisely, one associates to the morphism $f : F(I) \to G(I)$ the family $(g_i) = (f(x_i))$. The fact that the correspondence obtained in this way is bijective is clear.

Remark.
Along with $F(I)$ one may define the group $F_s(I)$ which is the projective limit of the $L(I)/M$ for those M just satisfying a). This is the p-completion of $L(I)$; the morphisms of $F_s(I)$ into a pro-p-group are in one-to-one correspondence with *arbitrary* families $(g_i)_{i\in I}$ of elements of G. We shall see in §4.2 that $F_s(I)$ is *free*, i.e., isomorphic to $F(J)$ for a suitable J.

When $I = [1, n]$ one writes $F(n)$ instead of $F(I)$; the group $F(n)$ is the *free pro-p-group of rank n*. One has $F(0) = \{1\}$, and $F(1)$ is isomorphic to the additive group $\mathbf{Z}_p$. Here is an explicit description of the group $F(n)$:

Let $A(n)$ be the algebra of associative (but not necessarily commutative) formal series in n unknowns $t_1, \ldots, t_n$, with coefficients in $\mathbf{Z}_p$ (this is what Lazard calls the "Magnus algebra"). [The reader who does not like "not necessarily commutative" formal power series may define $A(n)$ as the completion of the tensor algebra of the $\mathbf{Z}_p$-module $(\mathbf{Z}_p)^n$.] With the topology of coefficient-wise convergence, $A(n)$ is a compact topological ring. Let U be the multiplicative group of the elements in A with constant term 1. One may easily verify that it is a pro-p-group. Since U contains the elements $1 + t_i$ prop. 5 shows that there exists a morphism, $\theta : F(n) \to U$, which maps x_i to the element $1 + t_i$ for every i.

Proposition 6. (Lazard) *The morphism $\theta : F(n) \to U$ is injective.*

[One may hence identify $F(n)$ with the closed subgroup of U generated by the $1 + t_i$.]

One can prove a stronger result. To formulate it, define the $\mathbf{Z}_p$-*algebra* of a pro-p-group G as the projective limit of the algebras of finite quotients of G, with coeffients in $\mathbf{Z}_p$; this algebra will be denoted $\mathbf{Z}_p[[G]]$. One has:

Proposition 7. *There is a continuous isomorphism α from $\mathbf{Z}_p[[F(n)]]$ onto $A(n)$ which maps x_i to $1 + t_i$.*

The existence of the morphism $\alpha : \mathbf{Z}_p[[F(n)]] \to A(n)$ is easy to see. On the other hand, let I be the augmentation ideal of $\mathbf{Z}_p[[F(n)]]$; the elementary properties of p-groups show that the powers of I tend to 0. Since the $x_i - 1$ belong to I, one deduces that there is a continuous homomorphism

$$\beta : A(n) \longrightarrow \mathbf{Z}_p[[F(n)]]$$

which maps t_i onto $x_i - 1$. One then has to check $\alpha \circ \beta = 1$ and $\beta \circ \alpha = 1$, which is obvious.

Remarks.

1) When $n = 1$, prop. 7 shows that the $\mathbf{Z}_p$-algebra of the group $\Gamma = \mathbf{Z}_p$ is isomorphic to the algebra $\mathbf{Z}_p[[T]]$, which is a regular local ring of dimension 2. This can be used to recover the Iwasawa theory of "Γ-modules" (cf. [143], and also Bourbaki AC VII, §4).

2) In Lazard's thesis [101] one finds a detailed study of $F(n)$ based on prop. 6 and 7. For example, if one filters $A(n)$ by powers of the augmentation ideal I, the filtration induced on $F(n)$ is that of the descending central series, and the associated graded algebra is the free Lie $\mathbf{Z}_p$-algebra generated by the classes T_i corresponding to the t_i. The filtration defined by the powers of (p, I) is also interesting.

§2. Cohomology

2.1 Discrete G-modules

Let G be a profinite group. The discrete abelian groups on which G acts continuously form an abelian category C_G, which is a full subcategory of the category of all G-modules. To say that a G-module A belongs to C_G means that the stabilizer of each element of A is open in G, or, again, that one has

$$A = \bigcup A^U,$$

where U runs over all open subgroups of G (as usual, A^U denotes the largest subgroup of A fixed by U).

An element A of C_G will be called a *discrete G-module* (or even simply a *G-module*). It is for these modules that the cohomology of G will be defined.

2.2 Cochains, cocycles, cohomology

Let $A \in C_G$. We denote by $C^n(G, A)$ the set of all *continuous* maps of G^n to A (note that, since A is discrete, "continuous" amounts to "locally constant"). One first defines the coboundary

$$d : C^n(G, A) \longrightarrow C^{n+1}(G, A)$$

by the usual formula

$$\begin{aligned}(df)(g_1, \ldots, g_{n+1}) = {} & g_1 \cdot f(g_2, \ldots, g_{n+1}) \\ & + \sum_{i=1}^{i=n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ & + (-1)^{n+1} f(g_1, \ldots, g_n) \ .\end{aligned}$$

One thus obtains a complex $C^*(G, A)$ whose cohomology groups $H^q(G, A)$ are called the *cohomology groups of G with coefficients in A*. If G is finite, one recovers the standard definition of the cohomology of finite groups; moreover, the general case can be reduced to that one, by the following proposition:

Proposition 8. *Let (G_i) be a projective system of profinite groups, and let (A_i) be an inductive system of discrete G_i-modules* (the homomorphisms $A_i \to A_j$ have to be compatible in an obvious sense with the morphisms $G_i \to G_j$). *Set* $G = \varprojlim G_i$, $A = \varinjlim A_i$. *Then one has*

$$H^q(G, A) = \varinjlim H^q(G_i, A_i) \quad \text{for each} \quad q \geq 0.$$

Indeed, one checks easily that the canonical homomorphism

$$\varinjlim C^*(G_i, A_i) \longrightarrow C^*(G, A)$$

is an isomorphism, whence the result follows by passing to homology.

Corollary 1. *Let A be a discrete G-module. One has:*

$$H^q(G, A) = \varinjlim H^q(G/U, A^U) \quad \text{for each } q \geq 0,$$

where U runs over all open normal subgroups of G.

Indeed, $G = \varprojlim G/U$ and $A = \varinjlim A^U$.

Corollary 2. *Let A be a discrete G-module. Then we have:*

$$H^q(G, A) = \varinjlim H^q(G, B) \quad \text{for all } q \geq 0$$

when B runs over the set of finitely generated sub-G-modules of A.

Corollary 3. *For $q \geq 1$, the groups $H^q(G, A)$ are torsion groups.*

When G is finite, this result is classical. The general case follows from this, thanks to Corollary 1.

One can thus easily reduce everything to the case of finite groups, which is well known (see, for example, Cartan-Eilenberg [25], or "Corps Locaux" [145]). One may deduce, for example, that the $H^q(G, A)$ are zero, for $q \geq 1$, when A is an injective object in C_G (the A^U are thus injective over the G/U). Since the category C_G has enough injective objects (but not enough projective ones), one sees that the functors $A \mapsto H^q(G, A)$ are *derived functors* of the functor $A \mapsto A^G$, as they should be.

2.3 Low dimensions

$H^0(G, A) = A^G$, as usual.

$H^1(G, A)$ is the group of classes of *continuous* crossed-homomorphisms of G into A.

$H^2(G, A)$ is the group of classes of continuous *factor systems* from G to A. If A is finite, this is also the group of classes of extensions of G by A (standard proof, based on the existence of a continuous section proved in §1.2).

Remark.

This last example suggests defining the $H^q(G, A)$ for any topological G-module A. This type of cohomology is actually useful in some applications, cf. [148].

2.4 Functoriality

Let G and G' be two profinite groups, and let $f : G \to G'$ be a morphism. Assume $A \in C_G$ and $A' \in C_{G'}$. There is the notion of a morphism $h : A' \to A$ which is *compatible* with f (this is a G-morphism, if one regards A' as a G-module via f). Such a pair (f, h) defines, by passing to cohomology, the homomorphisms

$$H^q(G', A') \longrightarrow H^q(G, A) , \quad q \geq 0.$$

This can be applied when H is a closed subgroup of G, and when $A = A'$ is a discrete G-module; one obtains the *restriction* homomorphisms

$$\mathrm{Res} : H^q(G, A) \longrightarrow H^q(H, A) , \quad q \geq 0.$$

When H is open in G, with index n, one defines (for example, by a limit process starting from finite groups) the *corestriction* homomorphisms

$$\mathrm{Cor} : H^q(H, A) \longrightarrow H^q(G, A) .$$

One has $\mathrm{Cor} \circ \mathrm{Res} = n$, whence follows:

Proposition 9. *If $(G : H) = n$, the kernel of* Res $: H^q(G, A) \to H^q(H, A)$ *is killed by n.*

Corollary. *If $(G : H)$ is prime to p,* Res *is injective on the p-primary component of $H^q(G, A)$.*

[This corollary may be applied in particular to the case when H is a Sylow p-subgroup of G.]

When $(G : H)$ is finite, the corollary is an immediate consequence of the preceding proposition. One may reduce to this case by writing H as an intersection of open subgroups and using prop. 8.

Exercise.

Let $f : G \to G'$ be a morphism of profinite groups.

(a) Let p be a prime number. Prove the equivalence of the following properties:

(1_p) The index of $f(G)$ in G' is prime to p.

(2_p) For any p-primary G'-module A, the homomorphism $H^1(G', A) \to H^1(G, A)$ is injective.

[Reduce this to the case where G and G' are pro-p-groups.]

(b) Show the equivalence of:

(1) f is surjective.

(2) For any G'-module A, the homomorphism $H^1(G', A) \to H^1(G, A)$ is injective.

(3) Same assertion as in (2), but restricted to finite G'-modules A.

2.5 Induced modules

Let H be a closed subgroup of a profinite group G, and let $A \in C_H$. The induced module $A^* = M_G^H(A)$ is defined as the group of continuous maps a^* from G to A such that $a^*(hx) = h \cdot a^*(x)$ for $h \in H, x \in G$. The group G acts on A^* by

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

If $H = \{1\}$, one writes $M_G(A)$; the G-modules obtained in this way are called *induced* ("co-induced" in the terminology of [145]).

If to each $a^* \in M_G^H(A)$ one associates its value at the point 1, one obtains a homomorphism $M_G^H(A) \to A$ which is compatible with the injection of H into G (cf. §2.4); hence the homomorphisms

$$H^q(G, M_G^H(A)) \longrightarrow H^q(H, A) \ .$$

Proposition 10. *The homomorphisms $H^q(G, M_G^H(A)) \to H^q(H, A)$ defined above are isomorphisms.*

One first remarks that, if $B \in C_G$, one has $\mathrm{Hom}^G(B, M_G^H(A)) = \mathrm{Hom}^H(B, A)$. This implies that the functor M_G^H transforms injective objects into injective objects. Since, on the other hand, it is exact, the proposition follows from a standard comparison theorem.

Corollary. *The cohomology of an induced module is zero in dimension ≥ 1.*

This is just the special case $H = \{1\}$.

Proposition 10, which is due to Faddeev and Shapiro, is very useful: it reduces the cohomology of a subgroup to that of the group. Let us indicate how, from this point of view, one may recover the homomorphisms Res and Cor:

(a) If $A \in C_G$, one defines an injective G-homomorphism

$$i : A \longrightarrow M_G^H(A)$$

by setting

$$i(a)(x) = x \cdot a \ .$$

By passing to cohomology, one checks that one gets the *restriction*

$$\mathrm{Res} : H^q(G, A) \longrightarrow H^q(G, M_G^H(A)) = H^q(H, A) \ .$$

(b) Let us assume H is open in G and $A \in C_G$. One defines a surjective G-homomorphism

$$\pi : M_G^H(A) \longrightarrow A$$

by putting

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

a formula which makes sense because in fact $a^*(x^{-1})$ only depends on the class of x mod H. Upon passing to cohomology, π gives the *corestriction*

$$\mathrm{Cor} : H^q(H, A) = H^q(G, M_G^H(A)) \longrightarrow H^q(G, A) \ .$$

It is a morphism of cohomological functors which coincides with the trace in dimension zero.

Exercises.

1) Assume H is *normal* in G. If $A \in C_G$, one makes G act on $M_G^H(A)$ by setting

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

Show that H acts trivially, which allows one to view G/H as acting on $M_G^H(A)$; show that the action thus defined *commutes* with the action of G defined in the text. Deduce, for each integer q, an action of G/H on $H^q(G, M_G^H(A)) = H^q(H, A)$. Show that this action coincides with the natural action (cf. the following section).

Show that $M_G^H(A)$ is isomorphic to $M_{G/H}(A)$ if H acts trivially on A. Deduce from this, when $(G : H)$ is finite, the formulas

$$H_0(G/H, M_G^H(A)) = A \quad \text{and} \quad H_i(G/H, M_G^H(A)) = 0 \quad \text{for } i \geq 1.$$

2) Assume $(G : H) = 2$. Let ε be the homomorphism of G onto $\{\pm 1\}$ whose kernel is H. Making G act on $\mathbf{Z}$ through ε, one obtains a G-module $\mathbf{Z}_\varepsilon$.

(a) Assume $A \in C_G$, and let $A_\varepsilon = A \otimes \mathbf{Z}_\varepsilon$. Show that there is an exact sequence of G-modules:

$$0 \longrightarrow A \longrightarrow M_G^H(A) \longrightarrow A_\varepsilon \longrightarrow 0 \ .$$

(b) Deduce from this the exact cohomology sequence

$$\cdots \longrightarrow H^i(G, A) \xrightarrow{\mathrm{Res}} H^i(H, A) \xrightarrow{\mathrm{Cor}} H^i(G, A_\varepsilon) \xrightarrow{\delta} H^{i+1}(G, A) \longrightarrow \cdots \ ,$$

and show that, if $x \in H^i(G, A_\varepsilon)$, one has $\delta(x) = e \cdot x$ (cup product), where e is some explicit element of $H^1(G, \mathbf{Z}_\varepsilon)$.

(c) Apply this to the case when $2 \cdot A = 0$, whence $A_\varepsilon = A$.

[This is the profinite analogue of the Thom-Gysin exact sequence for coverings of degree 2, such a covering being identified with a fibration into spheres of dimension 0.]

2.6 Complements

The reader is left with the task of dealing with the following points (which will be used later):

a) Cup products

Various properties, especially with regard to exact sequences. Formulae:

$$\mathrm{Res}(x \cdot y) = \mathrm{Res}(x) \cdot \mathrm{Res}(y)$$
$$\mathrm{Cor}(x \cdot \mathrm{Res}(y)) = \mathrm{Cor}(x) \cdot y \ .$$

b) Spectral sequence for group extensions

If H is a closed normal subgroup of G, and if $A \in C_G$, the group G/H acts in a natural way on the $H^q(H, A)$, and the action is continuous. One has a spectral sequence:

$$H^p(G/H, H^q(H, A)) \Longrightarrow H^n(G, A) \ .$$

In low dimensions, this gives the exact sequence

$$0 \longrightarrow H^1(G/H, A^H) \longrightarrow H^1(G, A)$$
$$\longrightarrow H^1(H, A)^{G/H} \longrightarrow H^2(G/H, A^H) \longrightarrow H^2(G, A) \ .$$

Exercises.

(Relations between the cohomology of discrete groups and of profinite groups)

1) Let G be a discrete group, and let $G \to K$ be a homomorphism of G into a profinite group K. Assume that the image of G is *dense* in K. For all $M \in C_K$, on has the homomorphisms

$$H^q(K, M) \longrightarrow H^q(G, M) \ , \quad q \geq 0.$$

We restrict ourselves to the subcategory C'_K of C_K formed by the finite M.

(a) Show the equivalence of the following four properties:

A_n. *$H^q(K, M) \to H^q(G, M)$ is bijective for $q \leq n$ and injective for $q = n+1$* (for any $M \in C'_K$).

B_n. *$H^q(K, M) \to H^q(G, M)$ is surjective for all $q \leq n$.*

C_n. *For all $x \in H^q(G, M)$, $1 \leq q \leq n$, there exists an $M' \in C_K$ containing M such that x maps to 0 in $H^q(G, M')$.*

D_n. *For all $x \in H^q(G, M)$, $1 \leq q \leq n$, there exists a subgroup G_0 of G, the inverse image of an open subgroup of K, such that x induces zero in $H^q(G_0, M)$.*

[The implications $\mathrm{A}_n \Rightarrow \mathrm{B}_n \Rightarrow \mathrm{C}_n$ are immediate, as is $\mathrm{B}_n \Rightarrow \mathrm{D}_n$. The assertion $\mathrm{C}_n \Rightarrow \mathrm{A}_n$ is proved by induction on n. Finally, $\mathrm{D}_n \Rightarrow \mathrm{C}_n$ follows by taking M' as the induced module $M_G^{G_0}(M)$.]

(b) Show that $\mathrm{A}_0, \ldots, \mathrm{D}_0$ hold. Show that, if K is equal to the profinite group $\widehat{G}$ associated to G, properties $\mathrm{A}_1, \ldots, \mathrm{D}_1$ are true.

(c) Take for G the discrete group $\mathbf{PGL}(2, \mathbf{C})$; show that $\widehat{G} = \{1\}$ and that $H^2(G, \mathbf{Z}/2\mathbf{Z}) \neq 0$ [make use of the extension of G given by $\mathbf{SL}(2, \mathbf{C})$]. Deduce that G does not satisfy A_2.

(d) Let K_0 be an open subgroup of K, and G_0 be its inverse image in G. Show that, if $G \to K$ satisfies A_n, the same is true for $G_0 \to K_0$, and conversely.

2) [In the following, we say that "G satisfies A_n" if the canonical map $G \to \widehat{G}$ satisfies A_n. A group will be called "good" if it satisfies A_n for all n.]

Let $E/N = G$ be an extension of a group G satisfying A_2.

(a) Assume first that N is *finite*. Let I be the centralizer of N in E. Show that I is of finite index in E; deduce that $I/(I \cap N)$ satisfies A_2 [apply 1, (d)], since there exists subgroup E_0 of finite index in E such that $E_0 \cap N = \{1\}$.

(b) Assume from now on that N is *finitely generated*. Show (using (a)) that every subgroup of N of finite index contains a subgroup of the form $E_0 \cap N$, where E_0 is of finite index in E. Deduce from this the exact sequence:

$$1 \longrightarrow \widehat{N} \longrightarrow \widehat{E} \longrightarrow \widehat{G} \longrightarrow 1 .$$

(c) Assume in addition that N and G are good, and that the $H^q(N, M)$ are finite for every finite E-module M. Show that E is good [compare the spectral sequences of $\widehat{E}/\widehat{N} = \widehat{G}$ and of $E/N = G$].

(d) Show that a succession of extensions of free groups of finite type is a good group. This applies to braid groups ("*groupes de tresses*").

(e) Show that $\mathbf{SL}(2, \mathbf{Z})$ is a good group [use the fact that it contains a free subgroup of finite index].

[One can show that $\mathbf{SL}_n(\mathbf{Z})$ is not good if $n \geq 3$.]

§3. Cohomological dimension

3.1 p-cohomological dimension

Let p be a prime number, and G a profinite group. One calls the *p-cohomological dimension* of G, and uses the notation $\mathrm{cd}_p(G)$ for, the lower bound 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.

(Of course, if there is no such integer n, then $\mathrm{cd}_p(G) = +\infty$.)

One puts $\mathrm{cd}(G) = \sup \mathrm{cd}_p(G)$: this is the *cohomological dimension* of G.

Proposition 11. *Let G be a profinite group, let p be a prime, and let n be an integer. The following properties are equivalent:*

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

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

(iii) $H^{n+1}(G, A) = 0$ *when A is a simple discrete G-module killed by p.*

Let A be a torsion G-module, and let $A = \bigoplus A(p)$ be its canonical decomposition into p-primary components. One can easily see that $H^q(G, A(p))$ may be identified with the p-primary component of $H^q(G, A)$. The equivalence of (i) and (ii) follows from this. The implication (ii) $\Rightarrow$ (iii) is trivial. On the other hand, if (iii) holds, an immediate *dévissage* argument shows that $H^{n+1}(G, A) = 0$ if A is finite, and annihilated by a power of p; by taking the inductive limit (cf. prop. 8, cor. 2) the same result extends to every discrete G-module A which is a p-primary torsion group. One deduces (ii) by using induction on q: imbed A in the induced module $M_G(A)$, and apply the induction hypothesis to $M_G(A)/A$, which is also a p-primary torsion module.

Proposition 12. *Assume $\mathrm{cd}_p(G) \leq n$, and let A be a discrete p-divisible G-module* (i.e. such that $p : A \to A$ is onto). *The p-primary component of $H^q(G, A)$ is zero for $q > n$.*

The exact sequence

$$0 \longrightarrow A_p \longrightarrow A \xrightarrow{p} A \longrightarrow 0$$

gives the exact sequence

$$H^q(G, A_p) \longrightarrow H^q(G, A) \xrightarrow{p} H^q(G, A) \ .$$

For $q > n$, one has $H^q(G, A_p) = 0$ by hypothesis. Multiplication by p is therefore injective in $H^q(G, A)$, which means that the p-primary component of this group reduces to 0.

Corollary. *If* $\mathrm{cd}(G) \leq n$, *and* $A \in C_G$ *is divisible, then* $H^q(G, A) = 0$ *for* $q > n$.

3.2 Strict cohomological dimension

Keep the same hypotheses and notation as above. The *strict p-cohomological dimension* of G, denoted $\mathrm{scd}_p(G)$, is the lower bound of the integers n such that:

(**) For any $A \in C_G$, one has $H^q(G, A)(p) = 0$ for $q > n$.

[This is the same condition as (*), except that it is no longer assumed that A is a torsion module.]

One sets $\mathrm{scd}(G) = \sup \mathrm{scd}_p(G)$; this is the *strict cohomological dimension* of G.

Proposition 13. $\mathrm{scd}_p(G)$ *equals* $\mathrm{cd}_p(G)$ *or* $\mathrm{cd}_p(G) + 1$.

It is obvious that $\mathrm{scd}_p(G) \geq \mathrm{cd}_p(G)$. Thus we have to prove

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

Let $A \in C_G$, and write the canonical decomposition of the morphism $p : A \to A$. It consists in two exact sequences:

$$0 \longrightarrow N \longrightarrow A \longrightarrow I \longrightarrow 0 \ ,$$

$$0 \longrightarrow I \longrightarrow A \longrightarrow Q \longrightarrow 0 \ ,$$

with $N = A_p$, $I = pA$, $Q = A/pA$, the composed map $A \to I \to A$ being multiplication by p. Let $q > \mathrm{cd}_p(G) + 1$. Since N and Q are p-primary torsion groups, one has $H^q(G, N) = H^{q-1}(G, Q) = 0$. Therefore

$$H^q(G, A) \longrightarrow H^q(G, I) \quad \text{and} \quad H^q(G, I) \longrightarrow H^q(G, A)$$

are injective. Multiplication by p in $H^q(G, A)$ is thus injective, which means that $H^q(G, A)(p) = 0$, and shows that $\mathrm{scd}_p(G) \leq \mathrm{cd}_p(G) + 1$, QED.

Examples.

1) Take $G = \widehat{\mathbf{Z}}$. One has $\mathrm{cd}_q(G) = 1$ for every p (this is obvious, cf. for example [145], p. 197, prop. 2). On the other hand, $H^2(G, \mathbf{Z})$ is isomorphic to $H^1(G, \mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z}$, whence $\mathrm{scd}_p(G) = 2$.

2) Let $p \neq 2$, and let G be the group of affine transformations $x \mapsto ax + b$, with $b \in \mathbf{Z}_p$, and $a \in U_p$ (the group of units of $\mathbf{Z}_p$). One can show that $\mathrm{cd}_p(G) = \mathrm{scd}_p(G) = 2$ [use prop. 19 in §3.5].

3) Let ℓ be a prime number, and let G_ℓ be the Galois group of the algebraic closure $\overline{\mathbf{Q}}_l$ of the ℓ-adic field $\mathbf{Q}_l$. Tate has showed $\mathrm{cd}_p(G_\ell) = \mathrm{scd}_p(G_\ell) = 2$ for all p, cf. chap. II, §5.3.

Exercise.

Show that $\mathrm{scd}_p(G)$ cannot equal 1.

3.3 Cohomological dimension of subgroups and extensions

Proposition 14. *Let H be a closed subgroup of the profinite group G. One has*

$$\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$$
$$\mathrm{scd}_p(H) \leq \mathrm{scd}_p(G)$$

with equality in each of the following cases:
(i) *$(G : H)$ is prime to p.*
(ii) *H is open in G, and $\mathrm{cd}_p(G) < +\infty$.*

We will consider only cd_p, since the argument is analogous for scd_p. If A is a discrete torsion H-module, $M_G^H(A)$ is a discrete torsion G-module and $H^q(G, M_G^H(A)) = H^q(H, A)$, whence obviously the inequality

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

The inequality in the opposite direction follows, in case (i), from the fact that Res is injective on the p-primary components (corollary to proposition 9). In the case (ii), set $n = \mathrm{cd}_p(G)$, and let A be a discrete torsion G-module such that $H^n(G, A)(p) \neq 0$. We will see that $H^n(H, A)(p) \neq 0$, which will show that $\mathrm{cd}_p(H) = n$. For this, it is enough to prove the following lemma:

Lemma 4. *The homomorphism* Cor : $H^n(H, A) \to H^n(G, A)$ *is surjective on the p-primary components.*

In fact, let $A^* = M_G^H(A)$, and let $\pi : A^* \to A$ be the homomorphism defined in §2.5, b). This homomorphism is surjective, and its kernel B is a torsion module. Therefore $H^{n+1}(G, B)(p) = 0$, which shows that

$$H^n(G, A^*) \longrightarrow H^n(G, A)$$

is surjective on p-primary components. Since this homomorphism may be identified with the corestriction (cf. §2.5), the lemma follows.

Corollary 1. *If G_p is a Sylow p-subgroup of G, then one has*

$$\mathrm{cd}_p(G) = \mathrm{cd}_p(G_p) = \mathrm{cd}(G_p) \quad \textit{and} \quad \mathrm{scd}_p(G) = \mathrm{scd}_p(G_p) = \mathrm{scd}(G_p) \ .$$

This is clear.

Corollary 2. *In order that $\mathrm{cd}_p(G) = 0$ it is necessary and sufficient that the order of G be prime to p.*

This is obviously sufficient. To show that it is necessary, one can assume that G is a pro-p-group (cf. cor. 1). If $G \neq \{1\}$, there exists a continuous homomorphism of G onto $\mathbf{Z}/p\mathbf{Z}$, by an elementary property of p-groups (cf. for example [145], p. 146). One thus has $H^1(G, \mathbf{Z}/p\mathbf{Z}) \neq 0$, whence $\mathrm{cd}_p(G) \geq 1$.

Corollary 3. *If $\mathrm{cd}_p(G) \neq 0, \infty$, the exponent of p in the order of G is infinite.*

Here again, one may assume G is a pro-p-group. If G were finite, part (ii) of the proposition would show $\mathrm{cd}_p(G) = \mathrm{cd}_p(\{1\}) = 0$, in contradiction to our hypothesis. Therefore G is infinite.

Corollary 4. *Assume* $\mathrm{cd}_p(G) = n$ *is finite. In order that* $\mathrm{scd}_p(G) = n$, *the following condition is necessary and sufficient:*

For every open subgroup H *of* G, *one has* $H^{n+1}(H, \mathbf{Z})(p) = 0$.

The condition is clearly necessary. In the opposite direction, if it holds, then $H^{n+1}(G, A)(p) = 0$ for any discrete G-module A which is isomorphic to some $M_G^H(\mathbf{Z}^m)$,with $m \geq 0$. But every discrete G-module B of finite rank over $\mathbf{Z}$ is isomorphic to a quotient A/C of such an A (take for H an open normal subgroup of G which acts trivially on B). Since $H^{n+2}(G, C)(p)$ is 0, one infers that $H^{n+1}(G, B)(p) = 0$, and, by passing to the limit, this result extends to every discrete G-module, QED.

Prop. 14 can be complemented as follows:

Proposition 14′. *If* G *is* p*-torsion-free, and if* H *is an open subgroup of* G, *then*

$$\mathrm{cd}_p(G) = \mathrm{cd}_p(H) \quad \textit{and} \quad \mathrm{scd}_p(G) = \mathrm{scd}_p(H) \ .$$

In view of prop. 14, one has to show that $\mathrm{cd}_p(H) < \infty$ implies $\mathrm{cd}_p(G) < \infty$; for this, see [149], as well as [151], p. 98, and Haran [66].

Proposition 15. *Let* H *be a closed normal subgroup of the profinite group* G. *One has the inequality:*

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

One uses the spectral sequence of group extensions:

$$E_2^{i,j} = H^i(G/H, H^j(H, A)) \Longrightarrow H^n(G, A) \ .$$

Therefore let A be a discrete torsion G-module, and take

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

If $i + j = n$, then, either $i > \mathrm{cd}_p(G/H)$, or $j > \mathrm{cd}_p(H)$, and the p-primary component of $E_2^{i,j}$ is zero in both cases. From this it follows that the p-primary component of $H^n(G, A)$ is zero, QED.

Remark.

Let us assume that $n = \mathrm{cd}_p(H)$ and $m = \mathrm{cd}_p(G/H)$ are finite. The spectral sequence then gives a canonical isomorphism:

$$H^{n+m}(G, A)(p) = H^m(G/H, H^n(H, A))(p) \ .$$

This isomorphism allows us to give conditions for $\mathrm{cd}_p(G)$ to be *equal* to $\mathrm{cd}_p(H) + \mathrm{cd}_p(G/H)$, cf. §4.1.

Exercises.

1) Show that, in assertion (ii) of prop. 14, one can replace the hypothesis "H is open in G" by "the exponent of p in $(G : H)$ is finite".

2) With the same notation as in prop. 15, assume that the exponent of p in $(G : H)$ is not zero (i.e. $\mathrm{cd}_p(G/H) \neq 0$). Show that one has the inequality $\mathrm{scd}_p(G) \leq \mathrm{cd}_p(H) + \mathrm{scd}_p(G/H)$.

3) Let n be an integer. Assume that for each open subgroup H of G, the p-primary components of $H^{n+1}(H, \mathbf{Z})$ and $H^{n+2}(H, \mathbf{Z})$ are zero. Show that

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

[If G_p is a Sylow p-subgroup of G, show that $H^{n+1}(G_p, \mathbf{Z}/p\mathbf{Z}) = 0$, and then apply prop. 21 of §4.1 to prove $\mathrm{cd}_p(G) \leq n$.]

3.4 Characterization of the profinite groups G such that $\mathrm{cd}_p(G) \leq 1$

Let $1 \to P \to E \xrightarrow{\pi} W \to 1$ be an extension of profinite groups. We shall say that a profinite group G has the *lifting property* for that extension if every morphism $f : G \to W$ lifts to a morphism $f' : G \to E$ (i.e. if there exists an f' such that $f = \pi \circ f'$). This is equivalent to saying that the extension

$$1 \longrightarrow P \longrightarrow E_f \longrightarrow G \longrightarrow 1 \ ,$$

the pull-back of E by f, *splits* (i.e. has a continuous section $G \to E_f$ which is a homomorphism).

Proposition 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 possesses the lifting property for the extensions*

$$1 \longrightarrow P \longrightarrow E \longrightarrow W \longrightarrow 1$$

where E is finite, and where P is an abelian p-group killed by p.

(ii bis) *Every extension of G by a finite abelian p-group killed by p splits.*

(iii) *The group G possesses the lifting property for the extensions*

$$1 \longrightarrow P \longrightarrow E \longrightarrow W \longrightarrow 1$$

where P is a pro-p-group.

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

It is obvious that (iii) $\Leftrightarrow$ (iii bis) and that (ii bis) $\Rightarrow$ (ii). To prove that (ii) $\Rightarrow$ (ii bis), consider an extension

$$1 \longrightarrow P \longrightarrow E_0 \longrightarrow G \longrightarrow 1$$

of G by a finite abelian p-group P killed by p. Let us choose a normal subgroup H of E_0 such that $H \cap P = 1$; the projection $E_0 \to G$ identifies H with an open normal subgroup of G. Set $E = E_0/H$ and $W = G/H$. We have an exact sequence

$$1 \longrightarrow P \longrightarrow E \longrightarrow W \longrightarrow 1 .$$

By (ii), the morphism $G \to W$ lifts to E. Since the square

$$\begin{array}{ccc} E_0 & \longrightarrow & G \\ \downarrow & & \downarrow \\ E & \longrightarrow & W \end{array}$$

is Cartesian, one deduces that G lifts to E_0, i.e. that E_0 splits. Whence (ii bis).

The correspondence between elements of $H^2(G, A)$ and classes of extensions of G by A (cf. 2.3) shows that (i) $\Leftrightarrow$ (ii bis). One has trivially (iii bis) $\Rightarrow$ (ii bis). Thus it remains to show that (ii bis) implies (iii bis). For that one calls upon the following:

Lemma 5. *Let H be a closed normal subgroup of the profinite group E, and let H' be an open subgroup of H. Then there exists an open subgroup H'' of H, contained in H', and normal in E.*

Let N be the normalizer of H' in E, that is the set of $x \in E$ such that $x H' x^{-1} = H'$. Since $x H' x^{-1}$ is contained in H, one sees that N is the set of elements which map a compact set (i.e. H') into an open set (i.e. H', considered as a subspace of H). It follows that N is open, and hence that the number of conjugates of H' is finite. Their intersection H'' satisfies the conditions required.

Let us return now to the proof of (ii bis) $\Rightarrow$ (iii bis). We suppose $1 \to P \to E \to G \to 1$ is an extension of G by a pro-p-group P. Let X be the set of pairs (P', s), where P' is closed in P and normal in E, and where s is a lifting of G into the extension

$$1 \longrightarrow P/P' \longrightarrow E/P' \longrightarrow G \longrightarrow 1 .$$

As in 1.2, order X by defining $(P'_1, s'_1) \geq (P'_2, s'_2)$ if $P'_1 \subset P'_2$ and if s_2 is the composition of s_1 with the map $E/P'_1 \to E/P'_2$. The ordered set X is inductive. Let (P', s) be a *maximal element* of X; all that remains is to show $P' = 1$.

Let E_s be the inverse image of $s(G)$ in E. We have an exact sequence

$$1 \longrightarrow P' \longrightarrow E_s \longrightarrow G \longrightarrow 1 .$$

If $P' \neq 1$, lemma 5 shows that there is an open subgroup P'' of P', not equal to P', and normal in E. By *dévissage* (since P'/P'' is a p-group), one can assume that P'/P'' is abelian and killed by p. By (ii bis), the extension

$$1 \longrightarrow P'/P'' \longrightarrow E_s/P'' \longrightarrow G \longrightarrow 1$$

splits. Therefore there is a lifting of G to E_s/P'' and *a fortiori* to E/P''. This contradicts the assumption that (P', s) is maximal. Thus $P' = 1$, which finishes the proof.

Corollary. *A free pro-p-group $F(I)$ has cohomological dimension ≤ 1.*

Let us check, for example, property (iii bis). Let $E/P = G$ be an extension of $G = F(I)$ by a pro-p-group P, and let x_i be the canonical generators of $F(I)$. Let $u : G \to E$ be a continuous section including the neutral element (cf. prop. 1), and let $e_i = s(x_i)$. Since the x_i converge to 1, this is also true for the e_i, and prop. 5 shows there exists a morphism $s : G \to E$ such that $s(x_i) = e_i$. The extension E thus splits, QED.

Exercises.

1) Let G be a group and let p be a prime. Consider the following property:

$(*_p)$. For any extension $1 \to P \to E \to W \to 1$, where E is finite and P is a p-group, and for any *surjective* morphism $f : G \to W$, there exists a *surjective* morphism $f' : G \to E$ which lifts f.

(a) Show that this property is equivalent to the conjunction of the following two:

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

(2_p). For every open normal subgroup U of G, and for any integer $N \geq 0$, there exist $z_1, \ldots, z_N \in H^1(U, \mathbf{Z}/p\mathbf{Z})$ such that the elements $s(z_i)$ ($s \in G/U$, $1 \leq i \leq N$) are linearly independent over $\mathbf{Z}/p\mathbf{Z}$.

[Start by showing that it suffices to prove $(*_p)$ in the two following cases: (i) every subgroup of E which projects onto W is equal to E; (ii) E is a semi-direct product of W by P, and P is an abelian p-group killed by p. Case (i) is equivalent to (1_p) and case (ii) to (2_p).]

(b) Show that, in order to verify (2_p), it is enough to consider sufficiently small subgroups U (i.e. contained in a fixed open subgroup).

2) (a) Let G and G' be two profinite groups satisfying $(*_p)$ for all p. Assume there is a neighbourhood base (G_n) (resp. (G'_n)) of the neutral element in G (resp. G') formed of normal open subgroups such that G/G_n (resp. G'/G'_n) are solvable for all n. Show that G and G' are isomorphic.

[Construct, by induction on n, two decreasing sequences (H_n) and (H'_n), with $H_n \subset G_n$, $H'_n \subset G'_n$, H_n and H'_n open and normal in G and G', and a coherent sequence (f_n) of isomorphisms $G/H_n \to G'/H'_n$.]

(b) Let L be the free (non-abelian) group generated by a countable family of elements (x_i); let $\widehat{L}_{\mathrm{res}} = \varprojlim L/N$, with N normal in L, and containing almost all the x_i, and such that L/N is solvable and finite. Show that $\widehat{L}_{\mathrm{res}}$ is a metrisable pro-solvable group (i.e. a projective limit of solvable finite groups) which satisfies $(*_p)$ for all p; show, using (a), that any profinite group satisfying these properties is isomorphic to $\widehat{L}_{\mathrm{res}}$.

[Cf. Iwasawa, [75].]

3) Let G be a finite group, S a Sylow p-subgroup of G, and N the normalizer of S in G. Assume that S has the "trivial intersection property", $S \cap gSg^{-1} = 1$ if $g \notin N$.

(a) If A is a finite p-primary G-module, show that the map

$$\mathrm{Res} : H^i(G, A) \longrightarrow H^i(N, A) = H^i(S, A)^{N/S}$$

is an isomorphism for all $i > 0$. [Use the characterization of the image of Res given in [25], Chap. XII, th. 10.1.]

(b) Let $1 \to P \to E \to G \to 1$ be an extension of G by a pro-p-group P. Show that every lifting of N to E can be extended to a lifting of G. [Reduce to the case where P is finite and commutative and use (a) with $i = 1, 2$.]

4) Give an example of an extension $1 \to P \to E \to G \to 1$ of profinite groups with the following properties:

(i) P is a pro-p-group.

(ii) G is finite.

(iii) A Sylow p-subgroup of G lifts to E.

(iv) G does not lift to E.

[For $p > 5$, one may take $G = \mathbf{SL}_2(\mathbf{F}_p)$, $E = \mathbf{SL}_2(\mathbf{Z}_p[w])$, where w is a primitive p-th root of unity.]

3.5 Dualizing modules

Let G be a profinite group. Denote by C_G^f (resp. C_G^t) the category of discrete G-modules A which are finite groups (resp. torsion groups). The category C_G^t may be identified with the category $\varinjlim C_G^f$ of inductive limits of objects of C_G^f.

We denote the category of abelian groups by (Ab). If $M \in$ (Ab), one sets $M^* = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$, and gives this group the topology of pointwise convergence ($\mathbf{Q}/\mathbf{Z}$ being considered as discrete). When M is a torsion group (resp. a finite group), its dual M^* is profinite (resp. finite). In this way one obtains (cf. 1.1, example 4) an equivalence ("Pontryagin duality") between the category of torsion abelian groups and the opposite category to that of profinite commutative groups.

Proposition 17. *Let n be an integer ≥ 0. Assume:*

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

(b) *For every $A \in C_G^f$, the group $H^n(G, A)$ is finite.*

Then the functor $A \mapsto H^n(G, A)^*$ is representable on C_G^f by an element I of C_G^t.

[In other words, there exists $I \in C_G^t$ such that the functors $\mathrm{Hom}^G(A, I)$ and $H^n(G, A)^*$ are isomorphic for A running over C_G^f.]

Put $S(A) = H^n(G, A)$ and $T(A) = H^n(G, A)^*$. Hypothesis (a) shows that S is a covariant and right-exact functor from C_G^f into (Ab); hypothesis (b) shows that its values belong to the subcategory (Ab^f) of (Ab) formed by the *finite* groups. Since the functor * is exact, one sees that T is a contravariant and left-exact functor from C_G^f to (Ab). Prop. 17 is thus a consequence of the following lemma:

Lemma 6. *Let C be a noetherian abelian category, and let $T : C^0 \to$ (Ab) be a contravariant right-exact functor from C to* (Ab). *The functor T is then representable by an object I in $\varinjlim C$.*

This result can be found in a Bourbaki seminar by Grothendieck [61], and in Gabriel's thesis ([52], Chap. II, §4). Let us sketch the proof:

A pair (A, x), with $A \in C$ and $x \in T(A)$, is called *minimal* if x is not an element of any $T(B)$, where B is a quotient of A distinct from A (if B is a quotient of A, one identifies $T(B)$ with a subgroup of $T(A)$). If (A', x') and (A, x) are minimal pairs, one says that (A', x') is *larger* than (A, x) if there exists a morphism $u : A \to A'$ such that $T(u)(x') = x$ (in which case u is unique). The set of minimal pairs is a filtered ordered set, and one takes $I = \varinjlim A$ along this filter. If one puts $T(I) = \varprojlim T(A)$, the x defines a canonical element $i \in T(I)$. If $f : A \to I$ is a morphism, one sends f to $T(f)(i)$ in $T(A)$, and one gets a homomorphism of $\mathrm{Hom}(A, I)$ into $T(A)$. One checks (it is here that the noetherian hypothesis comes in) that this homomorphism is an isomorphism.

Remarks.

1) Here $T(I)$ is just the (compact) dual of the torsion group $H^n(G, I)$ and the canonical element $i \in T(I)$ is a homomorphism

$$i : H^n(G, I) \longrightarrow \mathbf{Q}/\mathbf{Z} .$$

The map $\mathrm{Hom}^G(A, I) \to H^n(G, A)^*$ can be defined by making $f \in \mathrm{Hom}^G(A, I)$ correspond to the homomorphism

$$H^n(G, A) \xrightarrow{f} H^n(G, I) \xrightarrow{i} \mathbf{Q}/\mathbf{Z} .$$

2) The module I is called the *dualizing module* of G (in dimension n). It is well-defined up to isomorphism; or, more precisely, *the pair (I, i) is determined uniquely, up to unique isomorphism.*

3) If one had stuck to p-primary G-modules, one would have only needed the hypothesis $\mathrm{cd}_p(G) \leq n$.

4) By taking limits, one concludes from prop. 17 that, if $A \in C_G^t$, the group $H^n(G, A)$ is the dual of the *compact* group $\mathrm{Hom}^G(A, I)$, the topology of the latter group being that of pointwise convergence. If one sets $\widetilde{A} = \mathrm{Hom}(A, I)$, and considers $\widetilde{A}$ as a G-module by the formula $(gf)(a) = g \cdot f(g^{-1}a)$, one has $\mathrm{Hom}^G(A, I) = H^0(G, \widetilde{A})$ and prop. 17 then gives a *duality between $H^n(G, A)$ and $H^0(G, \widetilde{A})$*, the first group being discrete, and the second compact.

Proposition 18. *If I is the dualizing module for G, then I is also the dualizing module for every open subgroup H of G.*

If $A \in C_H^f$, then $M_G^H(A) \in C_G^f$ and $H^n(G, M_G^H(A)) = H^n(H, A)$. One concludes that $H^n(H, A)$ is dual to $\mathrm{Hom}^G(M_G^H(A), I)$. But it is easy to see that this latter group may be functorially identified with $\mathrm{Hom}^H(A, I)$. It follows that I is indeed the dualizing module of H.

Remark.

The canonical injection of $\mathrm{Hom}^G(A, I)$ into $\mathrm{Hom}^H(A, I)$ defines by duality a surjective homomorphism $H^n(H, A) \to H^n(G, A)$, which is nothing else than the *corestriction*: this can be seen from the interpretation given in §2.5.

Corollary. *Let $A \in C_G^f$. The group $\widetilde{A} = \mathrm{Hom}(A, I)$ is the inductive limit of the duals of the $H^n(H, A)$, for H running over the open subgroups of G* (the maps between these groups being the transposes of the corestrictions).

This follows by duality from the obvious formula

$$\widetilde{A} = \varinjlim \mathrm{Hom}^H(A, I) \ .$$

Remark.

One can make the above statement more precise by proving that the action of G on $\widetilde{A}$ can be obtained by passing to the limit starting from the natural actions of G/H on $H^n(H, A)$, for H an open normal subgroup of G.

Proposition 19. *Assume $n \geq 1$. In order that $\mathrm{scd}_p(G) = n + 1$, it is necessary and sufficient that there exists an open subgroup H of G such that I^H contains a subgroup isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$.*

To say that I^H contains a subgroup isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ amounts to saying that $\mathrm{Hom}^H(\mathbf{Q}_p/\mathbf{Z}_p, I) \neq 0$, or that $H^n(H, \mathbf{Q}_p/\mathbf{Z}_p) \neq 0$. But $H^n(H, \mathbf{Q}_p/\mathbf{Z}_p)$ is the p-primary component of $H^n(H, \mathbf{Q}/\mathbf{Z})$, which is itself isomorphic to $H^{n+1}(H, \mathbf{Z})$ (use the standard exact sequence

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Q} \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0$$

as well as the hypothesis $n \geq 1$). The proposition then follows from cor. 4 of prop. 14.

Examples.

1) Take $G = \widehat{\mathbf{Z}}$, $n = 1$. Assume $A \in C_G^t$, and denote by σ the automorphism of A defined by the canonical generator of G. One can easily verify that (cf. [145], p. 197) $H^1(G, A)$ may be identified with $A_G = A/(\sigma - 1)A$. One concludes that the dualizing module of G is the module $\mathbf{Q}/\mathbf{Z}$, with trivial operators. In particular, we recover the fact that $\mathrm{scd}_p(G) = 2$ for all p.

2) Let $\overline{\mathbf{Q}}_\ell$ be the algebraic closure of the ℓ-adic field $\mathbf{Q}_l$, and let G be the Galois group of $\overline{\mathbf{Q}}_\ell$ over $\mathbf{Q}_l$. Then $\mathrm{cd}(G) = 2$, and the corresponding dualizing module is the group μ of all the roots of unity (chap. II, §5.2). The above proposition again gives the fact that $\mathrm{scd}_p(G) = 2$ for all p, cf. chap. II, §5.3.

§4. Cohomology of pro-p-groups

4.1 Simple modules

Proposition 20. *Let G be a pro-p-group. Every discrete G-module killed by p and simple is isomorphic to* $\mathbf{Z}/p\mathbf{Z}$ (with trivial action).

Let A be such a module. It is obvious that A is finite, and we may view it as a G/U-module, where U is some suitable normal open subgroup of G. In this way one is lead to the case when G is a (finite) p-group, which is well known (cf. for example [145], p. 146).

Corollary. *Any finite discrete and p-primary G-module has a composition series whose successive quotients are isomorphic to* $\mathbf{Z}/p\mathbf{Z}$.

This is obvious.

Proposition 21. *Let G be a pro-p-group and n an integer. In order that* $\mathrm{cd}(G) \leq n$, *it is necessary and sufficient that* $H^{n+1}(G, \mathbf{Z}/p\mathbf{Z}) = 0$.

This follows from prop. 11 and 20.

Corollary. *Assume that* $\mathrm{cd}(G)$ *equals n. If A is a discrete finite, p-primary and nonzero G-module, then* $H^n(G, A) \neq 0$.

In fact, from the corollary to prop. 20, there exists a surjective homomorphism $A \to \mathbf{Z}/p\mathbf{Z}$. Since $\mathrm{cd}(G) \leq n$, the corresponding homomorphism

$$H^n(G, A) \longrightarrow H^n(G, \mathbf{Z}/p\mathbf{Z})$$

is surjective. But prop. 21 shows that $H^n(G, \mathbf{Z}/p\mathbf{Z}) \neq 0$. From this follows the result.

Proposition 21′. *Let G be a profinite group and $n \geq 0$ an integer. If p is a prime number, the following properties are equivalent:*

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

(ii) $H^{n+1}(H, \mathbf{Z}/p\mathbf{Z}) = 0$ *for every closed subgroup H of G.*

(iii) $H^{n+1}(U, \mathbf{Z}/p\mathbf{Z}) = 0$ *for every open subgroup U of G.*

That (i) $\Rightarrow$ (ii) follows from prop. 14. The implication (ii) $\Rightarrow$ (iii) is obvious, and (iii) $\Rightarrow$ (ii) follows from prop. 8 by writing the cohomology groups of a closed subgroup H as the inductive limit of the cohomology groups of the open subgroups U containing H. To prove that (ii) $\Rightarrow$ (i), we may assume by cor. 1 to prop. 14 that G is a pro-p-group, in which case we apply prop. 21.

The following proposition refines prop. 15:

Proposition 22. *Let G be a profinite group and H a closed normal subgroup of G. Assume that $n = \mathrm{cd}_p(H)$ and that $m = \mathrm{cd}_p(G/H)$ are finite. One has the equality*

$$\mathrm{cd}_p(G) = n + m$$

in each of the following two cases:

(i) *H is a pro-p-group and $H^n(H, \mathbf{Z}/p\mathbf{Z})$ is finite.*

(ii) *H is contained in the center of G.*

Let $(G/H)'$ be a Sylow p-subgroup of G/H, and let G' be its inverse image in G. One knows that $\mathrm{cd}_p(G') \leq \mathrm{cd}_p(G) \leq n + m$, and that $\mathrm{cd}_p(G'/H) = m$. It is then sufficient to prove that $\mathrm{cd}_p(G') = n + m$, in other words *one may assume that G/H is a pro-p-group.* On the other hand (cf. §3.3):

$$H^{n+m}(G, \mathbf{Z}/p\mathbf{Z}) = H^m(G/H, H^n(H, \mathbf{Z}/p\mathbf{Z}))\ .$$

In case (i), $H^n(H, \mathbf{Z}/p\mathbf{Z})$ is finite and not 0 (proposition 21). It follows that $H^m(G/H, H^n(H, \mathbf{Z}/p\mathbf{Z}))$ is not 0 (cor. to prop. 21), and from which we get $H^{n+m}(G, \mathbf{Z}/p\mathbf{Z}) \neq 0$ and $\mathrm{cd}_p(G) = n + m$.

In case (ii), the group H is abelian, and therefore a direct product of its Sylow subgroups H_ℓ. By prop. 21, one has $H^n(H_p, \mathbf{Z}/p\mathbf{Z}) \neq 0$ and since H_p is a direct factor of H, it follows that $H^n(H, \mathbf{Z}/p\mathbf{Z}) \neq 0$. On the other hand, the action of G/H on $H^n(H, \mathbf{Z}/p\mathbf{Z})$ is trivial. Indeed, in the case of an arbitrary $H^q(H, A)$, this action comes from the action of G on H (by inner automorphisms) and on A (cf. [145], p. 124), and here both actions are trivial. As a G/H-module, $H^n(H, \mathbf{Z}/p\mathbf{Z})$ is therefore isomorphic to a direct sum of $(\mathbf{Z}/p\mathbf{Z})^{(I)}$, the set of indices I being non-empty. Therefore one has:

$$H^{n+m}(G, \mathbf{Z}/p\mathbf{Z}) = H^m(G/H, \mathbf{Z}/p\mathbf{Z})^{(I)} \neq 0\ ,$$

which finishes the proof as above.

Exercise.

Let G be a pro-p-group. Assume that $H^i(G, \mathbf{Z}/p\mathbf{Z})$ has a finite dimension n_i over $\mathbf{Z}/p\mathbf{Z}$ for each i, and that $n_i = 0$ for sufficiently large i (i.e. $\mathrm{cd}(G) < +\infty$). Put $E(G) = \sum(-1)^i n_i$; this is the *Euler-Poincaré characteristic* of G.

(a) Let A be a discrete G-module, of finite order p^a. Show that the $H^i(G, A)$ are finite. If $p^{n_i(A)}$ denotes their orders, one puts

$$\chi(A) = \sum(-1)^i n_i(A)\ .$$

Show that $\chi(A) = a \cdot E(G)$.

(b) Let H be an open subgroup of G. Show that H has the same properties as G, and that $E(H) = (G : H) \cdot E(G)$.

(c) Let $X/N = H$ be an extension of G by a pro-p-group N verifying the same properties. Show that this is also the case for X and that one has $E(X) = E(N) \cdot E(G)$.

(d) Let G_1 be a pro-p-group. Assume that there exists an open subgroup G of G_1 verifying the above properties. Put $E(G_1) = E(G)/(G_1 : G)$. Show that this number (which is not necessarily an integer) does not depend on the choice of G_1. Generalize (b) and (c).

Show that $E(G_1) \notin \mathbf{Z} \Rightarrow G_1$ contains an element of order p (use prop. 14′).

(e) Assume that G is a p-adic Lie group of dimension ≥ 1. Show, by using the results due to M. Lazard ([102], 2.5.7.1) that $E(G) = 0$.

(f) Let G be the pro-p-group defined by two generators x and y and the relation $x^p = 1$. Let H be the kernel of the homomorphism $f : G \to \mathbf{Z}/p\mathbf{Z}$ such that $f(x) = 1$ and $f(y) = 0$. Show that H is free over the basis $\{x^i y x^{-i}\}$, $0 \leq i \leq p-1$. Deduce that $E(H) = 1 - p$ and $E(G) = p^{-1} - 1$.

4.2 Interpretation of H^1: generators

Let G be a pro-p-group. In the rest of this section we set:

$$H^i(G) = H^i(G, \mathbf{Z}/p\mathbf{Z}) .$$

In particular, $H^1(G)$ denotes $H^1(G, \mathbf{Z}/p\mathbf{Z}) = \mathrm{Hom}(G, \mathbf{Z}/p\mathbf{Z})$.

Proposition 23. *Let $f : G_1 \to G_2$ be a morphism of pro-p-groups. For f to be surjective, it is necessary and sufficient that $H^1(f) : H^1(G_2) \to H^1(G_1)$ be injective.*

The necessity is obvious. Conversely, assume $f(G_1) \neq G_2$. Then there exists a finite quotient P_2 of G_2 such that the image P_1 of $f(G_1)$ in P_2 is different from P_2. It is known (cf., for example, Bourbaki A I.73, Prop. 12) that there a normal subgroup P_2, of index p, which contains P_1. In other words, there is a nonzero morphism $\pi : P_2 \to \mathbf{Z}/p\mathbf{Z}$ which maps P_1 onto 0. If one views π as an element of $H^1(G_2)$, then one has $\pi \in \mathrm{Ker}\, H^1(f)$, QED.

Remark.

Let G be a pro-p-group. Denote by G^* the subgroup of G which is the intersection of the kernels of the continuous homomorphisms $\pi : G \to \mathbf{Z}/p\mathbf{Z}$. One can easily see that $G^* = G^p \cdot \overline{(G, G)}$, where $\overline{(G, G)}$ denotes the closure of the commutator subgroup of G. The groups G/G^* and $H^1(G)$ are each other's duals (the first being compact and the second discrete). Prop. 23 can therefore be restated as follows:

Proposition 23 bis. *In order that a morphism $G_1 \to G_2$ be surjective, it is necessary and sufficient that the same be true of the morphism $G_1/G_1^* \to G_2/G_2^*$ which it induces.*

Thus, G^* plays the rôle of a "radical", and the proposition is analogous to "Nakayama's lemma", so useful in commutative algebra.

Example.

If G is the free group $F(I)$ defined in §1.5, prop. 5 shows that $H^1(G)$ may be identified with the direct sum $(\mathbf{Z}/p\mathbf{Z})^{(I)}$, and G/G^* with the direct product $(\mathbf{Z}/p\mathbf{Z})^I$.

Proposition 24. *Let G be a pro-p-group and I a set. Let*

$$\theta : H^1(G) \longrightarrow (\mathbf{Z}/p\mathbf{Z})^{(I)}$$

be a homomorphism.

(a) *There exists a morphism $f : F(I) \to G$ such that $\theta = H^1(f)$.*

(b) *If θ is injective, such a morphism f is surjective.*

(c) *If θ is bijective, and if $\mathrm{cd}(G) \leq 1$, such a morphism f is an isomorphism.*

By duality, θ gives rise to a morphism of compact groups $\theta' : (\mathbf{Z}/p\mathbf{Z})^I \to G/G^*$, whence, by composition a morphism $F(I) \to G/G^*$. Since $F(I)$ has the lifting property (cf. §3.4), one deduces a morphism $f : F(I) \to G$ which obviously answers the question. If θ is injective, prop. 23 shows that f is surjective. If, moreover, $\mathrm{cd}(G) \leq 1$, prop. 16 shows that there exists a morphism $g : G \to F(I)$ such that $f \circ g = 1$. One knows $H^1(g) \circ H^1(f) = 1$. If $\theta = H^1(f)$ is bijective, it follows that $H^1(g)$ is bijective, therefore that g is surjective. Since $f \circ g = 1$, this shows that f and g are isomorphisms, and finishes the proof.

Corollary 1. *For a pro-p-group G to be isomorphic to a quotient of the free pro-p-group $F(I)$, it is necessary and sufficient that $H^1(G)$ have a basis of cardinality $\leq \mathrm{Card}(I)$.*

In fact, if this condition is satisfied, one may embed $H^1(G)$ in $(\mathbf{Z}/p\mathbf{Z})^{(I)}$, and apply (b).

In particular, *every pro-p-group is a quotient of a free pro-p-group.*

Corollary 2. *In order that a pro-p-group be free, it is necessary and sufficient that its cohomological dimension be ≤ 1.*

One knows this is necessary. Conversely, if $\mathrm{cd}(G) \leq 1$, choose a basis $(e_i)_{i \in I}$ for $H^1(G)$; this gives an isomorphism

$$\theta : H^1(G) \longrightarrow (\mathbf{Z}/p\mathbf{Z})^{(I)} ,$$

and prop. 24 shows that G is isomorphic to $F(I)$.

Let us point out two special cases of the preceding corollary:

Corollary 3. *Let G be a pro-p-group, and let H be a closed subgroup of G.*
(a) *If G is free, H is free.*
(b) *If G is torsion-free and H is free and open in G, then G is free.*

Assertion (a) follows at once. Assertion (b) follows from prop. 14′.

Corollary 4. *The pro-p-groups $F_s(I)$ defined in* §1.5 *are free.*

Indeed, these groups have the *lifting property* mentioned in prop. 16. They are therefore of cohomological dimension ≤ 1.

We shall sharpen corollary 1 a little in the special case that I is finite. If g_1, ..., g_n are elements of G, we shall say that the g_i *generate* G (topologically) if the subgroup they generate (in the algebraic sense) is dense in G; this comes down to the same thing as saying that every quotient G/U, with U open, is generated by the images of the g_i.

Proposition 25. *Let $g_1, \ldots, g_n$ be elements of a pro-p-group G. The following conditions are equivalent:*
(a) *$g_1, \ldots, g_n$ generate G.*
(b) *The homomorphism $g : F(n) \to G$ defined by the g_i* (cf. prop. 5) *is surjective.*
(c) *The images in G/G^* of the g_i generate this group.*
(d) *Each $\pi \in H^1(G)$ which is zero on the g_i is equal to* 0.

The equivalence (a)⇔(b) can be seen directly (it also follows from prop. 24). The equivalence (b)⇔(c) results from prop. 23 bis, and (c)⇔(d) can be inferred from the duality between $H^1(G)$ and G/G^*.

Corollary. *The minimum number of generators of G is equal to the dimension of $H^1(G)$.*
This is clear.

The number thus defined is called the *rank* of G.

Exercises.
1) Show that, if I is an infinite set, $F_s(I)$ is isomorphic to $F(2^I)$.

2) For a pro-p-group G to be metrisable, it is necessary and sufficient that $H^1(G)$ be denumerable.

3) Let G be a pro-p-group. Put $G_1 = G$, and define G_n by induction using the formula $G_n = (G_{n-1})^*$. Show that the G_n form a decreasing sequence of closed normal subgroups of G, with intersection $\{1\}$. Show that the G_n are open if and only if G is of finite rank.

4) Use the notation $n(G)$ for the rank of a pro-p-group G.
(a) Let F be a free pro-p-group of finite rank, and let U be an open subgroup of F. Show that U is a finite-rank pro-p-group, and that we have the equality:

$$n(U) - 1 = (F : U)(n(F) - 1) .$$

[Use the exercise in §4.1 noting that $E(F) = 1 - n(F)$.]

(b) Let G be a finite-rank pro-p-group. Show that, if U is an open subgroup of G, then U is also of finite rank. Prove the inequality:

$$n(U) - 1 \leq (G : U)(n(G) - 1) \ .$$

[Write G as a quotient of a free pro-p-group F of the same rank, and apply (a) to the inverse image U' of U in F.]

Show that, if we have equality in this formula for every U, the group G is free. [Use the same method as above. Compare the filtrations (F_n) and (G_n) defined in exercise 3; show by induction on n that the projection $F \to G$ defines an isomorphism of F/F_n onto G/G_n. Deduce from this that it is an isomorphism.]

5) Let G be a nilpotent group generated by a finite family of elements $\{x_1, \ldots, x_n\}$.

(a) Show that each element of (G, G) may be written in the form

$$(x_1, y_1) \cdots (x_n, y_n) \ , \quad \text{with } y_i \in G.$$

[Argue by induction on the nilpotence class of G, and use the descending central filtration $C^m(G)$, cf. Bourbaki LIE II.44.]

State (and prove) an analogous result for $C^m(G)$, $m > 2$.

(b) Assume that G is a finite p-group. Show that every element of the group $G^* = G^p(G, G)$ may be written in the form

$$y_0^p (x_1, y_1) \cdots (x_n, y_n) \ , \quad \text{with } y_i \in G.$$

6) Let G be a pro-p-group of finite rank n, and let $\{x_1, \ldots, x_n\}$ be a family of elements that generates G topologically.

(a) Let $\varphi : G^n \to G$ be the map given by $(y_1, \ldots, y_n) \mapsto (x_1, y_1) \cdots (x_n, y_n)$. Show that the image of φ is equal to the derived group (G, G) de G. [Reduce to the case where G is finite and use exerc. 5.] Deduce that (G, G) is *closed* in G. The same holds true for other terms of the descending central series of G.

(b) Show (by the same method) that each element of G^* can be written in the form $y_0^p (x_1, y_1) \cdots (x_n, y_n)$, with $y_i \in G$.

(c) Let F be a finite group, and let $f : G \to F$ be a group homomorphism (not necessarily continuous). Show that f is continuous, i.e. that $\mathrm{Ker}(f)$ is open in G. [Use exerc. 1 in §1.3 to prove that F is a p-group if f is surjective. Then argue by induction on the order of F. If this order is equal to p, use (b) to show G^* is contained in $\mathrm{Ker}(f)$, which is therefore open. If this order is $> p$, apply the induction hypothesis to the restriction of f to G^*.]

(d) Deduce from (c) that *each finite-index subgroup of G is open.* [I do not know if this property extends to all profinite groups G which are topologically finitely generated.]

4.3 Interpretation of H^2: relations

Let F be a pro-p-group, and let R be a closed *normal* subgroup of F. Assume $r_1, \ldots, r_n \in R$. We say that the r_i *generate* R (as a normal subgroup of F) if the conjugates of the r_i generate (in an algebraic sense) a dense subgroup of R. This amounts to saying that R is the smallest closed normal subgroup of F containing the r_i.

Proposition 26. *In order that the r_i generate R* (as a normal subgroup of F), *it is necessary and sufficient that any element $\pi \in H^1(R)^{F/R}$ which is zero on the r_i equal* 0.

[One has $H^1(R) = \mathrm{Hom}(R/R^*, \mathbf{Z}/p\mathbf{Z})$ and the group F/R acts on R/R^* by inner automorphisms. It therefore operates on $H^1(R)$ – this is a special case of the results in §2.6.]

Let us assume that the conjugates $g\,r_i\,g^{-1}$ of the r_i generate a dense subgroup of R, and let π be an element of the group $H^1(R)^{F/R}$ such that $\pi(r_i) = 0$ for all i. Since π is invariant under F/R, one has $\pi(g\,x\,g^{-1}) = \pi(x)$ for $g \in F$ and $x \in R$. We conclude that π takes the value zero on the $g\,r_i\,g^{-1}$, and therefore on R, whence $\pi = 0$.

Conversely, assume this condition verified, and let R' be the smallest closed normal subgroup of F containing the r_i. The injection $R' \to R$ defines a homomorphism $f : H^1(R) \to H^1(R')$, and so by restriction a homomorphism $\bar{f} : H^1(R)^F \to H^1(R')^F$. If $\pi \in \mathrm{Ker}(\bar{f})$, π vanishes on R', and so on the r_i, and $\pi = 0$ by hypothesis. It follows that $\mathrm{Ker}(f)$ contains no non-zero element which is F-invariant. By the corollary to prop. 20, this implies $\mathrm{Ker}(f) = 0$, and prop. 23 shows that $R' \to R$ is surjective, whence $R' = R$, QED.

Corollary. *In order that R can be generated by n elements* (as a normal subgroup of F), *it is necessary and sufficient that*

$$\dim H^1(R)^{F/R} \leq n\ .$$

The condition is obviously necessary. Conversely, if $\dim H^1(R)^{F/R} \leq n$, the duality between $H^1(R)$ and R/R^* implies that there exist n elements $r_i \in R$ such that $\langle r_i, \pi \rangle = 0$ for all i implies $\pi = 0$. Whence we have the required result.

Remark.

The dimension of $H^1(R)^{F/R}$ will be called the *rank* of the *normal* subgroup R.

We shall apply the preceding considerations to the case when F is the free pro-p-group $F(n)$, and put $G = F/R$ (the group G is therefore given "by generators and relations").

Proposition 27. *The two following conditions are equivalent*:

(a) *The subgroup R is of finite rank* (as a closed normal subgroup of $F(n)$).

(b) *$H^2(G)$ is of finite dimension.*

If these conditions are satisfied, one has the equality

$$r = n - h_1 + h_2 \ ,$$

where r is the rank of the normal subgroup R, and $h_i = \dim H^i(G)$. (Notice that h_1 is the *rank* of the group G.)

We make use of the exact sequence in §2.6, and of $H^2(F(n)) = 0$. One finds:

$$0 \longrightarrow H^1(G) \longrightarrow H^1(F(n)) \longrightarrow H^1(R)^G \xrightarrow{\delta} H^2(G) \longrightarrow 0 \ .$$

This exact sequence shows that $H^1(R)^G$ and $H^2(G)$ are either finite or infinite together, from which follows the first part of the proposition. The second part also is a consequence of this exact sequence (form the alternating sum of the dimensions).

Corollary. *Let G be a pro-p-group such that $H^1(G)$ and $H^2(G)$ are finite. Let $x_1, \ldots, x_n$ be a minimal system of generators of G. The number r of relations between the x_i is then equal to the dimension of $H^2(G)$.*

[The x_i define a surjective morphism $F(n) \to G$, with kernel R, and the rank of R (as a normal subgroup) is by definition, the "number of relations between the x_i".]

In fact, the hypothesis according to which the x_i form a *minimal* system of generators is equivalent to saying that $n = \dim H^1(G)$, cf. the corollary to prop. 25. The proposition shows that $r = h_2$, QED.

Remark.

The proof of prop. 27 uses in an essential way the homomorphism $\delta : H^1(R)^G \to H^2(G)$, defined by using the spectral sequence, i.e. by "transgression". It is possible to give a more elementary definition (cf. Hochschild-Serre [72]): Start from the extension

$$1 \longrightarrow R/R^* \longrightarrow F/R^* \longrightarrow G \longrightarrow 1 \ ,$$

with an abelian kernel R/R^*. If $\pi : R/R^* \to \mathbf{Z}/p\mathbf{Z}$ is an element of $H^1(R)^G$, π maps this extension into an extension E_π of G by $\mathbf{Z}/p\mathbf{Z}$. The class of E_π in $H^2(G)$ is then equal to $-\delta(\pi)$. In particular, under the hypotheses of the corollary, one obtains a direct definition of the isomorphism

$$\delta : H^1(R)^G \longrightarrow H^2(G) \ .$$

4.4 A theorem of Shafarevich

Let G be a finite p-group. Let $n(G)$ be the minimum number of generators of G, and $r(G)$ the number of relations betweeen these generators (in the corresponding free pro-p-group). We have just seen that $n(G) = \dim H^1(G)$ and $r(G) = \dim H^2(G)$.

[One could also introduce, $R(G)$, the minimum number of relations defining G *as a discrete group*. It is trivial that $R(G) \geq r(G)$, but I see no reason (any more in 1994 than I did in 1964) why there should always be an equality.]

Proposition 28. *For any finite p-group G, one has $r(G) \geq n(G)$. The difference $r(G) - n(G)$ is equal to the p-rank of the group $H^3(G, \mathbf{Z})$.*

The exact sequence $0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \to 0$ gives the exact cohomology sequence:

$$0 \longrightarrow H^1(G) \longrightarrow H^2(G, \mathbf{Z}) \xrightarrow{p} H^2(G, \mathbf{Z}) \longrightarrow H^2(G) \longrightarrow H^3(G, \mathbf{Z})_p \longrightarrow 0 ,$$

where $H^3(G, \mathbf{Z})_p$ denotes the subgroup of $H^3(G, \mathbf{Z})$ formed by the elements killed by p. Since G is finite, all these groups are finite, and by taking the alternating product of their orders, one obtains 1. This gives the equality:

$$r(G) = n(G) - t , \quad \text{with } t = \dim H^3(G, \mathbf{Z})_p .$$

It is obvious that t is also the number of cyclic factors of $H^3(G, \mathbf{Z})$, i.e. the p-rank of this group, whence the proposition.

The result above leads one to ask the following question: may the difference $r(G) - n(G)$ be small? For example, can one have $r(G) - n(G) = 0$ for large values of $n(G)$? [In the only examples known, one has $n(G) = 0$, 1, 2 or 3, cf. exerc. 2.]

The answer is "no". In [135], Shafarevich made the following conjecture:

(*) – *The difference $r(G) - n(G)$ goes to infinity with $n(G)$.*

A little later, Golod et Shafarevich [56] proved this conjecture. More precisely (see Appendix 2):

Theorem 1. *If G is a finite pro-p-group $\neq 1$, then $r(G) > n(G)^2/4$.*

(The inequality proved in [56] is weaker. That given above is due to Gaschütz and Vinberg, cf. [27], Chap. IX.)

The reason Shafarevich was interested in this question was:

Theorem 2. (cf. [135], [136]) *If the conjecture (*) is true* (which is the case), *the classical problem of "class field towers" has a negative answer, i.e. there exist infinite "towers".*

More precisely:

Theorem 2′. *For each p, there exists a number field k, and an infinite Galois extension L/k which is unramified and whose Galois group is a pro-p-group.*

In particular:

Corollary 1. *There exists a number field k such that every finite extension of k has a class number divisible by p.*

Corollary 2. *There exists an increasing sequence of number fields k_i, with degrees $n_i \to \infty$ and discriminants D_i, such that $|D_i|^{1/n_i}$ is independent of i.*

The proof of th. 2′ is based on the following result:

Proposition 29. *Let K/k be an unramified Galois extension of a number field k, whose Galois group G is a finite p-group. Assume that K has no unramified cyclic extension of degree p. Denote by r_1* (resp. r_2) *the number of real* (resp. *complex*) *conjugates of k. Then one has:*

$$r(G) - n(G) \leq r_1 + r_2 \ .$$

(When $p = 2$, the requirement "no ramification" also extends to archimedean places.)

Proof. of prop. 29 (after K. Iwasawa [77]). Set:

I_K = the group of idèles of K,

$C_K = I_K/K^*$, the group of idèle classes of K,

U_K = the subgroup of I_K formed by the elements (x_v) such that x_v is a unit of the field K_v, for each non-archimedean v,

$E_K = K^* \cap U_K$, the group of units of the field K,

E_k = the group of units of the field k,

$\mathrm{Cl}_K = I_K/U_K \cdot K^*$ = the group of idèle classes of K.

There are the following exact sequences of G-modules:

$$0 \longrightarrow U_K/E_K \longrightarrow C_K \longrightarrow \mathrm{Cl}_K \longrightarrow 0$$
$$0 \longrightarrow E_K \longrightarrow U_K \longrightarrow U_K/E_K \longrightarrow 0 \ .$$

That K has no unramified cyclic extension of degree p translates, *via* class field theory, to saying that Cl_K is of order prime to p; the cohomology groups $\widehat{H}^q(G, \mathrm{Cl}_K)$ are therefore trivial. The same is true for the groups $\widehat{H}^q(G, U_K)$: that follows because K/k is unramified. Using the cohomology exact sequence, one gets isomorphisms

$$\widehat{H}^q(G, C_K) \longrightarrow \widehat{H}^{q+1}(G, E_K) \ .$$

On the other hand, class field theory shows that $\widehat{H}^q(G, C_K)$ is isomorphic to $\widehat{H}^{q-2}(G, \mathbf{Z})$. Combining these isomorphisms, and taking $q = -1$, we see that $\widehat{H}^{-3}(G, \mathbf{Z}) = \widehat{H}^0(G, E_K) = E_k/N(E_K)$. But $\widehat{H}^{-3}(G, \mathbf{Z})$ is the dual of $H^3(G, \mathbf{Z})$, cf. [25], p. 250, and hence has the same p-rank. Using prop. 28, we have that $r(G) - n(G)$ is equal to the rank of $E_k/N(E_K)$. By Dirichlet's theorem, the group E_k can be generated by $r_1 + r_2$ elements. The rank of $E_k/N(E_K)$ is therefore $\leq r_1 + r_2$, which proves the proposition. (If k does not contain a primitive p-th root of unity, one can even bound $r(G) - n(G)$ by $r_1 + r_2 - 1$.)

Let us now return to theorem 2'. Let k be an algebraic number field (totally imaginary if $p = 2$) and let $k(p)$ be the largest unramified Galois extension of k whose Galois group G is a pro-p-group. We have to prove the existence of a field k such that $k(p)$ is infinite. Suppose that in fact $k(p)$ is finite. Applying the preceding proposition to $k(p)/k$, we have:

$$r(G) - n(G) \leq r_1 + r_2 \leq [k : \mathbf{Q}] \ .$$

However, $n(G)$ is easy to compute, thanks to class field theory: it is the rank of the p-primary component of the group Cl_k. One can construct fields k, of bounded degrees, such that $n(G) \to \infty$. This contradicts the conjecture $(*)$, QED.

Example.

Take $p = 2$. Let $p_1, \ldots, p_N$ be prime numbers, pairwise distinct, and congruent to 1 mod 4. Let $k = \mathbf{Q}(\sqrt{-p_1 \cdots p_N})$. The field k is an imaginary quadratic field. We have $r_1 = 0$, $r_2 = 1$. On the other hand, it is easy to see that the quadratic extensions of k generated by the $\sqrt{p_i}$, with $1 \leq i \leq N$, are unramified and independent. Thus $n(G) \geq N$ and $r(G) - n(G) \leq 1$.

Remark.

There are analogous results for function fields of one variable over a finite field $\mathbf{F}_q$ (one looks at "towers" where some given places decompose completely – as the archimedean places do for number fields). This allows, for all q, the construction of irreducible smooth projective curves X_i over $\mathbf{F}_q$ with the following properties (cf. [153], and also Schoof [142]):

(a) *The genus g_i of X_i tends to infinity.*

(b) *The number of $\mathbf{F}_q$-points on X_i is $\geq c(q)(g_i - 1)$, where $c(q)$ is a constant > 0 which depends only on q* (for example $c(q) = 2/9$ if $q = 2$, cf. [142]).

Exercises.

1) Prove the inequality $r(G) \geq n(G)$ in prop. 28 by taking the quotient with respect to the commutator subgroup of G.

2) Let n be an integer. Consider families of integers $c(i,j,k)$, with $i,j,k \in [1,n]$, which are alternating in (i,j).

(a) Show that, for every $n \geq 3$, there exists such a family with the following property:

$(*)$ – If the elements $x_1, \ldots, x_n$ of a Lie algebra of characteristic p satisfy the relations

$$[x_i, x_j] = \sum_k c(i,j,k) x_k \ ,$$

then $x_i = 0$ for all i.

(b) To each family $c(i,j,k)$, one associates the pro-p-group G_c defined by n generators x_i, and by the relations

$$(x_i, x_j) = \prod x_k^{p \cdot c(i,j,k)} \ , \quad i < j,$$

with $(x,y) = x\,y\,x^{-1}\,y^{-1}$.

Show that $\dim H^1(G_c) = n$ and $\dim H^2(G_c) = n(n-1)/2$.

(c) Assume $p \neq 2$. Show that, if the family $c(i,j,k)$ satisfies property $(*)$ of (a), the corresponding group G_c is *finite*.

[Filter G by setting $G_1 = G$, $G_{n+1} = G_n^p \cdot \overline{(G, G_n)}$. The associated graded algebra $\mathrm{gr}(G)$ is a Lie algebra over $\mathbf{Z}/p\mathbf{Z}[\pi]$, where $\deg(\pi) = 1$. Show that $[x_i, x_j] = \sum c(i,j,k)\pi \cdot x_k$ in $\mathrm{gr}(G)$.

Deduce that $\mathrm{gr}(G)[\frac{1}{\pi}] = 0$, from which follows the finiteness of $\mathrm{gr}(G)$, and that of G.]

(d) How should the above be modified when $p = 2$?

(e) Show that the pro-p-group generated by three generators x, y, z with the three defining relations

$$x\,y\,x^{-1} = y^{1+p}\ , \quad y\,z\,y^{-1} = z^{1+p}\ , \quad z\,x\,z^{-1} = x^{1+p}$$

is a finite group (cf. J. Mennicke, [106]).

4.5 Poincaré groups

Let n be an integer ≥ 1, and let G be a pro-p-group. We shall say that G is a *Poincaré group of dimension* n if G satisfies the following conditions:

(i) $H^i(G) = H^i(G, \mathbf{Z}/p\mathbf{Z})$ *is finite for all* i.

(ii) $\dim H^n(G) = 1$.

(iii) *The cup-product*

$$H^i(G) \times H^{n-i}(G) \longrightarrow H^n(G)\ , \quad i \geq 0 \text{ arbitrary},$$

is a nondegenerate bilinear form.

These conditions can be expressed more succinctly by saying the algebra $H^*(G)$ is finite-dimensional, and satisfies Poincaré duality. Notice that condition (iii) implies that $H^i(G) = 0$ for $i > n$. Therefore we have $\mathrm{cd}(G) = n$.

Examples.

1) The only Poincaré group of dimension 1 is $\mathbf{Z}_p$ (up to isomorphism).

2) A Poincaré group of dimension 2 is called a *Demuškin group* (cf. [147]). For such a group, we have $\dim H^2(G) = 1$, which shows (cf. §4.3) that G may be defined by a single relation

$$R(x_1, \ldots, x_d) = 1\ , \qquad \text{where} \quad d = \mathrm{rank}(G) = \dim H^1(G)\ .$$

This relation is not an arbitrary one. One may put it in canonical form, cf. Demuškin [43], [44], [45] and Labute [92]. For example, if $p \neq 2$, one may take:

$$R = x_1^{p^h}(x_1, x_2)(x_3, x_4)\cdots(x_{2m-1}, x_{2m})\ , \quad m = \tfrac{1}{2}\dim H^1(G),\ h = 1, 2, \cdots, \infty,$$

with the understanding that $x_1^{p^h} = 1$ if $h = \infty$.

3) M. Lazard [102] has shown that, if G is a p-adic analytic group of dimension n, which is compact and torsion-free, then G is a Poincaré group of dimension n. This provides an ample supply of such groups (as many as — and even more — than there are n-dimensional Lie algebras over $\mathbf{Q}_p$).

If G is an n-dimensional Poincaré group, condition (i), together with the corollary to prop. 20, shows that the $H^i(G, A)$ are finite, for all finite A. Since, on the other hand, we have $\mathrm{cd}(G) = n$, the *dualizing module* I of G is defined (cf. §3.5). We shall see that this provides a genuine "Poincaré duality":

Proposition 30. *Let G be an n-dimensional Poincaré pro-p-group, and let I be its dualizing module. Then:*

(a) *I is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ as an abelian group.*

(b) *The canonical homomorphism $i : H^n(G, I) \to \mathbf{Q}/\mathbf{Z}$ is an isomorphism of $H^n(G, I)$ with $\mathbf{Q}_p/\mathbf{Z}_p$* (viewed as a subgroup of $\mathbf{Q}/\mathbf{Z}$).

(c) *For all $A \in C_G^f$ and for all integers i, the cup-product*

$$H^i(G, A) \times H^{n-i}(G, \widetilde{A}) \longrightarrow H^n(G, I) = \mathbf{Q}_p/\mathbf{Z}_p$$

gives a duality between the two finite groups $H^i(G, A)$ and $H^{n-i}(G, \widetilde{A})$.

[C_G^f denotes the category of finite discrete p-primary G-modules. If A is a G-module, one sets $\widetilde{A} = \mathrm{Hom}(A, I)$, cf. §3.5.]

The proof is carried out in several stages:

(1) – *Duality when A is killed by p.*

It is therefore a $\mathbf{Z}/p\mathbf{Z}$ vector space. Its dual will be written A^* (we shall see later that it may be identified with $\widetilde{A}$). The cup-product defines for any i a bilinear form

$$H^i(G, A) \times H^{n-i}(G, A^*) \longrightarrow H^n(G) = \mathbf{Z}/p\mathbf{Z} \ .$$

This form is *nondegenerate*. Indeed, this is true whenever $A = \mathbf{Z}/p\mathbf{Z}$ from the definition of Poincaré groups. In the light of the corollary to prop. 20, it is therefore sufficient to show that, if one has an exact sequence

$$0 \longrightarrow B \longrightarrow A \longrightarrow C \longrightarrow 0,$$

and if the assertion holds for B and for C, it holds for A. This follows from a standard diagram chase. More precisely, the bilinear form written above amounts to a homomorphism

$$\alpha_i : H^i(G, A) \longrightarrow H^{n-i}(G, A^*)^* \ ,$$

and to say that it is nondegenerate means that α_i is an isomorphism. On the other hand, we have the exact sequence:

$$0 \longrightarrow C^* \longrightarrow A^* \longrightarrow B^* \longrightarrow 0 \ .$$

Passing to cohomology, and dualizing, we obtain the diagram:

$$\begin{array}{ccccccccccc}
\cdots \to & H^{i-1}(G,C) & \to & H^i(G,B) & \to & H^i(G,A) & \to & H^i(G,C) & \to \cdots \\
& \downarrow & - & \downarrow & + & \downarrow & + & \downarrow & \\
\cdots \to & H^{j+1}(G,C^*)^* & \to & H^j(G,B^*)^* & \to & H^j(G,A^*)^* & \to & H^i(G,C^*)^* & \to \cdots
\end{array}$$

with $j = n - i$.

One may verify, by a simple cochain computation, that the squares in this diagram commute up to sign [more precisely, the squares marked with a + are commutative, and the square marked − has the signature $(-1)^i$]. Since the vertical arrows relative to the B and C terms are isomorphisms, the same is true for those relative to the A terms, which proves the assertion.

(2) – *The subgroup I_p of I formed of the elements killed by p is isomorphic to* $\mathbf{Z}/p\mathbf{Z}$.

Assume A is killed by p. The result we have just proved shows that $H^n(G, A)^*$ is functorially isomorphic to $\mathrm{Hom}^G(A, \mathbf{Z}/p\mathbf{Z})$. On the other hand, the definition of a dualizing module shows that it is also isomorphic to $\mathrm{Hom}^G(A, I_p)$. By the uniqueness of the object representing a given functor, we do indeed have $I_p = \mathbf{Z}/p\mathbf{Z}$.

(3) – *The dualizing module I is isomorphic (as an abelian group) to* $\mathbf{Z}/p^k\mathbf{Z}$ *or to* $\mathbf{Q}_p/\mathbf{Z}_p$.

This follows from $I_p = \mathbf{Z}/p\mathbf{Z}$, and elementary properties of p-primary torsion groups.

(4) – *If U is an open subgroup of G, U is an n-dimensional Poincaré group, and* $\mathrm{Cor} : H^n(U) \to H^n(G)$ *is an isomorphism.*

Let $A = M_G^U(\mathbf{Z}/p\mathbf{Z})$. One checks easily that A^* is isomorphic to A and the duality proved in (1) shows that $H^i(U)$ and $H^{n-i}(U)$ are each other's duals. In particular, $\dim H^n(U) = 1$, and since $\mathrm{Cor} : H^n(U) \to H^n(G)$ is surjective (§3.3, lemma 4), it is an isomorphism. Finally, it is not difficult to show that the duality between $H^i(U)$ and $H^{n-i}(U)$ is given by the cup-product.

(5) – *For each $A \in C_G^f$, set $T^i(A) = \varprojlim H^i(U, A)$, for U open in G* (the homomorphisms are those of corestriction). *Then we have $T^i(A) = 0$ for $i \neq n$, and $T^n(A)$ is an exact functor in A (with values in the category of profinite abelian groups).*

It is obvious that the T^i make up a cohomological functor since $\varprojlim$ is exact on the category of profinite groups. To show $T^i = 0$ for $i \neq n$, it is therefore enough to prove it for $A = \mathbf{Z}/p\mathbf{Z}$. But then the $H^i(U)$ are the duals of the $H^{n-i}(U)$, and one is reduced to proving $\varprojlim H^j(U) = 0$ for $j \neq 0$, the homomorphisms being those of *restriction*, which is trivial (and true for any profinite group and any module).

Once the vanishing of the T^i, $i \neq n$, has been shown, the exactness of the T^n is automatic.

(6) – *The group I is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$, as an abelian group.*

We know that $H^n(U, A)$ is dual to $\mathrm{Hom}^U(A, I)$. Taking the limit, we deduce that $T^n(A) = \varprojlim H^n(U, A)$ is dual to $\varinjlim \mathrm{Hom}^U(A, I)$. From (5), the functor $\mathrm{Hom}(A, I)$ is exact; this means that I is $\mathbf{Z}$-divisible, and, looking back at (3), we see that it is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$.

(7) - *The homomorphism $H^n(G,I) \to \mathbf{Q}_p/\mathbf{Z}_p$ is an isomorphism.*

The group of $\mathbf{Z}$-endomorphisms of I is isomorphic to $\mathbf{Z}_p$ (acting in an obvious way). Since these actions commute with the action of G, we see that $\mathrm{Hom}^G(I,I) = \mathbf{Z}_p$. But, $\mathrm{Hom}^G(I,I)$ is also equal to the dual of $H^n(G,I)$, cf. §3.5. Therefore we have a canonical isomorphism $H^n(G,I) \to \mathbf{Q}_p/\mathbf{Z}_p$, and it is not difficult to see that it is the homomorphism i.

(8) - *End of the proof.*

There remains part (c), i. e. the duality between $H^i(G,A)$ and $H^{n-i}(G,\tilde{A})$. This duality holds for $A = \mathbf{Z}/p\mathbf{Z}$, by assumption. Starting from there, we proceed by "dévissage", exactly as in (1). It is enough to notice that, if

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is an exact sequence at C_G^f, the sequence $0 \to \tilde{C} \to \tilde{B} \to \tilde{A} \to 0$ is also exact (because I is divisible): one can use the same type of diagram.

Corollary. *Every open subgroup of a Poincaré group is also a Poincaré group of the same dimension.*

This was proved along the way.

Remarks.

1) The fact that I is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ shows that $\tilde{\tilde{A}}$ *is canonically isomorphic to* A (as a G-module). We get an excellent duality.

2) Denote by $\mathbf{U}_p$ the group of p-adic units (invertible elements of $\mathbf{Z}_p$). This is the automorphism group of I. Since G acts on I, we see that this action is given by a *canonical homomorphism*

$$\chi : G \longrightarrow \mathbf{U}_p \ .$$

This homomorphism is continuous; it determines I (up to isomorphism); one may say that it plays the rôle of the orientation homomorphism $\pi_1 \to \{\pm 1\}$ in Topology. Notice that, since G is a pro-p-group, χ takes its values in the subgroup $\mathbf{U}_p^{(1)}$ of $\mathbf{U}_p$ consisting of elements $\equiv 1 \bmod p$. The homomorphism χ is one of the most interesting invariants of the group G:

a) When G is a Demuškin group (i.e. $n = 2$), G is determined up to isomorphism by the two following invariants: its rank, and the image of χ in $\mathbf{U}_p$, cf. Labute [92], th. 2.

b) The strict cohomological dimension of G depends only on $\mathrm{Im}(\chi)$:

Proposition 31. *Let G be an n-dimensional Poincaré pro-p-group, and let $\chi : G \to \mathbf{U}_p$ be the homomorphism associated to it. For* $\mathrm{scd}(G)$ *to be equal to $n+1$, it is necessary and sufficient that the image of χ be finite.*

To say that $\mathrm{Im}(\chi)$ is finite amounts to saying that there exists an open subgroup U of G such that $\chi(U) = \{1\}$. But this last condition means that I^U contains (and is in fact equal to) $\mathbf{Q}_p/\mathbf{Z}_p$. Whence the result, by prop. 19.

Remark.

The structure of the group $\mathbf{U}_p^{(1)}$ is well-known: if $p \neq 2$, it is isomorphic to $\mathbf{Z}_p$, and if $p = 2$, it is isomorphic to $\{\pm 1\} \times \mathbf{Z}_2$ (cf. for example [145], p. 220). Proposition 31 can therefore be formulated as follows:

For $p \neq 2$, $\mathrm{scd}(G) = n+1 \iff \chi$ is trivial.

For $p = 2$, $\mathrm{scd}(G) = n+1 \iff \chi(G) = \{1\}$ or $\{\pm 1\}$.

Example.

Assume that G is an analytic p-adic group of dimension n, and let $L(G)$ be its Lie algebra. By a result of Lazard ([102], V.2.5.8), the character χ associated to G is given by:

$$\chi(s) = \det \mathrm{Ad}(s) \quad (s \in G),$$

where $\mathrm{Ad}(s)$ denotes the automorphism of $L(G)$ defined by $t \mapsto sts^{-1}$. In particular, we have $\mathrm{scd}_p(G) = n+1$ if and only if $\mathrm{Tr}\,\mathrm{ad}(x) = 0$ for all $x \in L(G)$; this is the case if $L(G)$ is a reductive Lie algebra.

The following proposition is useful in the study of Demuškin groups:

Proposition 32. *Let G be a pro-p-group, and let n be an integer ≥ 1. Assume that $H^i(G)$ is finite for $i \leq n$, that $\dim H^n(G) = 1$, and that the cup-product $H^i(G) \times H^{n-i}(G) \to H^n(G)$ is nondegenerate for $i \leq n$. If moreover G is infinite, it is an n-dimensional Poincaré group.*

It is clearly enough to prove $H^{n+1}(G) = 0$. To this end, we have to establish some properties of duality first:

(1) *Duality for the finite G-modules A killed by p.*

We proceed as in part (1) of the proof of prop. 30. The cup-product defines homomorphisms

$$\alpha_i : H^i(G, A) \longrightarrow H^{n-i}(G, A^*)^* , \qquad 0 \leq i \leq n.$$

By assumption, these are isomorphisms for $A = \mathbf{Z}/p\mathbf{Z}$. By "dévissage" one easily deduces that these are isomorphisms for $1 \leq i \leq n-1$, that α_0 is surjective, and that α_n is injective [the difference from the situation in prop. 30 is that one does not know whether the functor H^{n+1} vanishes, which makes for some small problems at the end of the exact sequences].

(2) *The functor $H^0(G, A)$ is coeffaceable.*

This is a general property of profinite groups whose order is divisible by p^∞:

If A is killed by p^k (here $k = 1$, but it makes little difference), one chooses an open subgroup U of G acting trivially on A, and an open subgroup V of U with an index divisible by p^k. We put $A' = M_G^V(A)$, and consider the surjective homomorphism $\pi : A' - A$, defined in §2.5. By going to H^0, we obtain $\mathrm{Cor} : H^0(V, A) \to H^0(G, A)$. This homomorphism is zero; indeed, it is equal to $N_{G/V}$, which is equal to $(U : V) \cdot N_{G/U}$. The homomorphism $H^0(G, A') \to H^0(G, A)$ is therefore zero, which implies that H^0 is coeffaceable.

(3) *The duality holds in dimensions* 0 *and* n.

We have to prove that α_0 and α_n are bijective for all A annihilated by p. It is enough (by transposition) to do this for α_0. One chooses an exact sequence $0 \to B \to C \to A \to 0$, such that $H^0(G,C) \to H^0(G,A)$ is zero, cf. (2). Then one has the diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(G,A) & \longrightarrow & H^1(G,B) & \longrightarrow & H^1(G,C) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^n(G,C^*)^* & \longrightarrow & H^n(G,A^*)^* & \longrightarrow & H^{n-1}(G,B^*)^* & \longrightarrow & H^{n-1}(G,C^*)^* \ . \end{array}$$

The arrows relative to H^1 are isomorphisms. It follows that α_0 is injective, whence the result, since one already knows that it is surjective.

(4) *The functor* H^n *is right exact.*

This follows by duality from the fact that H^0 is left exact.

(5) *End of the proof.*

The result we have just proved implies that $\mathrm{cd}(G) \leq n$. Indeed, if $x \in H^{n+1}(G,A)$, x induces 0 on an open subgroup U of G, and thus gives 0 in $H^{n+1}(G, M_G^U(A))$. Making use of the exact sequence, and of the fact that H^n is right exact, we see that $x = 0$, QED.

Exercises.

1) Let G be a commutative pro-p-group. Show the equivalence of:
(a) $\mathrm{cd}_p(G) = n$;
(b) G is isomorphic to $(\mathbf{Z}_p)^n$;
(c) G is a Poincaré group of dimension n.

2) Let G be the fundamental group of a compact surface S of genus g; assume $g \geq 1$ if S is orientable and $g \geq 2$ if not. Let $\widehat{G}_p$ be the p-completion of G. Show that it is a Demuškin group, and that, for every finite and p-primary $\widehat{G}_p$-module A, $H^i(\widehat{G}_p; A) \to H^i(G,A)$ is an isomorphism. Show that the strict cohomological dimension of $\widehat{G}_p$ is equal to 3, and compute explicitly the invariant χ of $\widehat{G}_p$.

3) Let G be the pro-p-group defined by two generators x and y with the relation $x\,y\,x^{-1} = y^q$, where $q \in \mathbf{Z}_p$, $q \equiv 1 \bmod p$. Show that G is a Demuškin group and that its invariant χ is given by the formulas:

$$\chi(y) = 1 \ , \qquad \chi(x) = q \ .$$

When is this group of strict cohomological dimension 3?

Apply this to the Sylow p-subgroup of the affine group $ax + b$ over $\mathbf{Z}_p$.

4) Let G be a Poincaré pro-p-group of dimension n, and let I be its dualizing module. Let $J = \mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, I)$. The G-module J is isomorphic to $\mathbf{Z}_p$ as a compact group, with the group G acting through χ.

(a) Let A a finite p-primary G-module. Set $A_0 = A \otimes J$, the tensor product being taken over $\mathbf{Z}_p$. Show that $\widetilde{A}_0$ is canonically isomorphic to the dual A^* of A.

(b) For all integers $i \geq 0$, one considers the projective limit $H_i(G, A)$ of the *homology* groups $H_i(G/U, A)$, where U is an open normal subgroup of G and acts trivially in A. Construct a canonical isomorphism

$$H_i(G, A) = H^{n-i}(G, A_0) \ .$$

[Use the duality between $H_i(G/U, A)$ and $H^i(G/U, A^*)$, cf. [25], p. 249–250.]

5) Let G be a Poincaré pro-p-group of dimension $n > 0$.

(a) Let H be a closed subgroup of G, distinct from G. Show that

$$\text{Res} : H^n(G) \longrightarrow H^n(H)$$

is 0. [Reduce to the case when H is open, and use part (4) of the proof of prop. 30.]

(b) Assume that $(G : H) = \infty$, i.e. that H is not open. Show that $\text{cd}(H) \leq n - 1$.

In particular, every closed subgroup of infinite index of a Demuškin group is a free pro-p-group.

6) Let G be a Demuškin group and let H be an open subgroup of G. Let r_G and r_H be their ranks. Show that one has:

$$r_H - 2 = (G : H)(r_G - 2) \ .$$

[Use the exercise in §4.1, noting that $E(G) = 2 - r_G$ and $E(H) = 2 - r_H$.]

Conversely, this property *characterizes* Demuškin groups, cf. Dummit-Labute [48].

§5. Nonabelian cohomology

In what follows, G denotes a profinite group.

5.1 Definition of H^0 and of H^1

A *G-set* E is a discrete topological space on which G acts continuously; as in the case of G-modules, this amounts to saying that $E = \bigcup E^U$, for U running over the set of open subgroups of G (we denote by E^U the subset of E of elements fixed under U). If $s \in G$ and $x \in E$, the image $s(x)$ of x under s will often be denoted by ${}^s x$ [but never x^s, to avoid the ugly formula $x^{(st)} = (x^t)^s$)]. If E and E' are two G-sets, a *morphism* of E to E' is a map $f : E \to E'$ which commutes with the action of G; if we wish to be explicit about G, we will write "G-morphism". The G-sets form a category.

A *G-group* A is a group in the above-mentioned category; this amounts to saying that it is a G-set, with a group structure invariant under G (i.e. ${}^s(xy) = {}^s x {}^s y$). When A is commutative, one recovers the notion of a *G-module*, used in the previous sections.

If E is a G-set, we put $H^0(G, E) = E^G$, the set of elements of E fixed under G. If E is a G-group, $H^0(G, E)$ is a group.

If A is a G-group, one calls *1-cocycle* (or simply *cocycle*) *of G in A* a map $s \mapsto a_s$ of G to A which is continuous and such that:

$$a_{st} = a_s {}^s a_t \quad (s, t \in G).$$

The set of these cocycles will be denoted $Z^1(G, A)$. Two cocycles a and a' are said to be *cohomologous* if there exists $b \in A$ such that $a'_s = b^{-1} a_s {}^s b$. This is an equivalence relation in $Z^1(G, A)$, and the quotient set is denoted $H^1(G, A)$. This is the "first cohomology set of G in A"; it has a distinguished element (called the "neutral element" even though there is in general no composition law on $H^1(G, A)$): the class of the unit cocycle; we denote it by either 0 or 1. One checks that

$$H^1(G, A) = \varinjlim H^1(G/U, A^U) ,$$

for U running over the set of open normal subgroups of G; moreover, the maps $H^1(G/U, A^U) \to H^1(G, A)$ are injective.

The cohomology sets $H^0(G, A)$ and $H^1(G, A)$ are functorial in A, and coincide with the cohomology groups of dimensions 0 and 1 when A is commutative.

Remarks.

1) One would like also to define $H^2(G, A)$, $H^3(G, A)$, ... I will not attempt to do so; the interested reader may consult Dedecker [38], [39] and Giraud [54].

2) The nonabelian H^1 are *pointed* sets; the notion of an exact sequence therefore makes sense (the image of a map is equal to the inverse image of the neutral element); however, such an exact sequence gives no information about the *equivalence relation* defined by a map; this defect (particularly obvious in [145], p. 131–134), can be remedied thanks to the notion of twisting, to be developed in §5.3.

Exercises.

1) Let A be a G-group, and let $A \cdot G$ be the semidirect product of G by A (defined in such a way that $sas^{-1} = {}^s a$ for $a \in A$ and $s \in G$).

A cocycle $a = (a_s) \in Z^1(G, A)$ defines a continuous lifting

$$f_a : G \longrightarrow A \cdot G$$

by $f_a(s) = a_s \cdot s$, and conversely. Show that the liftings f_a and $f_{a'}$ associated to the cocycles a and a' are conjugate by an element of A if and only if a and a' are cohomologous.

2) Let $G = \widehat{\mathbf{Z}}$; denote by σ the canonical generator of G.

(a) If E is a G-set, σ defines a permutation of E all of whose orbits are finite; conversely, such a permutation defines a G-set structure.

(b) Let A be a G-group. Let (a_s) be a cocycle of G in A, and let $a = a_\sigma$. Show that there exists $n \geq 1$ such that $\sigma^n(a) = a$ and that $a \cdot \sigma(a) \cdots \sigma^{n-1}(a)$ is of finite order. Conversely, every $a \in A$ for which there exists such an n corresponds to one and only one cocycle. If a and a' are two such elements, the corresponding cocycles are cohomologous if and only if there exists $b \in A$ such that $a' = b^{-1} \cdot a \cdot \sigma(b)$.

(c) How does the above need modifying when one replaces $\widehat{\mathbf{Z}}$ by $\mathbf{Z}_p$?

5.2 Principal homogeneous spaces over A – a new definition of $H^1(G, A)$

Let A be a G-group, and let E be a G-set. One says that A *acts on the left* on E (in a manner compatible with the action of G) if it acts on E in the usual sense and if ${}^s(a \cdot x) = {}^s a \cdot {}^s x$ for $a \in A$, $x \in E$ (this amounts to saying that the canonical map of $A \times E$ to E is a G-morphism). This is also written ${}_A E$ as a reminder that A acts on the left (there is an obvious similar notation for right actions).

A *principal homogeneous space* (or *torsor*) over A is a non-empty G-set P, on which A acts on the right (in a manner compatible with G) so as to make of it an "affine space" over A (i.e. for each pair $x, y \in P$, there exists a unique $a \in A$ such that $y = x \cdot a$). The notion of an isomorphism between two such spaces is defined in an obvious way.

Proposition 33. *Let A be a G-group. There is a bijection between the set of classes of principal homogeneous spaces over A and the set $H^1(G, A)$.*

Let $P(A)$ be the first set. One defines a map

$$\lambda : P(A) \longrightarrow H^1(G, A)$$

in the following way:

If $P \in P(A)$, we choose a point $x \in P$. If $s \in G$, one has ${}^s x \in P$, therefore there exists $a_s \in A$ such that ${}^s x = x \cdot a_s$. One checks that $s \mapsto a_s$ is a cocycle. Substituting $x \cdot b$ for x changes this cocycle into $s \mapsto b^{-1} a_s {}^s b$, which is cohomologous to it. One may thus define λ by taking $\lambda(P)$ as the class of a_s.

Vice versa, one defines $\mu : H^1(G, A) \to P(A)$ as follows:

If $a_s \in Z^1(G, A)$, denote by P_a the group A on which G acts by the following "twisted" formula:

$${}^{s'} x = a_s \cdot {}^s x \ .$$

If one lets A act on the right on P_a by translations, one obtains a principal homogeneous space. Two cohomologous cocycles give two isomorphic spaces. This defines the map μ, and one checks easily that $\lambda \circ \mu = 1$ and $\mu \circ \lambda = 1$.

Remark.

The principal spaces considered above are *right* principal spaces. One may similarly define the notion of a *left* principal space; we leave to the reader the task of defining a bijection between the two notions.

5.3 Twisting

Let A be a G-group, and let P be a principal homogeneous space over A. Let F be a G-set on which A acts on the left (compatibly with G). On $P \times F$, consider the equivalence relation which identifies an element (p, f) with the elements $(p \cdot a, a^{-1} f)$, $a \in A$. This relation is compatible with the action of G, and the quotient is a G-set, denoted $P \times^A F$, or ${}_P F$. An element of $P \times^A F$ can be written in the form $p \cdot f$, $p \in P$, $f \in F$, and one has $(pa) f = p(af)$, which explains the notation. Remark that, for all $p \in P$, the map $f \mapsto p \cdot f$ is a bijection of F onto ${}_P F$; for this reason, one says that ${}_P F$ is obtained from F *by twisting it using* P.

The twisting process can also be defined from the cocycle point of view. If $(a_s) \in Z^1(G, A)$, denote by ${}_a F$ the set F on which G acts by the formula

$${}^{s'} f = a_s \cdot {}^s f \ .$$

One says that ${}_a F$ is obtained *by twisting F using the cocycle a_s*.

The connection between these points of view is easy to make: if $p \in P$, we have seen that p defines a cocycle a_s by the formula ${}^s p = p \cdot a_s$. The map $f \mapsto p \cdot f$ defined above is *an isomorphism of the G-set ${}_a F$ with the G-set ${}_P F$*; indeed one has

$$p \cdot {}^{s'} f = p \cdot a_s \cdot {}^s f = {}^s p \cdot {}^s f = {}^s (p \cdot f) \ .$$

This shows in particular that ${}_a F$ *is isomorphic to ${}_b F$ if a and b are cohomologous.*

Remark.

Note that there is, in general, no canonical isomorphism between ${}_aF$ and ${}_bF$, and that consequently it is *impossible to identify* these two sets, as one would be tempted to do. In particular, the notation ${}_\alpha F$, with $\alpha \in H^1(G, A)$, is dangerous (even if sometimes convenient...). Of course, the same difficulty occurs in Topology, in the theory of fiber spaces (which we are mimicking).

The twisting operation enjoys a number of elementary properties:

(a) ${}_aF$ is functorial in F (for A-morphisms $F \to F'$).
(b) We have ${}_a(F \times F') = {}_aF \times {}_aF'$.
(c) If a G-group B acts on the right on F (so that it commutes with the action of A), B also acts on ${}_aF$.
(d) If F has a G-group structure invariant under A, the same structure on ${}_aF$ is also a G-group structure.

Examples.

1) Take for F the group A, acting on itself by left translations. Since right translations commute with left translations, property (c) above shows that A acts on the right on ${}_aF$, and one obtains thus a principal homogeneous space over A (namely the space denoted by ${}_aP$ in the previous subsection).

In the notation $P \times {}^AF$, this can be written:

$$P \times {}^AA = P\ ,$$

a cancellation formula analogous to $E \otimes_A A = E$.

2) Again take for F the group A, acting this time by *inner automorphisms.* Since this action preserves the group structure of A, property (d) shows that ${}_aA$ *is a G-group* [one could twist any normal subgroup of A in the same way]. By definition, ${}_aA$ has the same underlying group as A, and the action of G on ${}_aA$ is given by the formula

$$ {}^{s'}x = a_s \cdot {}^s x \cdot a_s^{-1} \qquad (s \in G,\ x \in A).$$

Proposition 34. *Let F be a G-set where A acts on the left* (compatibly with G), *and let a be a cocycle of G in A. Then the twisted group ${}_aA$ acts on ${}_aF$, compatibly with G.*

One needs to check that the map $(a, x) \mapsto ax$ of ${}_aA \times {}_aF$ an ${}_aF$ is a G-morphism. This is a simple computation.

Corollary. *If P is a principal homogeneous space over A, the group ${}_PA$ acts on the left on P, and makes P into a principal left-homogeneous space over ${}_PA$.*

The fact that ${}_PA$ acts on P is a special case of prop. 34 (or can be seen directly, if one wishes). It is clear that this makes P into a principal left-homogeneous space over ${}_PA$.

Remark.

If A and A' are two G-groups, one defines the notion of an (A, A')-principal space in an obvious way: it is a principal (left) A-space, and a principal (right) A'-space, with the actions of A and A' commuting. If P is such a space, the above corollary shows that A may be identified with ${}_PA'$. If Q is an (A', A'')-principal space (A'' being some other G-group), the space $P \circ Q = P \times^{A'} Q$ has a canonical structure of an (A, A'')-principal space. In this way one obtains a composition law (not everywhere defined) on the set of "biprincipal" spaces.

Proposition 35. *Let P be a right principal homogeneous space for a G-group A, and let $A' = {}_PA$ be the corresponding group. If one associates to each principal* (right)*-homogeneous space Q over A' the composition $Q \circ P$, one obtains 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 $H^1(G, A)$.*

[More briefly: if one twists a group A by a cocycle of A itself, one gets a group A' which has the same cohomology as A in dimension 1.]

Define the opposite $\overline{P}$ of P as follows: it is an (A, A')-principal space, identical to P as a G-set, with the group A acting on the left by $a \cdot p = p \cdot a^{-1}$, and the group A' on the right by $p \cdot a' = a'^{-1} \cdot p$. By associating with each principal right A-space R the composition $R \circ \overline{P}$, we obtain the inverse map of that given by $Q \mapsto Q \circ P$. The proposition follows.

Proposition 35 bis. *Let $a \in Z^1(G, A)$, and let $A' = {}_aA$. To each cocycle a'_s in A' let us associate $a'_s \cdot a_s$; this gives a cocycle of G in A, whence a bijection*

$$t_a : Z^1(G, A') \longrightarrow Z^1(G, A) .$$

By taking quotients, t_a defines a bijection

$$\tau_a : H^1(G, A') \longrightarrow H^1(G, A)$$

mapping the neutral element of $H^1(G, A')$ into the class α of a.

This is essentially a translation of prop. 35 in terms of cocycles. It may also be proved by direct computation.

Remarks.

1) When A is *abelian*, we have $A' = A$ and τ_a is simply the *translation by the class α of a.*

2) Propositions 35 and 35 bis, elementary as they are, are nonetheless useful. As we shall see, they give a method to determine the equivalence relations which occur in various "cohomology exact sequences".

Exercise.

Let A be a G-group. Let $E(A)$ be the set of classes of (A, A)-principal spaces. Show that the composition makes $E(A)$ into a *group*, and that 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 $H^1(G, A)$. In the general case, show that $E(A)$ contains the quotient of $\mathrm{Aut}(A)$ by the inner automorphisms defined by the elements of A^G. How may one define $E(A)$ using cocycles?

5.4 The cohomology exact sequence associated to a subgroup

Let A and B be two G-groups, and let $u : A \to B$ be a G-homomorphism. This homomorphism defines a map

$$v : H^1(G, A) \longrightarrow H^1(G, B) .$$

Let $\alpha \in H^1(G, A)$. We wish to describe the fiber of α for v, that is the set $v^{-1}(v(\alpha))$. Choose a representative cocycle a for α, and let b be its image in B. If one puts $A' = {}_aA$, $B' = {}_bB$, it is clear that u defines a homomorphism

$$u' : A' \longrightarrow B' ,$$

hence a map $v' : H^1(G, A') \to H^1(G, B')$.

We also have the following commutative diagram (where the letters τ_a and τ_b denote the bijections defined in 5.3):

$$\begin{array}{ccc} H^1(G, A) & \xrightarrow{v} & H^1(G, B) \\ {\scriptstyle \tau_a}\uparrow & & {\scriptstyle \tau_b}\uparrow \\ H^1(G, A') & \xrightarrow{v'} & H^1(G, B') . \end{array}$$

Since τ_b transforms the neutral element of $H^1(G, B')$ into $v(\alpha)$, we see that τ_a *is a bijection of the kernel of* v' *onto to the fiber* $v^{-1}(v(\alpha))$ *of* α. In other words, twisting allows one to transform each fiber of v into a kernel – and these kernels themselves may occur in exact sequences (cf. [145], *loc. cit.*).

Let us apply this principle to the simplest possible case, that in which A *is a subgroup of* B.

Consider the homogeneous space B/A of *left* A*-classes* of B; it is a G-set, and $H^0(G, B/A)$ is well-defined. Moreover, if $x \in H^0(G, B/A)$, the inverse image X of x in B is a principal (right-)homogeneous A-space; its class in $H^1(G, A)$ will be denoted by $\delta(x)$. The coboundary thus defined has the following property:

Proposition 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.

It is easy to translate the definition of δ into cocycle terms; if $c \in (B/A)^G$, choose $b \in B$ which projects onto c, and set $a_s = b^{-1} \cdot {}^s b$; this is a cocycle whose class is $\delta(c)$. Its definition shows that it is cohomologous to 0 in B, and that each cocycle of G in A which is cohomologous to 0 in B is of this form. The proposition follows.

Corollary 1. *The kernel of* $H^1(G, A) \to H^1(G, B)$ *may be identified with the quotient space of* $(B/A)^G$ *by the action of the group* B^G.

The identification is made *via* δ; we need to check that $\delta(c) = \delta(c')$ if and only if there exists $b \in B^G$ such that $bc = c'$; this is easy.

Corollary 2. *Let $\alpha \in H^1(G, A)$, and let a be a cocycle representing α. The elements of $H^1(G, A)$ with the same image as α in $H^1(G, B)$ are in one-to-one correspondence with the elements of the quotient of $H^0(G, {}_aB/{}_aA)$ by the action of the group $H^0(G, {}_aB)$.*

This follows from corollary 1 by twisting, as has been explained above.

Corollary 3. *In order that $H^1(G, A)$ be countable* (resp. *finite*, resp. *reduced to one element*), *it is necessary and sufficient that the same be true of its image in $H^1(G, B)$, and of all the quotients $({}_aB/{}_aA)^G/({}_aB)^G$, for $a \in Z^1(G, A)$.*

This follows from corollary 2.

One can also describe the *image* of $H^1(G, A)$ in $H^1(G, B)$ explicitly [just as if $H^1(G, B/A)$ made sense]:

Proposition 37. *Let $\beta \in H^1(G, B)$ and let $b \in Z^1(G, B)$ be a representative for β. In order that β belong to the image of $H^1(G, A)$, it is necessary and sufficient that the space ${}_b(B/A)$, obtained by twisting B/A by b, have a point fixed under G.*

[Combined with cor. 2 to prop. 36, this shows that the set of elements in $H^1(G, A)$ with image β is in one-to-one correspondence with the quotient $H^0(G, {}_b(B/A))/H^0(G, {}_bB)$.]

In order that β belong to the image of $H^1(G, A)$, it is necessary and sufficient that there exist $b \in B$ such that $b^{-1}b_s{}^s b$ belong to A for all $s \in G$. If c denotes the image of b in B/A, this means that $c = b_s \cdot {}^s c$, i.e. that $c \in H^0(G, {}_b(B/A))$, QED.

Remark.

Prop. 37 is an analogue of the classical theorem of Ehresmann: in order that the structural group A of a principal fiber bundle may be reduced to a given subgroup B, it is necessary and sufficient that the associated fiber space with fiber A/B have a section.

5.5 Cohomology exact sequence associated to a normal subgroup

Assume A normal in B, and set $C = B/A$; here, C is a G-group.

Proposition 38. *The sequence of pointed sets:*

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C)$$

is exact.

The verification is immediate (cf. [145], p. 133).

The fibers of the map $H^1(G,A) \to H^1(G,B)$ were described in §5.4. However, the fact that A is normal in B simplifies that description. Note first:

The group C^G acts naturally (on the right) on $H^1(G,A)$. Indeed, let $c \in C^G$, and let $X(c)$ be its inverse image in B; the G-set $X(c)$ has, in a natural way, the structure of a principal (A,A)-space; if P is principal for A, the product $P \circ X(c)$ is also principal for A; it is the transform of P by c. [Translation into cocycle terms: lift c to $b \in B$; then ${}^s b = b \cdot x_s$, with $x_s \in A$; to each cocycle a_s of G in A, one associates the cocycle $b^{-1}a_s b\, x_s = b^{-1}a_s {}^s b$; its cohomology class is the image under c of that of (a_s).]

Proposition 39. (i) *If $c \in C^G$, then $\delta(c) = 1 \cdot c$, where 1 represents the neutral element of $H^1(G,A)$.*

(ii) *Two elements of $H^1(G,A)$ have the same image in $H^1(G,B)$ if and only if they are in the same C^G-orbit.*

(iii) *Let $a \in Z^1(G,A)$, let α be its image in $H^1(G,A)$, and let $c \in C^G$. For $\alpha \cdot c = \alpha$, it is necessary and sufficient that c belong to the image of the homomorphism $H^0(G, {}_aB) \to H^0(G,C)$.*

[We denote by ${}_aB$ the group obtained by twisting B with the cocycle a — with A acting on B by inner automorphisms.]

The equation $\delta(c) = 1 \cdot c$ is a consequence of the definition of δ. On the other hand, if two cocycles a_s and a'_s of A are cohomologous in B, there exists $b \in B$ such that $a'_s = b^{-1}a_s {}^s b$; if c is the image of b in C, one has ${}^s c = c$, whence $c \in C^G$, and it is clear that c maps the class of a_s into that of a'_s. The converse is trivial, which proves (ii). Finally, if $b \in B$ is a lift of c, and if $\alpha \cdot c = \alpha$, there exists $x \in A$ such that $a_s = x^{-1}b^{-1}a_s {}^s b\, {}^s x$; this can also be written $bx = a_s {}^s(bx) a_s^{-1}$, i.e. $bx \in H^0(G, {}_aB)$. Hence (iii).

Corollary 1. *The kernel of $H^1(G,B) \to H^1(G,C)$ may be identified with the quotient of $H^1(G,A)$ by the action of the group C^G.*

This is clear.

Corollary 2. *Let $\beta \in H^1(G,B)$, and let b be a cocycle representing β. The elements of $H^1(G,B)$ with the same image as β in $H^1(G,C)$ correspond bijectively with the elements of the quotient of $H^1(G, {}_bA)$ by the action of the group $H^0(G, {}_bC)$.*

[The group B acts on itself by inner automorphisms, and leaves A stable; this allows the *twisting* of the exact sequence $1 \to A \to B \to C \to 1$ by the cocycle b.]

This follows from cor. 1 by twisting, as was explained in the previous section.

Remark.

Proposition 35 shows that $H^1(G, {}_bB)$ may be identified with $H^1(G,B)$, and similarly $H^1(G, {}_bC)$ may be identified with $H^1(G,C)$. In contrast, $H^1(G, {}_bA)$ *bears, in general, no relation to* $H^1(G,A)$.

Corollary 3. *In order that* $H^1(G,B)$ *be countable* (resp. *finite*, resp. *reduced to a single element*), *it is necessary and sufficient that the same be true for its image in* $H^1(G,C)$, *and for all the quotients* $H^1(G,{}_bA)/({}_bC)^G$, *for* $b \in Z^1(G,B)$.

This follows from cor. 2.

Exercise.

Show that, if one associates to each $c \in C^G$ the class of the principal (A,A)-space $X(c)$, one obtains a homomorphism of C^G into the group $E(A)$ defined in the exercise in §5.3.

5.6 The case of an abelian normal subgroup

Assume A is abelian and normal in B. Keep the notation of the preceding section. Write $H^1(G,A)$ additively, since it is now an abelian group. If $\alpha \in H^1(G,A)$, and $c \in C^G$, denote by α^c the image of α by c, defined as above. Let us make this operation more explicit.

To this end, we note that the obvious homomorphism $C^G \to \mathrm{Aut}(A)$ makes C^G act (on the left) on the group $H^1(G,A)$; the image of α by c (for this new action) will be denoted $c \cdot \alpha$.

Proposition 40. *We have* $\alpha^c = c^{-1} \cdot \alpha + \delta(c)$ *for* $\alpha \in H^1(G,A)$ *and* $c \in C^G$.

This is a simple computation: if we lift c to $b \in B$, we have ${}^s b = b \cdot x_s$, and the class of x_s is $\delta(c)$. On the other hand, if a_s is a cocycle in the class α, we can take as a representative of α^c the cocycle $b^{-1}a_s{}^s b$, and to represent $c^{-1}\cdot\alpha$ the cocycle $b^{-1}a_s b$. We have $b^{-1}a_s{}^s b = b^{-1}a_s b \cdot x_s$, from which the formula follows.

Corollary 1. *We have* $\delta(c'c) = \delta(c) + c^{-1} \cdot \delta(c')$.

Write $\alpha^{c'c} = (\alpha^{c'})^c$. Expanding this gives the formula we want.

Corollary 2. *If* A *is in the center of* B, $\delta : C^G \to H^1(G,A)$ *is a homomorphism, and* $\alpha^c = \alpha + \delta(c)$.

This is obvious.

Now we shall make use of the group $H^2(G,A)$. *A priori*, one would like to define a coboundary: $H^1(G,C) \to H^2(G,A)$. In this form, this is not possible unless A is contained in the center of B (cf. §5.7). However, one does have a partial result, namely the following:

Let $c \in Z^1(G,C)$ be a cocycle for G in C. Since A is abelian, C *acts on* A, and the twisted group ${}_cA$ is well defined. We shall associate to c a cohomology class $\Delta(c) \in H^2(G,{}_cA)$. To do this, we lift c_s to a continuous map $s \mapsto b_s$ of G into B, and we define:

$$a_{s,t} = b_s{}^s b_t b_{st}^{-1} .$$

This 2-cochain is a *cocycle* with values in ${}_cA$. Indeed, if we take into account the way G acts on ${}_cA$, we see that this amounts to the identity:

$$a_{s,t}^{-1} \cdot b_s{}^s a_{t,u} b_s^{-1} \cdot a_{s,tu} \cdot a_{st,u}^{-1} = 1 \ , \quad (s,t,u \in G),$$

i.e.

$$b_{st}{}^s b_t^{-1} b_s^{-1} \cdot b_s{}^s b_t{}^{st} b_u{}^s b_{tu}^{-1} b_s^{-1} \cdot b_s{}^s b_{tu} b_{stu}^{-1} \cdot b_{stu}{}^{st} b_u^{-1} b_{st}^{-1} = 1 \ ,$$

which is true (all the terms cancel out).

On the other hand, if we replace the lift b_s by the lift $a'_s b_s$, the cocycle $a_{s,t}$ is replaced by the cocycle $a'_{s,t} \cdot a_{s,t}$, with

$$a'_{s,t} = (\delta a')_{s,t} = a'_s \cdot b_s{}^s a'_t b_s^{-1} \cdot a'_{st}{}^{-1} \ ;$$

this can be checked by a similar (and simpler) computation. Thus, the equivalence class of the cocycle $a_{s,t}$ is well defined; we denote it $\Delta(c)$.

Proposition 41. *In order that the cohomology class of c belongs to the image of $H^1(G,B)$ in $H^1(G,C)$, it is necessary and sufficient that $\Delta(c)$ vanish.*

This is clearly necessary. Conversely, if $\Delta(c) = 0$, the above shows that we may choose b_s so that $b_s{}^s b_t b_{st}^{-1} = 1$, and b_s is a cocycle for G in B with image equal to c. Whence the proposition.

Corollary. *If $H^2(G, {}_cA) = 0$ for all $c \in Z^1(G,C)$, the map*

$$H^1(G,B) \longrightarrow H^1(G,C)$$

is surjective.

Exercises.

1) Rederive prop. 40 using the exercise in §5.5 and the fact that $E(A)$ is the semi-direct product of $\mathrm{Aut}(A)$ with $H^1(G,A)$.

2) Let c and $c' \in Z^1(G,C)$ be two cohomologous cocycles. Compare $\Delta(c)$ and $\Delta(c')$.

5.7 The case of a central subgroup

We assume now that A is *contained in the center* of B. If $a = (a_s)$ is a cocycle for G in A, and $b = (b_s)$ is a cocycle for G in B, it is easy to see that $a \cdot b = (a_s \cdot b_s)$ is a cocycle for G in B. Moreover, the class of $a \cdot b$ depends only on the classes of a and of b. Hence the abelian group $H^1(G,A)$ *acts on the set* $H^1(G,B)$.

Proposition 42. *Two elements of $H^1(G,B)$ have the same image in $H^1(G,C)$ if and only if they are in the same $H^1(G,A)$-orbit.*

The proof is immediate.

Now let $c \in Z^1(G, C)$. Since C acts trivially on A, the twisted group ${}_cA$ used in §5.6 may be identified with A, and the element $\Delta(c)$ belongs to $H^2(G, A)$. An easy computation (cf. [145], p. 132) shows that $\Delta(c) = \Delta(c')$ if c and c' are cohomologous. This defines a map $\Delta : H^1(G, C) \to H^2(G, A)$. Putting together prop. 38 and 41, we obtain:

Proposition 43. *The sequence*

$$1 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G$$

$$\xrightarrow{\delta} H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) \xrightarrow{\Delta} H^2(G, A)$$

is exact.

As usual, this sequence only gives us information about the kernel of $H^1(G, C) \to H^2(G, A)$, and not on the corresponding equivalence relation. To obtain that, we must twist the groups under consideration. More precisely, observe that C acts on B by automorphisms and that these automorphisms are trivial on A. If $c = (c_s)$ is a cocycle for G in C, we may twist the exact sequence $1 \to A \to B \to C \to 1$ with c, and we obtain the new exact sequence

$$1 \longrightarrow A \longrightarrow {}_cB \longrightarrow {}_cC \longrightarrow 1 \ .$$

This gives a new coboundary operator $\Delta_c : H^1(G, {}_cC) \to H^2(G, A)$. Since we also have a canonical bijection $\tau_c : H^1(G, {}_cC) \to H^1(G, C)$, we can use it to compare Δ and Δ_c. The result is the following:

Proposition 44. *We have $\Delta \circ \tau_c(\gamma') = \Delta_c(\gamma') + \Delta(\gamma)$, where $\gamma \in H^1(G, C)$ denotes the equivalence class of c, and γ' belongs to $H^1(G, {}_cC)$.*

Let c'_s be a cocycle representing γ'. Choose as above a cochain b_s (resp. b'_s) in B (resp. in ${}_cB$) as a lift of c_s (resp. c'_s). We may represent $\Delta(\gamma)$ by the cocycle

$$a_{s,t} = b_s {}^s b_t b_{st}^{-1} \ ,$$

and $\Delta_c(\gamma')$ by the cocycle

$$a'_{s,t} = b'_s \cdot b_s {}^s b'_t b_s^{-1} \cdot {b'_{st}}^{-1} \ .$$

On the other hand $\tau_c(\gamma')$ can be represented by $c'_s c_s$, which we may lift to $b'_s b_s$. Thus we may represent $\Delta \circ \tau_c(\gamma')$ by the cocycle

$$a''_{s,t} = b'_s b_s \cdot {}^s b'_t {}^s b_t \cdot b_{st}^{-1} {b'_{st}}^{-1} \ .$$

Since $a_{s,t}$ is in the center of B, we may write:

$$a'_{s,t} \cdot a_{s,t} = b'_s b_s {}^s b'_t b_s^{-1} a_{s,t} {b'_{st}}^{-1} \ .$$

Replacing $a_{s,t}$ by its value and simplifying, we see that we find $a''_{s,t}$; the proposition follows.

Corollary. *The elements of $H^1(G,C)$ having the same image as γ under Δ correspond bijectively with the elements of the quotient of $H^1(G,{}_cB)$ by the action of $H^1(G,A)$.*

Indeed, the bijection τ_c^{-1} transforms these elements into those of the kernel of

$$\Delta_c : H^1(G,{}_cC) \longrightarrow H^2(G,A) ,$$

and prop. 42 and 43 show that this kernel may be identified with the quotient of $H^1(G,{}_cB)$ by the action of $H^1(G,A)$.

Remarks.

1) Here again it is, in general, false that $H^1(G,{}_cB)$ is in bijective correspondence with $H^1(G,B)$.

2) We leave to the reader the task of stating the criteria for denumerability, finiteness, etc., which follow from the corollary.

Exercise.

Since C^G acts on B by inner automorphisms, it also acts on $H^1(G,B)$. Let us denote this action by

$$(c,\beta) \mapsto c * \beta \quad (c \in C^G,\ \beta \in H^1(G,B)).$$

Show that:

$$c * \beta = \delta(c)^{-1} \cdot \beta ,$$

where $\delta(c)$ is the image of c in $H^1(G,A)$, cf. §5.4, and where the product $\delta(c)^{-1}\cdot\beta$ is relative to the action of $H^1(G,A)$ on $H^1(G,B)$.

5.8 Complements

We leave to the reader the task of treating the following topics:

a) Group extensions

Let H be a closed normal subgroup in G, and let A be a G-group. The group G/H acts on A^H, which means that $H^1(G/H,A^H)$ is well-defined. On the other hand, if $(a_h) \in Z^1(H,A)$ and $s \in G$, we can define the transform $s(a)$ of the cocycle $a = (a_h)$ by the formula:

$$s(a)_h = s(a_{s^{-1}hs}) .$$

By passing to the quotient, the group G acts on $H^1(H,A)$, and one checks that H acts trivially. Thus G/H *acts on* $H^1(H,A)$, just as in the abelian case. We have the exact sequence:

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

and the map $H^1(G/H,A^H) \to H^1(G,A)$ is injective.

b) Induction

Let H be a closed subgroup of G, and let A be an H-group. Let $A^* = M_G^H(A)$ be the group of continuous maps $a^* : G \to A$ such that $a^*({}^h x) = {}^h a^*(x)$ for $h \in H$ and $x \in G$. We let G act on A^* by the formula $({}^g a^*)(x) = a^*(xg)$. We obtain in this way a G-group A^* and one has canonical bijections

$$H^0(G, A^*) = H^0(H, A) \qquad \text{and} \qquad H^1(G, A^*) = H^1(H, A) \ .$$

5.9 A property of groups with cohomological dimension ≤ 1

The following result could have been given in §3.4:

Proposition 45. *Let I be a set of prime numbers, and assume that $\mathrm{cd}_p(G) \leq 1$ for every $p \in I$. Then the group G has the lifting property for the extensions $1 \to P \to E \to W \to 1$, where the order of E is finite, and the order of P is only divisible by prime numbers belonging to I.*

We use induction on the order of P, the case $\mathrm{Card}(P) = 1$ being trivial. Assume therefore $\mathrm{Card}(P) > 1$, and let p be a prime divisor of $\mathrm{Card}(P)$. By hypothesis, we have $p \in I$. Let R be a Sylow p-subgroup in P. There are two cases:

a) R is normal in P. Then it is the only Sylow p-subgroup in P, and it is normal in E. We have the extensions:

$$1 \longrightarrow R \longrightarrow E \longrightarrow E/R \longrightarrow 1$$

$$1 \longrightarrow P/R \longrightarrow E/R \longrightarrow W \longrightarrow 1 \ .$$

Since $\mathrm{Card}(P/R) < \mathrm{Card}(P)$, the induction hypothesis shows that the given homomorphism $f : G \to W$ lifts to $g : G \to E/R$. On the other hand, since R is a p-group, prop. 16 in §3.4 shows that g lifts to $h : G \to E$. We have thus lifted f.

b) R is not normal in P. Let E' be the normalizer of R in E, and let P' be the normalizer of R in P. We have $P' = E' \cap P$. Also, the image of E' in W is equal to all of W. Indeed, if $x \in E$, it is clear that $x R x^{-1}$ is a Sylow p-subgroup of P, and the conjugacy of Sylow subgroups implies the existence of $y \in Pv$ such that $x R x^{-1} = y R y^{-1}$. Thus we have $y^{-1}x \in E'$, which shows that $E = P \cdot E'$, from which our assertion follows. We thus get the extension:

$$1 \longrightarrow P' \longrightarrow E' \longrightarrow W \longrightarrow 1 \ .$$

Since $\mathrm{Card}(P') < \mathrm{Card}(P)$, the induction hypothesis shows that the morphism $f : G \to W$ lifts to $h : G \to E'$, and because E' is a subgroup of E, this finishes the proof.

Corollary 1. *Every extension of G by a profinite group P whose order is not divisible by the primes belonging to I splits.*

The case where P is finite follows directly from the proposition and from lemma 2 in §1.2. The general case is handled by "Zornification", as in §3.4 (see also exerc. 3).

Remark.

The above corollary gives the fact that a group extension of a finite group A by a finite group B splits when the orders of A and of B are prime to each other (cf. Zassenhaus, [189], Chap. IV, §7).

A profinite group G is said to be *projective* (in the category of profinite groups) if it has the lifting property for every extension; this amounts to saying that, for any surjective morphism $f : G' \to G$, where G' is profinite, there exists a morphism $r : G \to G'$ such that $f \circ r = 1$.

Corollary 2. *If G is a profinite group, the following properties are equivalent:*

(i) *G is projective.*

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

(iii) *For any prime number p, the Sylow p-subgroups of G are free pro-p-groups.*

The equivalence (ii) $\Leftrightarrow$ (iii) has already been proved. The implication (i) $\Rightarrow$ (ii) is clear (cf. prop. 16). The implication (ii) $\Rightarrow$ (i) follows from cor. 1, applied to the case where I is the set of all prime numbers.

Examples of projective groups: (a) the completion of a free (discrete) group in the topology induced by subgroups of finite index; (b) a direct product $\prod_p F_p$, where each F_p is a free pro-p-group.

Proposition 46. *With the same hypotheses as in prop. 45, let*

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

be an exact sequence of G-groups. Assume that A is finite, and that each prime divisor of the order of A belongs to I. The canonical map $H^1(G, B) \to H^1(G, C)$ is surjective.

Let (c_s) be a cocycle for G with values in C. If π denotes the homomorphism $B \to C$, let E be the set of pairs (b, s), with $b \in B$, $s \in G$, such that $\pi(b) = c_s$. We put on E the following composition law (cf. exerc. 1 in §5.1):

$$(b, s) \cdot (b', s') = (b \cdot {}^s b', ss') \ .$$

The fact that $c_{ss'} = c_s \cdot {}^s c_{s'}$ shows that $\pi(b \cdot {}^s b') = c_{ss'}$, which means that the above definition is legitimate. One checks that E, with this composition law and the topology induced by that of the product $B \times G$, is a compact group. The obvious morphisms $A \to E$ and $E \to G$, make of E *an extension of G by A*. By cor..1 to prop. 45, this extension splits. Therefore there exists a continuous

section $s \mapsto e_s$ which is a morphism of G into E. If we write $e_s \in E$ in the form (b_s, s), the fact that $s \mapsto e_s$ is a morphism shows that b_s is a cocycle for G in B which is a lift of the given cocycle c_s. The proposition follows.

Corollary. *Let* $1 \to A \to B \to C \to 1$ *be an exact sequence of* G*-groups. If* A *is finite, and if* $\mathrm{cd}(G) \leq 1$, *the canonical map* $H^1(G, B) \to H^1(G, C)$ *is surjective.*

This is the special case where I is the set of all prime numbers.

Exercises.

1) Let $1 \to A \to B \to C \to 1$ be an exact sequence of G-groups, with A a finite abelian group. The method used in the proof of prop. 46 associates to each $c \in Z^1(G, C)$ an extension E_c of G by A. Show that the action of G on A resulting from this extension is that of ${}_cA$, and that the image of E_c in $H^2(G, {}_cA)$ is the element $\Delta(c)$ defined in §5.6.

2) Let A be a finite G-group, with order prime to the order of G. Show that $H^1(G, A) = 0$. [Reduce to the finite case, where the result is known: it is a consequence of the Feit-Thompson theorem which says that groups of odd order are solvable.]

3) Let $1 \to P \to E \to G \to 1$ be an extension of profinite groups, where G and P satisfy the hypotheses of cor. 1 to prop. 45. Let E' be a closed subgroup of E which projects onto G, and which is minimal for this property (cf. §1.2, exerc. 2); let $P' = P \cap E'$. Show that $P' = 1$. [Otherwise, there would exist an open subgroup P'' of P', normal in E', with $P'' \neq P'$. Applying prop. 45 to the extension $1 \to P'/P'' \to E'/P'' \to G \to 1$, one would get a lifting of G into E'/P'', and therefore a closed subgroup E'' of E', projecting onto G, such that $E'' \cap P' = P''$; this would contradict the minimality of E'.] Deduce from this another proof of cor. 1 to prop. 45.

4) (a) Let P be a profinite group. Show the equivalence of the following properties:

(i) P is a projective limit of finite nilpotent groups.

(ii) P is a direct product of pro-p-groups.

(iii) For any prime p, P has only one Sylow p-subgroup.

Such a group is called *pronilpotent.*

(b) Let $f : G \to P$ be a surjective morphism of profinite groups. Assume that P is pronilpotent. Show that there exists a pronilpotent subgroup P' of G such that $f(P') = P$. [Write P as a quotient of a product $F = \prod_p F_p$, where the F_p are free pro-p-groups, and lift $F \to G$ to $F \to G$ by cor. 2 of prop. 45.]

When P and G are finite groups, one recovers a known result, (cf. Huppert [74], III.3.10.)

5) Show that a closed subgroup of a projective group is projective.

Bibliographic remarks for Chapter I

Almost all the results in §§1, 2, 3 and 4 are due to Tate. Tate himself did not publish them; however, some of his results were written out by Lang, then by Douady (cf. [47], [97], [98]). Others (especially the proofs reproduced in §4.5) were communicated directly to me.

Exceptions: §3.5 (dualizing module), and §4.4 (Shafarevich's theorem).

§5 (non-abelian cohomology) is taken from Borel-Serre [18]; it is directly inspired by the nonabelian sheaf cohomology; in this respect, Grothendieck's Kansas report [58] is particularly useful.

Appendix 1. J. Tate – Some duality theorems

From a letter dated 28 March 1963

... You are unnecessarily cautious concerning the dualizing module: no finiteness assumptions are needed. Quite generally, suppose R is a topological ring in which the open two-sided ideals form a fundamental system of neighborhoods of 0. For each such ideal I and each R-module M, let

$$M_I = \mathrm{Hom}_R(R/I, M) = \{x \in M |\ Ix = 0\}.$$

Let $C(R)$ be the category of R-modules M such that $M = \bigcup_{I \text{ open}} M_I$. Let $T : C(R)^0 \to (\mathrm{Ab})$ be an additive contrafunctor which transforms inductive limits into projective limits. Then T *is "sexy", i.e. left exact, if and only if it is representable.* Indeed, in the case where R is discrete, this is well known: The map $M = \mathrm{Hom}_R(R, M) \to \mathrm{Hom}(T(M), T(R))$ gives a functorial homomorphism

$$\alpha_M : T(M) \longrightarrow \mathrm{Hom}_R(M, T(R))$$

which is bijective in case M is free, and consequently is bijective for every M if T is sexy, in view of the fact that M has a free resolution. In the general case, then for each open two-sided ideal I the category $C(R/I)$ is a full subcategory of $C(R)$, and the inclusion functor $C(R/I) \subset C(R)$ is exact and commutes with $\varinjlim$. Therefore, if T is sexy, its restriction to $C(R/I)$ is sexy for every I, and consequently, for $M \in C(R/I)$ we have a functorial isomorphism

$$(*) \qquad T(M) \xrightarrow{\simeq} \mathrm{Hom}_R(M, T(R/I)) \ .$$

Now apply this with $M = R/I_0$, where $I_0 \supset I$, and you see $T(R/I_0) \simeq T(R/I)_{I_0}$. Let $I \to 0$, and you see $T(R/I_0) \simeq E_{I_0}$, where $E = \lim_{I \to 0} T(R/I)$. Going back to the formula $(*)$ with I_0 instead of I, we find now that

$$T(M) \simeq \mathrm{Hom}_R(M, E) \quad \text{for all } M \in C(R/I_0).$$

Finally, for an arbitrary $M \in C(R)$, we get

$$T(M) = \varprojlim T(M_{I_0}) = \varprojlim \mathrm{Hom}_R(M_{I_0}, E) = \mathrm{Hom}_R(M, E) \ .$$

Of course, whether T is sexy or not, we have functorial homomorphisms

$$T(M) \xrightarrow{\alpha_M} \mathrm{Hom}_R(M, E),$$

also whether or not, $T \circ \varinjlim = \varprojlim \circ T$; and the fancy statement is that the following are equivalent:

(i) T is sexy, $T \circ \varinjlim = \varprojlim \circ T$;
(ii) T is half-exact, $(T \circ \varinjlim) \to (\varprojlim \circ T)$ is surjective, and a_M injective for all M;
(iii) a_M is bijective for all M.

* * *

Now for profinite G and any $A \in C_G$ and any closed subgroup $S \subset G$, we put

$$D_r(S, A) = \varinjlim_{V \supset S} H^r(V, A)^* ,$$

the limit taken as the open subgroups V shrink down to S, with respect to the transposes Cor* of the corestriction maps [recall that, if B is an abelian group, B^* denotes $\mathrm{Hom}(B, \mathbf{Q}/\mathbf{Z})$.] Clearly, $A \mapsto D_r(S, A)$ is a connected sequence of contrafunctors: , i.e. an exact $0 \to A' \to A \to A'' \to 0$ gives exact

$$\cdots \longrightarrow D_r(S, A) \longrightarrow D_r(S, A') \longrightarrow D_{r-1}(S, A'') \longrightarrow D_{r-1}(S, A) \longrightarrow \cdots .$$

In particular, we write $D_r(A) = D_r(\{1\}, A)$ and have $D_r(A) \in C_G$ because G/U operates on $H^r(U, A)$ for all normal U.

In particular, put

$$E_r = D_r(\mathbf{Z}) = \varinjlim H^r(G, \mathbf{Z}[G/U])^*$$
$$E'_r = \varinjlim_m D_r(\mathbf{Z}/m\mathbf{Z}) = \varinjlim_{U,m} H^r(G, (\mathbf{Z}/m\mathbf{Z})[G/U])^* .$$

Then, applying the general nonsense above to the rings

$$R = \mathbf{Z}[G] = \varprojlim \mathbf{Z}[G/U] \qquad \text{and} \qquad R' = \widehat{\mathbf{Z}}[G] = \varprojlim (\mathbf{Z}/m\mathbf{Z})[G/U] ,$$

and noting that $C(R) = C_G$, $C(R') = C_G^t$, we get arrows

$$\alpha_M : H^r(G, M)^* \longrightarrow \mathrm{Hom}_G(M, E_r) \quad \text{for } M \in C_G$$
$$\alpha'_M : H^r(G, M)^* \longrightarrow \mathrm{Hom}_G(M, E'_r) \quad \text{for } M \in C_G^t .$$

Moreover α_M (resp. α'_M) is bijective for all $M \in C_G$ (resp. C_G^t) iff α_M (resp. α'_M) is injective for all $M \in C_G$ (resp. C_G^t) iff $\mathrm{scd}\, G \leq r$ (resp. $\mathrm{cd}\, G \leq r$).

Suppose now $\mathrm{cd}(G) \leq r$. Then we have

$$E_{r+1} = D_{r+1}(\mathbf{Z}) = D_r(\mathbf{Q}/\mathbf{Z}) = \varinjlim H^r(U, \mathbf{Q}/\mathbf{Z})^*$$
$$= \varinjlim \mathrm{Hom}_U(\mathbf{Q}/\mathbf{Z}, E'_r) = \bigcup \mathrm{Hom}(\mathbf{Q}/\mathbf{Z}, E'_r)^U .$$

Hence your criterion

$$\mathrm{scd}_p(G) = r + 1 \iff (E'_r)^U \text{ contains a subgroup isomorphic to } \mathbf{Q}_p/\mathbf{Z}_p.$$

Example: $G = \widehat{\mathbf{Z}}$, $E'_1 = \mathbf{Q}/\mathbf{Z}$, hence $E_2 = \mathrm{Hom}(\mathbf{Q}/\mathbf{Z}, \mathbf{Q}/\mathbf{Z}) = \widehat{\mathbf{Z}}$. Thus for any M in C_G we have $H^2(G, M)^* = \mathrm{Hom}_G(M, \widehat{\mathbf{Z}})$.

If $\mathrm{cd}(G) = \mathrm{scd}(G) = r$, then of course E_r' is the torsion submodule of E_r. Example: if $G = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, then by class field theory we have $E_2 = \varinjlim \widehat{K}^*$, the limit over all finite extensions K of $\mathbf{Q}_p$ of the compactifications of the multiplicative groups, and $E_2' = \mu$ is the torsion subgroup.

* * *

But what about a *general duality theorem*? The best I can do so far is the following crazy theory.

Definition. For $A \in C_G$, we say $\mathrm{cd}(G, A) \leq n$ iff $H^r(S, A) = 0$ for all $r > n$ and all closed subgroups S of G.

Lemma 1. *The following statements are equivalent for* $A \in C_G$:

(i) $\mathrm{cd}(G, A) = 0$.

(ii) *For every open normal subgroup* $U \subset G$, A^U *is a cohomologically trivial* G/U*-module.*

(iii) *For every open normal subgroup* U, *and every* $V \supset U$, *the trace map* $N : H_0(V/U, A^U) \to H^0(V/U, A^U)$ *is bijective.*

The equivalence of (ii) and (iii) results from Theorem 8, p. 152, of *Corps Locaux*, the two successive values of q being $-1, 0$. If (i) holds, the spectral sequence $H^p(V/U, H^q(U, A)) \Rightarrow H(V, A)$ degenerates, but the limit degenerates, too, so $H^p(V/U, A^U) = 0$ for $p > 0$, i.e. (ii) is true. Conversely, from (ii) we conclude, for $p > 0$, $H^p(V, A) = \varinjlim H^p(V/U, A^U) = 0$ for every open V, hence $H^p(S, A) = \varinjlim_{V \supset S} H^p(V, A) = 0$ for all closed S, i.e., (i) holds, QED.

Let $A \in C_G$ and let

$$0 \longrightarrow A \longrightarrow X^0 \longrightarrow X^1 \longrightarrow \cdots$$

be a canonical resolution of A, say by homogeneous cochains (not necessarily "equivariant"), or, if you wish by repeating the standard dimension shift $0 \to A \to \mathrm{Map}\,(G, A)$. Let Z^n be the group of cocycles in X^n, so that we have the exact sequence

$$(1) \qquad 0 \longrightarrow A \longrightarrow X^0 \longrightarrow X^1 \longrightarrow \cdots \longrightarrow X^{n-1} \longrightarrow Z^n \longrightarrow 0\ .$$

Lemma 2. $\mathrm{cd}(G, A) \leq n \iff \mathrm{cd}(G, Z^n) = 0$.

Because, for $r > 0$, we have

$$H^r(S, Z^n) = H^{r+1}(S, Z^{n-1}) = \cdots = H^{r+n}(S, A)\ .$$

Theorem 1. *If* $\mathrm{cd}(G, A) \leq n$, *then there is a spectral sequence of homological type*

$$(2) \qquad E^2_{pq} = H_p(G/U, H^{n-q}(U, A)) \Longrightarrow H_{p+q} = H^{n-(p+q)}(G, A)\ .$$

This is functorial in U, when you look at the maps, for $V \subset U$,

$$H_p(G/V, H^{n-q}(V, A)) \longrightarrow H_p(G/U, H^{n-q}(U, A))$$

which come from $G/V \to G/U$ and Cor : $H^{n-q}(V, A) \to H^{n-q}(U, A)$.

Corollary. *If* $\mathrm{cd}(G, A) \leq n$, *then for every normal subgroup* $N \subset G$ *there is a spectral sequence of cohomological type*

$$E_2^{p,q} = H^p(G/N, D_{n-q}(N, A)) \Longrightarrow H^{n-(p+q)}(G, A)^* \ . \tag{3}$$

In particular, for $N = \{1\}$:

$$H^p(G, D_{n-q}(A)) \Longrightarrow H^{n-(p+q)}(G, A)^* \ . \tag{4}$$

Indeed, you get (3) from (2) if you apply *, use the duality for finite group cohomology, i.e. $H_p(G/U, B)^* \simeq H^p(G/U, B^*)$, and then take $\varinjlim$ over $U \supset N$.

The proof of (2) is not hard. You consider (1) and the resulting complex:

$$0 \longrightarrow (X^0)^U \longrightarrow (X^1)^U \longrightarrow \cdots \longrightarrow (X^{n-1})^U \longrightarrow (Z^n)^U \longrightarrow 0 \tag{5}$$

which we rewrite as

$$0 \longrightarrow Y_n \longrightarrow Y_{n-1} \longrightarrow \cdots \longrightarrow Y_1 \longrightarrow Y_0 \longrightarrow 0 \ , \tag{6}$$

so that we have "homology". In fact, $H_q(Y_\cdot) = H^{n-q}(U, A)$ for all q. Now apply the standard G/U *chain* functor to Y, getting a double complex $C_{\cdot\cdot}$ of homological type:

$$C_{p,q} = C_p(G/U, Y_q) \ .$$

Taking homology in the q-direction we get $C_p(G/U, H^{n-q}(U, A))$ because C_p is an exact functor. Following this with homology in the p-direction gives $E^2_{pq} = H_p(G/U, H^{n-q}(U, A))$ as desired. The other way around, taking first the p-direction homology gives $H_p(G/U, Y_q)$. This vanishes for $p > 0$ by lemmas 1 and 2, and by the same lemmas we have for, $p = 0$,

$$H_0(G/U, Y_q) = H^0(G/U, Y_q) = Y_q^{G/U} = ((X^{n-q})^U)^{G/U} = (X^{n-q})^G,$$

a complex whose (co)homology is $H^{n-q}(G, A)$ as contended (replace X by Z for $q = 0$), QED.

The most obvious applications are:

Theorem 2. *Let* G *be profinite and* $n \geq 0$. *The following conditions are equivalent*:

(i) $\mathrm{scd}(G) = n$, $E_n = D_n(\mathbf{Z})$ *is divisible, and* $D_q(\mathbf{Z}) = 0$ *for* $q < n$.
(ii) $\mathrm{scd}(G) = n$, $D_q(A) = 0$ *for* $q < n$ *for all* A *in* C_G *of finite type over* $\mathbf{Z}$.
(iii) $H^r(G, \mathrm{Hom}(A, E_n)) \simeq H^{n-r}(G, A)^*$ *for all* A *in* C_G *of finite type over* $\mathbf{Z}$ *and all* r.

Similarly,

Theorem 3. *Equivalent are*:

(i) $\mathrm{cd}(G) = n$, $D_q(\mathbf{Z}/p\mathbf{Z}) = 0$ *for all* $q < n$ *and all primes* p.
(ii) $\mathrm{cd}(G) = n$, $D_q(A) = 0$ *for all* $q < n$ *and all* $A \in C_G^f$.
(iii) $H^r(G, \mathrm{Hom}(A, E_n')) = H^{n-r}(G, A)^*$ *for all* r *and for all* $A \in C_G^f$.

Notice that $D_1(\mathbf{Z}) = 0$ always, and $D_0(\mathbf{Z}) = 0$ if $p^\infty | (G : 1)$ for all p. Hence, if $\mathrm{scd}(G) = 2$, the G satisfies the conditions of Theorem 2 (for $n = 2$) if and only if E_2 is divisible. That is the case, for example, if $G = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. But not for $G = \mathrm{Gal}(\overline{k}/k)$, for k a totally imaginary number field. Tant pis!

...
J. Tate

Appendix 2.
The Golod-Shafarevich inequality

We prove the following statement (cf. §4.4):

Theorem 1. *If G is a p-group $\neq 1$, then $r > d^2/4$, with*

$$d = \dim H^1(G, \mathbf{Z}/p\mathbf{Z}) \quad \textit{and} \quad r = \dim H^2(G, \mathbf{Z}/p\mathbf{Z}) \ .$$

We shall see that this theorem is a special case of a general result on local algebras.

§ 1. The statement

Let R be a finite-dimensional algebra over a field k, and let I be a two-sided ideal of R. We assume the following:

(a) $R = k \oplus I$.

(b) I is nilpotent.

These hypotheses imply that R is a *local ring* (not necessarily a commutative one) with radical I and residue field k, cf. Bourbaki AC II, §3.1.

If P is a finitely generated left R-module, the $\mathrm{Tor}_i^R(P, k)$ are finite-dimensional k-vector spaces. We set:

$$t_i(P) = \dim_k \mathrm{Tor}_i^R(P, k) \ .$$

Let $m = t_0(P) = \dim_k P/I{\cdot}P$. If $\bar{x}_1, \ldots, \bar{x}_m$ is a k-basis of $P/I{\cdot}P$, let $x_1, \ldots, x_m$ be preimages in P of $\bar{x}_1, \ldots, \bar{x}_m$. By Nakayama's lemma, the x_i generate P. Therefore they define a surjective morphism

$$x : R^m \longrightarrow P \ ,$$

and we have $\mathrm{Ker}(x) \subset I.R^m$.

This can be applied to $P = k$, with $m = 1$, $x_1 = 1$ and $\mathrm{Ker}(x) = I$. We have:

$$\begin{aligned} t_0(k) &= 1 \ , \\ t_1(k) &= \dim_k \mathrm{Tor}_1^R(k, k) = \dim_k I/I^2 \ , \\ t_2(k) &= \dim_k \mathrm{Tor}_2^R(k, k) = \dim_k \mathrm{Tor}_1^R(I, k) \ . \end{aligned}$$

We shall prove:

Theorem 1'. *If $I \neq 0$, then $t_2(k) > t_1(k)^2/4$.*

This statement *implies th.* 1. Indeed, if we take $k = \mathbf{F}_p$ and $R = \mathbf{F}_p[G]$, the algebra R is a local algebra whose radical I is the augmentation ideal of R (this follows, for example, from prop. 20 in §4.1). Also, we have $\mathrm{Tor}_i^R(k,k) = H_i(G, \mathbf{Z}/p\mathbf{Z})$, and thus

$$t_i(k) = \dim H_i(G, \mathbf{Z}/p\mathbf{Z}) = \dim H^i(G, \mathbf{Z}/p\mathbf{Z}) ,$$

since $H_i(G, \mathbf{Z}/p\mathbf{Z})$ and $H^i(G, \mathbf{Z}/p\mathbf{Z})$ are dual to each other. From this follows th. 1.

§ 2. Proof

Let us put $d = t_1(k)$ and $r = t_2(k)$. We have:

$$d = t_1(k) = t_0(I) = \dim_k I/I^2 \quad \text{and} \quad r = t_2(k) = t_1(I) .$$

The hypothesis $I \neq 0$ is equivalent to $d \geq 1$. From what was said above, there exists an exact sequence

$$0 \longrightarrow J \longrightarrow R^d \longrightarrow I \longrightarrow 0 ,$$

with $J \subset I.R^d$. Since $r = t_1(I) = t_0(J)$, we see that J is isomorphic to a quotient of R^r. Therefore we have an exact sequence

$$R^r \xrightarrow{\varepsilon} R^d \longrightarrow I \longrightarrow 0 ,$$

with $\mathrm{Im}(\varepsilon) = J$ (the start of a *minimal resolution* of I, cf., e.g. ,[24], [66]).

By tensoring this exact sequence with R/I^n, where n is an integer > 0, we obtain the exact sequence

$$(R/I^n)^r \longrightarrow (R/I^n)^d \longrightarrow I/I^{n+1} \longrightarrow 0 .$$

But the fact that the image of ε is contained in $I.R^d$ shows that the homomorphism $(R/I^n)^r \to (R/I^n)^d$ factors through $(R/I^{n-1})^r$. In this way we get an exact sequence

$$(R/I^{n-1})^r \longrightarrow (R/I^n)^d \longrightarrow I/I^{n+1} \longrightarrow 0 .$$

From this we get the inequality

$$d \cdot \dim_k R/I^n \leq r \cdot \dim_k R/I^{n-1} + \dim_k I/I^{n+1} ,$$

which holds for all $n \geq 1$. If we put $a(n) = \dim_k R/I^n$, this can be written:

$$(*_n) \qquad d \cdot a(n) \leq r \cdot a(n-1) + a(n+1) - 1 \qquad (n \geq 1).$$

A first consequence of $(*_n)$ is the inequality $r \geq 1$. Indeed, if $r = 0$, we have $d \cdot a(n) \leq a(n+1) - 1$, hence $a(n) < a(n+1)$, which is impossible since $a(n) = \dim_k R/I^n$ is constant for large n (I being nilpotent).

Suppose that $d^2 - 4r$ is ≥ 0. Let us factor the polynomial $X^2 - dX + r$ into $(X - \lambda)(X - \mu)$, where λ and μ are reals > 0, with $\mu \geq \lambda$ (whence $\mu \geq 1$, since $\lambda\mu = r$). Set

$$A(n) = a(n) - \lambda a(n-1) \ .$$

We have

$$\begin{aligned} A(n+1) - \mu A(n) &= a(n+1) - (\lambda + \mu)a(n) + \lambda\mu a(n-1) \\ &= a(n+1) - d \cdot a(n) + r \cdot a(n-1) \ , \end{aligned}$$

which allows us to write $(*_n)$ in the form:

$$(*'_n) \qquad A(n+1) - \mu A(n) \geq 1 \qquad \text{for } n \geq 1.$$

But we have $a(0) = 0$, $a(1) = 1$, $a(2) = d + 1$, whence $A(0) = 0$, $A(1) = 1$, $A(2) = d + 1 - \lambda = 1 + \mu$. We therefore deduce from $(*'_n)$, by induction on n, that

$$A(n) \geq 1 + \mu + \cdots + \mu^{n-1} \qquad (n \geq 1).$$

Because $\mu \geq 1$, this implies $A(n) \geq n$. But that is absurd since $a(n)$, and therefore also $A(n)$, is constant for large n. Therefore we do have $d^2 - 4r < 0$, QED.

Exercise.

Let G be a pro-p-group. Put $d = \dim H^1(G, \mathbf{Z}/p\mathbf{Z})$, $r = \dim H^2(G, \mathbf{Z}/p\mathbf{Z})$ and assume that d and r are finite (so that G is "finitely presented").

(a) Let R be the projective limit of the algebras $\mathbf{F}_p[G/U]$, where U runs over the set of open normal subgroups of G. Prove that R is a local $\mathbf{F}_p$-algebra, with radical $I = \mathrm{Ker} : R \to \mathbf{F}_p$.

(b) Prove that I^n has finite codimension in R. Set $a(n) = \dim R/I^n$. Prove that $\dim I/I^2 = d$, and that, if one writes I in the form R^d/J, then $\dim J/IJ = r$, cf. Brumer [24] and Haran [66]. Deduce from this that the inequality $(*_n)$ still holds (same proof).

(c) Assume $d > 2$ and $r \leq d^2/4$. Deduce from $(*_n)$ that there exists a constant $c > 1$ such that $a(n) > c^n$ for n sufficiently large. Using results of Lazard ([102], A.3.11), this implies that G *is not a p-adic analytic group.*

Chapter II

Galois cohomology, the commutative case

§1. Generalities

1.1 Galois cohomology

Let k be a field, and let K be a Galois extension of k. The Galois group $\mathrm{Gal}(K/k)$ of the extension K/k is a profinite group (cf. Chap. I, §1.1), and one can apply to it the methods and results of Chapter I; in particular, if $\mathrm{Gal}(K/k)$ acts on a discrete group $A(K)$, the $H^q(\mathrm{Gal}(K,k), A(K))$ are well-defined (if $A(K)$ is not commutative, we assume that $q = 0, 1$).

In fact, it is often more convenient not to work with a fixed extension K/k. The situation is the following:

One has a *ground field* k, and a *functor* $K \mapsto A(K)$ defined on the category of algebraic separable extensions of k, with values in the category of groups (resp. abelian groups), and this functor verifies the following axioms:

(1) $A(K) = \varinjlim A(K_i)$, for K_i running over the set of sub-extensions of K of finite type over k.

(2) If $K \to K'$ is an injection, the corresponding morphism $A(K) \to A(K')$ is also an injection.

(3) If K'/K is a Galois extension, one has $A(K) = H^0(\mathrm{Gal}(K'/K), A(K'))$.

[This makes sense, because the group $\mathrm{Gal}(K'/K)$ acts — functorially — on $A(K')$. Moreover, axiom (1) implies that this action is continuous.]

Remarks.

1) If k_s denotes a separable closure of k, the group $A(k_s)$ is well-defined, and it is a $\mathrm{Gal}(k_s/k)$-group. To know it *is the same as* knowing the functor A (up to an isomorphism of functors).

2) It is often the case that the functor A can be defined for *all extensions of* k (not necessarily algebraic nor separable), and in such a way as to verify (1), (2), and (3). The most important example is that of "group schemes": if A is a group scheme over k, locally of finite type, the points of A with values in an extension K/k form a group $A(K)$ which depends functorially on K, and this functor verifies the axioms (1), (2), and (3) [axiom (1) follows from A being locally of finite type]. This applies in particular to "algebraic groups", that is, to group schemes of finite type over k.

Let A be a functor verifying the above axioms. If K'/K is a Galois extension, the $H^q(\mathrm{Gal}(K'/K), A(K'))$ are defined (if A is not commutative, we consider only $q = 0, 1$). We use the notation $H^q(K'/K, A)$.

Let K_1'/K_1 and K_2'/K_2 be two Galois extensions, with Galois groups G_1 and G_2. Assume we are given an injection $K_1 \xrightarrow{i} K_2$. Let us suppose that there exists an injection $K_1' \xrightarrow{j} K_2'$ which extends the inclusion i. Using j, we get a homomorphism $G_2 \to G_1$ and a morphism $A(K_1') \to A(K_2')$; these two maps are compatible, and define maps

$$H^q(G_1, A(K_1')) \longrightarrow H^q(G_2, A(K_2'));$$

these maps *do not depend on the choice of* j (cf. [145], p. 164). Thus we have maps

$$H^q(K_1'/K_1, A) \longrightarrow H^q(K_2'/K_2, A)$$

which depend only on i (and on *the existence* of j).

In particular, we see that two separable closures of k define cohomology groups $H^q(k_s/k, A)$ which correspond bijectively and canonically to each other. This allows us to drop the symbol k_s and to write simply $H^q(k, A)$. The $H^q(k, A)$ depend functorially on k.

1.2 First examples

Let $\mathbf{G}_a$ (resp. $\mathbf{G}_m$) be the additive (resp. multiplicative) group, defined by the relation $\mathbf{G}_a(K) = K$ (resp. $\mathbf{G}_m(K) = K^*$). We have (cf. [145], p. 158):

Proposition 1. *For every Galois extension K/k, we have $H^1(K/k, \mathbf{G}_m) = 0$ and $H^q(K/k, \mathbf{G}_a) = 0$ $(q \geq 1)$.*

In fact, when K/k is *finite*, the modified cohomology groups $\widehat{H}^q(K/k, \mathbf{G}_a)$ are zero for all $q \in \mathbf{Z}$.

Remark.

The groups $H^q(K/k, \mathbf{G}_m)$ are not in general zero for $q \geq 2$. Recall that the group $H^2(K/k, \mathbf{G}_m)$ may be identified with the part of the *Brauer group* $\mathrm{Br}(k)$ which is split by K; in particular, $H^2(k, \mathbf{G}_m) = \mathrm{Br}(k)$ (cf. [145], Chap. X).

Corollary. *Let n be an integer ≥ 1, prime to the characteristic of k. Let μ_n be the group of n-th roots of unity* (in k_s). *We have*:

$$H^1(k, \mu_n) = k^*/k^{*n}.$$

We have an exact sequence:

$$1 \longrightarrow \mu_n \longrightarrow \mathbf{G}_m \xrightarrow{n} \mathbf{G}_m \longrightarrow 1\ ,$$

where n denotes the endomorphism $x \mapsto x^n$. From this follows the cohomology exact sequence:

$$k^* \xrightarrow{n} k^* \longrightarrow H^1(k, \mu_n) \longrightarrow H^1(k, \mathbf{G}_m).$$

The corollary follows since $H^1(k, \mathbf{G}_m) = 0$, by prop. 1.

Remarks.

1) The same argument shows that $H^2(k, \mu_n)$ may be identified with $\mathrm{Br}_n(k)$, the kernel of multiplication by n in $\mathrm{Br}(k)$.

2) If μ_n is contained in k^*, one may identify μ_n with $\mathbf{Z}/n\mathbf{Z}$ by choosing a primitive n-th root of unity. The corollary above thus gives an isomorphism between the groups:

$$k^*/k^{*n} \quad \text{and} \quad \mathrm{Hom}(G_k, \mathbf{Z}/n\mathbf{Z}) = H^1(k, \mathbf{Z}/n\mathbf{Z}).$$

We recover the classical "Kummer theory" (cf. Bourbaki A.V. §11.8).

§2. Criteria for cohomological dimension

In the following sections, we denote by G_k the Galois group of k_s/k, where k_s is a separable closure of k. This group is determined up to a non-unique isomorphism.

If p is a prime number, we denote by $G_k(p)$ the largest quotient of G_k which is a pro-p-group; the group $G_k(p)$ is the Galois group of the extension $k_s(p)/k$; this extension is called the *maximal p-extension of k*. We shall give some criteria allowing the computation of the cohomological dimension of G_k and of $G_k(p)$ (cf. Chap. I, §3).

2.1 An auxiliary result

Proposition 2. *Let G be a profinite group, and let $G(p) = G/N$ be the largest quotient of G which is a pro-p-group. Assume that $\mathrm{cd}_p(N) \leq 1$. The canonical maps*

$$H^q(G(p), \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^q(G, \mathbf{Z}/p\mathbf{Z})$$

are isomorphisms. In particular, $\mathrm{cd}(G(p)) \leq \mathrm{cd}_p(G)$.

Let N/M be the largest quotient of N which is a pro-p-group. It is clear that M is normal in G, and that G/M is a pro-p-group. In view of the definition of $G(p)$, this implies $M = N$. Thus, every morphism of N into a pro-p-group is trivial. In particular, we have $H^1(N, \mathbf{Z}/p\mathbf{Z}) = 0$. Also, since $\mathrm{cd}_p(N) \leq 1$, we have $H^i(N, \mathbf{Z}/p\mathbf{Z}) = 0$ for $i \geq 2$. It follows therefore from the spectral sequence of group extensions that the homomorphism

$$H^q(G/N, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^q(G, \mathbf{Z}/p\mathbf{Z})$$

is an isomorphism for all $q \geq 0$. The equality $\mathrm{cd}(G/N) \leq \mathrm{cd}_p(G)$ follows from this, thanks to prop. 21 in Chapter I.

Exercise.

With the same hypotheses as in prop. 2, let A be a p-primary torsion $G(p)$-module. Show that the canonical map of $H^q(G(p), A)$ into $H^q(G, A)$ is an isomorphism for every $q \geq 0$.

2.2 Case when p is equal to the characteristic

Proposition 3. *If k is a field of characteristic p, we have* $\mathrm{cd}_p(G_k) \leq 1$ *and* $\mathrm{cd}(G_k(p)) \leq 1$.

Put $x^p - x = f(x)$. The map f is additive, and gives the exact sequence:

$$0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow \mathbf{G}_a \xrightarrow{f} \mathbf{G}_a \longrightarrow 0 .$$

Indeed, this means (by definition!) that the sequence of abelian groups

$$0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow k_s \xrightarrow{f} k_s \longrightarrow 0$$

is exact, which is easy to see. By passing to cohomology, we get the exact sequence:

$$H^1(k, \mathbf{G}_a) \longrightarrow H^2(k, \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^2(k, \mathbf{G}_a).$$

From proposition 1, we deduce that $H^2(k, \mathbf{Z}/p\mathbf{Z}) = 0$, i.e. $H^2(G_k, \mathbf{Z}/p\mathbf{Z}) = 0$. This result may also be applied to the closed subgroups of G_k (since these are Galois groups), and in particular to its Sylow p-subgroups. If H denotes one of these, we then have $\mathrm{cd}(H) \leq 1$ (cf. Chap. I, prop. 21), whence $\mathrm{cd}_p(k) \leq 1$ (Chap. I, cor. 1 to prop. 14). If N is the kernel of $G_k \to G_k(p)$, the preceding also applies to N and shows that $\mathrm{cd}_p(N) \leq 1$. Proposition 2 allows us to conclude that $\mathrm{cd}(G_k(p)) \leq \mathrm{cd}_p(G_k) \leq 1$, QED.

Corollary 1. *The group $G_k(p)$ is a free pro-p-group.*

This follows from Chap. I, cor. 2 to prop. 24.

[Because $H^1(G_k(p))$ can be identified with $k/f(k)$, we can even compute the *rank* of $G_k(p)$.]

Corollary 2. (Albert-Hochschild) *If k' is a purely inseparable extension of k, the canonical map* $\mathrm{Br}(k) \to \mathrm{Br}(k')$ *is surjective.*

Let k'_s be a separable closure of k' containing k_s. Since k'/k is purely inseparable, we can identify G_k with the Galois group of k'_s/k'. We have:

$$\mathrm{Br}(k) = H^2(G_k, k_s^*) , \qquad \mathrm{Br}(k') = H^2(G_k, {k'_s}^*) .$$

Moreover, for each $x \in k'_s$, there exists a power q of p such that $x^q \in k_s$; in other words, the group ${k'_s}^*/k_s^*$ is a p-primary torsion group. Since $\mathrm{cd}_p(G_k) \leq 1$, we therefore have $H^2(G_k, {k'_s}^*/k_s^*) = 0$, and the cohomology exact sequence shows that $H^2(G_k, k_s^*) \to H^2(G_k, {k'_s}^*)$ is surjective, QED.

Remarks.

1) When k' is a purely inseparable extension of k of height 1, the kernel of $\mathrm{Br}(k) \to \mathrm{Br}(k')$ can be computed with the help of the cohomology of the p-Lie algebra of derivations of k'/k, cf. G.P. Hochschild, [70], [71].

2) Let $\mathrm{Br}_p(k)$ be the kernel of multiplication by p in $\mathrm{Br}(k)$. One may describe $\mathrm{Br}_p(k)$ using *differential forms* as follows:

Let $\Omega^1_{\mathbf{Z}}(k)$ be the k-vector space of differential 1-forms $\sum x_i\,dy_i$ on k, and let $H^2_p(k)$ be the quotient of $\Omega^1_{\mathbf{Z}}(k)$ by the subgroup generated by the exact differentials dz ($z \in k$), and by the $(x^p - x)dy/y$ ($x \in k$, $y \in k^*$), cf. Kato [81]. There exists a *unique isomorphism* $H^2_p(k) \to \mathrm{Br}_p(k)$ which associates to the differential form $x\,dy/y$ the class $[x, y)$ of the simple central algebra defined by the generators X, Y, related by:

$$X^p - X = x\ , \quad Y^p = y\ , \quad YXY^{-1} = X + 1\ ,$$

cf. [145], Chap. XIV, §5.

Exercise.

Let $x, y \in k$. Define an element $[x, y]$ of $\mathrm{Br}_p(k)$ by:

$$[x, y] = [xy, y) \quad \text{if} \quad y \neq 0\ , \qquad \text{and} \qquad [x, y] = 0 \quad \text{if} \quad y = 0\ ,$$

(cf. Remark 2). Prove that $[x, y]$ is the class in $\mathrm{Br}(k)$ of the simple central algebra of rank p^2 defined by two generators X, Y and the relations

$$X^p = x\ , \quad Y^p = y\ , \quad XY - YX = -1\ .$$

Prove that $[x, y]$ is a biadditive and alternating function of the pair (x, y).

2.3 Case when p differs from the characteristic

Proposition 4. *Let k be a field with characteristic $\neq p$, and let n be an integer ≥ 1. The following conditions are equivalent:*

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

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

(iii) *Same assertion as in* (ii), *but restricted to extensions K/k which are separable, finite, and of degree prime to p.*

[Recall that, if A is a torsion abelian group, $A(p)$ denotes the p-primary component of A.]

Let μ_p be the group of p-th roots of unity; it is contained in k_s. We have the exact sequence:

$$1 \longrightarrow \mu_p \longrightarrow \mathbf{G}_m \xrightarrow{p} \mathbf{G}_m \longrightarrow 1\ ,$$

cf. §1.2. The cohomology exact sequence shows that condition (ii) amounts to saying that $H^{n+1}(K, \mu_p) = 0$ for all K; there is an analogous translation for (iii).

Assume now that $\mathrm{cd}_p(G_k) \leq n$. Since G_K is isomorphic to a closed subgroup of G_k, we also have $\mathrm{cd}_p(G_K) \leq n$, hence $H^{n+1}(K, \mu_p) = 0$. Thus (i) $\Rightarrow$ (ii). The implication (ii) $\Rightarrow$ (iii) is trivial. Now assume (iii) holds. Let H be a Sylow p-subgroup in G_k, and let K/k be the corresponding extension. Then:

$$K = \varinjlim K_i\ ,$$

where the K_i are finite separable extensions of k, with degrees prime to p. By (iii), we have $H^{n+1}(K_i, \mu_p) = 0$ for all i, hence $H^{n+1}(K, \mu_p) = 0$, i.e. $H^{n+1}(H, \mu_p) = 0$.

But H is a pro-p-group, and so it acts trivially on $\mathbf{Z}/p\mathbf{Z}$; thus we may identify μ_p and $\mathbf{Z}/p\mathbf{Z}$, and prop. 21 of Chapter I shows that $\mathrm{cd}(H) \leq n$, from which condition (i) follows, QED.

§3. Fields of dimension ≤ 1

3.1 Definition

Proposition 5. *Let k be a field. The following properties are equivalent:*

(i) *We have* $\mathrm{cd}(G_k) \leq 1$. *If, moreover, k has characteristic $p \neq 0$, then* $\mathrm{Br}(K)(p) = 0$, *for every algebraic extension K/k.*

(ii) *We have* $\mathrm{Br}(K) = 0$ *for every algebraic extension K/k.*

(iii) *If L/K is any finite Galois extension, with K algebraic over k, the* $\mathrm{Gal}(L/K)$*-module L^* is cohomologically trivial* ([145], Chap. IX, § 3).

(iv) *Under the assumptions of* (iii), *the norm $N_{L/K} : L^* \to K^*$ is surjective.*

(i) bis, (ii) bis, (iii) bis, (iv) bis: *same assertions as* (i), ..., (iv) *but restricted to extensions K/k which are finite and separable over k.*

The equivalences (i) $\Leftrightarrow$ (i) bis, (ii) $\Leftrightarrow$ (ii) bis follow from cor. 2 to prop. 3. The equivalence (i) $\Leftrightarrow$ (ii) follows from prop. 3 and 4. The equivalences (ii) bis $\Leftrightarrow$ (iii) bis $\Leftrightarrow$ (iv) bis are proved in [145], p. 169. Moreover, if k satisfies (ii), every algebraic extension K/k satisfies (ii), therefore also (ii) bis and (iii) bis, which means that k satisfies (iii). Since (iii) $\Rightarrow$ (iii) bis trivially, we see that (ii) $\Rightarrow$ (iii), and the same argument shows that (ii) $\Rightarrow$ (iv), QED.

Remark.

The condition $\mathrm{Br}(k) = 0$ is not enough to imply (i), ..., (iv), cf. exerc. 1.

Definition. A field k is said to be of dimension ≤ 1 if it satisfies the equivalent conditions of prop. 5.

We then write $\dim(k) \leq 1$.

Proposition 6. (a) *Every algebraic extension of a field of dimension* ≤ 1 *is also of dimension* ≤ 1.

(b) *Let k be a perfect field. In order that* $\dim(k) \leq 1$, *it is necessary and sufficient that* $\mathrm{cd}(G_k) \leq 1$.

Assertion (a) is trivial. For (b), notice that, if k is perfect, the map $x \mapsto x^p$ is a bijection of k_s^* onto itself; it follows from this that the p-component of the $H^q(k, \mathbf{G}_m)$ vanishes, and in particular $\mathrm{Br}(k)(p)$. Since this may be applied to any algebraic extension K/k, we see that condition (i) in prop. 5 reduces to $\mathrm{cd}(G_k) \leq 1$, QED.

Proposition 7. *Let k be a field of dimension ≤ 1, and let p be a prime. Then* $\mathrm{cd}(G_k(p)) \leq 1$.

Put $G_k(p) = G_k/N$. Since $\mathrm{cd}(G_k) \leq 1$, we have $\mathrm{cd}(N) \leq 1$, and prop. 2 shows that $\mathrm{cd}(G_k/N) \leq \mathrm{cd}_p(G_k)$, from which prop. 7 follows.

Exercises.

1) (M. Auslander) Let k_0 be a field of characteristic 0 with the following properties: k_0 is not algebraically closed; k_0 has no nontrivial abelian extension; $\dim(k_0) \leq 1$. (Example of such a field: the compositum of all the finite solvable Galois extensions of $\mathbf{Q}$.) Let $k = k_0((T))$. Prove that $\mathrm{Br}(k) = 0$ and that k is not of dimension ≤ 1.

2) In characteristic $p > 0$, show that there exists a field k of dimension ≤ 1 such that $[k : k^p] = p^r$, where r is a given integer ≥ 0 (or $+\infty$). [Take for k a separable closure of $\mathbf{F}_p(T_1, \ldots, T_r)$.] If $r \geq 2$, deduce that there exists a finite purely inseparable extension K/k such that $N_{K/k} : K^* \to k^*$ is not surjective. [This shows that the separability hypotheses in prop. 5 cannot be suppressed.]

3.2 Relation with the property (C_1)

The (C_1) property is:

(C_1). *Every equation $f(x_1, \ldots, x_n) = 0$, where f is a homogeneous polynomial of degree $d \geq 1$, with coefficients in k, has a nontrivial solution in k^n if $n > d$.*

We shall see examples of such fields in §3.3.

Proposition 8. *Let k be a field satisfying* (C_1).

(a) *Every algebraic extension k' of k satisfies* (C_1).

(b) *If L/K is a finite extension, with K algebraic over k, then $N_{L/K}(L^*) = K^*$.*

To prove (a), we can assume k' finite over k. Let $F(x)$ be a homogeneous polynomial, of degree d, in n variables, and with coefficients in k'. Set $f(x) = N_{k'/k}F(x)$; by choosing a basis $e_1, \ldots, e_m$ for k'/k, and expressing the components of x with respect to this basis, we see that f may be identified with a homogeneous polynomial, of degree dm, in nm variables, and with coefficients in k. If $d < n$, we have $dm < nm$, and this polynomial has a nontrivial zero x. That means that $N_{k'/k}F(x) = 0$, whence $F(x) = 0$.

Now let us put ourselves under the hypotheses of (b), and let $a \in K^*$. If $d = [L : K]$, consider the equation

$$N(x) = a \cdot x_0^d \ , \quad \text{with } x \in L,\ x_0 \in K.$$

This is an equation of degree d, in $d + 1$ unknowns. Since, by (a), the field K satisfies (C_1), this equation has a nontrivial solution (x, x_0). If x_0 were to vanish, one would have $N(x) = 0$ whence $x = 0$, contrary to the hypothesis. Therefore $x_0 \neq 0$, and $N(x/x_0) = a$, which proves the surjectivity of the norm.

Corollary. *If k satisfies (C_1), we have $\dim(k) \leq 1$, and, if k is of characteristic $p > 0$, $[k : k^p]$ equals 1 or p.*

By the above proposition, the field k satisfies condition (iv) of prop. 5. Therefore we have $\dim(k) \leq 1$. Moreover, assume $k \neq k^p$, and let K be a purely inseparable extension of k of degree p. By the preceding proposition, we have $N(K) = k$. But $N(K) = K^p$. Therefore $K^p = k$, from which $K^{p^2} = k^p$ and $[k : k^p] = [K : K^p] = p$.

Remarks.

1) The relation "$[k : k^p] = 1$ or p" can also be expressed by saying that the only purely inseparable extensions of k are the extensions $k^{p^{-i}}$, with $i = 0, 1, \ldots, \infty$.

2) The converse of the preceding corollary is false: there exist perfect fields k of dimension ≤ 1 which are not (C_1), cf. the exercise below.

Exercise. (after J. Ax [8])

(a) Construct a field k_0 of characteristic 0, containing all the roots of unity, such that $\mathrm{Gal}(\bar{k}_0/k_0) = \mathbf{Z}_2 \times \mathbf{Z}_3$. [Take a suitable algebraic extension of $\mathbf{C}((X))$.]

(b) Construct a homogeneous polynomial $f(X, Y)$, of degree 5, with coefficients in k_0, which does not represent 0. [Take the product of a polynomial of degree 2 and a polynomial of degree 3.]

(c) Let $k_1 = k_0((T))$, and let k be the field obtained by adjoining to k_1 the n-th roots of T, for every integer n prime to 5. Show that

$$\mathrm{Gal}(\bar{k}/k) = \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \ , \quad \text{whence } \dim(k) \leq 1.$$

Show that the polynomial

$$F(X_1, \ldots, X_5, Y_1, \ldots, Y_5) = \sum_{i=1}^{i=5} T^i f(X_i, Y_i)$$

is of degree 5 and does not represent 0 over k. The field k is therefore not (C_1).

[An analogous construction, but more complicated, gives an example of a field of dimension ≤ 1 which is not (C_r) for any r, cf. [8].]

3.3 Examples of fields of dimension ≤ 1

a) A *finite* field is (C_1): Chevalley's theorem [31]. In particular, it is of dimension ≤ 1.

b) An extension of transcendence degree 1 of an algebraically closed field is (C_1): Tsen's theorem (cf. [95]). In particular ... etc.

c) Let K be a field equipped with a discrete valuation with an algebraically closed residue field. Assume that K is *Henselian*, and that $\widehat{K}$ is *separable* over K. Then K satisfies (C_1): Lang's theorem [95]. This applies to the maximal unramified extension of a local field with perfect residue field.

d) Let k be an algebraic extension of the field $\mathbf{Q}$. Write $k = \varinjlim k_i$, the k_i being finite over $\mathbf{Q}$, and let us denote by V_i the set of "places" of k_i (a "place" of a number field can be defined as a topology on the field, defined by a nontrivial absolute value). Let $V = \varprojlim V_i$. If $v \in V$, the place v induces a place on each k_i, and the completion $(k_i)_v$ is well defined. Put:

$$n_v(k) = \operatorname{lcm}[(k_i)_v : \mathbf{Q}_v] \ ;$$

this is a "supernatural number" (cf. Chap. I, §1.3) called the *degree of k at v*.

Proposition 9. *Let k be an algebraic extension of $\mathbf{Q}$, and let p be a prime. Assume that $p \neq 2$, or that k is totally imaginary. If, for each ultrametric place v of k, the exponent of p in the local degree $n_v(k)$ is infinite, we have* $\operatorname{cd}_p(G_k) \leq 1$.

[We say that k is "totally imaginary" if it does not have any embedding in $\mathbf{R}$, i.e., if $n_v(k) = 2$ for every place v of k defined by an archimedean absolute value.]

Proof. Let us first prove that the p-primary component of $\operatorname{Br}(k)$ vanishes. To do so, let $x \in \operatorname{Br}(k)$, with $px = 0$. Since $k = \varinjlim k_i$, we have $\operatorname{Br}(k) = \varinjlim \operatorname{Br}(k_i)$, and x comes from some element $x_0 \in \operatorname{Br}(k_{i_0})$. But one knows (cf., for example, Artin-Tate [6], Chap. 7) that an element of the Brauer group of a number field is determined by its local images, which are themselves given by invariants belonging to $\mathbf{Q}/\mathbf{Z}$. If $i \geq i_0$, the image $x(i)$ of x in $\operatorname{Br}(k_i)$ has well-defined local invariants; let W_i be the subset of V_i consisting of the places where the local invariant of $x(i)$ is not zero. The W_i form a projective system (for $i \leq i_0$); we shall see that $\varprojlim W_i = \emptyset$. Indeed, if $v \in \varprojlim W_i$, the image of x in each Brauer group $\operatorname{Br}((k_i)_v)$ is not zero. But one knows that, when one extends a local field, the invariant of an element of the Brauer group is multiplied by the degree of the extension (cf. [145], p. 201). If then v is ultrametric, p^∞ divides $n_v(k)$ and, for i large enough, the degree of $(k_i)_v$ over $(k_{i_0})_v$ is divisible by p, which implies that the invariant of $x(i)$ at v is zero, contrary to our hypothesis; similarly, if v is archimedean (which is not possible unless $p = 2$), the field $(k_i)_v$ equals $\mathbf{C}$ for large enough i, and the invariant of $x(i)$ at v is again zero. Hence we have $\varprojlim W_i = \emptyset$, and since the W_i are finite, this implies $W_i = \emptyset$ for large enough i (cf. Chap. I, §1.4, lemma 3), whence $x(i) = 0$ and $x = 0$. Thus we have proved that $\operatorname{Br}(k)(p) = 0$.

The same argument shows that $\operatorname{Br}(k')(p) = 0$ for every algebraic extension k' of k, and prop. 4 shows that $\operatorname{cd}_p(G_k) \leq 1$, QED.

Corollary. *If k is totally imaginary, and if the local degree of every ultrametric place of k equals ∞, we have* $\dim(k) \leq 1$.

Indeed, k is perfect, and $\operatorname{cd}_p(G_k)$ is ≤ 1 for all p; one may apply prop. 6.

Remark.

It is unknown whether a field which satisfies the conditions of the corollary above is necessarily (C_1); it does not look likely.

Exercises.

1) Prove the converse of prop. 9 [use the surjectivity of the canonical maps $\mathrm{Br}(k) \to \mathrm{Br}(k_v)$].

2) Show that $G_{\mathbf{Q}}$ does not contain any subgroup isomorphic to $\mathbf{Z}_p \times \mathbf{Z}_p$ [notice that such a subgroup has cohomological dimension 2, and use prop. 9]. By Artin-Schreier [5], $G_{\mathbf{Q}}$ does not contain a finite subgroup of order > 2, and does not contain $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}_p$.

Deduce that every closed commutative subgroup of $G_{\mathbf{Q}}$ is isomorphic, either to $\mathbf{Z}/2\mathbf{Z}$, or to a product $\prod_{p \in I} \mathbf{Z}_p$, where I is a subset of the prime numbers. In particular such a subgroup is topologically cyclic.

3) Let k be perfect field. Show that the following three properties are equivalent:

(i) k is algebraically closed;

(ii) $\dim k((t)) \leq 1$;

(iii) $\dim k(t) \leq 1$.

§4. Transition theorems

4.1 Algebraic extensions

Proposition 10. *Let k' be an algebraic extension of a field k, and let p be a prime. Then* $\mathrm{cd}_p(G_{k'}) \leq \mathrm{cd}_p(G_k)$, *and there is equality in each of the following two cases*:

(i) $[k' : k]_s$ *is prime to* p.

(ii) $\mathrm{cd}_p(G_k) < \infty$ *and* $[k' : k]_s < \infty$.

The Galois group $G_{k'}$ may be identified with a subgroup of the Galois group G_k and its index equals $[k' : k]_s$. The proposition follows therefore from prop. 14 in Chapter I.

Remark.

In fact there is a more precise result:

Proposition 10′. *Assume* $[k' : k] < \infty$. *Then* $\mathrm{cd}_p(G_{k'}) = \mathrm{cd}_p(G_k)$, *unless the following conditions are simultaneously satisfied*:

(a) $p = 2$;

(b) k *can be ordered* (i. e., -1 is not a sum of squares in k);

(c) $\mathrm{cd}_2(G_{k'}) < \infty$.

(Example: $k = \mathbf{R}$, $k' = \mathbf{C}$.)

We apply prop. 14′ of Chap. I to the profinite group G_k and to its open subgroup $G_{k'}$. One sees that, if $\mathrm{cd}_p(G_k) \neq \mathrm{cd}_p(G_{k'})$, the group G_k contains an element of order p. But, by a theorem due to Artin-Schreier ([5], see also Bourbaki A VI.42, exerc. 31), this is impossible unless $p = 2$ and k can be ordered. Hence the proposition.

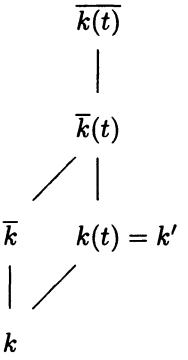
4.2 Transcendental extensions

Proposition 11. *Let k' be an extension of k, of transcendence degree N. If p is a prime, we have*

$$\mathrm{cd}_p(G_{k'}) \leq N + \mathrm{cd}_p(G_k) \ .$$

There is equality when k' is finitely generated over k, $\mathrm{cd}_p(G_k) < \infty$, *and p is distinct from the characteristic of k.*

Using prop. 10, we can restrict ourselves to the case $k' = k(t)$; therefore $N = 1$. If $\overline{k}$ denotes an algebraic closure of k, $\overline{k}/k$ is a quasi-Galois extension with Galois group G_k. Moreover, this extension is linearly disjoint from the extension $k(t)/k$. Hence the Galois group of the extension $\overline{k}(t)/k(t)$ may be identified with G_k. On the other hand, if H denotes the Galois group of $\overline{k(t)}/\overline{k}(t)$, Tsen's theorem shows that $\mathrm{cd}(H) \leq 1$. Since $G_{k'}/H = G_k$, prop. 15 of Chapter I gives the inequality we seek.



It remains to see that there is equality when $\mathrm{cd}_p(G_k) < \infty$ and p is distinct from the characteristic of k. After replacing G_k by one of its Sylow p-subgroups, we may assume that G_k is a *pro-p-group*. If μ_p denotes the group of p-th roots of unity, G_k acts in a trivial way on μ_p, which shows that the p-th roots of unity belong to k.

Put $d = \mathrm{cd}_p(G_k)$. We shall see that $H^{d+1}(G_{k'}, \mu_p) \neq 0$, which will establish the inequality we are after. The spectral sequence of group extensions (cf. Chapter I, §3.3) gives

$$H^{d+1}(G_{k'}, \mu_p) = H^d(G_k, H^1(H, \mu_p)) \ .$$

However, $H^1(H, \mu_p) = H^1(\overline{k}(t), \mu_p)$. To simplify the notation, set $K = \overline{k}(t)$. The exact sequence $0 \to \mu_p \to \mathbf{G}_m \xrightarrow{p} \mathbf{G}_m \to 0$, applied to the field K, shows that $H^1(K, \mu_p) = K^*/K^{*p}$, and this isomorphism is compatible with the action of the group $G_k = G_{k'}/H$. We have therefore:

$$H^{d+1}(G_{k'}, \mu_p) = H^d(G_k, K^*/K^{*p}) \ .$$

Let $w : K^* \to \mathbf{Z}$ be the valuation of $K = \overline{k}(t)$ defined by an element of k (for example 0); by passing to the quotient, w defines a surjective homomorphism $K^*/K^{*p} \to \mathbf{Z}/p\mathbf{Z}$ which is compatible with the action of G_k. We deduce from this a homomorphism

$$H^d(G_k, K^*/K^{*p}) \longrightarrow H^d(G_k, \mathbf{Z}/p\mathbf{Z})$$

which is surjective (since $\mathrm{cd}_p(G_k) \leq d$). But, since G_k is a pro-p-group, we have $H^d(G_k, \mathbf{Z}/p\mathbf{Z}) \neq 0$. It follows that $H^d(G_k, K^*/K^{*p}) \neq 0$, hence $H^{d+1}(G_k, \mu_p) \neq 0$, QED.

Corollary. *If k is either a function field in one variable over a finite field or a function field in two variables over an algebraically closed field, then* $\mathrm{cd}(G_k) = 2$.

[By "a function field in r variables" over a field k_0, we mean a finitely generated extension of k_0 of transcendence degree r.]

This follows from the fact that $\mathrm{cd}(G_{k_0})$ equals 1 (resp. 0) when k_0 is a finite field (resp. an algebraically closed field).

Remarks.

1) When k' is a purely transcendental extension of k, the projection $G_{k'} \to G_k$ *splits* (it is enough to see this when $k' = k(t)$, in which case it is a consequence of the analogous result for $k((t))$, cf. §4.3, exerc. 1, 2). It follows (cf. Ax [8]), that for any G_k-module A, the canonical map

$$H^i(k, A) \longrightarrow H^i(k', A) \ , \quad i = 0, 1, \ldots$$

is injective. This shows, in particular, $\mathrm{cd}_p(G_{k'}) \geq \mathrm{cd}_p(G_k)$, even if $\mathrm{cd}_p(G_k) = \infty$.

2) For more details on these relations between the Galois cohomology of $k(t)$ and that of finite extensions of k (values, residues, etc.), see §4 of the Appendix.

4.3 Local fields

Proposition 12. *Let K be a complete field with respect to a discrete valuation with residue field k. For any prime p, we have:*

$$\mathrm{cd}_p(G_K) \leq 1 + \mathrm{cd}_p(G_k) \ .$$

There is equality when $\mathrm{cd}_p(G_k) < \infty$ *and p is different from the characteristic of K.*

The proof is analogous to the one above. One uses the maximal unramified extension K_{nr} of K. The Galois group of that extension can be identified with G_k; furthermore, $\mathrm{Gal}(K_s/K_{nr})$ is of cohomological dimension ≤ 1 (cf. §3.3 as well as [145], Chap. XII). Prop. 15 of Chapter I can be applied and shows that $\mathrm{cd}_p(G_K) \leq 1 + \mathrm{cd}_p(G_k)$.

When $d = \mathrm{cd}_p(G_k)$ is finite, and p is prime to the characteristic of K, we may assume, as above, that G_k is a pro-p-group. One computes $H^{d+1}(G_K, \mu_p)$. One finds:

$$H^{d+1}(G_K, \mu_p) = H^d(G_k, K_{nr}^*/K_{nr}^{*p}) \ .$$

The valuation of K_{nr} defines a surjective homomorphism

$$K_{nr}^*/K_{nr}^{*p} \longrightarrow \mathbf{Z}/p\mathbf{Z} \ ,$$

which gives a surjective homomorphism $H^d(G_k, K_{nr}^*/K_{nr}^{*p}) \to H^d(G_k, \mathbf{Z}/p\mathbf{Z})$, and we see again that $H^{d+1}(G_k, \mu_p)$ is $\neq 0$, QED.

Corollary. *If the residue field k of K is finite, we have $\mathrm{cd}_p(G_K) = 2$ for every p different from the characteristic of K.*

Indeed one has $G_k = \widehat{\mathbf{Z}}$, hence $\mathrm{cd}_p(G_k) = 1$ for all p.

Remark.

If $\mathrm{cd}_p(G_k) = \infty$, then $\mathrm{cd}_p(G_K) = \infty$, cf. exerc. 3 below.

Exercises.

In these exercises, K and k satisfy the hypotheses of prop. 12.

1) Assume k has characteristic 0. There is an exact sequence

$$(*) \qquad 1 \longrightarrow N \longrightarrow G_K \longrightarrow G_k \longrightarrow 1 \ ,$$

where $N = \mathrm{Gal}(\overline{K}/K_{nr})$ is the inertia group of G_K.

(a) Define a canonical isomorphism of N onto $\varprojlim \mu_n$, where μ_n denotes the group of n-th roots of unity in $\bar{k}$ (or of $\overline{K}$, which is the same). Deduce from this that N is isomorphic (not canonically) to $\widehat{\mathbf{Z}}$.

(b) Show that the extension $(*)$ splits. [If π is a uniformizer of K, show that one may choose π_n, $n \geq 1$, in $\overline{K}$ such that $\pi_1 = \pi$ and $(\pi_{nm})^m = \pi_n$ for each pair $n, m \geq 1$. If H is the subgroup G_K which fixes the π_n, show that G_K is the semi-direct product of H and N.]

2) Assume k has characteristic $p > 0$. A finite Galois extension of K is said to be *tame* if its inertia group is of order prime to p. Let K_{mod} be the compositum of all such extensions. We have $K_s \supset K_{\mathrm{mod}} \supset K_{nr} \supset K$. The residue fields of K_{mod} and K_{nr} are equal to k_s; that of K_s is $\bar{k}$.

(a) Let $N = \mathrm{Gal}(K_{\mathrm{mod}}/K_{nr})$. Show that $N = \varprojlim \mu_n$, where n runs over the integers ≥ 1 prime to p.

Show that the extension

$$1 \longrightarrow N \longrightarrow \mathrm{Gal}(K_{\mathrm{mod}}/K) \longrightarrow G_k \longrightarrow 1$$

splits [same method as in exerc. 1].

(b) Let $P = \mathrm{Gal}(K_s/K_{\mathrm{mod}})$. Show that P is a pro-p-group.

(c) Show that the extension

$$1 \longrightarrow \mathrm{Gal}(K_s/K_{nr}) \longrightarrow G_K \longrightarrow G_k \longrightarrow 1$$

splits [use (a) as well as the fact that every extension of G_k by P splits since $\mathrm{cd}_p(G_k) \leq 1$, cf. prop. 3; see also Hazewinkel [41], App., thm. 2.1, for the case when k is perfect].

3) Use the splitting of $G_K \to G_k$, proved in the two exercises above, to prove that, if A is a G_k-module, the canonical maps

$$H^i(k, A) \longrightarrow H^i(K, A) \ , \quad i = 0, 1, \ldots ,$$

are injective (cf. [8]). Therefore we have $\mathrm{cd}_p(G_k) \leq \mathrm{cd}_p(G_K)$ for all p.

4.4 Cohomological dimension of the Galois group of an algebraic number field

Proposition 13. *Let k be an algebraic number field. If $p \neq 2$, or if k is totally imaginary, we have* $\mathrm{cd}_p(G_k) \leq 2$.

The proof depends on the following lemma:

Lemma 1. *For every prime p there exists an abelian extension K of $\mathbf{Q}$ whose Galois group is isomorphic to $\mathbf{Z}_p$, and whose local degrees $n_v(K)$ are equal to p^∞, for every ultrametric place v of K.*

[Since K is Galois over $\mathbf{Q}$, the local degree $n_v(K)$ of a place v of K only depends on the place induced by v on $\mathbf{Q}$; if this last is defined by the prime number ℓ, we write $n_\ell(K)$ instead of $n_v(K)$.]

First let $\mathbf{Q}(p)$ be the field obtained by adjoining to $\mathbf{Q}$ the roots of unity with order a power of p. It is well known ("irreducibility of the cyclotomic polynomials") that the Galois group of this extension can be identified canonically with the group $\mathbf{U}_p$ of units of the field $\mathbf{Q}_p$. Moreover, the decomposition group D_ℓ of a prime ℓ is equal to $\mathbf{U}_p$ if $\ell = p$, and to the closure of the subgroup of $\mathbf{U}_p$ generated by ℓ if $\ell \neq p$ (cf. [145], p. 85). This shows that D_ℓ is infinite, and therefore that its order (which is nothing else than $n_\ell(\mathbf{Q}(p))$) is divisible by p^∞. Note now that $\mathbf{U}_p$ is a direct product of a finite group by the group $\mathbf{Z}_p$ (cf. for example [145], p. 220). Such a decomposition defines a subfield K of $\mathbf{Q}(p)$ such that $\mathrm{Gal}(K/\mathbf{Q}) = \mathbf{Z}_p$. Since $[\mathbf{Q}(p) : K]$ is finite, the local degrees of $K/\mathbf{Q}$ are necessarily equal to p^∞, which finishes the proof of the lemma.

Now let us return to prop. 13. Let K be a field with the properties listed in lemma 1, and let L be a compositum of K with k. The Galois group of L/k may be identified with a closed subgroup of finite index of the group $\mathrm{Gal}(K/\mathbf{Q})$; therefore it is also isomorphic to $\mathbf{Z}_p$. The same argument shows that the local degrees of the ultrametric places of K are equal to p^∞. By prop. 9, we have $\mathrm{cd}_p(G_L) \leq 1$. Since we also have $\mathrm{cd}_p(\mathbf{Z}_p) = 1$, prop. 15 of Chapter I proves that $\mathrm{cd}_p(G_k) \leq 2$, QED.

4.5 Property (C_r)

It is the following :

(C_r). *Every homogeneous equation $f(x_1, \ldots, x_n) = 0$, of degree $d \geq 1$, with coefficients in k, has a nontrivial solution in k^n if $n > d^r$.*

(Notice that (C_0) $\Leftrightarrow$ k is algebraically closed; for (C_1), see §3.2.)

Property (C_r) enjoys "transition theorems" analogous to those of §§4.1 and 4.2. More precisely:

(a) If k' is an algebraic extension of k, and if k is (C_r), then k' is (C_r), cf. Lang [95].

(b) More generally, if k' is an extension of k with transcendence degree n, and if k is (C_r), then k' is (C_{r+n}), cf. Lang [95], completed by Nagata [118].

In particular, every extension of transcendence degree $\leq r$ of an algebraically closed field is (C_r); this applies, for instance, to the fields of meromorphic functions on a compact complex analytic variety of dimension r.

On the other hand prop. 12 has no analogue for (C_r): if K is a local field whose residue field k is (C_r), *it is not true in general that* K *is* (C_{r+1}). The simplest example is that of Terjanian [174], where $r = 1$, $k = \mathbf{F}_2$, $K = \mathbf{Q}_2$; Terjanian constructs a homogeneous polynomial f, of degree 4, in 18 variables, with integer coefficients, which does not have a nontrivial zero in $\mathbf{Q}_2$; since $18 > 4^2$, this shows $\mathbf{Q}_2$ is not (C_2), even though its residue field is (C_1). For other examples, see Greenberg [57], and Borevič-Šafarevič [21], Chap. I, §6.5.

The case $r = 2$

Property (C_2) is especially interesting. It implies:

(*) *If* D *is a skew field with center* k *which is finite over* k, *the reduced norm* $\mathrm{Nrd} : D^* \to k^*$ *is surjective.*

Indeed, if $[D : k] = n^2$, and if $a \in k^*$, the equation $\mathrm{Nrd}(x) = at^n$ is homogeneous and of degree n in $n^2 + 1$ unknowns (namely t and the components of x); if k is (C_2), it therefore has a nontrivial solution, which shows that a is the reduced norm of some element of D^*.

Another consequence of (C_2) is:

(**) *Every quadratic form in* 5 *variables* (or more) *over* k *is isotropic* (i.e. represents 0).

This allows a complete classification of quadratic forms over k (assuming the characteristic $\neq 2$) using their ranks, their *discriminants* (in $k^*/k^{*2} = H^1(k, \mathbf{Z}/2\mathbf{Z})$), and their *Hasse-Witt invariants* (in $\mathrm{Br}_2(k) = H^2(\mathbf{Z}/2\mathbf{Z})$), cf. Witt [187] and also Scharlau [139], II.14.5.

Connection between (C_r) *and* $\mathrm{cd}(G_k) \leq r$

We have seen in §3.2 that $(C_1) \Rightarrow \mathrm{cd}(G_k) \leq 1$. *It is probable that*

$$(C_r) \Rightarrow \mathrm{cd}(G_k) \leq r \quad \textit{for all } r \geq 0.$$

This is (trivially) true for $r = 0$, and it holds (nontrivially) for $r = 2$, by results of Merkurjev and Suslin. More precisely:

Theorem MS. (Suslin [167], cor. 24.9) *Let* k *be a perfect field. The following properties are equivalent*:

(a) $\mathrm{cd}(G_k) \leq 2$.

(b) *The property* (*) *above* (surjectivity of the reduced norm) *is true for all finite extensions of* k.

Since $(C_2) \Rightarrow$ (b), this shows that $(C_2) \Rightarrow \mathrm{cd}(G_k) \leq 2$ when k is perfect; the general case reduces immediately to this one.

Remarks.

1) An essential point in the proof of the Merkurjev-Suslin theorem is the construction of a homomorphism $k^*/\mathrm{Nrd}(D^*) \to H^3(k, \mu_n^{\otimes 2})$, which is *injective* if n is square-free, cf. Merkurjev-Suslin [109], th. 12.2.

2) One may ask whether $\mathrm{cd}(G_k) \leq 2$ implies (**). The answer is "no". Merkurjev has shown (cf. [108]) that, for every $N \geq 1$, there exists a field k of characteristic 0, with $\mathrm{cd}(G_k) = 2$, which has an anisotropic quadratic form of rank N. If $N > 4$, such a field is not (C_2); it is not even (C_r) if one takes $N > 2^r$.

3) For a partial result in the direction $(C_r) \stackrel{?}{\Rightarrow} \mathrm{cd}(G_k) \leq r$, see exerc. 2.

Exercises.

1) Assume k has characteristic $\neq 2$; denote by I the augmentation ideal of the Witt ring of k.

Show, as a consequence of the results of Merkurjev and Suslin (cf. [4], [111]), that the following properties are equivalent:

(a) A quadratic form over k is characterized by its rank, its discriminant and its Hasse-Witt invariant.

(b) $I^3 = 0$.

(c) $H^3(k, \mathbf{Z}/2\mathbf{Z}) = 0$.

2) Assume k has characteristic $\neq 2$. For $x \in k^*$ denote by (x) the corresponding element of $H^1(k, \mathbf{Z}/2\mathbf{Z}) = k^*/k^{*2}$, cf. §1.2.

Denote by (M_i) the following property of k (a special case of conjectures due to Milnor [117]): $H^i(k, \mathbf{Z}/2\mathbf{Z})$ is generated by the cup-products of elements of $H^1(k, \mathbf{Z}/2\mathbf{Z})$.

Assume that k is (C_r) for some integer $r \geq 1$.

(a) Let $x_1, \ldots, x_i \in k^*$. Show that the cup-product $(x_1) \cdots (x_i) \in H^i(k, \mathbf{Z}/2\mathbf{Z})$ is 0 if $i > r$. [Let q be the i-fold Pfister form $\langle 1, -x_1 \rangle \otimes \cdots \otimes \langle 1, -x_i \rangle$. The Arason invariant [3] of q is $(x_1) \cdots (x_i)$. If $i > r$, (C_r) implies that q is isotropic, therefore hyperbolic, and its invariant is 0.]

(b) Assume that the finite extensions of k have property (M_{r+1}). Show that $\mathrm{cd}_2(G_k) \leq r$.

(c) Same assertion as in (b), but with (M_{r+1}) replaced by (M_r).

[Hence, we have $(C_r) \Rightarrow \mathrm{cd}_2(G_k) \leq r$ if we assume Milnor's conjectures.]

3) Assume that k is (C_r) of characteristic $p > 0$.

(a) Show that $[k : k^p] \leq p^r$. Deduce that the cohomology groups $H_p^i(k)$, defined by Bloch and Kato (cf. [81]), are 0 for $i > r + 1$.

(b) Assume $p = 2$. Show, using the results of Kato on Pfister forms (*loc. cit.*, prop. 3) that $H_p^i(k) = 0$ for $i = r + 1$.

(It is probable that this result also holds for $p \neq 2$.)

§5. p-adic fields

In this section, the letter k denotes a *p-adic field*, i.e., a finite extension of the field $\mathbf{Q}_p$. Such a field is complete with respect to a discrete valuation v and its residue field k_0 is a finite extension $\mathbf{F}_{p^f}$ of the prime field $\mathbf{F}_p$; it is a locally compact field.

5.1 Summary of known results

a) *The structure of k^**

If $U(k)$ denotes the group of units of k, there is an exact sequence

$$0 \longrightarrow U(k) \longrightarrow k^* \xrightarrow{v} \mathbf{Z} \longrightarrow 0.$$

The group $U(k)$ is a compact commutative p-adic analytic group; its dimension N is equal to $[k : \mathbf{Q}_p]$. By Lie theory, $U(k)$ is therefore isomorphic to a product of a finite group F with $(\mathbf{Z}_p)^N$; it is obvious that F is nothing else than the set of roots of unity contained in k; in particular it is a *cyclic* finite group.

By dévissage from k^* it follows that the quotients k^*/k^{*n} are *finite* for all $n \geq 1$, and one may readily evaluate their orders.

b) The Galois group G_k of $\overline{k}/k$ has *cohomological dimension* 2 (cf. §4.3, cor. to prop. 12).

c) The *Brauer group* $\mathrm{Br}(k) = H^2(k, \mathbf{G}_m)$ *may be identified with* $\mathbf{Q}/\mathbf{Z}$, cf. [145], Chap. XIII. Let us recall briefly how this identification is done:

If k_{nr} is the maximal unramified extension of k, one first shows that $\mathrm{Br}(k) = H^2(k_{nr}/k, \mathbf{G}_m)$, i.e. that every element of $\mathrm{Br}(k)$ is split by an unramified extension. From this one shows that the valuation v gives an isomorphism of $H^2(k_{nr}/k, \mathbf{G}_m)$ onto $H^2(k_{nr}/k, \mathbf{Z})$; since $\mathrm{Gal}(k_{nr}/k) = \widehat{\mathbf{Z}}$, the group $H^2(k_{nr}/k, \mathbf{Z})$ may be identified with $\mathbf{Q}/\mathbf{Z}$, which gives the isomorphism desired.

5.2 Cohomology of finite G_k-modules

Let us denote by μ_n the group of n-th roots of unity in $\overline{k}$; it is a G_k-module.

Lemma 2. *We have $H^1(k, \mu_n) = k^*/k^{*n}$, $H^2(k, \mu_n) = \mathbf{Z}/n\mathbf{Z}$ and $H^i(k, \mu_n) = 0$ for $i \geq 3$. In particular, the groups $H^i(k, \mu_n)$ are finite.*

We write the cohomology exact sequence corresponding to the exact sequence

$$0 \longrightarrow \mu_n \longrightarrow \mathbf{G}_m \xrightarrow{n} \mathbf{G}_m \longrightarrow 0 ,$$

cf. §1.2. We have $H^0(k, \mathbf{G}_m) = k^*$, $H^1(k, \mathbf{G}_m) = 0$ and $H^2(k, \mathbf{G}_m) = \mathbf{Q}/\mathbf{Z}$. This gives $H^i(k, \mu_n)$ for $i \leq 2$; the case $i \geq 3$ is trivial because $\mathrm{cd}(G_k) = 2$.

Proposition 14. *If A is a finite G_k-module, $H^n(k, A)$ is finite for every n.*

There exists a finite Galois extension K of k such that A is isomorphic (as a G_K-module) to a direct sum of modules of type μ_n. In view of lemma 2, the groups $H^j(K, A)$ are finite. The spectral sequence

$$H^i(\mathrm{Gal}(K/k), H^j(K, A)) \Longrightarrow H^n(k, A)$$

therefore shows that the $H^n(k, A)$ are finite.

In particular, the groups $H^2(k, A)$ are finite; thus one may apply to the group G_k the results of Chap. I, §3.5, and define the *dualizing module* I of G_k.

Theorem 1. *The dualizing module I is isomorphic to the union μ of the μ_n, $n \geq 1$.*

[Note that μ is isomorphic to $\mathbf{Q}/\mathbf{Z}$ as an abelian group, but not as a G_k-module.]

Let us put $G = G_k$ to simplify the notation. Let n be an integer ≥ 1, and let I_n be the submodule of I formed of elements killed by n. If H is a subgroup of G, we know that I is a dualizing module for H, and $\mathrm{Hom}^H(\mu_n, I_n) = \mathrm{Hom}^H(\mu_n, I)$ may be identified with the dual of $H^2(H, \mu_n)$, which is itself isomorphic to $\mathbf{Z}/n\mathbf{Z}$ by lemma 2 (applied to the extension of k corresponding to H). In particular, the result is *independent of H*. It follows that $\mathrm{Hom}(\mu_n, I_n) = \mathbf{Z}/n\mathbf{Z}$ and that G acts trivially on this group. If $f_n : \mu_n \to I_n$ denotes the element of $\mathrm{Hom}(\mu_n, I_n)$ corresponding to the canonical generator of $\mathbf{Z}/n\mathbf{Z}$, one checks that f_n is an *isomorphism of μ_n onto I_n* compatible with the actions of G on these two groups. Letting n go to infinity (multiplicatively!) we obtain an isomorphism of μ onto I, which proves the theorem.

Theorem 2. *Let A be a finite G_k-module, and put:*

$$A' = \mathrm{Hom}(A, \mu) = \mathrm{Hom}(A, \mathbf{G}_m) .$$

For any integer i, $0 \leq i \leq 2$, the cup-product

$$H^i(k, A) \times H^{2-i}(k, A') \longrightarrow H^2(k, \mu) = \mathbf{Q}/\mathbf{Z}$$

gives a duality between the finite groups $H^i(k, A)$ and $H^{2-i}(k, A')$.

For $i = 2$, this is the very definition of the dualizing module. The case $i = 0$ reduces to the case $i = 2$ by replacing A by A' and noting that $(A')' = A$. For the same reason, in the case $i = 1$, it is enough to prove that the canonical homomorphism

$$H^1(k, A) \longrightarrow H^1(k, A')^* = \mathrm{Hom}(H^1(k, A'), \mathbf{Q}/\mathbf{Z})'$$

is injective. However, this is "purely formal" starting from what we already know. Indeed, since the functor $H^1(k, A)$ is effaceable, we can embed A in such a G_k-module B that $H^1(k, A) \to H^1(k, B)$ is zero. By setting $C = B/A$, we have a commutative diagram:

$$\begin{array}{ccccc} H^0(k, B) & \longrightarrow & H^0(k, C) & \xrightarrow{\delta} & H^1(k, A) \\ \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow \\ H^2(k, B')^* & \longrightarrow & H^2(k, C')^* & \longrightarrow & H^1(k, A')^* \ . \end{array}$$

Since α and β are bijective and δ surjective, we conclude that γ is injective, QED.

Remarks.

1) The duality theorem above is due to Tate [171]. Tate's original proof made use of the cohomology of "tori"; it used Nakayama's theorems in an essential way (cf. [145], Chap. IX). Poitou gave another proof, which proceeds by reduction to the case of μ_n by dévissage (cf. exerc. 1).

2) When the field k, instead of being p-adic, is a field of formal power series $k_0((T))$ over a finite field k_0 with p^f elements, the above results remain true without change, provided that the module A is of order *prime to* p. For p-primary modules, the situation is different. One must interpret $A' = \mathrm{Hom}(A, \mathbf{G}_m)$ as an algebraic group of dimension zero (corresponding to an algebra which may have nilpotent elements), and take the cohomology of the group not from the Galois point of view (which would lead to nothing) but from the "flat topology" standpoint. Moreover, since $H^1(k, A)$ is not in general finite, it is necessary to put some topology on it, and to take characters which are continuous for this topology; then the duality theorem becomes again applicable. For more details, see Shatz [157] and Milne [116].

Exercises.

1) By applying the duality theorem to the module $A = \mathbf{Z}/n\mathbf{Z}$, show that one recovers the duality (given by local class field theory) between $\mathrm{Hom}(G_k, \mathbf{Z}/n\mathbf{Z})$ and k^*/k^{*n}. When k contains the n-th roots of unity, one may identify A with $A' = \mu_n$; show that the mapping of $k^*/k^{*n} \times k^*/k^{*n}$ into $\mathbf{Q}/\mathbf{Z}$ thus obtained is the *Hilbert symbol* (cf. [145], Chap. XIV).

2) Take as k a field which is complete for a discrete valuation, whose residue field k_0 is quasi-finite (cf. [145], p. 198). Show that theorems 1 and 2 continue to hold, provided one restricts oneself to finite modules of order prime to the characteristic of k_0.

3) The "purely formal" part of the proof of theorem 2 is in fact a theorem about morphisms of cohomology functors. What is this theorem?

5.3 First applications

Proposition 15. *The group G_k has strict cohomological dimension 2.*

Indeed, the group $H^0(G_k, I) = H^0(G_k, \mu)$ is none other than the group of roots of unity contained in k, and we have seen in §5.1 that this group is finite; the proposition follows from this, and from prop. 19 of Chap. I.

Proposition 16. *If A is an abelian variety defined over k, we have*

$$H^2(k, A) = 0 .$$

For any $n \geq 1$, let A_n be the subgroup of A which is the kernel of multiplication by n. One has $H^2(k, A) = \varinjlim H^2(k, A_n)$. By the duality theorem, $H^2(k, A_n)$ is dual to $H^0(k, A'_n)$. In addition, if B denotes the abelian variety *dual* to A (in the sense of duality of abelian varieties), A'_n can be identified with B_n. We are thus reduced to proving:

$$\varprojlim H^0(k, B_n) = 0 .$$

But $B(k) = H^0(k, B)$ is a compact abelian p-adic Lie group. Its torsion subgroup is therefore finite, which proves that the $H^0(k, B_n)$ are contained in a fixed finite subgroup of B; the vanishing of $\varprojlim H^0(k, B_n)$ is an easy consequence.

Remark.

Tate proved that $H^1(k, A)$ can be identified with the dual of the compact group $H^0(k, B)$, cf. [97], [170]; it does not seem that this result can be deduced directly from the duality theorem of the previous section.

Exercise.

Let T be a torus defined over k. Show that the following conditions are equivalent:

(i) $T(k)$ is compact,
(ii) Every k-homomorphism of T into $\mathbf{G}_m$ is trivial,
(iii) $H^2(k, T) = 0$.

5.4 The Euler-Poincaré characteristic (elementary case)

Let A be a finite G_k-module, and let $h^i(A)$ be the order of the finite group $H^i(k, A)$. Set:

$$\chi(A) = \frac{h^0(A) \cdot h^2(A)}{h^1(A)} .$$

We obtain a rational number > 0 which is called the *Euler-Poincaré characteristic of* A. If $0 \to A \to B \to C \to 0$ is an exact sequence of G_k-modules, we see easily that:

$$\chi(B) = \chi(A) \cdot \chi(C) \ .$$

This is the "additivity" of Euler-Poincaré characteristics. Tate showed that $\chi(A)$ depends only on the *order* a of A (more precisely, he proved the equality $\chi(A) = 1/(\mathfrak{o} : a\mathfrak{o})$, where $\mathfrak{o}$ denotes the ring of integers of k, cf. §5.7). We shall be satisfied, for the time being, with an elementary special case:

Proposition 17. *If the order of A is prime to p, then $\chi(A) = 1$.*

We use the spectral sequence associated with the extensions $k \to k_{nr} \to \overline{k}$. One knows that the group $\mathrm{Gal}(k_{nr}/k)$ is $\widehat{\mathbf{Z}}$. If we denote by U the group $\mathrm{Gal}(\overline{k}/k_{nr})$, the theory of ramification groups shows that the Sylow p-subgroup U_p of U is normal in U, and that the quotient $V = U/U_p$ is isomorphic to the product of the $\mathbf{Z}_\ell$, for $\ell \neq p$ (cf. §4.3, exerc. 2). We deduce easily from this that $H^i(U, A)$ is finite for all i, and vanishes for $i \geq 2$. The spectral sequence

$$H^i(k_{nr}/k, H^j(k_{nr}, A)) \Longrightarrow H^n(k, A)$$

here becomes

$$H^i(\widehat{\mathbf{Z}}, H^j(U, A)) \Longrightarrow H^n(k, A) \ .$$

We conclude from this:

$$H^0(k, A) = H^0(\widehat{\mathbf{Z}}, H^0(U, A)) \ , \qquad H^2(k, A) = H^1(\widehat{\mathbf{Z}}, H^1(U, A)) \ ,$$

and we have an exact sequence:

$$0 \longrightarrow H^1(\widehat{\mathbf{Z}}, H^0(U, A)) \longrightarrow H^1(k, A) \longrightarrow H^0(\widehat{\mathbf{Z}}, H^1(U, A)) \longrightarrow 0 \ .$$

But, if M is a finite $\mathbf{Z}$-module, it is immediate that the groups $H^0(\widehat{\mathbf{Z}}, M)$ and $H^1(\widehat{\mathbf{Z}}, M)$ have the same numbers of elements. By applying this to $M = H^0(U, A)$ and to $M = H^1(U, A)$, we see that $h^1(A) = h^0(A) \cdot h^2(A)$, i.e. that $\chi(A) = 1$.

Exercise.

Show that the group U_p defined in the proof of prop. 17 is a free pro-p-group. Deduce that $H^j(U, A) = 0$ for $j \geq 2$ and for every torsion G_k-module A. Show that, if A is a p-group $\neq 0$, the group $H^1(U, A)$ *is not* finite.

5.5 Unramified cohomology

We keep the notation of the preceding section. A G_k-module A is said to be *unramified* if the group $U = \mathrm{Gal}(\overline{k}/k_{nr})$ acts *trivially* on A; this allows one to view A as a $\widehat{\mathbf{Z}}$-module, since $\mathrm{Gal}(k_{nr}/k) = \widehat{\mathbf{Z}}$. In particular, the cohomology groups $H^i(k_{nr}/k, A)$ are defined. We shall denote them $H^i_{nr}(k, A)$.

Proposition 18. *Let A be a finite unramified G_k-module. We have:*

(a) $H^0_{nr}(k, A) = H^0(k, A)$.

(b) $H^1_{nr}(k, A)$ *can be identified with a subgroup of* $H^1(k, A)$; *its order is equal to that of* $H^0(k, A)$.

(c) $H^i_{nr}(k, A) = 0$ *for* $i \geq 2$.

Assertion (a) is trivial; assertion (b) follows from the fact that $H^0(\widehat{\mathbf{Z}}, A)$ and $H^1(\widehat{\mathbf{Z}}, A)$ have the same number of elements; assertion (c) follows from $\widehat{\mathbf{Z}}$ having cohomological dimension 1.

Proposition 19. *Let A be an unramified finite G_k-module of order prime to p. The module $A' = \mathrm{Hom}(A, \mu)$ enjoys the same properties. Moreover, in the duality between $H^1(k, A)$ and $H^1(k, A')$, each of the subgroups $H^1_{nr}(k, A)$ and $H^1_{nr}(k, A')$ is the orthogonal of the other.*

Let $\overline{\mu}$ be the submodule of μ formed by elements of order prime to p. It is well-known that $\overline{\mu}$ is an unramified G_k-module (the canonical generator F of $\mathrm{Gal}(k_{nr}/k) = \widehat{\mathbf{Z}}$ acts on $\overline{\mu}$ by $\lambda \mapsto \lambda^q$, q being the number of elements in the residue field k_0). Since $A' = \mathrm{Hom}(A, \overline{\mu})$, we see that A' is unramified.

The cup-product $H^1_{nr}(k, A) \times H^1_{nr}(k, A') \to H^2(k, \mu)$ factorizes through $H^2_{nr}(k, \overline{\mu})$, which is zero. It follows that $H^1_{nr}(k, A)$ and $H^1_{nr}(k, A')$ are orthogonal. To prove that each is the orthogonal of the other, it is sufficient to check that the order $h^1(A)$ of $H^1(k, A)$ is equal to the product $h^1_{nr}(A) \cdot h^1_{nr}(A')$ of the orders of $H^1_{nr}(k, A)$ and $H^1_{nr}(k, A')$. However prop. 18 shows that $h^1_{nr}(A) = h^0(A)$, and also $h^1_{nr}(A') = h^0(A')$. From the duality theorem, $h^0(A') = h^2(A)$. Since $\chi(A) = 1$ (cf. prop. 17), we deduce that

$$h^1(A) = h^0(A) \cdot h^2(A) = h^1_{nr}(A) \cdot h^1_{nr}(A') \ , \qquad \text{QED.}$$

Exercise.

Extend prop. 17, 18, and 19 to the fields which are complete for a discrete valuation with quasi-finite residue field. Can one do the same for prop. 15 and 16?

5.6 The Galois group of the maximal p-extension of k

Let $k(p)$ be the maximal p-extension of k, in the sense of §2. By definition, the Galois group $G_k(p)$ of $k(p)/k$ is the largest quotient of G_k which is a pro-p-group. We now study the structure of this group.

Proposition 20. *Let A be a torsion $G_k(p)$-module which is p-primary. For every integer $i \geq 0$, the canonical homomorphism*

$$H^i(G_k(p), A) \longrightarrow H^i(G_k, A)$$

is an isomorphism.

We use the following lemma:

Lemma 3. *If K is an algebraic extension of k whose degree is divisible by p^∞, we have* $\mathrm{Br}(K)(p) = 0$.

Write K as a union of finite subextension K_α of k. Then $\mathrm{Br}(K) = \varinjlim \mathrm{Br}(K_\alpha)$. Moreover each $\mathrm{Br}(K_\alpha)$ can be identified with $\mathbf{Q}/\mathbf{Z}$, and if K_β contains K_α, the corresponding homomorphism from $\mathrm{Br}(K_\alpha)$ into $\mathrm{Br}(K_\beta)$ is simply multiplication by the degree $[K_\beta : K_\alpha]$ (cf. [145], p. 201). The lemma follows easily from this (cf. the proof of prop. 9, §3.3).

Let us return to the proof of proposition 20. The field $k(p)$ contains the maximal unramified p-extension of k, whose Galois group is $\mathbf{Z}_p$; therefore we have $[k(p) : k] = p^\infty$ and lemma 3 may be applied to all the algebraic extensions K of $k(p)$. If $I = \mathrm{Gal}(\bar{k}/k(p))$, that implies that $\mathrm{cd}_p(I) \leq 1$, cf. §2.3, prop. 4. Therefore we have $H^i(I, A) = 0$ for $i \geq 2$; but we also have $H^1(I, A) = 0$, because each homomorphism of I into a p-group is trivial (cf. §2.1, proof of prop. 2). The spectral sequence of group extensions shows then that the homomorphisms

$$H^i(G_k/I, A) \longrightarrow H^i(G_k, A)$$

are isomorphisms, QED.

Theorem 3. *If k does not contain a primitive p-th root of unity, the group $G_k(p)$ is a free pro-p-group, of rank $N + 1$, with $N = [k : \mathbf{Q}_p]$.*

From prop. 20, we have $H^2(G_k(p), \mathbf{Z}/p\mathbf{Z}) = H^2(k, \mathbf{Z}/p\mathbf{Z})$; the duality theorem shows that this last group is the dual of $H^0(k, \mu_p)$, which is zero by hypothesis. Therefore we have $H^2(G_k(p), \mathbf{Z}/p\mathbf{Z}) = 0$, which means that $G_k(p)$ is free, cf. Chap. I, §4.2. To compute its rank, one has to determine the dimension of $H^1(G_k(p), \mathbf{Z}/p\mathbf{Z})$, which is isomorphic to $H^1(G_k, \mathbf{Z}/p\mathbf{Z})$. By local class field theory (or by the duality theorem) this group is dual to k^*/k^{*p}; in view of the results recalled in §5.1, k^*/k^{*p} is an $\mathbf{F}_p$-vector space of dimension $N + 1$, QED.

Theorem 4. *If k contains a primitive p-th root of unity, the group $G_k(p)$ is a Demuškin pro-p-group of rank $N + 2$, with $N = [k : \mathbf{Q}_p]$. Its dualizing module is the p-primary component $\mu(p)$ of the group μ of roots of unity.*

We have $H^0(k, \mu_p) = \mathbf{Z}/p\mathbf{Z}$, from which follows $H^2(k, \mathbf{Z}/p\mathbf{Z}) = \mathbf{Z}/p\mathbf{Z}$. Applying prop. 20, we see that $H^2(G_k(p), \mathbf{Z}/p\mathbf{Z}) = \mathbf{Z}/p\mathbf{Z}$, and $H^i(G_k(p), \mathbf{Z}/p\mathbf{Z}) = 0$ for $i > 2$, which already shows that $\mathrm{cd}_p(G_k(p)) = 2$. To check that $G_k(p)$ is a Demuškin group, it remains to prove that the cup-product

$$H^1(G_k(p), \mathbf{Z}/p\mathbf{Z}) \times H^1(G_k(p), \mathbf{Z}/p\mathbf{Z}) \longrightarrow H^2(G_k(p), \mathbf{Z}/p\mathbf{Z}) = \mathbf{Z}/p\mathbf{Z}$$

is a nondegenerate bilinear form. But that is a consequence of prop. 20, and of the analogous result for the cohomology of k (note that μ_p and $\mathbf{Z}/p\mathbf{Z}$ are isomorphic).

The rank of $G_k(p)$ equals the dimension of $H^1(G_k(p), \mathbf{Z}/p\mathbf{Z})$, which is equal to that of k^*/k^{*p}, that is, $N+2$.

It remains to show that the dualizing module of $G_k(p)$ is $\mu(p)$. To start with, since k contains μ_p, the field obtained by adjoining to k the p^n-th roots of unity is an abelian extension of k, of degree $\leq p^{n-1}$; it is therefore contained in $k(p)$. That already shows that $\mu(p)$ is a $G_k(p)$-module; by prop. 20, we have

$$H^2(G_k(p), \mu(p)) = H^2(k, \mu(p)) = (\mathbf{Q}/\mathbf{Z})(p) = \mathbf{Q}_p/\mathbf{Z}_p.$$

Now let A be a finite and p-primary $G_k(p)$-module. Set:

$$A' = \mathrm{Hom}(A, \mu) = \mathrm{Hom}(A, \mu(p)).$$

In this way we obtain a $G_k(p)$-module. If $0 \leq i \leq 2$, the cup-product defines a bilinear map:

$$H^i(G_k(p), A) \times H^{2-i}(G_k(p), A') \longrightarrow H^2(G_k(p), \mu(p)) = \mathbf{Q}_p/\mathbf{Z}_p \ .$$

By prop. 20, this map may be identified with the corresponding map for the cohomology of G_k; by theorem 2, this is therefore a duality between $H^i(G_k(p), A)$ and $H^{2-i}(G_k(p), A')$; this finishes the proof that $\mu(p)$ is the dualizing module of $G_k(p)$.

Corollary (Kawada). *The group $G_k(p)$ can be defined by $N+2$ generators and one relation.*

This follows from the equalities:

$$\dim H^1(G_k(p), \mathbf{Z}/p\mathbf{Z})) = N+2 \quad \text{and} \quad \dim H^2(G_k(p), \mathbf{Z}/p\mathbf{Z})) = 1 \ .$$

Remark.

The structure of $G_k(p)$ has been determined completely by Demuškin [43], [44] and Labute [92]. The result is the following: let us denote by p^s the largest power of p such that k contains the p^s-th roots of unity, and *let us assume first that* $p^s \neq 2$ (this is notably the case if $p \neq 2$). One can then choose generators $x_1, \ldots, x_{N+2}$ of $G_k(p)$, and the relation r between these generators, so that:

$$r = x_1^{p^s}(x_1, x_2) \cdots (x_{N+1}, x_{N+2}) \ .$$

[Here (x, y) denotes the commutator $xyx^{-1}y^{-1}$. Note that the hypothesis $p^s \neq 2$ implies that N is even.]

When $p^s = 2$ and N is odd, the relation r can be written

$$r = x_1^2 x_2^4 (x_2, x_3)(x_4, x_5) \cdots (x_{N+1}, x_{N+2}) \ ,$$

cf. [147] and also Labute [92], th. 8. In particular, for $k = \mathbf{Q}_2$, the group $G_k(2)$ is generated (topologically) by three elements x, y, and z with the relation $x^2y^4(y, z) = 1$.

When $p^s = 2$ and N is even, the structure of $G_k(2)$ depends on the image of the cyclotomic character $\chi : G_k \to \mathbf{U}_2 = \mathbf{Z}_2^*$ (cf. [92], th. 9):

if $\mathrm{Im}(\chi)$ is the closed subgroup of $\mathbf{U}_2$ generated by $-1+2^f$ ($f \geq 2$), we have

$$r = x_1^{2+2^f}(x_1, x_2)(x_3, x_4)\cdots(x_{N+1}, x_{N+2}) \ ;$$

if $\mathrm{Im}(\chi)$ is generated by -1 and $1+2^f$ ($f \geq 2$), we have

$$r = x_1^2(x_1, x_2)x_3^{2^f}(x_3, x_4)\cdots(x_{N+1}, x_{N+2}) \ .$$

Exercises.

In these exercises k is a field which is complete for a discrete valuation with residue field $\mathbf{F}_q$, with $q = p^f$.

1) Let k_{mod} be the compositum of all the tame Galois extensions of k, cf. §4.3, exerc. 2. Show that $\mathrm{Gal}(k_{\mathrm{mod}}/k)$ is isomorphic to the semi-direct product of $\widehat{\mathbf{Z}}$ by $\widehat{\mathbf{Z}}'$, where $\widehat{\mathbf{Z}}' = \prod_{\ell \neq p} \mathbf{Z}_\ell$ and the canonical generator of $\widehat{\mathbf{Z}}$ acts on $\mathbf{Z}'$ by $\lambda \mapsto q\lambda$.

Show that this group is isomorphic to the profinite group associated to the discrete group defined by two generators x, y with the relation $yxy^{-1} = x^q$.

2) Let ℓ be a prime $\neq p$. We are going to determine the structure of the pro-ℓ-group $G_k(\ell)$, cf. §2.

(a) Assume that $\mathbf{F}_q$ does not contain a primitive ℓ-th root of unity, i.e. that ℓ does not divide $q-1$. Show that $G_k(\ell)$ is a free pro-ℓ-group of rank 1, and that the extension $k(\ell)/k$ is unramified.

(b) Assume that $q \equiv 1 \pmod{\ell}$. Show that $G_k(\ell)$ is a Demuškin group of rank 2. Show, using exercise 1, that $G_k(\ell)$ can be defined by two generators x, y with the relation $yxy^{-1} = x^q$. Show that this group is isomorphic to the subgroup of the affine group $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ consisting of the matrices such that $b \in \mathbf{Z}_\ell$, and that $a \in \mathbf{Z}_\ell^*$ is an ℓ-adic power of q.

(c) With the same hypotheses as in (b), denote by m the ℓ-adic valuation of $q-1$. Show that m is the largest integer such that k contains the ℓ^m-th roots of unity. Show that, if $\ell \neq 2$, or if $\ell = 2$ and $m \neq 1$, the group $G_k(\ell)$ can be defined by two generators x and y with the relation

$$yxy^{-1} = x^{1+\ell^m} \ .$$

If $\ell = 2$, $m = 1$, let n be the 2-adic valuation of $q+1$. Show that $G_k(2)$ can be defined by two generators x and y with the relation

$$yxy^{-1} = x^{-(1+2^n)} \ .$$

(d) Find explicitly the dualizing module of $G_k(\ell)$ in case (b).

5.7 Euler-Poincaré characteristics

Return to the notations in §5.4. In particular, $\mathfrak{o}$ denotes the ring of integers in k. If $x \in k$, we denote by $\|x\|_k$ the *normalized absolute value* of x, cf. [145], p. 37. For every $x \in \mathfrak{o}$, we have:

$$\|x\|_k = \frac{1}{(\mathfrak{o} : x\mathfrak{o})} .$$

In particular:

$$\|p\|_k = p^{-N} , \quad \text{with } N = [k : \mathbf{Q}_p].$$

If A is a finite G_k-module, we denote by $\chi(k, A)$ (or simply by $\chi(A)$ if there is no risk of confusion over k) the *Euler-Poincaré characteristic* of A (§5.4). Tate's theorem can be stated as follows:

Theorem 5. *If the order of the finite G_k-module A is a, we have:*

$$\chi(A) = \|a\|_k.$$

The two sides of this formula depend "additively" on A. We are then led, by an immediate dévissage, to the case where A is a vector space over a prime field. If this field is of characteristic $\neq p$, the theorem has already been proved (prop. 17). We may therefore assume that *A is a vector space over $\mathbf{F}_p$*. Therefore we may view A as a *$\mathbf{F}_p[G]$-module*, where G denotes a finite quotient of G_k. Let $K(G)$ be *the Grothendieck group* of the category of $\mathbf{F}_p[G]$-modules of finite type (cf. for example Swan [168]); the functions $\chi(A)$ and $\|a\|_k$ define homomorphisms χ and φ of $K(G)$ into $\mathbf{Q}_+^*$, and *everything reduces to proving that $\chi = \varphi$*. Since $\mathbf{Q}_+^*$ is a *torsionfree* abelian group, it is sufficient to show that χ and φ have the same values on the elements x_i of $K(G)$ which generate $K(G) \otimes \mathbf{Q}$. But one has the following lemma:

Lemma 4. *For any subgroup C of G, denote by M_G^C the homomorphism of $K(C) \otimes \mathbf{Q}$ into $K(G) \otimes \mathbf{Q}$ defined by the functors M_G^C of* Chap. I, §2.5 ("induced modules"). *The group $K(G) \otimes \mathbf{Q}$ is generated by the images of the M_G^C, for C running over the set of cyclic subgroups of G of order prime to p.*

This result can be deduced from the description of $K(G) \otimes \mathbf{Q}$ using "modular characters". One can also, more simply, apply general results of Swan [168], [169].

It is a consequence of this lemma that it is sufficient to prove the equality $\chi(A) = \|a\|_k$ when A is an $\mathbf{F}_p[G]$-module of the form $M_G^C(B)$, with C a cyclic subgroup of G, of order prime to p. However, if K is the extension of k corresponding to C, and if $b = \mathrm{Card}(B)$, we have:

$$\chi(K, B) = \chi(k, A) \qquad \text{and} \qquad \|b\|_K = \left(\|b\|_k\right)^{[K:k]} = \|a\|_k .$$

The formula to be proved is therefore equivalent to the formula $\chi(K, B) = \|B\|_K$, which means that we are reduced to the case of the module B, or even (up to a change of ground field), that *we are reduced to the case of where the group*

G is cyclic and of order prime to p. This will simplify the situation, especially because the algebra $\mathbf{F}_p[G]$ is now *semisimple.*

Let L be the extension of k such that $\mathrm{Gal}(L/k) = G$. Since the order of G is prime to that of A, we have:

$$H^i(k, A) = H^0(G, H^i(L, A)) \quad \text{for all } i.$$

This leads us to introduce the element $h_L(A)$ of $K(G)$ defined by the formula:

$$h_L(A) = \sum_{i=0}^{i=2} (-1)^i [H^i(L, A)]$$

where $[H^i(L, A)]$ denotes the element of $K(G)$ which corresponds to the $K(G)$-module $H^i(L, A)$.

Also let $\theta : K(G) \to \mathbf{Z}$ be the unique homomorphism of $K(G)$ into $\mathbf{Z}$ such that $\theta([E]) = \dim H^0(G, E)$ for any $K(G)$-module E. Obviously we have:

$$\log_p \chi(A) = \theta(h_L(A)) \ .$$

Moreover, we may compute $h_L(A)$ explicitly:

Lemma 5. *Let $r_G \in K(G)$ be the class of the module $\mathbf{F}_p[G]$* ("the regular representation"), *let $N = [k : \mathbf{Q}_p]$, and let $d = \dim(A)$. We have:*

$$h_L(A) = -dN \cdot r_G \ .$$

Assume this lemma. Since $\theta(r_G) = 1$, we see that $\theta(h_L(A)) = -dN$, from which $\chi(A) = p^{-dN} = \|p^d\|_k = \|a\|_k$ as wanted.

It remains to prove lemma 5. Remark first that the cup-product defines an isomorphism of G-modules:

$$H^i(L, \mathbf{Z}/p\mathbf{Z}) \otimes A \longrightarrow H^i(L, A) \ .$$

In the ring $K(G)$, we therefore have:

$$h_L(A) = h_L(\mathbf{Z}/p\mathbf{Z}) \cdot [A]$$

and we are reduced to proving $h_L(\mathbf{Z}/p\mathbf{Z}) = -N \cdot r_G$ (indeed, one checks easily that $r_G \cdot [A] = \dim(A) \cdot r_G$). *We thus need only to prove lemma 5 when $A = \mathbf{Z}/p\mathbf{Z}$.*

However, in this case, we have:

$H^0(L, \mathbf{Z}/p\mathbf{Z}) = \mathbf{Z}/p\mathbf{Z}$,
$H^1(L, \mathbf{Z}/p\mathbf{Z}) = \mathrm{Hom}(G_L, \mathbf{Z}/p\mathbf{Z}) =$ dual of L^*/L^{*p} (class field theory),
$H^2(L, \mathbf{Z}/p\mathbf{Z}) =$ dual of $H^0(L, \mu_p)$ (duality theorem).

Let U be the group of units of L. We have the exact sequence:

$$0 \longrightarrow U/U^p \longrightarrow L^*/L^{*p} \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow 0 \ .$$

If we denote by $h_L(\mathbf{Z}/p\mathbf{Z})^*$ the dual of $h_L(\mathbf{Z}/p\mathbf{Z})$, we then see that we have:

$$h_L(\mathbf{Z}/p\mathbf{Z})^* = -[U/U^p] + [H^0(L, \mu_p)] \ .$$

Let V be the subgroup of U formed of the elements congruent to 1 modulo the maximal ideal of the ring o_L. Then $V/V^p = U/U^p$, and the group $H^0(L, \mu_p)$ is just the subgroup ${}_pV$ of V consisting of the elements x of V with $x^p = 1$. We can thus write:

$$\begin{aligned} -h_L(\mathbf{Z}/p\mathbf{Z})^* &= [V/V^p] - [{}_pV] \\ &= [\mathrm{Tor}_0(V, \mathbf{Z}/p\mathbf{Z})] - [\mathrm{Tor}_1(V, \mathbf{Z}/p\mathbf{Z})] \ . \end{aligned}$$

But V is a finitely generated $\mathbf{Z}_p$-module, and one knows (this is one of the elementary results of Brauer theory, cf. for example Giorgiutti [53]) that the expression $[\mathrm{Tor}_0(V, \mathbf{Z}/p\mathbf{Z})] - [\mathrm{Tor}_1(V, \mathbf{Z}/p\mathbf{Z})]$ only depends on the *tensor product of V with $\mathbf{Q}_p$* (or else, if one likes, of the *Lie algebra* of the p-adic analytic group V). But, the normal basis theorem shows that this Lie algebra is a free $\mathbf{Q}[G]$-module of rank N. Therefore we have:

$$[\mathrm{Tor}_0(V, \mathbf{Z}/p\mathbf{Z})] - [\mathrm{Tor}_1(V, \mathbf{Z}/p\mathbf{Z})] = N \cdot r_G \ ,$$

and since $(r_G)^* = r_G$, we see that $h_L(\mathbf{Z}/p\mathbf{Z})$ equals $-N \cdot r_G$, which finishes the proof.

Remark.

Tate's original proof (cf. [171]) did not use lemma 4, but replaced it by a less precise "dévissage" argument: the reduction was to the case of tamely ramified Galois extensions L/k, of degree possibly divisible by p. The study of L^*/L^{*p} is then more delicate, and Tate had to use a result of Iwasawa [76]; he has also sent me a "cohomological" proof of the result in question (letter of April 7, 1963).

Exercises.

1) Show directly that, if V and V' are finitely generated $\mathbf{Z}_p[G]$-modules, such that $V \otimes \mathbf{Q}_p = V' \otimes \mathbf{Q}_p$, one has

$$[V/pV] - [{}_pV] = [V'/pV'] - [{}_pV'] \qquad \text{in } K(G).$$

[Reduce to the case where $V \supset V' \supset pV$, and use the exact sequence:

$$0 \longrightarrow {}_pV' \longrightarrow {}_pV \longrightarrow V/V' \longrightarrow V'/pV' \longrightarrow V/pV \longrightarrow V/V' \longrightarrow 0 \ .]$$

2) Let F be a field of characteristic p, let A be a finite-dimensional vector space over F, and assume that G_k acts continuously (and linearly) over A; the cohomology groups $H^i(k, A)$ are therefore vector spaces over F. We put:

$$\varrho(A) = \sum (-1)^i \dim H^i(k, A) \ .$$

Show that $\varrho(A) = -N \cdot \dim(A)$, with $N = [k : \mathbf{Q}_p]$. [Same proof as for theorem 5, replacing everywhere the field $\mathbf{F}_p$ by the field F.]

3) Same hypotheses as in the previous exercise. Consider a Galois extension L/k, with finite Galois group G, such that G_L acts trivially on A (i.e. A is an $F[G]$-module). Put

$$h_L(A) = \sum(-1)^i[H^i(L, A)] ,$$

in the Grothendieck group $K_F(G)$ of finitely generated $F[G]$-modules. Show that one still has the formula:

$$h_L(A) = -N \cdot \dim(A) \cdot r_G .$$

[Use the theory of modular characters to reduce to the case when G is cyclic of order prime to p.]

4) Assume the same hypotheses and notations as in the two exercises above, except that we assume F has characteristic $\neq p$. Show that one has $\varrho(A) = 0$ and $h_L(A) = 0$ for all A.

5.8 Groups of multiplicative type

Let A be a G_k-module *of finite type* over $\mathbf{Z}$. We define its *dual* A' by the usual formula:

$$A' = \mathrm{Hom}(A, \mathbf{G}_m) .$$

The group A' is the group of the $\bar{k}$-points of a commutative algebraic group, defined over k, and which we will again denote by $\mathrm{Hom}(A, \mathbf{G}_m)$. When A is finite, A' is finite; when A is free over $\mathbf{Z}$, A' is the *torus* whose character group is A (cf. Chap. III, §2.1). We are going to extend to the pair (A, A') the duality theorem from §5.2. The cup-product gives bilinear maps

$$\theta_i : H^i(k, A) \times H^{2-i}(k, A') \longrightarrow H^2(k, \mathbf{G}_m) = \mathbf{Q}/\mathbf{Z} \qquad (i = 0, 1, 2).$$

Theorem 6. (a) *Let $H^0(k, A)^\wedge$ be the completion of the abelian group $H^0(k, A)$ for the topology given by subgroups of finite index. The map θ_0 gives a duality between the compact group $H^0(k, A)^\wedge$ and the discrete group $H^2(k, A')$.*

(b) *The map θ_1 gives a duality between the finite groups $H^1(k, A)$ and $H^1(k, A')$.*

(c) *The group $H^0(k, A')$ has a natural structure of p-adic analytic group; let $H^0(k, A')^\wedge$ be its completion for the topology given by open subgroups of finite index. The map θ_2 gives a duality between the discrete group $H^2(k, A)$ and the compact group $H^0(k, A')^\wedge$.*

[When A is finite, we can skip the operations of completion in (a) and in (c), and recover th. 2 in §5.2.]

Let us sketch a proof using "dévissage": one could also proceed directly using the results of Appendix 1 to Chap. I.

i) Case where $A = \mathbf{Z}$

We have $A' = \mathbf{G}_m$; assertion (a) follows from the isomorphism $H^2(k, \mathbf{G}_m) = \mathbf{Q}/\mathbf{Z}$; assertion (b) results because $H^1(k, \mathbf{Z}) = 0$ and $H^1(k, \mathbf{G}_m) = 0$; assertion (c) follows because $H^2(k, \mathbf{Z})$ is isomorphic to $\mathrm{Hom}(G_k, \mathbf{Q}/\mathbf{Z})$, and local class field theory (including the "existence" theorem) shows that this group is dual to the completion of k^* for the topology given by open subgroups of finite index.

ii) Case where $A = \mathbf{Z}[G]$, *with* G *a finite quotient of* G_k

If G is the Galois group of the finite extension K/k, we have $H^i(k, A) = H^i(K, \mathbf{Z})$ and also $H^i(k, A') = H^i(K, \mathbf{G}_m)$. We are thus reduced to the previous case (for the field K).

iii) Finiteness of $H^1(k, A)$ *and of* $H^1(k, A')$

This finiteness is known when A itself is finite (cf. §5.2). By dévissage, we are thus reduced to the case where A is free over $\mathbf{Z}$. Let K/k be a finite Galois extension of k, with Galois group G, such that G_K acts trivially on A. We have $H^1(K, A) = \mathrm{Hom}(G_K, A) = 0$, and $H^1(K, A') = 0$ (th. 90). Therefore we have:

$$H^1(k, A) = H^1(G, A) \qquad \text{and} \qquad H^1(k, A') = H^1(G, A') \ .$$

It is clear that the group $H^1(G, A)$ is finite; the finiteness of the group $H^1(G, A')$ is easy to see (cf. Chap. III, §4.3).

iv) The general case

We write A as a quotient L/R, where L is a free $\mathbf{Z}[G]$-module of finite type, where G is a finite quotient of G_k. By (ii), theorem 6 is true for L, and we have $H^1(k, L) = H^1(k, L') = 0$. The cohomology exact sequences relative to the exact sequences of coefficients

$$0 \longrightarrow R \longrightarrow L \longrightarrow A \longrightarrow 0$$
$$0 \longrightarrow A' \longrightarrow L' \longrightarrow R' \longrightarrow 0$$

can each be cut into two pieces. We thus obtain the commutative diagrams (I) and (II) below. To write them more conveniently, we do not mention the field k explicitly, and we denote by E^* the *continuous* homomorphism group of a topological group E into the discrete group $\mathbf{Q}/\mathbf{Z}$; for the topological groups we have to consider, it happens that "continuous" is equivalent to "of finite order". This being so, the diagrams in question are the following:

$$\text{(I)} \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & H^1(R)^* & \longrightarrow & H^0(A)^* & \longrightarrow & H^0(L)^* & \longrightarrow & H^0(R)^* \longrightarrow 0 \\ & & f_1 \uparrow & & f_2 \uparrow & & f_3 \uparrow & & f_4 \uparrow \\ 0 & \longrightarrow & H^1(R') & \longrightarrow & H^2(A') & \longrightarrow & H^2(L') & \longrightarrow & H^2(R') \longrightarrow 0 \end{array}$$

and

$$\text{(II)} \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & H^1(A) & \longrightarrow & H^2(R) & \longrightarrow & H^2(L) & \longrightarrow & H^2(A) \longrightarrow 0 \\ & & g_1 \downarrow & & g_2 \downarrow & & g_3 \downarrow & & g_4 \downarrow \\ 0 & \longrightarrow & H^1(A')^* & \longrightarrow & H^0(R')^* & \longrightarrow & H^0(L')^* & \longrightarrow & H^0(A')^* \longrightarrow 0 \end{array}$$

Of course, the vertical arrows are defined by the bilinear maps θ_i. It should also be noted that the lines of the diagrams are *exact* sequences; this is obvious for diagram (I) and also for the first line of diagram (II); as for the second line of diagram (II), one uses the fact that the functor $\mathrm{Hom}_{\mathrm{cont}}(G, \mathbf{Q}/\mathbf{Z})$ is exact on the category of locally compact abelian groups G which are totally disconnected and denumerable at infinity.

Theorem 6 amounts to saying that the maps f_2, g_1 and g_4 are bijective. By (ii), g_3 is bijective. Hence g_4 is surjective. Since this result can be applied to any G_k-module A, it also holds true for R, which proves that g_2 is surjective; from this and from diagram (II), we conclude that g_4 is bijective, then that g_2 is bijective, and finally that g_1 is bijective. Returning to diagram (I), we see that f_1 and f_3 are bijective; from this we deduce that f_2 is injective, therefore also f_4, and finally f_2 is bijective, which finishes the proof.

Remark.

When A is free over $\mathbf{Z}$ (i.e. when A' is a *torus*), one can give a simpler proof of th. 6, based on theorems of Nakayama-Tate type (cf. [145], Chap. IX).

§6. Algebraic number fields

In this section, k is an *algebraic number field*, i.e. a finite extension of $\mathbf{Q}$. A place of k is an equivalence class of absolute values of k; the set of places is denoted V. If $v \in V$, the completion of k for the topology defined by v is written k_v; if v is archimedean, k_v is isomorphic to $\mathbf{R}$ or $\mathbf{C}$; if v is ultrametric, k_v is a p-adic field.

6.1 Finite modules – definition of the groups $P^i(k, A)$

Let A be a finite G_k-module. The base change $k \to k_v$ enables us to define the cohomology groups $H^i(k_v, A)$. [When v is an archimedean place, we shall make the convention that $H^0(k_v, A)$ denotes the 0-th *modified* cohomology group (cf. [145], Chap. VIII, §1) of the finite group G_{k_v} with values in A. If, for example, v is complex, we have $H^0(k_v, A) = 0$.]

From §1.1, we have canonical homomorphisms:

$$H^i(k, A) \longrightarrow H^i(k_v, A) \ .$$

These homomorphisms can be interpreted in the following way:

Let w be an extension of v to $\overline{k}$, and let D_w be the corresponding decomposition group (we have $s \in D_w$ if and only if $s(w) = w$). Denote by $\overline{k}_w$ the union of the completions of the finite subextensions of $\overline{k}$ [beware: *this is not* the completion of $\overline{k}$ for w, cf. exerc. 1]; one easily proves that $\overline{k}_w$ is an algebraic closure of k_v, and that its Galois group is D_w. We may thus identify $H^i(k_v, A)$ with $H^i(D_w, A)$, and the homomorphism

$$H^i(k, A) \longrightarrow H^i(k_v, A)$$

then becomes simply the *restriction* homomorphism:

$$H^i(G_k, A) \longrightarrow H^i(D_w, A) \ .$$

The family of homomorphisms $H^i(k, A) \to H^i(k_v, A)$ defines a homomorphism $H^i(k, A) \to \prod H^i(k_v, A)$. In fact, the direct product may be replaced by a smaller subgroup. More precisely, let K/k be a finite Galois extension of k such that G_k acts trivially on A, and let S be a finite set of places in k containing all the archimedean places and all the places which ramify in K. It is easy to see that, for $v \notin S$, the G_{k_v}-module A is *unramified* in the sense of §5.5, and

the subgroups $H^i_{nr}(k_v, A)$ are well defined. Let $P^i(k, A)$ be the subgroup of the product $\prod_{v \in V} H^i(k_v, A)$ consisting of the families (x_v) such that x_v belongs to $H^i_{nr}(k_v, A)$ for almost all $v \in V$. We have:

Proposition 21. *The canonical homomorphism $H^i(k, A) \to \prod H^i(k_v, A)$ maps $H^i(k, A)$ into $P^i(k, A)$.*

Indeed, every element x of $H^i(k, A)$ comes from an element $y \in H^i(L/k, A)$, where L/k is a suitable finite Galois extension. If T denotes the union of S and the set of places of k which are ramified in L, it is clear that the image x_v of x in $H^i(k_v, A)$ belongs to $H^i_{nr}(k_v, A)$ for all $v \notin T$, from which the proposition follows.

We shall denote by $f_i : H^i(k, A) \to P^i(k, A)$ the homomorphism defined by the preceding proposition. By prop. 18 of §5.5, we have:

$$P^0(k, A) = \prod H^0(k_v, A) \qquad \text{(direct product)},$$

$$P^2(k, A) = \coprod H^2(k_v, A) \qquad \text{(direct sum)}.$$

As for the group $P^1(k, A)$, Tate suggests denoting it by $\prod H^1(k_v, A)$, to emphasize that it is intermediate between a product and a sum.

The groups $P^i(k, A)$, $i \geq 3$, are simply the (finite) products of the $H^i(k_v, A)$, where v runs over the set of *real* archimedean places of k. In particular, we have $P^i(k, A) = 0$ for $i \geq 3$ if k is totally imaginary, or if A is of odd order.

Remark.

The map f_0 is obviously injective, and Tate has proved (cf. §6.3) that the f_i, $i \geq 3$, are bijective. In contrast, f_1 and f_2 are not necessarily injective (cf. Chap. III, §4.7).

Exercises.

1) Let w be an ultrametric place of the algebraic closure $\overline{k}$ of k. Show that the field $\overline{k}_w$ defined above is not complete [notice that it is a countable union of closed subspaces without interior point, and apply Baire's theorem]. Show that the completion of $\overline{k}_w$ is algebraically closed.

2) Define the $P^i(k, A)$ for negative i. Show that the system of $\{P^i(k, A)\}_{i \in \mathbf{Z}}$ forms a cohomological functor in A.

6.2 The finiteness theorem

The groups $P^i(k, A)$ defined in the preceding § can be given a natural *locally compact group topology* (a special case of the notion of a "restricted product" due to Braconnier): one takes as a neighborhood base of 0 the subgroups $\prod_{v \notin T} H^i_{nr}(k_v, A)$, where T runs over the set of finite subsets of V containing S. For $P^0(k, A) = \prod H^0(k_v, A)$, we get the *product* topology, which makes $P^0(k, A)$ a *compact* group. For $P^1(k, A) = \prod H^1(k_v, A)$ we get a locally compact group topology; for $P^2(k, A) = \coprod H^2(k_v, A)$, we get the *discrete* topology.

Theorem 7. *The canonical homomorphism*

$$f_i : H^i(k, A) \longrightarrow P^i(k, A)$$

is a proper map, when $H^i(k, A)$ is given the discrete topology, and $P^i(k, A)$ the topology defined above (i.e. the inverse image by f_i of a compact subset of $P^I(k, A)$ is *finite*).

We shall only prove this theorem for $i = 1$. The case $i = 0$ is trivial, and the case $i \geq 2$ follows from more precise results of Tate and Poitou which will be given in the next section.

Let T be a subset of V containing S, and let $P_T^1(k, A)$ be the subgroup $P_1(k, A)$ formed by the elements (x_v) such that $x_v \in H^1_{nr}(k_v, A)$ for all $v \notin T$. It is obvious that $P_T^1(k, A)$ is compact, and that conversely any compact subset of $P^1(k, A)$ is contained in one of the $P_T^1(k, A)$. It will therefore be enough to prove that the inverse image X_T of $P_T^1(k, A)$ in $H^1(k, A)$ is *finite*. By definition, an element $x \in H^1(k, A)$ belongs to X_T if and only if it is unramified outside T. Let us denote, as above, by K/k a finite Galois extension of k such that G_K acts trivially on A, and let T' be the set of places of K which extend the places of T. One can easily see that the image of X_T in $H^1(k, A)$ consists of the elements unramified outside T; since the kernel of $H^1(k, A) \to H^1(K, A)$ is finite, we are therefore led to showing that these elements are in finite number. So (up to replacing k with K), *we can assume that G_k acts trivially* on A. Therefore we have $H^1(k, A) = \mathrm{Hom}(G_k, A)$. If $\varphi \in \mathrm{Hom}(G_k, A)$, denote the extension of k corresponding to the kernel of φ by $k(\varphi)$; it is an abelian extension, and φ defines an isomorphism of the Galois group $\mathrm{Gal}(k(\varphi)/k)$ onto a subgroup of A. To say that φ is unramified outside T means that the extension $k(\varphi)/k$ is unramified outside T. Since the extensions $k(\varphi)$ are of bounded degree, the finiteness theorem we want is a consequence of the following more precise result:

Lemma 6. *Let k be an algebraic number field, and r an integer, and let T be a finite set of places of k. There exist only finitely many extensions of degree r of k which are unramified outside T.*

We reduce immediately to the case $k = \mathbf{Q}$. If E is an extension of $\mathbf{Q}$ of degree r unramified outside T, the discriminant d of E over $\mathbf{Q}$ is only divisible by prime numbers p belonging to T. In addition, the exponent of p in d is bounded (this follows, for instance, from the fact that there only exist a finite number of extensions of the local field $\mathbf{Q}_p$ which are of degree $\leq r$, cf. Chap. III, §4.2; see also [145], p. 67). Therefore there are only finitely many possible discriminants d. Since there exist only a finite number of number fields with a given discriminant (Hermite's theorem), this proves the lemma.

6.3 Statements of the theorems of Poitou and Tate

Retain the previous notations, and set $A' = \mathrm{Hom}(A, \mathbf{G}_m)$. The duality theorem for the local case, together with prop. 19 in §5.5, implies that $P^0(k, A)$ *is dual*

to $P^2(k, A')$ and $P^1(k, A)$ is dual to $P^1(k, A')$ [one has to be careful with the archimedean places – this works because of the convention made at the start of §6.1.].

The following three theorems are more difficult. We just state them without proof:

Theorem A. *The kernel of $f_1 : H^1(k, A) \to \prod H^1(k_v, A)$ and the kernel of $f_2' : H^2(k, A') \to \coprod H^2(k_v, A')$ are duals of each other.*

Note that this statement, applied to the module A', implies that the kernel of f_2 is finite; the case $i = 2$ of th. 7 follows immediately from that.

Theorem B. *For $i \geq 3$, the homomorphism*

$$f_i : H^i(k, A) \longrightarrow \prod H^i(k_v, A)$$

is an isomorphism.

[Of course, in the product, v runs through the real places of k, i.e. such that $k_v = \mathbf{R}$.]

Theorem C. *We have an exact sequence:*

$$\begin{array}{ccccccccc}
0 \to & H^0(k, A) & \to \prod H^0(k_v, A) & \to H^2(k, A')^* & \to & H^1(k, A) & \searrow & & \\
& \text{(finite)} & \text{(compact)} & \text{(compact)} & & \text{(discrete)} & & \prod H^1(k_v, A) & \\
& & & & & & & \swarrow \text{(loc. compact)} & \\
0 \leftarrow & H^0(k, A')^* & \leftarrow \coprod H^2(k_v, A) & \leftarrow H^2(k, A) & \leftarrow & H^1(k, A')^* & & &
\end{array}$$

$$\begin{array}{cccc}
\text{(finite)} & \text{(discrete)} & \text{(discrete)} & \text{(compact)}
\end{array}$$

All the homomorphisms occurring in this sequence are continuous.

(Here, G^* is the dual – in Pontryagin's sense – of the locally compact group G.)

These theorems are given in Tate's Stockholm lecture [171], with brief hints of proofs. Other proofs, due to Poitou, can be found in the 1963 Lille Seminar, cf. [126]. See also Haberland [65] and Milne [116].

Bibliographic remarks for Chapter II

The situation is the same as for Chapter I: almost all the results are due to Tate. The only paper published by Tate on this subject is his Stockholm lecture [171], which contains lots of results (many more than it has been possible to discuss here), but very few proofs. Fortunately, the proofs in the local case were worked out by Lang [97]; and others can be found in a lecture by Douady at the Bourbaki Seminar [47].

Let us also mention:

1) The notion of "cohomological dimension" (for the Galois group G_k of a field k) was introduced for the first time by Grothendieck, in connection with his study of "Weil cohomology." Prop. 11 in §4.2 is due to him.

2) Poitou obtained the results of §6 at about the same time as Tate. He lectured on his proofs (which seem different from those of Tate) in the Lille Seminar [126].

3) Poitou and Tate were both influenced by the results of Cassels on the Galois cohomology of elliptic curves, cf. [26].

Appendix.
Galois cohomology of purely transcendental extensions

[The following text reproduces, with minor changes, the *résumé de cours* published in *l'Annuaire du Collège de France*, 1991–1992, pp. 105–113.]

The course had two parts.

1. Cohomology of $k(T)$

The results are essentially known, and due to Faddeev [50], Scharlau [138], Arason [3], Elman [49], ... They may be summarized as follows:

§ 1. An exact sequence

Let G be a profinite group, N a closed normal subgroup of G, Γ the quotient G/N, and C a discrete G-module on which N acts trivially (i.e. a Γ-module). Let us make the hypothesis:

$$H^i(N, C) = 0 \quad \textit{for all } i > 1. \tag{1.1}$$

The spectral sequence $H^\bullet(\Gamma, H^\bullet(N, C)) \Rightarrow H^\bullet(G, C)$ therefore degenerates into an exact sequence:

$$\cdots \longrightarrow H^i(\Gamma, C) \longrightarrow H^i(G, C) \xrightarrow{r} H^{i-1}(\Gamma, \mathrm{Hom}(N, C)) \longrightarrow H^{i+1}(\Gamma, C) \longrightarrow \cdots \tag{1.2}$$

The homomorphism $r : H^i(G, C) \to H^{i-1}(\Gamma, \mathrm{Hom}(N, C))$ in (1.2) is defined in the following way (cf. Hochschild-Serre [72], Chap. II):

If α is an element of $H^i(G, C)$, one may represent α by a cocycle $a(g_1, \ldots, g_i)$ which is normalized (i.e. equal to 0 when one of the g_i equals 1), and which only depends on g_1 and the images $\gamma_2, \ldots, \gamma_i$ of $g_2, \ldots, g_i$ in Γ. For given $\gamma_2, \ldots, \gamma_i$, the map of N into C defined by

$$n \mapsto a(n, g_2, \ldots, g_i) \quad (n \in N),$$

is an element $b(\gamma_2, \ldots, \gamma_i)$ of $\mathrm{Hom}(N, C)$ and the $(i-1)$-cochain b thus defined on Γ is a $(i-1)$-cocycle with values in $\mathrm{Hom}(N, C)$; its cohomology class is $r(\alpha)$.

Make the supplementary hypothesis:

(1.3) *The extension* $1 \longrightarrow N \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$ *splits.*

The homomorphism $H^i(\Gamma, C) \to H^i(G, C)$ is therefore injective, and (1.2) reduces to the exact sequence:

$$(1.4) \qquad 0 \longrightarrow H^i(\Gamma, C) \longrightarrow H^i(G, C) \xrightarrow{r} H^{i-1}(\Gamma, \mathrm{Hom}(N, C)) \longrightarrow 0 .$$

§ 2. The local case

If K is a field, let K_s be a separable closure of K, and put $G_K = \mathrm{Gal}(K_s/K)$. If C is a (discrete) G_K-module, one writes $H^i(K, C)$ instead of $H^i(G_K, C)$.

Assume that K is equipped with a *discrete valuation* v, with residue field $k(v)$; denote by K_v the completion of K for v. Let us choose an extension of v to K_s; let D and I be the corresponding decomposition and inertia groups; we have $D \simeq G_{K_v}$ and $D/I \simeq G_{k(v)}$.

Let n be an integer > 0, prime to the characteristic of $k(v)$, and let C be a G_K-module such that $nC = 0$. Let us make the following hypothesis:

(2.1) *C is unramified at v* (i.e. I acts trivially on C).

We may therefore apply the results of §1 to the exact sequence

$$1 \longrightarrow I \longrightarrow D \longrightarrow G_{k(v)} \longrightarrow 1$$

(the hypotheses (1.1) and (1.3) can be checked easily). The $G_{k(v)}$-module $\mathrm{Hom}(I, C)$ can be identified with $C(-1) = \mathrm{Hom}(\mu_n, C)$, where μ_n denotes the group of n-th roots of unity (in $k(v)_s$ or in K_s; it amounts to the same thing). From (1.4) we get the exact sequence:

$$(2.2) \qquad 0 \longrightarrow H^i(k(v), C) \longrightarrow H^i(K_v, C) \xrightarrow{r} H^{i-1}(k(v), C(-1)) \longrightarrow 0 .$$

Assume $\alpha \in H^i(K, C)$ and let α_v be its image (under restriction) in $H^i(K_v, C)$. The element $r(\alpha_v)$ of $H^{i-1}(k(v), C(-1))$ is called the *residue of α at v*, and denoted $r_v(\alpha)$. If it is not zero, we say that *α has a pole at v*. If it is zero, we say that α is *regular* (or "holomorphic") *at v*; in this case, α_v may be identified with an element of $H^i(k(v), C)$, which is called the *value of α at v*, and denoted by $\alpha(v)$.

§ 3. Algebraic curves and function fields in one variable

Let X be a connected smooth projective curve over a field k, and let $K = k(X)$ be the corresponding function field. Let $\underline{X}$ be the set of closed points of the scheme X. An element x of $\underline{X}$ can be identified with a *discrete valuation* of K, which is trivial on k; we use the notation $k(x)$ for the corresponding residue field; it is a finite extension of k.

As above, let n be an integer > 0, which is prime to the characteristic of k, and let C be a G_k-module such that $nC = 0$. The choice of an embedding of k_s into K_s defines a homomorphism $G_K \to G_k$, which allows us to consider C as a G_K-module. For all $x \in \underline{X}$, hypothesis (2.1) is satisfied. If $\alpha \in H^i(K, C)$, we can then speak of the *residue* $r_x(\alpha)$ *of* α *at* x; we have $r_x(\alpha) \in H^{i-1}(k(x), C(-1))$. It can be shown that:

(3.1) *One has* $r_x(\alpha) = 0$ *for all but a finite number of* $x \in \underline{X}$ (i.e., the set of poles of α is finite).

More precisely, let L/K be a finite Galois extension of K which is large enough so that α comes from an element of $H^i(\mathrm{Gal}(L/K), C_L)$, where $C_L = H^0(G_L, C)$. Then $r_x(\alpha) = 0$ for all x at which the ramification index of L/K is prime to n.

(3.2) *There is a "residue formula"*:

$$\sum_{x \in \underline{X}} \mathrm{Cor}_k^{k(x)} r_x(\alpha) = 0 \quad \textit{in } H^{i-1}(k, C(-1)),$$

where $\mathrm{Cor}_k^{k(x)} : H^{i-1}(k(x), C(-1)) \to H^{i-1}(k, C(-1))$ *denotes the corestriction homomorphism relative to the extension* $k(x)/k$.

(Let us clarify what we mean by Cor_E^F if F/E is a finite extension: it is the product of the usual Galois corestriction (corresponding to the inclusion $G_F \to G_E$) with the inseparability degree $[F : E]_i$. The composition $\mathrm{Cor}_E^F \circ \mathrm{Res}_F^E$ equals multiplication by $[F : E]$.)

Application

Suppose $f \in K^*$, and let $D = \sum_{x \in \underline{X}} n_x x$ be the divisor of f. Assume D is disjoint from the set of poles of α. This allows us to define an element $\alpha(D)$ of $H^i(k, C)$ using the formula

$$\alpha(D) = \sum_{x \in |D|} n_x \, \mathrm{Cor}_k^{k(x)} \alpha(x) \ .$$

We deduce from (3.2) the following formula:

$$\alpha(D) = \sum_{x \text{ pole of } \alpha} \mathrm{Cor}_k^{k(x)}(f(x)) \cdot r_x(\alpha) \ , \tag{3.3}$$

where:

$(f(x))$ is the element of $H^1(k(x), \mu_n)$ defined by the element $f(x)$ of $k(x)$, *via* Kummer theory;

$r_x(\alpha) \in H^{i-1}(k(x), C(-1))$ is the residue of α at x;

$(f(x)) \cdot r_x(\alpha)$ is the cup-product of $(f(x))$ and $r_x(\alpha)$ in $H^i(k(x), C)$, relative to the bilinear map $\mu_n \times C(-1) \to C$.

When α has no poles, (3.3) reduces to

$$\alpha(D) = 0 \ ,$$

the cohomological analogue of *Abel's theorem*. This allows us to associate to α a homomorphism of the group of rational points of the Jacobian of X to the group $H^i(k, C)$; for $i = 1$, we are back to the situation studied in the 1956–1957 course, cf. *Groupes Algébriques et Corps de Classes* [144].

§ 4. The case $K = k(T)$

This is the case when X is the projective line $\mathbf{P}_1$. Since X has a rational point, the canonical homomorphism $H^i(k, C) \to H^i(K, C)$ is injective. An element of $H^i(K, C)$ is said to be *constant* if it belongs to $H^i(k, C)$. It can be shown that:

(4.1) *In order that $\alpha \in H^i(K, C)$ be constant, it is necessary and sufficient that $r_x(\alpha) = 0$ for all $x \in \underline{X}$* (i.e., that α have no poles).

(4.2) *For all $x \in \underline{X}$, let ϱ_x be an element of $H^{i-1}(k(x), C(-1))$. Suppose that $\varrho_x = 0$ for all but a finite number of x, and that:*

$$\sum_{x \in \underline{X}} \mathrm{Cor}_k^{k(x)} \varrho_x = 0 \quad \text{in } H^{i-1}(k, C(-1)).$$

Then there exists $\alpha \in H^i(K, C)$ such that $r_x(\alpha) = \varrho_x$ for every $x \in \underline{X}$.

We can sum up (3.1), (3.2), (4.1), and (4.2) by the exact sequence:

$$0 \longrightarrow H^i(k, C) \longrightarrow H^i(K, C) \longrightarrow \bigoplus_{x \in \underline{X}} H^{i-1}(k(x), C(-1)) \longrightarrow$$
$$\longrightarrow H^{i-1}(k, C(-1)) \longrightarrow 0 \ .$$

Remark.

Consider $\alpha \in H^i(K, C)$, and let P_α be the set of its poles. The statements above show that α is determined by its residues and by its value at some rational point of X not contained in P_α. In particular, the *value* of α can be computed from these data. Here is a formula for such a computation, if $\infty \notin P_\alpha$:

$$\alpha(x) = \alpha(\infty) + \sum_{y \in P_\alpha} \mathrm{Cor}_k^{k(y)}(x - y) \cdot r_y(\alpha) \ , \tag{4.3}$$

where

$\alpha(x)$ is the value of α at some rational point $x \in X(k)$, $x \notin P_\alpha$, $x \neq \infty$;

$\alpha(\infty)$ is the value of α at the point ∞;

$(x-y)$ is the element of $H^1(k(y), \mu_n)$ defined by $x-y$;

$(x-y)\cdot r_y(\alpha)$ is the cup-product of $(x-y)$ with the residue $r_y(\alpha)$, computed in $H^i(k(y), C)$;

$\mathrm{Cor}_k^{k(y)}$ is the corestriction: $H^i(k(y), C) \to H^i(k, C)$.

This follows from (3.3), applied to the function $f(T) = x - T$, whose divisor D is $(x) - (\infty)$.

Generalization to several variables

Let $K = k(T_1, \ldots, T_m)$ be the function field of the projective space $\mathbf{P}_m$ of dimension m. Each irreducible divisor W on $\mathbf{P}_m$ defines a discrete valuation v_W of K. The following assertion follows from (4.1) by induction on m:

(4.4) *In order that $\alpha \in H^i(K, C)$ be constant* (i.e. belongs to $H^i(k, C)$), *it is necessary and sufficient that α not have a pole at any valuation v_W* (it is enough to consider the W which are distinct from the hyperplane at infinity, i.e. one may work in m-dimensional *affine space*, and not in projective space).

2. Application: specialization of the Brauer group

§ 5. Notation

The notation is the same as that of §4, with $i = 2$ and $C = \mu_n$, so that $C(-1) = \mathbf{Z}/n\mathbf{Z}$.

We have $H^2(K, C) = \mathrm{Br}_n(K)$, the kernel of multiplication by n in the Brauer group $\mathrm{Br}(K)$. The exact sequence (4.3) can be written:

$$0 \longrightarrow \mathrm{Br}_n(k) \longrightarrow \mathrm{Br}_n(K) \longrightarrow \bigoplus_{x \in \underline{X}} H^1(k(x), \mathbf{Z}/n\mathbf{Z}) \longrightarrow H^1(k, \mathbf{Z}/n\mathbf{Z}) \longrightarrow 0 .$$

It is due to D.K. Faddeev [50].

Consider $\alpha \in \mathrm{Br}_n(K)$, and let $P_\alpha \subset \underline{X}$ be the set of its poles. If $x \in X(k)$ is a rational point of $X = \mathbf{P}_1$, and if $x \notin P_\alpha$, the value of α at x is an element $\alpha(x)$ of $\mathrm{Br}_n(k)$. We are interested in the variation of $\alpha(x)$ with x, and in particular in the set $V(\alpha)$ of x such that $\alpha(x) = 0$ ("*the zero-locus of* α"). One would like to understand the structure of $V(\alpha)$. (For example, if k is infinite, is it true that $V(\alpha)$ is, either empty, or of cardinality equal to that of k?)

The case $n = 2$ and $\alpha = (f, g)$, with $f, g \in K^*$, is particularly interesting, because of its interpretation in terms of *the conic fibering* with base X defined by the homogeneous equation

$$U^2 - f(T)V^2 - g(T)W^2 = 0 .$$

The study of $V(\alpha)$ can be made from several points of view. We consider three of them:

killing α by a rational base change (cf. §6),

Manin conditions and weak approximation (cf. §7),

sieve bounds (cf. §8).

§ 6. Killing by base change

Assume, for simplicity, that k has characteristic 0.

Consider $\alpha \in \mathrm{Br}_n(K)$, with $K = k(T)$ as above. Let $f(T')$ be a rational function in a variable T'; assume f is not constant. If one puts $T = f(T')$, one obtains an embedding of K into $K' = k(T')$. From this, by a base change, one gets an element $f^*\alpha$ of $\mathrm{Br}_n(K')$. We say that α is *killed by* K'/K (or by f) if $f^*\alpha = 0$ in $\mathrm{Br}_n(K')$. If that is so, then $\alpha(t) = 0$ for any $t \in X(k)$ which is not a pole of α, and which is of the form $f(t')$, with $t' \in \mathbf{P}_1(k)$. In particular, $V(\alpha)$ is *not empty* (and has the same cardinality as k). One may ask if there is a converse to this. Whence the following question:

(6.1) *Assume $V(\alpha)$ is not empty. Does there exist a non-constant rational function f which kills α?*

Here is a *base-point* variant of (6.1):

(6.2) *Consider $t_0 \in V(\alpha)$. Does there exist f as in* (6.1)*, such that t_0 is of the form $f(t'_0)$, with $t'_0 \in \mathbf{P}_1(k)$?*

It is known (Yanchevskiĭ [188]) that (6.2) has an affirmative answer if k is local and Henselian or if $k = \mathbf{R}$.

If one does not make any hypotheses on k, one only has results for $n = 2$. To state them, let us introduce the following notation:

$$d(\alpha) = \deg P_\alpha = \sum_{x \in P_\alpha} [k(x) : k] \,. \tag{6.3}$$

(The integer $d(\alpha)$ is the *number of poles* of α, with multiplicities taken into account.)

Theorem 6.4. (Mestre [112]) *The question* (6.2) *has an affirmative answer when $n = 2$ and $d(\alpha) \leq 4$.*

Remarks.

1) The proof of th. 6.4 gives additional information on the field $K' = k(T')$ which kills α; for example, one can choose it so that $[K' : K] = 8$.

2) Mestre has also obtained results in the case $n = 2$, $d(\alpha) = 5$.

Here is a consequence of th. 6.4 (cf. [113]):

Theorem 6.5. *The group* $\mathbf{SL}_2(\mathbf{F}_7)$ *has the property "*Gal_T*", i.e. is the Galois group of a* $\mathbf{Q}$*-regular Galois extension of* $\mathbf{Q}(T)$.

In particular there exists an infinity of Galois extensions of $\mathbf{Q}$, pairwise disjoint, with Galois group $\mathbf{SL}_2(\mathbf{F}_7)$.

There are analogous results for the groups $\widetilde{M}_{12}$, $6\cdot A_6$ and $6\cdot A_7$.

§ 7. Manin conditions, weak approximation and Schinzel's hypothesis

We now suppose that k is an *algebraic number field*, of finite degree over $\mathbf{Q}$. Let Σ be the set of its (archimedean and ultrametric) places; for $v \in \Sigma$, we denote by k_v the completion of k with respect to v. Let $\mathbf{A}$ *be the adèle ring* of k, i.e. the restricted product of the k_v ($v \in \Sigma$).

Let $X(\mathbf{A}) = \prod_v X(k_v)$ be the space of adelic points of $X = \mathbf{P}_1$. It is a compact space. To each element α of $\mathrm{Br}_n(K)$ we associate the subspace $V_{\mathbf{A}}(\alpha)$ defined in the following way:

an adelic point $\mathbf{x} = (x_v)$ belongs to $V_{\mathbf{A}}(\alpha)$ if, for all $v \in \Sigma$, we have $x_v \notin P_\alpha$ and $\alpha(x_v) = 0$ in $\mathrm{Br}_n(k_v)$.

(I.e. $V_{\mathbf{A}}(\alpha)$ is the set of *adelic solutions* of the equation $\alpha(x) = 0$.)

Any solution in k of $\alpha(x) = 0$ is clearly an adelic solution. There is thus an inclusion:

$$V(\alpha) \subset V_{\mathbf{A}}(\alpha) \ ,$$

and one may wonder what is the *closure* of $V(\alpha)$ in $V_{\mathbf{A}}(\alpha)$. To answer (or to try to answer) this question, it is convenient to introduce (following Colliot-Thélène and Sansuc) the "*Manin conditions*":

Let us say that an element β of $\mathrm{Br}_n(K)$ is *subordinate* to α if, for all $x \in \underline{X}$, $r_x(\beta)$ is an integer multiple of $r_x(\alpha)$; one has then $P_\beta \subset P_\alpha$. Let $\mathrm{Sub}(\alpha)$ be the set of such elements; it is a subgroup of $\mathrm{Br}_n(K)$ which contains $\mathrm{Br}_n(k)$, and the quotient $\mathrm{Sub}(\alpha)/\mathrm{Br}_n(k)$ is finite. If $\beta \in \mathrm{Sub}(\alpha)$, and if $\mathbf{x} = (x_v)$ is a point of $V_{\mathbf{A}}(\alpha)$, then $\beta(x_v) = 0$ for almost all v. This allows us to define an element $m(\beta, \mathbf{x})$ of $\mathbf{Q}/\mathbf{Z}$ by the formula:

$$m(\beta, \mathbf{x}) = \sum_v \mathrm{inv}_v\, \beta(x_v) \ , \tag{7.1}$$

where inv_v denotes the canonical homomorphism of $\mathrm{Br}(k_v)$ into $\mathbf{Q}/\mathbf{Z}$. The function

$$\mathbf{x} \mapsto m(\beta, \mathbf{x})$$

is locally constant on $V_{\mathbf{A}}(\alpha)$ and vanishes on $V(\alpha)$; moreover, it only depends on the equivalence class of β mod $\mathrm{Br}_n(k)$. Let us denote by $V_{\mathbf{A}}^M(\alpha)$ the subspace of $V_{\mathbf{A}}(\alpha)$ defined by the "Manin conditions":

$$m(\beta, \mathbf{x}) = 0 \quad \textit{for all } \beta \in \mathrm{Sub}(\alpha). \tag{7.2}$$

It is an *open and closed* subspace of $V_{\mathbf{A}}(\alpha)$ which contains $V(\alpha)$. It seems reasonable to venture the following *conjecture*:

(7.3 ?) *$V(\alpha)$ is dense in $V_{\mathbf{A}}^M(\alpha)$.*

In particular:

(7.4 ?) *If $V_{\mathbf{A}}^M(\alpha) \neq \emptyset$, then $V(\alpha) \neq \emptyset$*: the Manin conditions are "the only ones" preventing the existence of a rational solution to the equation $\alpha(x) = 0$.

(7.5 ?) *If* $\mathrm{Sub}(\alpha) = \mathrm{Br}_n(k)$ (i.e. in the absence of Manin conditions), *$V(\alpha)$ is dense in $V_{\mathbf{A}}(\alpha)$*; we have *weak approximation* : the Hasse principle holds.

Most of the available results about (7.3 ?), (7.4 ?) and (7.5 ?) are for $n = 2$. In the general case, one has the following theorem, which completes earlier results of Colliot-Thélène and Sansuc (1982) and Swinnerton-Dyer (1991), cf. [36], [37]:

Theorem 7.6. *Schinzel's hypothesis* (H) [141] *implies* (7.3 ?).

[Recall the statement of hypothesis (H): Consider polynomials $P_1(T), \ldots, P_m(T)$ with coefficients in $\mathbf{Z}$, irreducible over $\mathbf{Q}$, with dominant terms > 0, and such that, for any prime p, there exists $n_p \in \mathbf{Z}$ such that $P_i(n_p) \not\equiv 0 \pmod{p}$ for $i = 1, \ldots, m$. Then there exist an infinity of integers $n > 0$ such that $P_i(n)$ is a prime for $i = 1, \ldots, m$.]

Remark.

Theorem 7.6 can be extended to *systems of equations* $\alpha_i(x) = 0$, where the α_i are a finite number of elements of $\mathrm{Br}_n(K)$. One replaces $\mathrm{Sub}(\alpha)$ by the set of elements β of $\mathrm{Br}_n(K)$ such that, for $x \in \underline{X}$, $r_x(\beta)$ belongs to the subgroup of $H^1(k(x), \mathbf{Z}/n\mathbf{Z})$ generated by the $r_x(\alpha_i)$.

§ 8. Sieve bounds

Keep the notation above, and suppose (for simplicity) that $k = \mathbf{Q}$. If $x \in X(k) = \mathbf{P}_1(\mathbf{Q})$, denote by $H(x)$ the *height* of x: if $x = p/q$ where p and q are relatively prime integers, then $H(x) = \sup(|p|, |q|)$. If $H \to \infty$, the number of x such that $H(x) \leq H$ is $cH^2 + O(H \cdot \log H)$, with $c = 12/\pi^2$.

Let $N_\alpha(H)$ be the number of $x \in V(\alpha)$ such that $H(x) \leq H$. One would like to know the rate of increase of $N_\alpha(H)$ when $H \to \infty$. A sieve argument [155] gives at least an *upper bound*. To state the result, denote by $e_x(\alpha)$ the order of the residue $r_x(\alpha)$ of α at x (for $x \in \underline{X}$); we have $e_x(\alpha) = 1$ if x is not a pole of α. Let us put

$$\delta(\alpha) = \sum_{x \in \underline{X}} (1 - 1/e_x(\alpha)) \,. \tag{8.1}$$

Theorem 8.2. *One has* $N_\alpha(H) \ll H^2/(\log H)^{\delta(\alpha)}$ *for* $H \to \infty$.

Remark that, if α is not constant, then $\delta(\alpha) > 0$, and the theorem shows that "few" rational points are in $V(\alpha)$.

One can ask whether the upper bound obtained in this way is best possible, under the hypothesis $V(\alpha) \neq \emptyset$. In other words:

(8.2) *Is it true that* $N_\alpha(H) \gg H^2/(\log H)^{\delta(\alpha)}$ *for large enough* H, *if* $V(\alpha) \neq \emptyset$?

(For an encouraging result in this direction, see Hooley [73].)

Remark.

There are analogous statements for number fields, and for systems of equations $\alpha_i(x) = 0$; one then needs to replace $e_x(\alpha)$ by the order of the group generated by the $r_x(\alpha_i)$.

Chapter III

Nonabelian Galois cohomology

§1. Forms

This § is devoted to the illustration of a "general principle", which can be stated roughly as follows:

Let K/k be a field extension, and let X be an "object" defined over k. We shall say that an object Y, defined over k, is a *K/k-form* of X if Y becomes isomorphic to X when the ground field is extended to K. The classes of such forms (for the equivalence relation defined by the k-isomorphisms) form a set $E(K/k, X)$.

If K/k is a Galois extension, there is a bijective correspondence between $E(K/k, X)$ and $H^1(\mathrm{Gal}(K/k), A(K))$ where $A(K)$ denotes the group of K-automorphisms of X.

It would obviously be possible to justify this assertion by defining axiomatically the notions of "object defined over k", of "extension of scalars", and imposing on them some simple requirements. I will not do so, and I will limit myself to special cases: that of vector spaces with tensors, and that of algebraic varieties (or algebraic groups). The reader who is interested in the general case can look into Exposé VI of the Grothendieck Seminar [64], "Catégories fibrées et descente"; see also Giraud [54].

1.1 Tensors

This example is discussed in detail in [145], Chap. X, § 2. Let us quickly recap it:

The "object" is a pair (V, x), where V is a finite-dimensional k-vector space, and x is a tensor over V of a given type (p, q). We therefore have

$$x \in T_q^p(V) = T^p(V) \otimes T^q(V^*) .$$

The notion of k-isomorphism of two objects (V, x) and (V', x') is clear. If K is an extension of k, and if (V, x) is an object defined over k, we obtain an object (V_K, x_K) defined over K by taking for V_K the vector space $V \otimes_k K$ and for x_K the element $x \otimes 1$ of $T_q^p(V_K) = T_q^p(V) \otimes_k K$. This defines the notion of a *K/k-form* of (V, x); we shall denote by $E(K/k)$ the set of these forms (up to isomorphism). Suppose moreover that K/k is a Galois extension, and let $A(K)$ be the group of K-automorphisms of (V_K, x_K); if $s \in \mathrm{Gal}(K/k)$ and $f \in A(K)$, let us define ${}^s f \in A(K)$ by the formula:

$$ {}^s f = (1 \otimes s) \circ f \circ (1 \otimes s^{-1}) .$$

[If f is represented by a matrix (a_{ij}), ${}^s f$ is represented by the matrix $({}^s a_{ij})$.] We thus obtain a $\mathrm{Gal}(K/k)$-group structure on $A(K)$, and the cohomology set $H^1(\mathrm{Gal}(K/k), A(K))$ is well defined.

Now let (V', x') be a K/k-form of (V, x). The set P of isomorphisms of (V'_K, x'_K) onto (V_K, x_K) is a principal homogeneous space over $A(K)$, and defines therefore an element p of $H^1(\mathrm{Gal}(K/k), A(K))$, cf. Chap. I, §5.2. By making p correspond to (V', x') we get a canonical map

$$\theta : E(K/k) \longrightarrow H^1(\mathrm{Gal}(K/k), A(K)) .$$

Proposition 1. *The map θ defined above is bijective.*

The proof is given in [145], *loc. cit.* The injectivity is trivial, and the surjectivity follows from the following lemma:

Lemma 1. *For any integer n, we have $H^1(\mathrm{Gal}(K/k), \mathbf{GL}_n(K)) = 0$.*

(For $n = 1$ we recover the well-known "Theorem 90".)

Remark.

The group $A(K)$ is in fact defined for any commutative k-algebra K; it is the group of K-points of a certain algebraic subgroup A of $\mathbf{GL}(V)$. From a matrix point of view, one gets equations for A by writing down explicitly the equation $T_q^p(f)x = x$ [note that the algebraic group A defined in this way is not necessarily "smooth" over k (as a scheme) — its structure sheaf may have nonzero nilpotent elements (cf. §1.2, exerc. 2)]. According to the conventions of Chap. II, §1, we shall write $H^1(K/k, A)$ instead of $H^1(\mathrm{Gal}(K/k), A(K))$. When $K = k_s$, we simply write $H^1(k, A)$.

The above proposition only allows us to study *Galois extensions*. The next one often allows us to reduce to such a case.

Proposition 2. *Let $\mathfrak{g}$ be the Lie subalgebra of $\mathfrak{gl}(V)$ consisting of the elements which leave x invariant* (in the infinitesimal sense — cf. Bourbaki, LIE I, §3). *In order that the algebraic group A of automorphisms of (V, x) be smooth over k, it is necessary and sufficient that its dimension equal that of $\mathfrak{g}$. If this condition is fulfilled, every K/k-form of (V, x) is also a k_s/k-form.*

Let L be the local ring of A at the identity, and let $\mathfrak{m}$ be the maximal ideal of L. The Lie algebra $\mathfrak{g}$ is the dual of $\mathfrak{m}/\mathfrak{m}^2$.

Since $\dim(A) = \dim(L)$, the equality $\dim(\mathfrak{g}) = \dim(A)$ means that L is a regular local ring, i.e. that A is smooth over k at the identity (therefore everywhere, by translation). That proves the first assertion. Now let (V', x') be a K/k-form of (V, x), and let P be the k-variety of the isomorphisms of (V', x') onto (V, x) [we leave to the reader the task of defining this in functorial terms — or using explicit equations]; the fact that (V', x') and (V, x) are K-isomorphic shows that $P(K)$ is not empty. Hence P_K and A_K are K-isomorphic; in particular P_K is smooth over K, and it follows that P is smooth over k. By an elementary result from algebraic geometry, the points of P with values in k_s are dense in P. The existence of at least one such point is enough to ensure that (V, x) and (V', x') are k_s-isomorphic, QED.

1.2 Examples

a) Take for tensor x a non-degenerate alternating bilinear form. The group A is the symplectic group $\mathbf{Sp}$ associated with this form. On the other hand, the elementary theory of alternating forms shows that all forms of x are trivial (i.e. isomorphic to x). Whence:

Proposition 3. *For any Galois extension K/k, one has $H^1(K/k, \mathbf{Sp}) = 0$.*

b) Assume that the characteristic is not equal to 2, and take for x a non-degenerate symmetric form. The group A is the *orthogonal* group $\mathbf{O}(x)$ defined by x. We conclude from this:

Proposition 4. *For any Galois extension K/k, the set $H^1(K/k, \mathbf{O}(x))$ is in bijective correspondence with the set of quadratic forms defined over k which are K-equivalent to x.*

In characteristic 2, one must replace the symmetric bilinear form by a quadratic form, which makes it necessary to give up the context of tensor spaces (cf. exercise 2).

c) Take for x a tensor of type $(1,2)$, or, which amounts to the same thing, an *algebra* structure on V. The group A is therefore the automorphism group of this algebra, and $\mathfrak{g}$ the Lie algebra of its *derivations*. When $V = \mathbf{M}_n(k)$, the K/k-forms of V are just the central simple algebras of rank n^2 over k, split by K; the group A can be identified with the projective group $\mathbf{PGL}_n(k)$, and one obtains in this way an interpretation of $H^1(K/k, \mathbf{PGL}_n)$ in terms of central simple algebras, cf. [145], Chap. X, §5.

Exercises.

1) Show that every derivation of $\mathbf{M}_n(k)$ is inner. Use this fact, combined with prop. 2, to recover the theorem according to which every central simple algebra has a splitting field which is Galois over the ground field.

2) Let V be a vector space over a field of characteristic 2, let F be a quadratic form over V, and let b_F be the associated bilinear form. Show that the Lie algebra $\mathfrak{g}$ of the orthogonal group $\mathbf{O}(F)$ consists of the endomorphisms u of V such that $b_F(a, u(a)) = 0$ for all a. Compute the dimension of $\mathfrak{g}$ assuming that the form b_F is nondegenerate (which implies $\dim V \equiv 0 \bmod 2$); conclude the smoothness of the group $\mathbf{O}(F)$ in this case. Does this result remain true when b_F is degenerate?

1.3 Varieties, algebraic groups, etc.

We now choose for "object" an *algebraic variety* (resp. an algebraic group, resp. an algebraic homogeneous space over an algebraic group). If V is such a variety, defined over a field k, and if K is an extension of k, we denote by $A(K)$ the group of K-automorphisms of V_K (viewed as an algebraic variety, resp. as an

algebraic group, resp. as a homogeneous space). We thus get a *functor* Aut_V satisfying the hypotheses of Chap. II, §1.

Now let K/k be a Galois extension of k, and let V' be a K/k-form of V. The set P of K-isomorphisms of V'_K over V_K is obviously a principal homogeneous space over the $\mathrm{Gal}(K/k)$-group $A(K) = \mathrm{Aut}_V(K)$. This gives, as in §1.1, a canonical map

$$\theta : E(K/k, V) \longrightarrow H^1(K/k, \mathrm{Aut}_V) .$$

Proposition 5. *The map θ is injective. If V is quasiprojective, it is bijective.*

The injectivity of θ is trivial. To establish its surjectivity (when V is quasiprojective), one applies Weil's method of " descent". This means the following:

Assume, for simplicity, that K/k is finite, and let $c = (c_s)$ be a 1-cocycle of $\mathrm{Gal}(K/k)$ in $\mathrm{Aut}_V(K)$. Combining c_s with the automorphisms $1 \otimes s$ of V_K, we get an action of the group $\mathrm{Gal}(K/k)$ on V_K; the quotient variety

$$_cV = (V_K)/\mathrm{Gal}(K/k)$$

is therefore a K/k-form of V [the quotient exists because V is quasiprojective]. One says that $_cV$ is obtained *by twisting V with the cocycle c* (this terminology is clearly compatible with that in Chap. I, §5.3). It is easy to see that the image of $_cV$ by θ is equal to the cohomology class of c; whence the surjectivity of θ.

Corollary. *If V is an algebraic group, the map θ is bijective.*

Indeed, it is known that every group variety is quasiprojective.

Remarks.

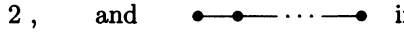
1) It follows from prop. 5 that two varieties V and W having *the same automorphisms functor* have K/k-forms which correspond *bijectively* to each other (K being a Galois extension of k). Examples:

octonion algebras	$\Longleftrightarrow$	simple groups of type G_2
central simple algebras of rank n^2	$\Longleftrightarrow$	Severi-Brauer varieties of dimension $n-1$
semisimple algebras with involution	$\Longleftrightarrow$	classical groups with trivial center

2) The functor Aut_V *is not always representable* (in the category of k-schemes); furthermore, even if it is representable, it may happen that the scheme which represents it is not of finite type over k, i.e. does not define an "algebraic group" in the usual sense of the term.

1.4 Example: the k-forms of the group $\mathbf{SL}_n$

We assume $n \geq 2$. The group $\mathbf{SL}_n$ is a simply connected split semisimple group whose root system is irreducible and of type (A_{n-1}). The corresponding Dynkin diagram is:

• if $n = 2$, and  if $n \geq 3$.

Its automorphism group is of order 1 if $n = 2$ and of order 2 if $n \geq 3$. That implies that the group $\mathrm{Aut}(\mathbf{SL}_n)$ is connected if $n = 2$, and has two connected components if $n \geq 3$. It is convenient to separate these two cases:

The case $n = 2$

We have $\mathrm{Aut}(\mathbf{SL}_2) = \mathbf{SL}_2/\mu_2 = \mathbf{PGL}_2$. But this group is also the automorphism group of the matrix algebra $\mathbf{M}_2$. Hence (cf. Remark 1 in §1.3) *the k-forms of $\mathbf{SL}_2$ and of $\mathbf{M}_2$ are in bijective correspondence.* However, those of $\mathbf{M}_2$ are the central simple algebras of rank 4 over k, i.e. the *quaternion algebras.* In this way we obtain a correspondence:

$$k\text{-forms of } \mathbf{SL}_2 \iff \text{quaternion algebras over } k\ .$$

More explicitly:

a) If D is a quaternion algebra over k, one associates to it the group $\mathbf{SL}_D$ (cf. §3.2), which is a k-form of $\mathbf{SL}_2$; the rational points of this group can be identified with the elements of D with reduced norm 1.

b) If L is a k-form of $\mathbf{SL}_2$, one may show (using, for example, Tits' general results [179]) that L has a k-linear representation

$$\varrho_2 : L \longrightarrow \mathbf{GL}_V\ ,$$

of dimension 4, which is k_s-isomorphic to two copies of the standard representation of $\mathbf{SL}_2$; moreover, this representation is unique, up to isomorphism. The commutant $D = \mathrm{End}^G(V)$ of ϱ_2 is the quaternion algebra corresponding to L. (When k is of characteristic 0, one finds other descriptions of D, based on the Lie algebra of L, in Bourbaki LIE VIII, §1, exerc. 16 and 17.)

The case $n \geq 3$

The group $\mathrm{Aut}(\mathbf{SL}_n)$ is generated by its identity component $\mathbf{PGL}_n$ and by the outer automorphism $x \mapsto {}^t x^{-1}$ (recall that ${}^t x$ denotes the transpose of a matrix x).

Consider now the algebra $\mathbf{M}_n^2 = \mathbf{M}_n \times \mathbf{M}_n$, equipped with the involution

$$(x, y) \mapsto (x, y)^* = ({}^t y, {}^t x)\ .$$

We can embed $\mathbf{GL}_n$ into the multiplicative group of $\mathbf{M}_n^2$ by $x \mapsto (x, {}^t x^{-1})$, and we obtain the group of elements u of $\mathbf{M}_n^2$ such that $u \cdot u^* = 1$. *A fortiori*, this gives an embedding of $\mathbf{SL}_n$. Moreover, these embeddings give identifications

$$\mathrm{Aut}(\mathbf{GL}_n) = \mathrm{Aut}(\mathbf{SL}_n) = \mathrm{Aut}(\mathbf{M}_n^2, *)\ ,$$

where $\mathrm{Aut}(\mathbf{M}_n^2, *)$ denotes the automorphism group of the algebra with involution $(\mathbf{M}_n^2, *)$.

Arguing as in the case $n = 2$, we see that *the k-forms of $\mathbf{SL}_n$* (as well as those of $\mathbf{GL}_n$) *correspond to the algebras with involution $(D, *)$ having the following properties*:

(i) *D is semisimple and $[D : k] = 2n^2$.*

(ii) *The center K of D is an étale k-algebra of rank* 2, i.e. $k \times k$, or a separable quadratic extension of k.

(iii) *The involution $*$ is "of second kind"*, i.e. it induces on K the unique nontrivial automorphism of K.

More precisely, the k-form of $\mathbf{GL}_n$ associated to $(D, *)$ is *the unitary group* $\mathbf{U}_D$; its k-points are the elements u of D such that $u \cdot u^* = 1$. As for the k-form of $\mathbf{SL}_n$, it is *the special unitary group* $\mathbf{SU}_D$; its k-points are the elements u of D such that $u \cdot u^* = 1$ and $\mathrm{Nrd}(u) = 1$, where $\mathrm{Nrd} : D \to K$ denotes the reduced norm.

We have an exact sequence:

$$1 \longrightarrow \mathbf{SU}_D \longrightarrow \mathbf{U}_D \xrightarrow{\mathrm{Nrd}} \mathbf{G}_m^{\varepsilon} \longrightarrow 1 \ ,$$

where $\mathbf{G}_m^{\varepsilon}$ denotes the group $\mathbf{G}_m$ *twisted* by the character $\varepsilon : G_k \to \{\pm 1\}$ associated with the quadratic algebra K/k. (Alternative definition of ε: it gives the action of the Galois group G_k on the Dynkin diagram.)

Two special cases deserve to be mentioned explicitly:

a) *Inner forms.* Here $K = k \times k$, i.e. $\varepsilon = 1$. The involutory algebra $(D, *)$ decomposes into $D = \Delta \times \Delta^0$, where Δ is a central simple algebra of rank n^2, Δ^0 is the opposite algebra, and the involution is $(x, y) \mapsto (y, x)$. The corresponding group $\mathbf{SU}_D$ is just $\mathbf{SL}_\Delta$, cf. §3.2. Notice that Δ and Δ^0 give isomorphic groups.

b) *The hermitian case.* It is the case when K is a field, and D is a matrix algebra $\mathbf{M}_n(K)$. One checks easily that the involution $*$ is of the form

$$x \mapsto q \cdot {}^t\bar{x} \cdot q^{-1} \ ,$$

where $\bar{x}$ is the conjugate of x under the involution of K, and q is an *invertible hermitian element* of $\mathbf{M}_n(K)$, defined up to multiplication by an element of k^*. The k-form of $\mathbf{SL}_n$ associated to $(D, *)$ is just *the special unitary group* $\mathbf{SU}_q$ defined by q (considered as a hermitian form over K). Its rational k-points are the elements u of $\mathbf{GL}_n(K)$ satisfying:

$$q = u \cdot q \cdot {}^t\bar{u} \qquad \text{and} \qquad \det(u) = 1 \ .$$

Remark.

There are analogous results for the other classical groups, cf. Weil [184] and Kneser [87] (if the characteristic is $\neq 2$), and Tits [178] (if the characteristic is 2).

Exercises.

1) Show that the automorphism $x \mapsto {}^t x^{-1}$ of $\mathbf{SL}_2$ coincides with the inner automorphism defined by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

2) Show that $\mathrm{Aut}(\mathbf{GL}_2) = \{\pm 1\} \times \mathrm{Aut}(\mathbf{SL}_2)$. Deduce the classification of k-forms of $\mathbf{GL}_2$.

3) The automorphism group of the projective line $\mathbf{P}_1$ is $\mathbf{PGL}_2$. Deduce from this that the k-forms of $\mathbf{P}_1$ (i.e. the absolutely irreducible smooth projective curves of genus 0) correspond to the k-forms of $\mathbf{SL}_2$ as well as to the quaternion algebras over k.

If k is of characteristic $\neq 2$, this correspondence associates to the quaternion algebra $i^2 = a$, $j^2 = b$, $ij = -ji$, the conic in $\mathbf{P}_2$ with the homogeneous equation $Z^2 = aX^2 + bY^2$.

If k is of characteristic 2, the quaternion algebra defined by $i^2 + i = a$, $j^2 = b$, $jij^{-1} = i + 1$, corresponds to the conic with the equation

$$X^2 + XY + aY^2 + bZ^2 = 0 \qquad (a \in k,\ b \in k^*\ ;\ \text{cf. Chap. II, §2.2}).$$

§2. Fields of dimension ≤ 1

Unless explicit mention to the contrary, the ground field k is supposed to be *perfect.*

We use the name "algebraic group" for group schemes over k which are *smooth of finite type* (these are essentially the "algebraic groups" according to Weil, except that we do not assume they are connected).

If A is such a group, we write $H^1(k, A)$ instead of $H^1(\overline{k}/k, A)$, where $\overline{k}$ denotes an algebraic closure of k, cf. §1.1.

2.1 Linear groups: summary of known results

(References: Borel [16], Borel-Tits [20], Chevalley [34], Demazure-Gabriel [41], Demazure-Grothendieck [42], Platonov-Rapinchuk [125], Rosenlicht [129], Steinberg [166], Tits [177].)

An algebraic group L is called *linear* if it is isomorphic to a subgroup of some $\mathbf{GL}_n$; this amounts to saying that the algebraic variety underlying L is *affine.*

A linear group U is said to be *unipotent* if, when it is embedded in $\mathbf{GL}_n$, all its elements are unipotent (this does not depend on the chosen embedding). For that, it is necessary and sufficient that U have a composition sequence whose successive quotients are isomorphic to the additive group $\mathbf{G}_a$ or to the group $\mathbf{Z}/p\mathbf{Z}$ (in characteristic p). These groups are not of much interest from a cohomological point of view. Indeed:

Proposition 6. *If U is a connected unipotent linear group, we have*

$$H^1(k, U) = 0 \ .$$

[This does not extend to the case of a ground field which is not perfect, cf. exerc. 3.]

This follows from the fact that $H^1(k, \mathbf{G}_a) = 0$ (Chap. II, Prop. 1).

A linear group T is called a *torus* if it is isomorphic (over $\overline{k}$) to a product of multiplicative groups. Such a group is determined up to isomorphism by its *character group* $X(T) = \mathrm{Hom}(T, \mathbf{G}_m)$, which is a free $\mathbf{Z}$-module of finite rank on which $\mathrm{Gal}(\overline{k}/k)$ acts continuously.

Every solvable connected linear group R has a largest unipotent subgroup U, which is normal in G. The quotient $T = R/U$ is a torus, and R is the semi-direct product of T and U.

Every linear group L has a largest connected solvable normal subgroup R, called its *radical*. When $R = 1$ and L is connected, we say that L is *semisimple*; in the general case, the identity component $(L/R)_0$ of L/R is semisimple. Thus, every linear group has a composition series whose successive quotients are of the following four types: $\mathbf{G}_a$, a torus, a finite group, a semisimple group.

A subgroup P of L is called *parabolic* when L/P is a *complete* variety; if P is, moreover, solvable and connected, one says that P is a *Borel subgroup* of L. Every parabolic subgroup contains the radical R of L.

Assume that k is algebraically closed, and L connected. The Borel subgroups B of L can be characterized as either:

a) a maximal connected solvable subgroup of L.

b) a minimal parabolic subgroup of L.

Moreover, the Borel subgroups are conjugate to each other, and equal to their normalizers. [Note that, if k is not algebraically closed, there may not be any Borel subgroup of L which is defined over k — cf. §2.2.]

A subgroup C of a linear group L is called a *Cartan subgroup* if it is nilpotent and equal to the identity component of its normalizer. There exists at least one Cartan subgroup defined over k, and these subgroups are conjugate (over $\bar{k}$, but not in general over k). When L is semisimple, the Cartan subgroups are nothing else than the *maximal tori*.

Exercises.

1) Let L be a connected reductive group, and P a parabolic subgroup of L. Show that the map $H^1(k, P) \to H^1(k, L)$ is injective.

[It is known, cf. Borel-Tits [20], th. 4.13, that $L(k)$ acts transitively on the k-points of the homogeneous space L/P. This implies (Chap. I, prop. 36), that the kernel of $H^1(k, P) \to H^1(k, L)$ is trivial. Conclude with a twisting argument.]

2) (after J. Tits) Let B and C be algebraic subgroups of a linear group D, and let $A = B \cap C$. Assume that the Lie algebras of A, B, C and D satisfy the conditions:

$$\operatorname{Lie} A = \operatorname{Lie} B \cap \operatorname{Lie} C \quad \text{and} \quad \operatorname{Lie} B + \operatorname{Lie} C = \operatorname{Lie} D \ .$$

It follows that $B/A \to D/C$ is an open immersion.

We assume that $D(k)$ is dense in the Zariski topology (this is so if D is connected, and k infinite and perfect).

(a) Show that the kernel of $H^1(k, B) \to H^1(k, D)$ is contained in the image of $H^1(k, A) \to H^1(k, B)$.

[If $b \in Z^1(k, B)$ is a coboundary in D, and if one twists the inclusion $B/A \to D/C$ by b, one finds ${}_b(B/A) \to {}_b(D/C) = D/C$. Since the rational points of D/C are dense, the open subset ${}_b(B/A)$ of ${}_b(D/C)$ contains a rational point. Conclude by using prop. 36 of Chap. I.]

(b) Same assertion, but with B replaced by C.

(c) Deduce from this that, if $H^1(k, A) = 0$, the kernel of $H^1(k, B) \to H^1(k, D)$ is trivial. In particular, if $H^1(k, A)$ and $H^1(k, D)$ are both 0, the same is true of $H^1(k, B)$ and of $H^1(k, C)$.

3) Let k_0 be a field of characteristic p, and let $k = k_0((t))$ be the field of formal power series in one variable over k_0. It is not a perfect field; if k_0 is algebraically closed, it is a field of dimension ≤ 1 (it is even a (C_1) field, cf. Chap. II, §3.2).

Let U be the subgroup of $\mathbf{G}_a \times \mathbf{G}_a$ made up of the pairs (y, z) which satisfy the equation $y^p - y = tz^p$. Show that U is a connected unipotent group of dimension 1, and is smooth over k. Determine $H^1(k, U)$, and show that this group does not reduce to 0 if $p \neq 2$. Prove an analogous result in characteristic 2 using the equation $y^2 + y = tz^4$.

2.2 Vanishing of H^1 for connected linear groups

Theorem 1. *Let k be a field. The following four 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 linear algebraic group L contains a Borel subgroup defined over k.*

Moreover, these properties imply that $\dim(k) \leq 1$ (cf. Chap. II, §3).

(Recall that k is assumed to be perfect.)

We proceed in stages:

(1) (ii) $\Leftrightarrow$ (ii′). This is clear.

(2) (ii′) $\Rightarrow \dim(k) \leq 1$. Let D be a skew field with center a finite extension k' of k, with $[D : k'] = n^2$, $n \geq 2$. Let $\mathbf{SL}_D$ be the corresponding algebraic k'-group (cf. §1.4 and §3.2); it is a semisimple group whose rational k'-points can be identified with the elements of D with reduced norm 1. Let $L = R_{k'/k}(\mathbf{SL}_D)$ be the algebraic k-group derived from this group by restriction of scalars à la Weil (cf. [119], [185]). This group is semisimple and $\neq 1$. If (ii′) holds, it contains a unipotent element $\neq 1$, which is impossible. Thus we have indeed $\dim(k) \leq 1$.

(3) (i′) $\Rightarrow \dim(k) \leq 1$. Let K be a finite extension of k, and let L be an algebraic K-group. Define the group $R_{K/k}(L)$ as above; the $\overline{k}$-points of this group form what we called in Chap. I, §5.8, the *induced group* of $L(\overline{k})$. Thus we have

$$H^1(K, L) = H^1(k, R_{K/k}(L)) \ , \quad \textit{loc. cit.}$$

If L is semisimple, so is $R_{K/k}(L)$, and therefore $H^1(K, L) = 0$, from the hypothesis (i′). Applying this to the group $\mathbf{PGL}_n$ (n arbitrary) we see that the Brauer group of K vanishes, whence $\dim(k) \leq 1$.

(4) $\dim(k) \leq 1 \Rightarrow H^1(k, R) = 0$ *when R is solvable.* The group R is an extension of a torus by a unipotent group. Since the cohomology of the latter

is zero, we are reduced to the case where R is a *torus*, a case treated in [145], p. 170.

(5) (i) $\Leftrightarrow$ (i'). The implication (i) $\Rightarrow$ (i') is clear. Suppose (i') is verified. By (3) and (4), we have $H^1(k, R) = 0$ when R is solvable, whence (i) by using the exact sequence of the H^1.

(6) (i') $\Leftrightarrow$ (ii'). We use the following general lemma:

Lemma 1. *Let A be an algebraic group, H a subgroup of A, and N the normalizer of H in A. Let c be a 1-cocycle of* $\mathrm{Gal}(K/k)$ *with values in $A(\overline{k})$, and let $x \in H^1(k, A)$ be the corresponding cohomology class. Let ${}_cA$ be the algebraic group obtained by twisting A by c* (with A acting on itself by inner automorphisms). *The following two conditions are equivalent:*

(a) *x belongs to the image of $H^1(k, N) \to H^1(k, A)$.*

(b) *The group ${}_cA$ contains a subgroup H' defined over k which is conjugate to H* (over the algebraic closure $\overline{k}$ of k).

This is a simple consequence of prop. 37 in Chap. I, applied to the injection of N into A; one needs only notice that the points of A/N correspond bijectively to the subgroups of A conjugate to H, and similarly for ${}_c(A/N)$.

Let us return to the proof of (i') $\Leftrightarrow$ (ii). If (ii) is true, and if we apply lemma 1 to a Borel subgroup B of the semisimple group L, we see that $H^1(k, B) \to H^1(k, L)$ is surjective. Since from (2) and (4) we have $H^1(k, B) = 0$, it follows that $H^1(k, L)$ vanishes. Conversely, suppose (i') is verified, and let L be a semisimple group. We may assume that the *center* of L is trivial (the center being defined as a group subscheme, which is not necessarily smooth), which we express by saying that L is an *adjoint group*. By Chevalley [42], cf. also [35], there exists a *form* L_d of L which is *split*, and L can be derived from L_d by *torsion* using a class $x \in H^1(k, \mathrm{Aut}(L_d))$. But the structure of the group $\mathrm{Aut}(L_d)$ has been determined by Chevalley; it a semi-direct product $E \cdot L_d$, where E is a finite group, isomorphic to the automorphism group of the corresponding Dynkin diagram. Taking into account hypothesis (i'), we see that $H^1(k, \mathrm{Aut}(L_d))$ may be identified with $H^1(k, E)$. However, the elements of E (identified with a subgroup of $\mathrm{Aut}(L_d)$) leave invariant a Borel subgroup B of L_d; then if N denotes the normalizer of B in $\mathrm{Aut}(L_d)$, we see that

$$H^1(k, N) \longrightarrow H^1(k, \mathrm{Aut}(L_d))$$

is surjective. Applying lemma 1, we deduce that L contains a Borel subgroup defined over k, QED.

Remark.

The semisimple groups with Borel subgroups defined over k are said to be *quasi-split*.

Theorem 2. *When k is of characteristic zero, the four properties of theorem* 1 *are equivalent to the following two assertions:*

(iii) *Every semisimple algebraic group not reduced to the identity contains a unipotent element* $\neq 1$.

(iv) *Every semisimple Lie algebra* $\mathfrak{g} \neq 0$ *contains a nilpotent element* $\neq 0$.

The equivalence of (iii) and (iv) follows from Lie theory. The implication (ii′) $\Rightarrow$ (iii) is trivial. To prove the reverse implication we use induction on the dimension of the semisimple group L. We may assume $L \neq 0$. Let us choose a minimal parabolic subgroup P of L defined over k (cf. Godement [55]), and let R be its radical. The quotient P/R is semisimple and has no unipotent element $\neq 1$. Its dimension is strictly less than that of L since L has at least one unipotent element $\neq 1$ (Godement, *loc. cit.*, th. 9). By the induction hypothesis, we then have $P = R$, which means that P is a Borel subgroup of L.

2.3 Steinberg's theorem

This is the converse of theorem 1:

Theorem 1′. ("Conjecture I" of [146]) *If* k *is perfect and* $\dim(k) \leq 1$, *the properties* (i), ..., (ii′) *of th.* 1 *are verified.*

In particular, we have $H^1(k, L) = 0$ *for every connected linear group* L.

This theorem is due to Steinberg [165]. It was first proved in the following special cases:

a) *When* k *is a finite field* (Lang [96]).

Lang proves a more general result: $H^1(k, L) = 0$ for any connected algebraic group L (not necessarily linear). The proof relies on the surjectivity of the map $x \mapsto x^{-1} \cdot F(x)$, where F is the Frobenius endomorphism of L, cf. Lang, *loc. cit.*

b) *When* L *is solvable, or semisimple of classical type* (the "triality" type D_4 being excluded), *cf.* [146]. The proof uses exerc. 2 below.

c) *When* k *is a* (C_1) *field of characteristic* 0 (Springer [162]).

By th. 2, we see that it is enough to show the nonexistence of a semisimple Lie algebra $\mathfrak{g}$, not equal to 0, all of whose elements are semisimple; we may assume the dimension n of $\mathfrak{g}$ is minimal. Let r be the rank of $\mathfrak{g}$. If $x \in \mathfrak{g}$, the characteristic polynomial $\det(T - \mathrm{ad}(x))$ is divisible by T^r; let $f_r(x)$ be the coefficient of T^r in this polynomial. It is clear that f_r is a polynomial function of degree $n - r$ over $\mathfrak{g}$. Since k is (C_1), it follows that there exists an $x \neq 0$ in $\mathfrak{g}$ such that $f_r(x) = 0$. Let $\mathfrak{c}$ be the centralizer of x in $\mathfrak{g}$; since x is semisimple, the fact that $f_r(x)$ vanishes means that $\dim \mathfrak{c} > r$; since $x \neq 0$, we have $\dim \mathfrak{c} < n$. It is known (cf. Bourbaki, LIE I, §6, no. 5) that $\mathfrak{c}$ is the product of an abelian algebra by a semisimple algebra. By the induction hypothesis, this last reduces to 0; therefore $\mathfrak{c}$ is commutative, whence the inequality $\dim(\mathfrak{c}) \leq r$, and we have a contradiction.

Proof (*of theorem* 1′). This rests on the following result, which is proved by an explicit construction (cf. Steinberg [165], reproduced in Appendix 1):

Theorem 2'. *Assume that L is a quasi-split simply connected semisimple group* (cf. §2.2), *and let C be a conjugacy class of $L(k_s)$ consisting of regular semisimple elements. If C is rational over k* (i.e. stable under the action of G_k), *it contains a point which is rational over k.*

(This assertion is true *over any field* k: one needs neither the hypothesis $\dim(k) \leq 1$, nor the hypothesis that k is perfect, cf. Borel-Springer [19], II.8.6.)

Corollary. *Let L be a quasi-split simply connected semisimple group. For each element x of $H^1(k, L)$ there exists a maximal torus T of L such that x belongs to the image of $H^1(k, T) \to H^1(k, L)$.*

Let us sketch how this corollary can be deduced from th. 2'.

By Lang [96], we can suppose that k is infinite. Let $a = (a_s)$ be a cocycle of G_k in $L(k_s)$ representing x. The group L acts by inner automorphisms on itself, therefore also on its universal covering $\widetilde{L}$. We can twist L and $\widetilde{L}$ with a; we obtain groups ${}_aL$ and ${}_a\widetilde{L}$. Let z be a k-rational strongly regular semisimple element of ${}_a\widetilde{L}$ (such an element exists because k is infinite). Let C be the conjugacy class of z in ${}_a\widetilde{L}(k_s) = \widetilde{L}(k_s)$. It is obvious that C is stable under G_k. By th. 2' there exists $z_0 \in C \cap \widetilde{L}(k)$. Let $\widetilde{T}$ be the unique maximal torus of $\widetilde{L}$ containing z_0, and let T be its image in L (which is a maximal torus of L). The centralizer of z_0 is $\widetilde{T}$. This shows that $\widetilde{L}/\widetilde{T} = L/T$ can be identified with the conjugacy class C. By construction, the twist of $\widetilde{L}/\widetilde{T}$ by a contains a rational point (namely z). Hence ${}_a(L/T)$ has a rational point. Prop. 37 of Chap. I shows that the class of a belongs to the image of $H^1(k, T)$ in $H^1(k, L)$, QED.

Let us return to the *proof of th.* 1'. Assume k is perfect and $\dim(k) \leq 1$. Then we have $H^1(k, A) = 0$ for all linear connected commutative A, cf. the proof of th. 1. In view of the corollary above, we then have $H^1(k, L) = 0$ for all quasi-split semisimple L. However, if M is an arbitrary semisimple group, we can write it as a *twist* $M = {}_aL$, where L is quasi-split, and where a is a cocycle in the adjoint group L^{adj} of L. Because $H^1(k, L^{\mathrm{adj}})$ vanishes, as was shown above, we have $M \simeq L$, which shows that M is quasi-split. We have therefore proved the property (ii') of th. 1, QED.

Remarks.

1) If k is not assumed to be perfect, theorem 1' continues to hold, provided one restricts oneself to the case where L is *connected and reductive* (Borel-Springer, *loc. cit.*). There are counterexamples when L is unipotent, cf. §2.1, exerc. 3.

2) When L is simple (or almost simple) of type (B_n), (C_n) or (G_2), one can prove that $H^1(k, L)$ vanishes under a weaker assumption than $\dim(k) \leq 1$; it is sufficient to have:

$\mathrm{cd}_2(G_k) \leq 1$ if characteristic$(k) \neq 2$;

k is perfect if characteristic$(k) = 2$.

There are analogous statements for the other types (A_n), ..., (E_8), cf. [156], §4.4.

Exercises.

1) Give an example of an elliptic curve E over a perfect field k such that $H^1(k, E) \neq 0$ and $\dim(k) \leq 1$.

(Hence Lang's theorem [96] does not extend to all fields of dimension ≤ 1.)

2) Let K/k be a separable quadratic extension, and let L be a connected reductive group over k.

(a) Let $x \in H^1(K/k, L)$. Show that there exists a maximal torus T in L such that x belongs to the image of $H^1(K/k, T)$ in $H^1(K/k, L)$.

[We can assume that k is infinite. Let σ be the nontrivial element of $\mathrm{Gal}(K/k)$. We can represent x by a cocycle (a_s) such that a_σ is a regular semisimple element of $L(K)$, cf. [146], §3.2. Then we have $a_\sigma \cdot \sigma(a_\sigma) = 1$, which shows that the maximal torus T containing a_σ is defined over k. The torus T works.]

(b) Suppose that k is perfect and of characteristic 2. Show that $H^1(K/k, L) = 0$. [Use (a) to reduce to the case when L is a torus. Notice that the map $z \mapsto z^2$ is then a bijection of $L(K)$ onto itself.]

(c) Use (a) and (b) to justify Remark 2 in the text.

3) Let $\mathfrak{g}$ be a simple Lie algebra over a field k of characteristic zero. Let n (resp. r) be the dimension (resp. the rank) of $\mathfrak{g}$. It is known (cf. Kostant, [89]) that the set $\mathfrak{g}_u$ of the nilpotent elements of $\mathfrak{g}$ is the set of common zeros of r homogeneous polynomials $I_1, \ldots, I_r$ of degrees $m_1, \ldots, m_r$ such that

$$m_1 + \cdots + m_r = (n + r)/2 \,.$$

Use this result to recover the fact that $\mathfrak{g}_u \neq 0$ if the field k is (C_1).

2.4 Rational points on homogeneous spaces

The results of the preceding §§ concern the first cohomology set H^1, that is, *principal* homogeneous spaces. The theorem below, due to Springer, allows us to pass on from there to arbitrary homogeneous spaces.

Theorem 3. *Suppose k is perfect and of dimension ≤ 1. Let A be an algebraic group and let X be a (right) homogeneous space over A. Then there exists a principal homogeneous space P over A and an A-homomorphism $\pi : P \to X$.*

(Of course, A, X, P, and π are assumed to be defined over k.)

Before giving the proof, we shall set out some consequences of this theorem (always assuming k is perfect and of dimension ≤ 1):

Corollary 1. *If $H^1(k, A) = 0$, then every homogeneous space X over A has a rational point.*

Indeed the principal homogeneous space P is trivial, and therefore has a rational point p; the image of p under π is a rational point of X.

This result applies *when A is linear and connected*, cf. th. 1′.

Corollary 2. *Let $f : A \to A'$ be a surjective homomorphism of algebraic groups. The corresponding map:*

$$H^1(k, A) \longrightarrow H^1(k, A')$$

is surjective.

Let $x' \in H^1(k, A')$, and let P' be a principal homogeneous space over A' corresponding to x'. By making A act on P' through f, we give P' the structure of a homogeneous A-space. It follows from theorem 3, that there exists a principal homogeneous space P over A and an A-homomorphism $\pi : P \to P'$. Let $x \in H^1(k, A)$ be the class of P. It is clear that the image of x in $H^1(k, A')$ equals x', QED.

Corollary 3. *Let L be a linear algebraic group defined over k, and let L_0 be its identity component. The canonical map*

$$H^1(k, L) \longrightarrow H^1(k, L/L_0)$$

is bijective.

Corollary 2 shows that this map is surjective. On the other hand, let c be a 1-cocycle of $\mathrm{Gal}(\overline{k}/k)$ with values in $L(\overline{k})$, and let ${}_cL_0$ be the group obtained by twisting L_0 with c (this makes sense because L acts on L_0 by inner automorphisms). Since the group ${}_cL_0$ is connected and linear, we have $H^1(k, {}_cL_0) = 0$ from th. 1′. By applying the exact sequence of non-abelian cohomology (cf. Chap. I, §5.5, cor. 2 to prop. 39), we deduce that $H^1(k, L) \to H^1(k, L/L_0)$ is injective, QED.

[The cohomology of linear groups is thus reduced to that of *finite* groups, provided, of course, that $\dim(k) \leq 1$.]

Proof of theorem 3

Let us choose a point $x \in X(\overline{k})$. For any $s \in \mathrm{Gal}(\overline{k}/k)$, we have ${}^s x \in X(\overline{k})$, and therefore there exists $a_s \in A(\overline{k})$ such that ${}^s x = x \cdot a_s$. One may assume that (a_s) depends continuously on s, i.e., that it is a 1-*cochain of the group* $\mathrm{Gal}(\overline{k}/k)$ *with values in* $A(\overline{k})$. *If* (a_s) *were a cocycle*, one could find a principal homogeneous space P over A and a point $p \in P(\overline{k})$ such that ${}^s p = p \cdot a_s$; by putting $\pi(p \cdot a) = x \cdot a$ one would then define an A-homomorphism $\pi : P \to X$ which would satisfy the conditions required. We are thus led to proving the following proposition:

Proposition 7. *Under the hypotheses above, one may choose the* 1-*cochain* (a_s) *so that it is a cocycle.*

Let us consider the systems $\{H, (a_s)\}$ consisting of an algebraic subgroup H of A (defined over $\overline{k}$) and a continuous 1-cochain (a_s) of $\mathrm{Gal}(\overline{k}/k)$ with values in $A(\overline{k})$, these two data being subject to the following axioms:

(1) $x \cdot H = x$ (H is contained in the stabilizer of x),
(2) ${}^s x = x \cdot a_s$ *for all* $s \in \mathrm{Gal}(\overline{k}/k)$,

(3) *For every pair* $s, t \in \mathrm{Gal}(\bar{k}/k)$, *there exists* $h_{s,t} \in H(\bar{k})$ *such that*

$$a_s \cdot {}^s a_t = h_{s,t} \cdot a_{st} \ .$$

(4) $a_s \cdot {}^s H \cdot a_s^{-1} = H$ *for all* $s \in \mathrm{Gal}(\bar{k}/k)$.

Lemma 2. *There exists at least one such system* $\{H, (a_s)\}$.

We take for H the stabilizer of x, and for (a_s) some cochain verifying (2). Since $x \cdot a_s {}^s a_t = {}^{st}x = x \cdot a_{st}$, we infer that there exists $h_{s,t} \in H(\bar{k})$ such that $a_s {}^s a_t = h_{s,t} \cdot a_{s,t}$, from which (3) follows. Property (4) is clear.

We shall now choose a system $\{H, (a_s)\}$ such that H is *minimal*. Everything comes down to proving that H is then reduced to the identity, because (3) shows that (a_s) is then a *cocycle*.

Lemma 3. *If* H *is minimal, the identity component* H_0 *of* H *is a solvable group.*

Let L be the largest connected linear subgroup of H_0. By a theorem due to Chevalley, L is normal in H_0, and the quotient H_0/L is an abelian variety. Let B be a Borel subgroup of L, and let N be its normalizer in H. We shall show that $N = H$; that will imply that B is normal in L, therefore equal to L, and H_0 will be a solvable group (an extension of an abelian variety by B).

Take $s \in \mathrm{Gal}(\bar{k}/k)$. It is clear that ${}^s B$ is a Borel subgroup of ${}^s L$, which is the largest connected linear subgroup of ${}^s H_0$. We conclude that $a_s {}^s B a_s^{-1}$ is a Borel subgroup of $a_s {}^s L a_s^{-1}$, which coincides with L (since it is the largest connected linear subgroup of $a_s {}^s H_0 a_s^{-1} = H_0$). Since Borel subgroups are conjugate, there exists $h_s \in L$ such that $h_s a_s {}^s B a_s^{-1} h_s^{-1} = B$; we can evidently arrange things so that h_s depends continuously on s. Let us now put $a'_s = h_s a_s$. *The system* $\{N, (a'_s)\}$ *verifies axioms* (1), (2), (3), *and* (4). This is obvious for (1) and (2). For (3), define $h'_{s,t}$ by the formula:

$$a'_s {}^s a'_t = h'_{s,t} a'_{st} \ .$$

A short computation gives:

$$h_s \cdot a_s {}^s h_t a_s^{-1} \cdot h_{s,t} = h'_{s,t} \cdot h_{st} \ .$$

Since $a_s {}^s h_t a_s^{-1} \in a_s {}^s H a_s^{-1} = H$, this formula shows that $h'_{s,t}$ belongs to H. Moreover, we have $a'_s {}^s B a'^{-1}_s = B$. It follows that the inner automorphisms defined by a'_{st} and $a'_s {}^s a'_t$ both transform ${}^{st}B$ into B; the inner automorphism defined by their quotient $h'_{s,t}$ therefore transforms B into itself, which shows that $h'_{s,t}$ is an element of N, and proves (3). Finally, since the inner automorphism defined by a'_s transforms ${}^s B$ into B, it also transforms ${}^s N$ into N, which proves (4).

Since H is minimal, we have $N = H$, which proves the lemma.

Lemma 4. *If* H *is minimal, then* H *is solvable.*

In view of lemma 3, it is enough to prove that H/H_0 is solvable. Let P be a Sylow subgroup of H/H_0, let B be its inverse image in H, and let N be its normalizer. The same argument as in the previous lemma can be applied to N (with conjugation of Sylow subgroups replacing that of Borel subgroups), and we conclude that $N = H$. Hence, *each Sylow subgroup of* H/H_0 *is normal*; the group H/H_0 is therefore the product of its Sylow subgroups, thus nilpotent, and *a fortiori* solvable.

Lemma 5. *If* $\dim(k) \leq 1$, *and if* H *is minimal, then* H *is equal to its commutator subgroup.*

Let H' be the commutator subgroup of H. We shall first let $\mathrm{Gal}(\overline{k}/k)$ act on H/H'. To this end, if $h \in H$ and $s \in \mathrm{Gal}(\overline{k}/k)$, set:

$$^{s\prime}h = a_s\,{}^s h a_s^{-1} .$$

Axiom (4) shows that $^{s\prime}h$ belongs to H; if also $h \in H'$, then $^{s\prime}h \in H'$. By passing to quotients, we obtain in this way an automorphism $y \mapsto {}^{s\prime}y$ of H/H'. Using formula (3), we see that $^{st\prime}y = {}^{s\prime}({}^{t\prime}y)$, which means that H/H' *is a* $\mathrm{Gal}(\overline{k}/k)$*-group.*

Let $\overline{h}_{s,t}$ be the image of $h_{s,t}$ in H/H'. *It is a 2-cocycle.* This follows from the identity:

$$a_{st}\,{}^s a_t^{-1} a_s^{-1} \cdot a_s\,{}^s a_t\,{}^{st} a_u\,{}^s a_{tu}^{-1} a_s^{-1} \cdot a_s\,{}^s a_{tu} a_{stu}^{-1} \cdot a_{stu}\,{}^{st} a_u^{-1} a_{st}^{-1} = 1 ,$$

which, by going to H/H', gives:

$$\overline{h}_{s,t}^{-1} \cdot {}^{s\prime}\overline{h}_{t,u} \cdot \overline{h}_{s,tu} \cdot \overline{h}_{st,u}^{-1} = 1 .$$

But the structure of commutative algebraic groups shows that $H/H'(\overline{k})$ has a composition sequence whose quotients are either torsion or divisible. Since $\dim(k) \leq 1$, we then have $H^2(\mathrm{Gal}(\overline{k}/k), H/H'(\overline{k})) = 0$, cf. Chap. I, §3.1. Thus the cocycle $(\overline{h}_{s,t})$ is a coboundary. Hence there exists a 1-cochain (h_s) with values in $H(\overline{k})$ such that:

$$h_{s,t} = h_s^{-1} \cdot {}^{s\prime}h_t^{-1} \cdot h'_{s,t} \cdot h_{st} , \quad \text{with } h'_{s,t} \in H'(\overline{k}).$$

We have

$$^{s\prime}h_t^{-1} = a_s\,{}^s h_t^{-1} a_s^{-1} \equiv h_s a_s\,{}^s h_t^{-1} a_s^{-1} h_s^{-1} \bmod H'(\overline{k}) .$$

Modifying $h'_{s,t}$ if necessary, we may then write:

$$h_{s,t} = h_s^{-1} \cdot h_s a_s\,{}^s h_t^{-1} a_s^{-1} h_s^{-1} \cdot h'_{s,t} \cdot h_{st} .$$

Upon putting $a'_s = h_s a_s$, the preceding formula becomes:

$$a'_s\,{}^s a'_t = h'_{s,t} a'_{st} .$$

The system $\{H', (a'_s)\}$ then satisfies the axioms (1), (2), and (3). Axiom (4) is easily checked. Since H is minimal, we conclude that $H = H'$.

End of the proof

If $\{H, (a_s)\}$ is a minimal system, lemmas 4 and 5 show that $H = \{1\}$, therefore that (a_s) is a cocycle, which proves prop. 7, and, at the same time, theorem 3.

Exercises.

1) With the notation of the proof of lemma 5, show there exists an algebraic k-group structure on H/H' such that the corresponding $\mathrm{Gal}(\overline{k}/k)$-module structure on $H/H'(\overline{k})$ is that defined in the text.

2) Show that theorem 3 remains true if one replaces the hypothesis

$$\dim(k) \leq 1$$

by the following:

The stabilizer of a point in X is a unipotent linear group. [Use the fact that $H^2(k, H) = 0$ for every unipotent commutative group H.]

3) Assume that $\dim(k) \leq 1$ and that the characteristic p is $\neq 2$. Let f be a nondegenerate quadratic form in n variables ($n \geq 2$). Show by making use of th. 3 that, for any constant $c \neq 0$, the equation $f(x) = c$ has a solution in k. [Observe that the system of solutions of this equation is a homogeneous space for the group $\mathbf{SO}(f)$, which is connected.] Recover this result by a direct proof, using only the hypothesis $\mathrm{cd}_2(G_k) \leq 1$.

§3. Fields of dimension ≤ 2

3.1 Conjecture II

Let L be a semisimple group and T be a maximal torus in L. The group $X(T)$ of the characters of T is a subgroup of finite index of the *group of weights* of the corresponding root system. If these two groups are equal, L is said to be *simply connected* (cf. for example [125], 2.1.13).

Conjecture II. *Let k be a perfect field such that* $\mathrm{cd}(G_k) \leq 2$, *and let L be a simply connected semisimple group. Then* $H^1(k, L) = 0$.

This conjecture has been proved in many special cases:

a) If k is a *p-adic field*: Kneser [86].

b) More generally, if k is a field which is *complete for a discrete valuation whose residue field is perfect and of dimension* ≤ 1: Bruhat-Tits [22] and [23], III.

c) If k is a *totally imaginary number field* (for L of classical type: Kneser [87]; for L of type D_4, G_2, F_4, E_6, E_7: Harder [67]; for L of type E_8: Chernousov [30]).

d) If L is *of inner type* A_n: Merkurjev-Suslin, cf. §3.2.

e) More generally, if L is *of classical type* (except for triality D_4): Bayer-Parimala [10].

f) If L is *of type* G_2 *or* F_4 (see, for example, [156]).

Remarks.

1) In the statement of Conjecture II, it should be possible to replace the hypothesis "k is perfect" by "$[k : k^p] \leq p$", for k of characteristic $p > 0$ (an even weaker hypothesis should actually suffice, cf. [156]).

For example, the conjecture should be applicable to all fields k which are transcendental extensions of degree 1 of a perfect field k_0 of dimension ≤ 1 (this is true at least when k_0 is *finite*, according to Harder [67], III).

2) Any semisimple group L_0 can be written uniquely as $L_0 = L/C$, where L is simply connected, and C is a finite subgroup of the center of L. If we assume that C is smooth, we may identify it with a Galois G_k-module, and we get a coboundary map (cf. Chap. I, §5.7)

$$\Delta : H^1(k, L_0) \longrightarrow H^2(k, C) \ .$$

If Conjecture II applies to k, this map is *injective* (Chap. I, cor. of prop. 44); this allows identifying $H^1(k, L_0)$ with a subset of the group $H^2(k, C)$ (notice that this subset is not always a subgroup, cf. §3.2, exercise).

3.2 Examples

a) The group $\mathbf{SL}_D$

Let D be a central simple algebra over k, of finite rank; then $[D:k] = n^2$, with n an integer ≥ 1 (sometimes called the *degree* of D). Let $\mathbf{G}_{m/D}$ be the algebraic k-group such that $\mathbf{G}_{m/D}(k') = (k' \otimes_k D)^*$ for every extension k' of k; this is a k-form of the group $\mathbf{GL}_n$. We have $\mathbf{G}_{m/D}(k) = D^*$. The reduced norm Nrd defines a surjective morphism

$$\mathrm{Nrd} : \mathbf{G}_{m/D} \longrightarrow \mathbf{G}_m.$$

Let $\mathbf{SL}_D$ be the kernel of Nrd. It is a k-form (called "inner") of the group $\mathbf{SL}_n$, cf. §1.4; thus it is a simply connected semisimple group. Its cohomology can be obtained via the exact sequence:

$$H^0(k, \mathbf{G}_{m/D}) \longrightarrow H^0(k, \mathbf{G}_m) \longrightarrow H^1(k, \mathbf{SL}_D) \longrightarrow H^1(k, \mathbf{G}_{m/D}) \ .$$

The two groups on the left are respectively equal to D^* and k^*. It can be shown easily (by the same argument as for $\mathbf{GL}_n$) that $H^1(k, \mathbf{G}_{m/D}) = 0$. We deduce from that a *bijection*

$$k^*/\mathrm{Nrd}(D^*) \simeq H^1(k, \mathbf{SL}_D) \ .$$

In particular, $H^1(k, \mathbf{SL}_D)$ is 0 *if and only if* $\mathrm{Nrd} : D^* \to k^*$ *is surjective.*

This is true, by results of Merkurjev-Suslin (cf. Chap. II, §4.5, theorem MS) if k is perfect and $\mathrm{cd}(G_k) \leq 2$ (the statement in theorem MS assumes that D is a skew field – the general case can easily be reduced to that). Conjecture II therefore holds for $\mathbf{SL}_D$.

Remark.

Theorem MS also gives a *converse* to Conjecture II: if k is a field such that $H^1(k, L) = 0$ for every simply connected semisimple L, then $\mathrm{cd}(G_k) \leq 2$.

b) The group $\mathbf{Spin}_n$

We assume the characteristic of k is not equal to 2.

Let q be a nondegenerate quadratic form of rank n, let $\mathbf{SO}_q$ be the corresponding special orthogonal group. It is a connected semisimple group (if $n \geq 3$, which we shall assume). Its universal covering is the spinor group $\mathbf{Spin}_q$. There is an exact sequence:

$$1 \longrightarrow \mu_2 \longrightarrow \mathbf{Spin}_q \longrightarrow \mathbf{SO}_q \longrightarrow 1 \ , \quad \text{with } \mu_2 = \{\pm 1\}.$$

According to §5.7 of Chap. I, this gives a cohomology exact sequence:

$$\mathbf{Spin}_q(k) \longrightarrow \mathbf{SO}_q(k) \xrightarrow{\delta} k^*/k^{*2} \longrightarrow H^1(k, \mathbf{Spin}_q) \longrightarrow H^1(k, \mathbf{SO}_q) \xrightarrow{\Delta} \mathrm{Br}_2(k) \ ,$$

since $H^1(k,\mu_2) = k^*/k^{*2}$ and $H^2(k,\mu_2) = \mathrm{Br}_2(k)$, cf. Chap. II, §1.2. The homomorphism

$$\delta : \mathbf{SO}_q(k) \longrightarrow k^*/k^{*2}$$

is the *spinor norm* (Bourbaki A IX.§9). The map

$$\Delta : H^1(k,\mathbf{SO}_q) \longrightarrow \mathrm{Br}_2(k)\ ,$$

is related to the *Hasse-Witt invariant* w_2 by the following formula:

If $x \in H^1(k,\mathbf{SO}_q)$ and q_x denotes the quadratic form derived from q by twisting using x, then $\Delta(x) = w_2(q_x) - w_2(q)$, cf. Springer [60], and also Appendix 2, §2.2.

Note that $H^1(k,\mathbf{SO}_q)$ can be identified with the set of classes of quadratic forms of rank n which have the same discriminant (in k^*/k^{*2}) as q. Taking into account the cohomology exact sequence above, we get:

In order that $H^1(k,\mathbf{Spin}_q)$ *be* 0, *it is necessary and sufficient that the following two conditions be satisfied*:

(i) *The spinor norm* $\delta : \mathbf{SO}_q(k) \to k^*/k^{*2}$ *is surjective.*

(ii) *Every quadratic form of rank* n, *which has the same discriminant and the same Hasse-Witt invariant as* q, *is isomorphic to* q.

According to Merkurjev-Suslin, these conditions are satisfied if $\mathrm{cd}_2(G_k) \leq 2$ (cf. Bayer-Parimala [10] – see also exerc. 1 in Chap. II, §4.5). Conjecture II is therefore true for $\mathbf{Spin}_q$.

Exercise.

Take $n = 3$, and choose as q the standard form $X^2 - YZ$.

(a) Show that the image $\Delta : H^1(k,\mathbf{SO}_q) \to \mathrm{Br}_2(k)$ consists of the *decomposable* elements of $\mathrm{Br}_2(k) = H^2(k,\mathbf{Z}/2\mathbf{Z})$, i.e. of those which are cup-products of two elements of $H^1(k,\mathbf{Z}/2\mathbf{Z})$.

(b) Deduce from this, and from Merkurjev [108], that there exists a field k of characteristic 0, with $\mathrm{cd}(G_k) = 2$, such that the image of Δ is not a subgroup of $\mathrm{Br}_2(k)$.

§4. Finiteness theorems

4.1 Condition (F)

Proposition 8. *Let G be a profinite group. The following three conditions are equivalent:*

a) *For every integer n, the group G has only a finite number of open subgroups of index n.*

a') *Same assertion as* a), *but restricted to open normal subgroups.*

b) *For every finite G-group A* (cf. Chap. I, §5.1), *$H^1(G, A)$ is a finite set.*

If H is an open subgroup of G with index n, the intersection H' of the conjugates of H is a normal open subgroup of G with index $\leq n!$ (indeed the quotient G/H' is isomorphic to a subgroup of the group of permutations of G/H). This shows that a) and a') are equivalent.

Let us show that a) $\Rightarrow$ b). Let n be the order of the finite G-group A, and let H be an open normal subgroup of G which acts trivially on A. In view of a), the open subgroups of H with index $\leq n$ are only finite in number. Their intersection H' is an open normal subgroup of G. Every continuous homomorphism $f : H \to A$ is trivial on H'. This shows that the composite map

$$H^1(G, A) \longrightarrow H^1(H, A) \longrightarrow H^1(H', A)$$

is trivial. That implies (cf. the exact sequence in Chap. I, §5.8) that $H^1(G, A)$ may be identified with $H^1(G/H', A)$, which is obviously finite.

Let us show that b) $\Rightarrow$ a). We need to show that, for any integer n, the group G has only a finite number of homomorphisms into the symmetric group S_n on n letters. This follows immediately from the finiteness of $H^1(G, S_n)$, with the group G acting trivially on S_n.

A profinite group G verifying the conditions of prop. 8 is said to be "of type (F)".

Proposition 9. *Each profinite group G which can be topologically generated by a finite number of elements is of type* (F).

Indeed, it is clear that the number of homomorphisms of G into a given finite group is finite (because they are determined by their values on the topological generators of G).

Corollary. *In order that a pro-p-group be of type* (F), *it is necessary and sufficient that it be of finite rank.*

This follows from the two propositions above, combined with prop. 25 of Chap. I.

Exercises.

1) Let G be a profinite group of type (F), and let $f : G \to G$ be a *surjective* homomorphism of G onto itself. Show that f is an isomorphism. [Let X_n be the set of open subgroups of G with a given index n. If $H \in X_n$, we have $f^{-1}(H) \in X_n$, and f defines in this way an injection $f_n : X_n \to X_n$. Since X_n is finite, f_n is bijective. Hence the kernel N of f is contained in every open subgroup of G, and thus reduces to $\{1\}$.]

2) Let Γ be a discrete group and $\widehat{\Gamma}$ the associated profinite group (Chap. I, §1.1). Assume:

(a) The canonical map $\Gamma \to \widehat{\Gamma}$ is injective.

(b) $\widehat{\Gamma}$ is of type (F).

Prove that Γ is *Hopfian*, i.e. that every surjective endomorphism of Γ is an isomorphism [apply exerc. 1 to $\widehat{\Gamma}$].

Show that a finitely generated subgroup of $\mathbf{GL}_n(\mathbf{C})$ satisfies (a) and (b). (This applies, in particular, to arithmetic groups.)

3) Let (N_p), $p = 2, 3, 5, \ldots$ be an unbounded family of integers ≥ 0, indexed by the primes. Let G_p be the N_p-th power of the group $\mathbf{Z}_p$ and let G be the product of the G_p's. Show that G is of type (F), although it cannot be generated topologically by a finite number of elements.

4.2 Fields of type (F)

Let k be a field. We shall say that k is *of type* (F) if k is perfect and the Galois group $\mathrm{Gal}(\overline{k}/k)$ is of type (F) in the sense defined above. This last condition amounts to saying that, for all integer n, there exist only a finite number of sub-extensions of $\overline{k}$ (resp. of Galois sub-extensions) which are of degree n over k.

Examples of fields of type (F).

a) The field $\mathbf{R}$ of *real numbers.*

b) A *finite* field. [In fact, such a field has a unique extension of a given degree — moreover its Galois group is $\widehat{\mathbf{Z}}$ and thus can be topologically generated by a single element.]

c) The field $C((T))$ of *formal power series* in one variable over an algebraically closed field C of characteristic zero. [Same argument as in the previous case, using the fact that the only finite extensions of $C((T))$ are the fields $C((T^{1/n}))$, by Puiseux's theorem (cf. [145], p. 76).]

d) A *p-adic* field (i.e. a finite extension of $\mathbf{Q}_p$). This is a well-known result. One can, for example, prove it as follows: each finite extension of k can be

obtained by first making an unramified extension, and then a totally ramified extension. Since there is only one unramified extension of a given degree, *one is led back to the totally ramified case.* But such an extension is given by an "Eisenstein equation" $T^n + a_1 T^{n-1} + \cdots + a_n = 0$, where the a_i belong to the maximal ideal of the ring of integers of k, and where a_n is a uniformizing element. The set of such equations is a *compact* space for the topology of coefficientwise convergence; moreover, it is known that two close enough equations define isomorphic extensions (this is a consequence of "Krasner's lemma", cf. for example [145], p. 40, exercises 1 and 2). Whence the finiteness sought.

[In fact one has much more precise results:

i) Krasner [91] has computed explicitly the number of extensions of degree n of a p-adic field k.

The result can be stated (and proved) more simply if one "counts" each extension with a certain *weight*, cf. [152]. More precisely, if k' is a totally ramified extension of degree n of k, the exponent of the discriminant of k'/k can be written in the form $n - 1 + c(k')$, where $c(k')$ is an integer ≥ 0 (the "wild" component). If we define the weight $w(k')$ of k' by the formula

$$w(k') = q^{-c(k')} ,$$

where q is the number of elements of the residue field of k, we have the following *mass formula* (cf. [152], th. 1):

$$\sum_{k'} w(k') = n ,$$

where k' runs over all totally ramified extensions of k, of degree n, contained in $\overline{k}$.

ii) Iwasawa [76] has shown that the group $\mathrm{Gal}(\overline{k}/k)$ can be generated topologically by a finite number of elements (the result is not explicitly stated, but it is an easy consequence of th. 3, p. 468).]

Exercise.

Let k be a perfect field. Assume that, for every integer $n \geq 1$ and for every finite extension K of k, the quotient K^*/K^{*n} is finite. Show that k has only a finite number of *solvable* Galois extensions of a given degree, prime to the characteristic of k. Apply this to the p-adic case.

4.3 Finiteness of the cohomology of linear groups

Theorem 4. *Let k be a field of type* (F), *and let L be a linear algebraic group defined over k. The set $H^1(k, L)$ is finite.*

We proceed in stages:

(i) The group L is *finite* (i.e. of dimension zero).

The set $L(\overline{k})$ of the points of L which are rational over $\overline{k}$ is therefore a finite $\mathrm{Gal}(\overline{k}/k)$-group, and one can apply prop. 8 to it. Whence the finiteness of

$$H^1(k, L) = H^1(\mathrm{Gal}(\overline{k}/k), L(\overline{k})) .$$

(ii) The group L is *connected and solvable.*

By applying cor. 3 of prop. 39 of Chap. I, we reduce to the case when L is unipotent and to the case when L is a torus. In the first case, we have $H^1(k, L) = 0$, cf. prop. 6. Assume now that L is a torus. There exists a finite Galois extension k'/k such that L is k'-isomorphic to a product of multiplicative groups $\mathbf{G}_m$. Since $H^1(k', \mathbf{G}_m)$ vanishes, we have $H^1(k', L) = 0$, and therefore $H^1(k, L)$ may be identified with $H^1(k'/k, L)$. In particular, if $n = [k' : k]$, we have $nx = 0$ for all $x \in H^1(k, L)$. Consider now the exact sequence

$$0 \longrightarrow L_n \longrightarrow L \xrightarrow{n} L \longrightarrow 0 ,$$

and the cohomology exact sequence associated to it. We see that $H^1(k, L_n)$ maps onto the kernel of $H^1(k, L) \xrightarrow{n} H^1(k, L)$, which is $H^1(k, L)$. Since L_n is finite, case (i) shows that $H^1(k, L_n)$ is finite, and the same is true of $H^1(k, L)$.

(iii) *The general case.*

We use the following result, due to Springer:

Lemma 6. *Let C be a Cartan subgroup of a linear group L, and let N be the normalizer of C in L. The canonical map $H^1(k, N) \to H^1(k, L)$ is surjective.*

(This result holds *for every perfect field k.*)

Let $x \in H^1(k, L)$, and let c be a cocycle representing x. Let ${}_cL$ be the group obtained by twisting L using c. By a theorem of Rosenlicht ([130], see also [16], th. 18.2), the group ${}_cL$ has a Cartan subgroup C' defined over k; when one extends the base field to $\overline{k}$, the groups C and C' become conjugate. From lemma 1 in §2.2 it follows that x belongs to the image of $H^1(k, N)$ in $H^1(k, L)$, which proves the lemma.

Let us go back to proving theorem 4. Suppose C is a Cartan subgroup of L, defined over k, and let N be its normalizer. By the preceding lemma, it suffices to prove that $H^1(k, N)$ is finite. But the quotient N/C is finite; by (i), $H^1(k, N/C)$ is finite. Also, for any cocycle c with values in N, the twisted group ${}_cC$ is connected and solvable, and $H^1(k, {}_cC)$ is finite by (ii). Then applying cor. 3 of prop. 39 in Chap. I, we see that $H^1(k, N)$ is finite, QED.

Corollary. *Let k be a field of type* (F).

a) *The k-forms of a semisimple group defined over k are finite in number* (up to isomorphism).

b) *So are the k-forms of a pair (V, x), where V is a vector space and x a tensor* (cf. §1.1).

This follows from the fact that, in both cases, the automorphism group of the given object is a linear algebraic group.

Remarks.

1) If k is a field of characteristic zero and type (F), one can show that there are only a finite number of k-forms of any *linear* algebraic group; for this it is necessary to extend theorem 4 to some groups which are not algebraic, namely those which are extensions of an "arithmetic" discrete group by a linear group; for more details, see Borel-Serre [18], §6.

2) Let k_0 be a finite field, and $k = k_0((T))$. Theorem 4 does not apply to k (if only because k is not perfect — moreover, one may show that $H^1(k, \mathbf{Z}/p\mathbf{Z})$ is infinite, if p is the characteristic of k). However, one can prove $H^1(k, L)$ is finite when L is *connected and reductive.*

[Sketch of proof (after J. Tits): Put $\widetilde{k} = \overline{k}_0((t))$. Then $\dim(\widetilde{k}) \leq 1$. By a result of Borel-Springer ([19], §8.6), this implies $H^1(\widetilde{k}, L) = 0$, cf. §2.3. Therefore we have $H^1(k, L) = H^1(\widetilde{k}/k, L)$. But Bruhat-Tits theory ([23], Chap. III, §3.12) shows that $H^1(\widetilde{k}/k, L)$ can be embedded in a finite union of cohomology sets of type $H^1(k_0, L_i)$, where the L_i are linear algebraic groups (not necessarily connected) over the residue field k_0. By th. 4, applied to k_0, each of the $H^1(k_0, L_i)$ is finite. Therefore the same is true of $H^1(\widetilde{k}/k, L)$, QED.]

4.4 Finiteness of orbits

Theorem 5. *Let k be a field of type* (F), *let G be an algebraic group defined over k, and let V be a homogeneous G-space. The quotient of $V(K)$ by the equivalence relation defined by $G(K)$ is finite.*

The space V is a finite union of orbits of the identity component of G; this allows reduction *to the case when G is connected.* If $V(k) = \emptyset$, there is nothing to prove. Otherwise, let $v \in V(k)$ and let H be the stabilizer of v. The canonical map $G/H \to V$ defines a bijection of $(G/H)(k)$ onto $V(k)$. By cor. 1 of prop. 36 in Chap. I, the quotient of $(G/H)(k)$ by $G(k)$ can be identified with the kernel of the canonical map $\alpha : H^1(k, H) \to H^1(k, G)$. Therefore it is enough to prove that this map is *proper*, i.e. that α^{-1} transforms a finite set into a finite set.

Let L be the largest connected linear subgroup of G, let $M = L \cap H$, and let $A = G/L$, $B = H/M$. By a theorem of Chevalley, A is an abelian variety, and B embeds into A. We have a commutative diagram:

$$\begin{array}{ccc} H^1(k, H) & \xrightarrow{\alpha} & H^1(k, G) \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\beta} \\ H^1(k, B) & \xrightarrow{\delta} & H^1(k, A)\ . \end{array}$$

Since M is linear, Theorem 4 (combined with prop. 39 in Chap. I) shows that γ is proper. By the "complete reducibility" of abelian varieties, there exists an abelian variety B' with the same dimension as B and a homomorphism $A \to B'$ such that the composition $B \to A \to B'$ is surjective; moreover, B' and $A \to B'$ can be defined over k. Since the kernel of $B \to B'$ is finite, the argument used

above shows that the map $H^1(k, B) \to H^1(k, A) \to H^1(k, B')$ is proper. It follows that δ is proper, therefore also $\delta \circ \gamma = \beta \circ \alpha$, from which it follows that α is proper, QED.

Corollary 1. *Let k be a field of type* (F), *and let G be a linear algebraic group defined over k. The maximal tori* (resp. *the Cartan subgroups*) *of G defined over k form a finite number of classes* (under conjugation by elements of $G(k)$).

Let T be a maximal torus (resp. a Cartan subgroup) of G defined over k (if there is none, there is nothing to be proved); let H be its normalizer in G. Since all maximal tori (resp. ...) are conjugate over $\overline{k}$, they correspond bijectively to the points of the homogeneous space G/H; those defined over k correspond to k-rational points of G/H; by theorem 5, they can be partitioned into a finite number of $G(k)$-orbits, whence the result we are after.

Corollary 2. *Let k be a field of characteristic zero and type* (F), *and let G be a semisimple group defined over k. The unipotent elements of $G(k)$ form a finite number of classes.*

The proof is the same as that of cor. 1, using the fact (proved by Kostant [89]) that the unipotent elements of $G(\overline{k})$ make up a finite number of conjugacy classes.

Exercises.

Denote by k a field of type (F).

1) Let $f : G \to G'$ be an algebraic group homomorphism. Suppose that the kernel of f is a linear group. Show that the corresponding map $H^1(k, G) \to H^1(k, G')$ is proper.

2) Let G be an algebraic group, and K a finite extension of k. Show that the map $H^1(k, G) \to H^1(K, G)$ is proper. [Apply exerc. 1 to the group $G' = R_{K/k}(G)$.]

4.5 The case $k = \mathbf{R}$

The results of the preceding sections of course apply to the field $\mathbf{R}$. Some of them can even be derived more simply by topological arguments. For example, theorem 5 follows from the fact (proved by Whitney) that any real algebraic variety has only a finite number of connected components.

We shall see that, for some groups, one can go further and determine H^1 explicitly.

Let us start with a *compact Lie group* K. Let R be the algebra of continuous functions on K which are linear combinations of coefficients of (complex) matrix representations of K. If R_0 denotes the subalgebra of R consisting of real-valued functions, then $R = R_0 \otimes_{\mathbf{R}} \mathbf{C}$. It is known (cf. e. g. Chevalley, [32], Chap. VI) that R_0 is the affine algebra of an algebraic $\mathbf{R}$-group L. The group $L(\mathbf{R})$ of the real points of L may be identified with K; the group $L(\mathbf{C})$ is called the *complexification* of K. The Galois group $\mathfrak{g} = \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ acts on $L(\mathbf{C})$.

Theorem 6. *The canonical map* $\varepsilon : H^1(\mathfrak{g}, K) \to H^1(\mathfrak{g}, L(\mathbf{C}))$ *is bijective.*

(Since $\mathfrak{g}$ acts trivially on K, $H^1(\mathfrak{g}, K)$ is the set of conjugacy classes in K of the elements x such that $x^2 = 1$.)

The group $\mathfrak{g}$ acts on the Lie algebra of $L(\mathbf{C})$; the invariant elements form the Lie algebra $\mathfrak{k}$ of K, and the anti-invariant elements form a complement $\mathfrak{p}$ for $\mathfrak{k}$. The exponential defines a real analytic isomorphism of $\mathfrak{p}$ onto a closed sub-variety P in $L(\mathbf{C})$; it is clear that $xpx^{-1} = p$ for all $x \in K$; moreover (Chevalley, *loc. cit.*) any element $x \in L(\mathbf{C})$ can be written uniquely in the form $z = xp$, with $x \in K$ and $p \in P$.

Having recalled these results, let us show that ε is *surjective*. A 1-cocycle for $\mathfrak{g}$ in $L(\mathbf{C})$ can be identified with an element $z \in L(\mathbf{C})$ such that $z\overline{z} = 1$. If we write z in the form xp, with $x \in K$ and $p \in P$, we find $xpxp^{-1} = 1$ (because $\overline{p} = p^{-1}$), from which follows $p = x^2 \cdot x^{-1}px$. But $x^{-1}px$ belongs to P, and uniqueness of the decomposition $L(\mathbf{C}) = K \cdot P$ shows that $x^2 = 1$ and $x^{-1}px = p$. If P_x is the subset of P consisting of the elements commuting with x, one checks easily that P_x is the exponential of a vector subspace of $\mathfrak{p}$. Hence one may write p as $p = q^2$, with $q \in P_x$. We get $z = qxq$ and since $\overline{q} = q^{-1}$, we see that the cocycle z is cohomologous to the cocycle x, which takes its values in K.

Let us now show that $H^1(\mathfrak{g}, K) \to H^1(\mathfrak{g}, L(\mathbf{C}))$ is *injective*. Let $x \in K$ and $x' \in K$ be two elements such that $x^2 = 1$, $x'^2 = 1$, and suppose that they are cohomologous in $L(\mathbf{C})$, i.e. that there exists $z \in L(\mathbf{C})$ such that $x' = z^{-1}x\overline{z}$. Write z in the form $z = yp$, with $y \in K$ and $p \in P$. We have:

$$x' = p^{-1}y^{-1}xyp^{-1}\ , \quad \text{and therefore} \quad x' \cdot x'^{-1}px' = y^{-1}xy \cdot p^{-1}\ .$$

By using again the uniqueness of the decomposition $L(\mathbf{C}) = K \cdot P$, we see that $x' = y^{-1}xy$, which means that x and x' are conjugate in K, and so finishes the proof.

Examples.

(a) Assume that K is *connected*, and that T is one of its maximal tori. Let T_2 be the set of $t \in T$ such that $t^2 = 1$. One knows that every element $x \in K$ such that $x^2 = 1$ is conjugate to an element $t \in T_2$; moreover, two elements t and t' of T_2 are conjugates in K if and only if they are in the same orbit of the *Weyl group* W of K. It then follows from theorem 6 that $H^1(\mathbf{R}, L) = H^1(\mathfrak{g}, L(\mathbf{C}))$ *can be identified with the quotient set* T_2/W.

(b) Take as K the *automorphism group* of a compact semisimple connected group S. Let A (resp. L) be the algebraic group associated with K (resp. with S). It is known that A *is the automorphism group of* L. The elements of $H^1(\mathbf{R}, A)$ then correspond to the *real forms* of the group L, and th. 6 gives the classification of these forms in terms of conjugacy classes of "involutions" of S (a result due to Elie Cartan).

4.6 Algebraic number fields (Borel's theorem)

Let k be an algebraic number field. It is clear that k *is not* of type (F). Nevertheless, we have the following finiteness theorem:

Theorem 7. *Let L be a linear algebraic group defined over k, and S a finite set of places of k. The canonical map*

$$\omega_S : H^1(k, L) \longrightarrow \prod_{v \notin S} H^1(k_v, L)$$

is proper.

Since the $H^1(k_v, L)$ are *finite* (cf. theorem 4), one may modify S at will, and, in particular, assume that $S = \emptyset$ (in which case we write ω instead of ω_S). Moreover, up to *twisting* L, it is enough to show that the *kernel* of ω is finite; in other words:

Theorem 7'. *The number of elements of $H^1(k, L)$ which vanish locally is finite.*

In this form the theorem was proved by Borel when L is connected and reductive ([14], p. 25). The case of a connected linear group can be reduced to the preceding one. It is less easy to get rid of the hypothesis of connectedness; for this I refer to Borel-Serre [18], §7.

4.7 A counter-example to the "Hasse principle"

Keep the notation of §4.6. There are important examples where the map

$$\omega : H^1(k, L) \longrightarrow \prod_{v} H^1(k_v, L)$$

is *injective*; this is notably the case when L is a projective group or an orthogonal group. One may ask whether this "Hasse principle" extends to all semisimple groups. We shall see that it is not so.

Lemma 7. *There exists a finite $\mathrm{Gal}(\overline{k}/k)$-module A such that the canonical map of $H^1(k, A)$ into $\prod_v H^1(k_v, A)$ is not injective.*

We start by choosing a finite Galois extension K/k whose Galois group G has the following property:

The lcm of the orders of the decomposition groups of the places v of k is strictly less than the order n of G.

[Example: $k = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{13}, \sqrt{17})$; the group G is of type $(2, 2)$ and its decomposition subgroups are cyclic of order 1 or 2. Similar examples exist for all number fields.]

Let $E = \mathbf{Z}/n\mathbf{Z}[G]$ be the group algebra of the group G over the ring $\mathbf{Z}/n\mathbf{Z}$, and let A be the kernel of the augmentation homomorphism $E \to \mathbf{Z}/n\mathbf{Z}$. Since the cohomology of E is trivial, the cohomology exact sequence shows that $H^1(G, A) = \mathbf{Z}/n\mathbf{Z}$. Let x be a generator of $H^1(G, A)$, let q be the lcm of the

orders of the decomposition groups G_v, and put $y = qx$. Obviously $y \neq 0$; moreover, since every element of $H^1(G, A)$ is killed by q, the images of y in the $H^1(G_v, A)$ vanish. Since $H^1(G, A)$ can be identified with a subgroup of $H^1(k, A)$, we have indeed constructed a nonzero element $y \in H^1(k, A)$ all of whose local images are zero.

Lemma 8. *There exists a finite* $\mathrm{Gal}(\overline{k}/k)$*-module* B *such that the canonical map of* $H^2(k, B)$ *into* $\prod_v H^2(k_v, B)$ *is not injective.*

This is distinctly less trivial. There are two ways to proceed:

(1) Start by constructing a finite $\mathrm{Gal}(\overline{k}/k)$-module A satisfying the condition in lemma 7. Then put

$$B = A' = \mathrm{Hom}(A, \overline{k}^*) .$$

By Tate's duality theorem (Chap. II, §6.3, th. A), the kernels of the maps

$$H^1(k, A) \longrightarrow \prod_v H^1(k_v, A) \quad \text{and} \quad H^2(k, B) \longrightarrow \prod_v H^2(k_v, B)$$

are dual to each other. Since the first is not zero, neither is the second.

(2) Explicit construction: Take for B an extension:

$$0 \longrightarrow \mu_n \longrightarrow B \longrightarrow \mathbf{Z}/n\mathbf{Z} \longrightarrow 0$$

where μ_n denotes the group of n-th roots of unity. Choose B such that, as an abelian group, it is the direct sum $\mathbf{Z}/n\mathbf{Z} \oplus \mu_n$; its $\mathrm{Gal}(\overline{k}/k)$-module structure is therefore determined by an element y of the group

$$H^1(k, \mathrm{Hom}(\mathbf{Z}/n\mathbf{Z}, \mu_n)) = H^1(k, \mu_n) = k^*/k^{*n} .$$

As element of $H^2(k, B)$, we take the canonical image $\overline{x}$ of an element $x \in H^2(k, \mu_n)$; such an element can be identified with an element whose order divides n in the Brauer group $\mathrm{Br}(k)$, and as such it is equivalent to giving *local invariants* $x_v \in (\frac{1}{n}\mathbf{Z})/\mathbf{Z}$ satisfying the usual conditions ($\sum x_v = 0$, $2x_v = 0$ if v is a real place, and $x_v = 0$ if v is a complex place). We need that $\overline{x}$ does not vanish, but does vanish locally. The first condition amounts to saying that x does not belong to the image of $d : H^1(k, \mathbf{Z}/n\mathbf{Z}) \to H^2(k, \mu_n)$. This map is not difficult to make explicit; first the group $H^1(k, \mathbf{Z}/n\mathbf{Z})$ is nothing else than the group of homomorphisms $\chi : \mathrm{Gal}(\overline{k}/k) \to (\frac{1}{n}\mathbf{Z})/\mathbf{Z}$; from class field theory, χ is a homomorphism of the group of idèle classes of k into $(\frac{1}{n}\mathbf{Z})/\mathbf{Z}$; denote by (χ_v) the local components of χ. Then one checks that the coboundary $d\chi$ of χ is the element of $H^2(k, \mu_n)$ whose local components $(d\chi)_v$ equal $\chi_v(y)$. The first condition on x is therefore the following:

(a) *There does not exist any character* $\chi \in H^1(k, \mathbf{Z}/n\mathbf{Z})$ *such that* $x_v = \chi_v(y)$ *for all* v.

By expressing that $\overline{x}$ vanishes locally, we obtain in the same way:

(b) *For every place* v, *there exists* $\varphi_v \in H^1(k_v, \mathbf{Z}/n\mathbf{Z})$ *such that* $x_v = \varphi_v(y)$.

Numerical example: $k = \mathbf{Q}$, $y = 14$, $n = 8$, $x_v = 0$ for $v \neq 2$, 17 and $x_2 = -x_{17} = \frac{1}{8}$. We must check conditions (a) and (b):

Verification of (a) – Suppose we have a global character χ such that $\chi_v(14) = x_v$. Let us look at the sum $\sum \chi_v(16)$ (which should be zero, since χ vanishes on the principal idèles). It is well-known that 16 is an 8-th power in the local fields $\mathbf{Q}_p$, $p \neq 2$ (cf. Artin-Tate, [6], p. 96); therefore $\chi_v(16) = 0$ for $v \neq 2$.

Moreover, one has $14^4 \equiv 16 \bmod \mathbf{Q}_2^{*8}$ [this amounts to $7^4 \in \mathbf{Q}_2^{*8}$, which is true because -7 is a 2-adic square]. We deduce that $\chi_2(16) = 4\chi_2(14) = \frac{1}{2}$, and the sum of the $\chi_v(16)$ does not vanish. This is the contradiction we were looking for.

Verification of (b) – For $v \neq 2$, 17, we take $\varphi_v = 0$. For $v = 2$, we take the character of $\mathbf{Q}_2^*$ defined by the formula $\varphi_2(\alpha) = w(\alpha)/8$, where $w(\alpha)$ denotes the valuation of α; we then have $\varphi_2(y) = \varphi_2(14) = \frac{1}{8}$. For $v = 17$, notice that the multiplicative group $(\mathbf{Z}/17\mathbf{Z})^*$ is cyclic of order 16, and has $y = 14$ for its generator [it is enough to check that $14^8 \equiv -1 \bmod 17$, but $2^8 \equiv 1 \bmod 17$, and $7^8 \equiv (-2)^4 \equiv -1 \bmod 17$]. Therefore there exists a character φ_{17} of the group of 17-adic units which is of order 8 and takes the value $-\frac{1}{8}$ on y; we extend it to a character of order 8 of $\mathbf{Q}_{17}^*$, and that completes the verification of (b).

[This example was pointed out to me by Tate. The one I originally used was more complicated.]

Lemma 9. *Let B be a finite $\mathrm{Gal}(\overline{k}/k)$-module, and let $x \in H^2(k, B)$. There exists a connected semisimple group S defined over k, whose center Z contains B, and which has the following two properties:*

(a) *The given element x belongs to the image of $d : H^1(k, Z/B) \to H^2(k, B)$.*

(b) *We have $H^1(k_v, S) = 0$ for every place v of k.*

Let n be an integer ≥ 1 such that $nB = 0$. One can find a finite Galois extension K/k large enough so that the following three conditions are satisfied:

i) B is a $\mathrm{Gal}(K/k)$-module;

ii) the given element x comes from an element $x' \in H^2(\mathrm{Gal}(K/k), B)$;

iii) the field K contains the n-th roots of unity.

Let $B' = \mathrm{Hom}(B, \mathbf{Q}/\mathbf{Z})$ be the dual of B; it is obviously possible to write B' as a quotient of a free module over $\mathbf{Z}/n\mathbf{Z}[\mathrm{Gal}(K/k)]$. By duality, we see that *one may embed B in a free module Z of some finite rank q over* $\mathbf{Z}/n\mathbf{Z}[\mathrm{Gal}(K/k)]$. From the fact that Z is free, we have $H^2(\mathrm{Gal}(K/k), Z) = 0$ and there exists an element $y \in H^1(\mathrm{Gal}(K/k), Z/B)$ such that $dy' = x'$; the element y' defines an element $y \in H^1(k, Z/B)$, and we have $dy = x$. Therefore it all comes down to finding a semisimple group S with center Z and verifying condition (b) of the lemma.

For that, we start with the group $L = \mathbf{SL}_n \times \cdots \times \mathbf{SL}_n$ (q factors). If we look at L as an algebraic group over K, its center is isomorphic to $\mathbf{Z}/n\mathbf{Z} \times \cdots \times \mathbf{Z}/n\mathbf{Z}$ (all the elements of the center are rational over the base field because we have taken the precaution of assuming that K contains the n-th roots of unity). Let S be the group $R_{K/k}(L)$ deduced from L by restriction of the ground field from K to k. The center of S is isomorphic (as a $\mathrm{Gal}(\overline{k}/k)$-module) to the direct sum of q copies of

$$R_{K/k}(\mathbf{Z}/n\mathbf{Z}) = \mathbf{Z}/n\mathbf{Z}[\mathrm{Gal}(K/k)] \ ;$$

therefore we can identify it with the module Z introduced above. It remains to verify condition (b). But it is easy to see that S is isomorphic over k_v to the product of the groups $R_{K_w/k_v}(L)$, where w runs over the set of places of K extending v (cf. Weil, [185], p. 8); therefore we have $H^1(k_v, S) = \prod_{w|v} H^1(K_w, L) = 0$ since the cohomology of $\mathbf{SL}_n$ is trivial.

We can now construct our counter-example:

Theorem 8. *There exists a connected semisimple algebraic group G defined over k and an element $t \in H^1(k, G)$ such that:*

(a) *We have $t \neq 0$.*

(b) *For every place v of k, the image t_v of t in $H^1(k_v, G)$ is trivial.*

By lemma 8, there exist a finite $\mathrm{Gal}(\overline{k}/k)$-module B and an $x \in H^2(k, B)$ such that $x \neq 0$ and that the local images x_v of x are all zero. Let S be a semisimple group satisfying the conditions of lemma 9 with respect to the pair (B, x). From these conditions, the center Z of S contains B, and there exists an element $y \in H^1(k, Z/B)$ such that $dy = x$. Let G be the group S/B, and let t be the image of y in $H^1(k, G)$. We shall see that the pair (G, t) satisfies the conditions of the theorem.

(a) Let $\Delta : H^1(k, G) \to H^2(k, B)$ be the coboundary operator defined by the exact sequence $1 \to B \to S \to G \to 1$. The commutative diagram:

$$\begin{array}{ccc} H^1(k, Z/B) & \xrightarrow{d} & H^2(k, B) \\ \downarrow & & \mathrm{id} \downarrow \\ H^1(k, G) & \xrightarrow{\Delta} & H^2(k, B) \end{array}$$

shows that $\Delta(t) = dy = x$. Since $x \neq 0$, we have $t \neq 0$.

(b) Use the exact sequence:

$$H^1(k_v, S) \longrightarrow H^1(k_v, G) \longrightarrow H^2(k_v, B) \ .$$

The same argument as above shows that $\Delta(t_v) = x_v = 0$; since $H^1(k_v, S) = 0$ (cf. lemma 9), we have $t_v = 0$, QED.

Remarks.

1) The preceding construction gives groups G which are "strictly between" simply connected and adjoint. This leads one to ask whether the "Hasse principle" is true in these two extreme cases. This is actually the case, as was shown in a series of papers culminating in Chernousov [30] on E_8 (for a general survey, see Platonov-Rapinchuk [125], Chap. 6). When G is *simply connected*, one even has the following result, which was conjectured by M. Kneser [85] (and proved by him for the classical groups, cf. [85], [87]):

The canonical map $H^1(k, G) \to \prod H^1(k_v, G)$ is bijective.

(The product is extended to the places v such that $k_v \simeq \mathbf{R}$; for the other places, one has $H^1(k_v, G) = 0$, cf. [86].)

Thus, for example, if G is of type G_2, $H^1(k, G)$ has 2^r elements, where r is the number of real places of k.

2) T. Ono has used a construction analogous to that in lemma 9 to construct a semisimple group *whose Tamagawa number is not an integer*, cf. [121]. This led Borel (see [15]) to ask the following question: are there relations between the Tamagawa number and the validity of Hasse's principle? The answer is affirmative: for this see Sansuc [137], as well as Kottwitz [90], who uses the Hasse principle to prove the conjecture due to Weil according to which the Tamagawa number of a simply connected group equals 1. (Conversely, there are many cases where one can deduce the Hasse principle from a computation of Tamagawa numbers.)

Bibliographic remarks for Chapter III

The contents of §1 are "well-known" but have nowhere been given a satisfactory exposition — the present course included.

Conjectures I and II were stated at the Brussels Colloquium [146], in 1962. Theorems 1, 2, and 3 are due to Springer; the first two occur in his lecture in Brussels [162], and he communicated the proof of theorem 3 directly to me. According to Grothendieck (unpublished), one may prove a somewhat stronger result, namely the vanishing of the "nonabelian H^2" over any field of dimension ≤ 1.

§4 has been extracted, with little change, from Borel-Serre [18]; I have simply added the construction of a counter-example to the "Hasse principle".

* * *

Finally, here is a short list of texts about various types of semisimple groups containing (explicitly or implicitly) results on Galois cohomology:

General semisimple groups:
Grothendieck [60], Kneser [85], [86], Tits [175], [177], [178], [179], [180], Springer [162], Borel-Serre [18], Borel-Tits [20], Steinberg [165], Harder [67], [68], Bruhat-Tits [23], Chap. III, Sansuc [137], Platonov-Rapinchuk [125], Rost [132].

Classical groups and algebras with involutions:
Weil [184], Grothendieck [63], Tits [178], Kneser [87], Merkurjev-Suslin [109], Bayer-Lenstra [9], Bayer-Parimala [10].

Orthogonal groups and quadratic forms:
Witt [187], Springer [159], [160], Delzant [40], Pfister [124], Milnor [117], Lam [94], Arason [3], Merkurjev [107], [108], Scharlau [139], Jacob-Rost [78].

The group G_2 and the octonions:
Jacobson [79], van der Blij-Springer [12], Springer [163].

The group F_4 and the exceptional Jordan algebras:
Albert-Jacobson [2], Springer [161], [163], Jacobson [80], McCrimmon [105], Petersson [122], Rost [131], Petersson-Racine [123].

The group E_8:
Chernousov [30].

Appendix 1.
R. Steinberg – Regular elements of semisimple groups, Publ. Math. I.H.E.S. **25** (1965), 281–312

§ 1. Introduction and statement of results

We assume given an algebraically closed field K which is to serve as domain of definition and universal domain for each of the algebraic groups considered below; each such group will be identified with its group of elements (rational) over K. The basic definition is as follows. An element x of a semisimple (algebraic) group (or, more generally, of a connected reductive group) G of rank r is called *regular* if the centralizer of x in G has dimension r. It should be remarked that x is not assumed to be semisimple; thus our definition is different from that of [8, p. 7-03]. It should also be remarked that, since regular elements are easily shown to exist (see, e.g., 2.11 below) and since each element of G is contained in a (Borel) subgroup whose quotient over its commutator subgroup has dimension r, a regular element is one whose centralizer has the least possible dimension, or equivalently, whose conjugacy class has the greatest possible dimension.

In the first part of the present article we obtain various criteria for regularity, study the varieties of regular and irregular elements, and in the simply connected case construct a closed irreducible cross-section N of the set of regular conjugacy classes of G. Then assuming that G is (defined) over a perfect field k and contains a Borel subgroup over k we show that N (or in some exceptional cases a suitable analogue of N) can be constructed over k, and this leads us to the solution of a number of other problems of rationality. In more detail our principal results are as follows. Until 1.9 the group G is assumed to be semisimple.

1.1. *Theorem. — An element of* G *is regular if and only if the number of Borel subgroups containing it is finite.*

1.2. *Theorem. — The map* $x \to x_s$, *from* x *to its semisimple part, induces a bijection of the set of regular classes of* G *onto the set of semisimple classes. In other words:*

a) *every semi-simple element is the semisimple part of some regular element*;

b) *two regular elements are conjugate if and only if their semisimple parts are.*

The author would like to acknowledge the benefit of correspondence with T. A. Springer on these results (cf. 3.13, 4.7 *d)* below). The special case of *a)* which asserts the existence of regular unipotent elements (all of which are conjugate by *b)*) is proved in § 4. The other parts of 1.2 and 1.1, together with the fact that the number

in 1.1, if finite, always divides the order of the Weyl group of G, are proved in § 3, where other characterizations of regularity may be found (see 3.2, 3.7, 3.11, 3.12 and 3.14). This material follows a preliminary section, § 2, in which we recall some basic facts about semisimple groups and some known characterizations of regular semisimple elements (see 2.11).

1.3. *Theorem.* — a) *The irregular elements of* G *form a closed set* Q.

b) *Each irreducible component of* Q *has codimension* 3 *in* G.

c) Q *is connected unless* G *is of rank* 1, *of characteristic not* 2, *and simply connected, in which case* Q *consists of* 2 *elements.*

This is proved in § 5 where it is also shown that the number of components of Q is closely related to the number of conjugacy classes of roots under the Weyl group. An immediate consequence of 1.3 is that the regular elements form a dense open subset of G.

It may be remarked here that 1.1 to 1.3 and appropriate versions of 1.4 to 1.6 which follow hold for connected reductive groups as well as for semisimple groups, the proofs of the extensions being essentially trivial.

In § 6 the structure of the algebra of class functions (those constant on conjugacy classes) is determined (see 6.1 and 6.9). In 6.11, 6.16, and 6.17 this is applied to the study of the closure of a regular class and to the determination of a natural structure of variety for the set of regular classes, the structure of affine r-space in case G is simply connected.

1.4. *Theorem.* — *Let* T *be a maximal torus in* G *and* $\{\alpha_i \mid 1 \leq i \leq r\}$ *a system of simple roots relative to* T. *For each* i *let* X_i *be the one-parameter unipotent subgroup normalized by* T *according to the root* α_i *and let* σ_i *be an element of the normalizer of* T *corresponding to the reflection relative to* α_i. *Let* $N = \prod_{i=1}^{r} (X_i \sigma_i) = X_1 \sigma_1 X_2 \sigma_2 \dots X_r \sigma_r$. *If* G *is a simply connected group, then* N *is a cross-section of the collection of regular classes of* G.

In 7.4 an example of N is given: in case G is of type $SL(r+1)$ we obtain one of the classical normal forms under conjugacy. This special case suggests the problem of extending the normal form N from regular elements to arbitrary elements. In 7.1 it is shown that N is a closed irreducible subset of G, isomorphic as a variety to affine r-space V, and in 7.9 (this is the main lemma concerning N) that, if G is simply connected, and χ_i $(1 \leq i \leq r)$ denote the fundamental characters of G, then the map $x \to (\chi_1(x), \chi_2(x), \dots, \chi_r(x))$ induces an isomorphism of N on V. Then in § 8 the proof of 1.4 is given and simultaneously the following important criterion for regularity is obtained.

1.5. *Theorem.* — *If* G *is simply connected, the element* x *is regular if and only if the differentials* $d\chi_i$ *are independent at* x.

At this point some words about recent work of B. Kostant are in order. In [3] and [4] he has proved, among other things, the analogues of our above discussed results that are obtained by replacing the semisimple group G by a semisimple Lie

algebra L over the complex field (any algebraically closed field of characteristic o will serve as well) and the characters χ_i of G by the basic polynomial invariants u_i of L. The χ_i turn out to be considerably more tractable than the u_i. Thus the proofs for G with no restriction on the characteristic are simpler than those for L in characteristic o. Assuming both G and L are in characteristic o, substantial parts of 1.1, 1.2, and 1.3 can be derived from their analogues for L, but there does not seem to be any simple way of relating 1.4 and 1.5 to their analogues for L.

We now introduce a perfect subfield k of K, although it appears from recent results of A. Grothendieck on semisimple groups over arbitrary fields that the assumption of perfectness is unnecessary for most of what follows.

1.6. *Theorem. — Let* G *be over k, and assume either that* G *splits over k or that* G *contains a Borel subgroup over k but no component of type* A_n *(n even). Then the set* N *of* 1.4 *can be constructed over k (by appropriate choice of* T, σ_i, *etc.).*

Together with 1.4 this implies that if G is simply connected in 1.6 the natural map from the set of regular elements over k to the set of regular classes over k is surjective. For a group of type A_n (n even) we have a substitute (see 9.7) for 1.6 which enables us to show:

1.7. *Theorem. — Assume that* G *is simply connected and over k and that* G *contains a Borel subgroup over k. Then the natural map from the set of semisimple elements over k to the set of semisimple classes over k is surjective. In other words, each semisimple class over k contains an element over k.*

Theorems 1.6 and 1.7 are proved in § 9 where it is also shown (see 9.1 and 9.10) that the assumption that G contains a Borel subgroup over k is essential.

1.8. *Theorem. — Under the assumptions of* 1.7 *each element of the cohomology set* $H^1(k, G)$ *can be represented by a cocycle whose values are in a torus over k.*

In § 10 this result is deduced from 1.7 by a method of proof due to M. Kneser, who has also proved 1.7 in a number of special cases and has formulated the general case as a conjecture. In 9.9 and 10.1 it is shown that 1.7 and 1.8 hold for arbitrary simply connected, connected linear groups, not just for semisimple ones.

In § 10 it is indicated how Theorem 1.8 provides the final step in the proof of the following result, 1.9, the earlier steps being due to J.-P. Serre and T. A. Springer (see [12], [13] and [15]). We observe that G is no longer assumed to be semisimple, and recall [12, p. 56-57] that (cohomological) $\dim k \leq 1$ means that every finite-dimensional division algebra over k is commutative.

1.9. *Theorem. — Let k be a perfect field. If* a) $\dim k \leq 1$, *then* b) $H^1(k, G) = 0$ *for every connected linear group* G *over k, and* c) *every homogeneous space* S *over k for every connected linear group* G *over k contains a point over k.*

The two parts of 1.9 are the conjectures I and I′ of Serre [12]. Conversely *b)* implies *a)* by [12, p. 58], and is the special case of *c)* in which only principal homogeneous spaces are considered; thus *a)*, *b)* and *c)* are equivalent. They are also equivalent to: every connected linear group over k contains a Borel subgroup over k [15, p. 129].

After some consequences of 1.9, of which only the following (cf. 1.7) will be stated here, the paper comes to a close.

1.10. *Theorem. — Let k be a perfect field such that* $\dim k \leq 1$ *and* G *a connected linear group over k. Then every conjugacy class over k contains an element over k.*

After the remark that Kneser, using extensions of 1.8, has recently shown (cf. 1.9) that $H^1(k, G) = 0$ if k is a p-adic field and G a simply connected semisimple group over k, this introduction comes to a close.

§ 2. Some recollections

In this section we recall some known facts, including some characterizations 2.11 of regular semisimple elements, and establish some notations which are frequently used in the paper. If k is a field, k^* is its multiplicative group. The term " algebraic group " is often abbreviated to " group ". If G is a group, G_0 denotes its identity component. If x is an element of G, then G_x denotes the centralizer of x in G, and x_s and x_u denote the semisimple and unipotent parts of x when G is linear. Assume now that G is a semisimple group, that is, G is a connected linear group with no nontrivial connected solvable normal subgroup. We write r for the rank of G. Assume further that T is a maximal torus in G and that an ordering of the (discrete) character group of T has been chosen. We write Σ for the system of roots relative to T and X_α for the subgroup corresponding to the root α.

2.1. *X_α is unipotent and isomorphic (as an algebraic group) to the additive group (of* K*). If x_α is an isomorphism from* K *to X_α, then $tx_\alpha(c)t^{-1} = x_\alpha(\alpha(t)c)$ for all α and c.*

For the proof of 2.1 to 2.6 as well as the other standard facts about linear groups, the reader is referred to [8].

We write U (resp. U^-) for the group generated by those X_α for which α is positive (resp. negative), and B for the group generated by T and U.

2.2. a) *U is a maximal unipotent subgroup of* G, *and* B *is a Borel (maximal connected solvable) subgroup.*

b) *The natural maps from the Cartesian product* $\prod_{\alpha>0} X_\alpha$ *(fixed but arbitrary order of the factors) to* U *and from* $T \times U$ *to* B *are isomorphisms of varieties.*

In *b)* the X_α component of an element of U may change with the order, but not if α is simple.

2.3. *The natural map from* $U^- \times T \times U$ *to* G *is an isomorphism onto an open subvariety of* G.

We write W for the Weyl group of G, that is, the quotient of T in its normalizer. W acts on T, via conjugation, hence also on the character group of T and on Σ. For each w in W we write σ_w for an element of the normalizer of T which represents w.

2.4. a) *The elements σ_w ($w \in W$) form a system of representatives of the double cosets of* G *relative to* B.

b) *Each element of $B\sigma_w B$ can be written uniquely $u\sigma_w b$ with u in $U \cap \sigma_w U^- \sigma^{-1}$ and b in* B.

The simple roots are denoted α_i $(1 \leq i \leq r)$. If $\alpha = \alpha_i$ we write X_i, x_i for X_α, x_α, and G_i for the group (semisimple of rank 1) generated by X_α and $X_{-\alpha}$. The reflection in W corresponding to α_i is denoted w_i. If $w = w_i$ we write σ_i in place of σ_w.

2.5. *The element σ_i can be chosen in G_i. If this is done, and $B_i = B \cap G_i = (T \cap G_i)X_i$, then G_i is the disjoint union of B_i and $X_i \sigma_i B_i$.*

The following may be taken as a definition of the term " simply connected ".

2.6. *The semisimple group G is simply connected if and only if there exists a basis $\{\omega_j\}$ of the dual (character group) of T such that $w_i \omega_j = \omega_j - \delta_{ij}\alpha_i$ (Kronecker delta, $1 \leq i, j \leq r$).*

An arbitrary connected linear group is simply connected if its quotient over its radical satisfies 2.6. If G is as in 2.6 we write χ_i for the i^{th} fundamental character of G, that is, for the trace of the irreducible representation whose highest weight on T is ω_i.

2.7. *Let G be a semisimple group of rank r and x a semisimple element of G.*

a) *G_{x0} is a connected reductive group of rank r. In other words, $G_{x0} = G'T'$ with G' a semisimple group, T' a central torus in G_{x0}, the intersection $G' \cap T'$ finite, and* rank G' + rank $T' = r$. *Further G' and T' are uniquely determined as the commutator subgroup and the identity component of the centre of G_{x0}.*

b) *The unipotent elements of G_x are all in G'.*

Part *b)* follows from *a)* because G_{x0} contains the unipotent elements of G_x by [8, p. 6-15, Cor. 2]. For the proof of *a)* we may imbed x in a maximal torus T and use the above notation. If y in G_x is written $y = u\sigma_w b$ as in 2.4 then the uniqueness in 2.4 implies that u, σ_w and b are in G_x. By 2.1 and 2.2 we get:

2.8. *G_x is generated by T, those X_α for which $\alpha(x) = 1$, and those σ_w for which $wx = x$.*

Then G_{x0} is generated by T and the X_α alone because the group so generated is connected and of finite index in G_x (see [8, p. 3-01, Th. 1]). Let G' be the group generated by the X_α alone, and let T' be the identity component of the intersection of the kernels of the roots α such that $\alpha(x) = 1$. Then G' is semisimple by [8, p. 17-02, Th. 1], and the other assertions of *a)* are soon verified.

2.9. *Corollary. — In 2.7 every maximal torus containing x also contains T'.*

For in the above proof T was chosen as an arbitrary torus containing x.

2.10. *Remark.* — That G_x in 2.7 need not be connected, even if x is regular, is shown by the example: $G = PSL(2)$, $x = \text{diag}(i, -i)$, $i^2 = -1$. If G is simply connected, however, G_x is necessarily connected and in 2.8 the elements σ_w may be omitted. More generally, the group of fixed points of a semisimple automorphism of a semisimple group G is reductive, and if the automorphism fixes no nontrivial point of the fundamental group of G, it is connected. (The proofs of these statements are forthcoming.)

2.11. *Let G and x be as in 2.7. The following conditions are equivalent:*

a) *x is regular.*

b) *G_{x0} is a maximal torus in G.*

c) *x is contained in a unique maximal torus T in G.*

d) *G_x consists of semisimple elements.*

e) *If T is a maximal torus containing x then $\alpha(x) \neq 1$ for every root α relative to T.*

G_{x0} contains every torus which contains x. Thus *a)* and *b)* are equivalent and *b)* implies *c)*. If *c)* holds, G_x normalizes T, whence G_x/T is finite and $G_{x0}=T$, which is *b)*. By 2.7 *b)*, *b)* implies *d)*, which in turn, by 2.1, implies *e)*. Finally *e)* implies, by 2.8, that G_x/T is finite, whence *b)*.

2.12. *Lemma. — Let* $B'=T'U'$ *with* B′ *a connected solvable group,* T′ *a maximal torus, and* U′ *the maximal unipotent subgroup. If t and u are elements of* T′ *and* U′, *there exists u′ in* U′ *such that tu′ is conjugate to tu via an element of* U′, *and u′ commutes with t.*

For the semisimple part of *tu* is conjugate, under U′, to an element of T′ by [8, p. 6-07], an element which must be *t* itself because U′ is normal in B′.

2.13. *Corollary. — In the semisimple group* G *assume that t is a regular element of* T *and u an arbitrary element of* U. *Then tu is a regular element, in fact is conjugate to t.*

By 2.12 we may assume that *u* commutes with *t*, in which case $u=1$ by 2.1 and 2.2 *b)*.

2.14. *The regular semisimple elements form a dense open set* S *in* G.

By 2.12, 2.13 and 2.11 (see *a)* and *e)*), $S\cap B$ is dense and open in B. Since the conjugates of B cover G by [8, p. 6-13, Th. 5], S is dense in G. Let A be the complement of $S\cap B$ in B, and let C be the closed set in $G/B\times G$ consisting of all pairs $(\overline{x},y)$ (here $\overline{x}$ denotes the coset xB) such that $x^{-1}yx\in A$. The first factor, G/B, is complete by [8, p. 6-09, Th. 4]. By a characteristic property of completeness, the projection on the second factor is closed. The complement, S, is thus open.

We will call an element of G *strongly regular* if its centralizer is a maximal torus. Such an element is regular and semisimple, the converse being true if G is simply connected by 2.10.

2.15. *The strongly regular elements form a dense open set in* G.

The strongly regular elements form a dense open set in T, characterized by $\alpha(t)\neq 1$ for all roots α, and $wt\neq t$ for all $w\neq 1$ in W. Thus the proof of 2.14 may be applied.

§ 3. Some characterizations of regular elements

Throughout this section and the next G denotes a semisimple group. Our aim is to prove 1.1 and 1.2 (of § 1). The case of unipotent elements will be considered first. The following critical result is proved in § 4.

3.1. *Theorem. — There exists in* G *a regular unipotent element.*

3.2. *Lemma. — There exists in* G *a unipotent element contained in only a finite number of Borel subgroups. Indeed let x be a unipotent element and n the number of Borel subgroups containing it. Then the following are equivalent:*

a) *n is finite.*

b) *n is* 1.

c) *If x is imbedded in a maximal unipotent subgroup* U *and the notation of* § 2 *is used, then for* $1\leq i\leq r$ *the* X_i *component of x is different from* 1.

Let T be a maximal torus which normalizes U, let $B = TU$, and let B′ be an arbitrary Borel subgroup. By the conjugacy theorem for Borel subgroups and 2.4 we have $B' = u\sigma_w B \sigma_w^{-1} u^{-1}$ with u and σ_w as in 2.4 *b)*. If *c)* holds and B′ contains x, then B contains $\sigma_w^{-1}u^{-1}xu\sigma_w$ and every X_i component of $u^{-1}xu$ is different from 1. Thus $w\alpha_i$ is positive for every simple root α_i and w is 1, whence $B' = B$ and *b)* holds. If *c)* fails, then for some i the Borel subgroups $u\sigma_i B \sigma_i^{-1} u^{-1}$ $(u \in X_i)$ all contain x, whence *a)* fails. Thus *a)*, *b)* and *c)* are equivalent. Since elements which satisfy *c)* exist in abundance, the first statement in 3.2 follows.

3.3. *Theorem.* — *For a unipotent element x of* G *the following are equivalent*:

a) *x is regular.*

b) *The number of Borel subgroups containing x is finite.*

Further the unipotent elements which satisfy a) *and* b) *form a single conjugacy class.*

Let y and z be arbitrary unipotent elements which satisfy *a)* and *b)*, respectively. Such elements exist by 3.1 and 3.2. We will prove all assertions of 3.3 together by showing that y is conjugate to z. By replacing y and z by conjugates we may assume they are both in the group U of § 2 and use the notations there. Let y_i and z_i denote the X_i components of y and z. By 3.2 every z_i is different from 1. We assert that every y_i is also different from 1. Assume the contrary, that $y_i = 1$ for some i, and let U_i be the subgroup of elements of U whose X_i components are 1. Then y is in U_i, so that in the normalizer $P_i = G_i T U_i$ of U_i we have $\dim(P_i)_y = \dim P_i - \dim(\text{class of } y) \geq \dim P_i - \dim U_i = r + 2$. This contradiction to the regularity of y proves our assertion. Hence by conjugating y by an element of T we may achieve the situation: $y_i = z_i$ for all i, or, in other words, zy^{-1} is in U′, the intersection of all U_i. Now the set $\{uyu^{-1}y^{-1} \mid u \in U\}$ is closed (by [7] every conjugacy class of U is closed). Its codimension in U is at most r because y is regular, whence its codimension in U′ is at most $r - (\dim U - \dim U') = 0$. The set thus coincides with U′. For some u in U we therefore have $uyu^{-1}y^{-1} = zy^{-1}$, whence $uyu^{-1} = z$, and 3.3 is proved.

In the course of the argument the following result has been proved.

3.4. *Corollary.* — *If x is unipotent and irregular, then* $\dim G_x \geq r + 2$.

If P_i is replaced by B in the above argument, the result is:

3.5. *Corollary.* — *If x is unipotent and irregular and* B *is any Borel subgroup containing x, then* $\dim B_x \geq r + 1$.

3.6. *Lemma.* — *Let x be an element of* G, *and y and z its semisimple and unipotent parts. Let* $G_{y0} = G'T'$ *with* G′ *and* T′ *as in* 2.7, *and let r' be the rank of* G′. *Let* S (*resp.* S′) *be the set of Borel subgroups of* G (*resp.* G′) *containing x* (*resp.* z):

a) $\dim G_x = \dim G'_z + r - r'$.

b) *If* B *in* S *contains* B′ *in* S′ *then* $\dim B_x = \dim B'_z + r - r'$.

c) *Each element* B *of* S *contains a unique element of* S′, *namely*, $B \cap G'$.

d) *Each element of* S′ *is contained in at least one but at most a finite number of elements of* S.

We have $G_x = (G_y)_z$ by [8, p. 4-08]. Thus $\dim G_x = \dim G'_z + \dim T'$, whence *a)*. Part *b)* may be proved in the same way, once it is observed that $B_y = B'T'$. For B_y is solvable, connected by [8, p. 6-09], and contains the Borel subgroup $B'T'$ of G_y. Let B be in S. Let T be a maximal torus in B containing y, and let the roots relative to T be ordered so that B corresponds to the set of positive roots. The group G' is generated by those X_α for which $\alpha(y) = 1$, and the corresponding α form a root system Σ' for G' by [8, p. 17-02, Th. 1]. By 2.2 *a)* the groups $T \cap G'$ and X_α ($\alpha > 0$, $\alpha \in \Sigma'$) generate a Borel subgroup of G' which is easily seen to be none other than $B \cap G'$ (by 2.1 and 2.2 *b)*), whence *c)* follows. Let B' be in S'. Then a Borel subgroup B of G contains B' and is in S if and only if it contains $B'T'$. For if B contains x, it also contains y, then a maximal torus containing y by [8, p. 6-13], then T' by 2.9; while if B contains the Borel subgroup $B'T'$ of G_{y0}, it contains the central element y by [8, p. 6-15], thus also x. The number of possibilities for B above is at least 1 because $B'T'$ is a connected solvable group, but it is at most the order of the Weyl group of G because $B'T'$ contains a maximal torus of G (this last step is proved in [8, p. 9-05, Cor. 3], and also follows from 2.4).

3.7. *Corollary. — In* 3.6 *the element x is regular in* G *if and only if z is regular in* G', *and the set* S *is finite if and only if* S' *is.*

The first assertion follows from 3.6 *a)*, the second from *c)* and *d)*.

3.8. *Corollary. — In* 3.6 *the element x is regular in* G *if and only if the set* S *is finite.*

Observe that this is Theorem 1.1 of § 1. It follows from 3.7 and 3.3 (applied to z).

3.9. *Corollary. — The assertions* 3.4 *and* 3.5 *are true without the assumption that x is unipotent.*

For the first part we use 3.6 *a)*, for the second *b)* and *c)*.

3.10. *Conjecture. — For any x in* G *the number* $\dim G_x - r$ *is even.*

It would suffice to prove this when x is unipotent. The corresponding result for Lie algebras over the complex field is a simple consequence of the fact that the rank of a skew symmetric matrix is always even (see [4, p. 364, Prop. 15]).

3.11. *Corollary. — If x is an element of* G, *the following are equivalent.*

a) $\dim G_x = r$, *that is, x is regular.*

b) $\dim B_x = r$ *for every Borel subgroup* B *containing x.*

c) $\dim B_x = r$ *for some Borel subgroup* B *containing x.*

As we remarked in the first paragraph of § 1, $\dim B_x \geq r$. Thus *a)* implies *b)*. By 3.5 as extended in 3.9 we see that *c)* implies *a)*.

3.12. *Corollary. — In* 3.6 *let x be regular and n the number of Borel subgroups containing x.*

a) $n = |W|/|W'|$, *the ratio of the orders of the Weyl groups of* G *and* G'.

b) $n = 1$ *if and only if z is a regular unipotent element of* G *and y is an element of the centre.*

c) $n = |W|$ *if and only if x is a regular semisimple element of* G.

By 3.7, 3.2 and 3.3 the element z is regular and contained in a unique Borel subgroup B' of G'. Let T be a maximal torus in B'T'. Then n is the number of Borel subgroups of G containing B' and T. Now each of the $|W'|$ Borel subgroups of G' normalized by T (these are just the conjugates of B' under W') is contained in the same number of Borel subgroups of G containing T, and each of the $|W|$ groups of the latter type contains a unique group of the former type by 3.6 *c)*. Thus *a)* follows. Then $n=1$ if and only if $|W'|=|W|$, that is, $G'=G$, which yields *b)*; and $n=|W|$ if and only if $|W'|=1$, that is, $G'=1$ and $G_{y0}=T'$, which by 2.11 (see *a)*, *b)* and *d)*) is equivalent to y regular and $x=y$, whence *c)*.

3.13. *Remark.* — Springer has shown that if x is regular in G then G_{x0} is commutative. Quite likely the converse is true (it is for type A_r). It would yield the following characterization of the regular elements, in the abstract group, G_{ab}, underlying G. The element x of G_{ab} is regular in G if and only if G_x contains a commutative subgroup of finite index. We have the following somewhat bulkier characterization.

3.14. *Corollary.* — *The element x of G_{ab} is regular if and only if it is contained in only a finite number of subgroups each of which is maximal solvable and without proper subgroups of finite index.*

For each such subgroup is closed and connected, hence a Borel subgroup. We remark that G_{ab} determines also the sets of semisimple and unipotent elements (hence also the decomposition $x=x_sx_u$), as well as the semisimplicity, rank, dimension, and base field (to within an isomorphism), all of which would be false if G were not semisimple. If G is simple, then G_{ab} determines the topology (the collection of closed sets) in G completely, which is not always the case if G is semisimple.

To close this section we now prove Theorem 1.2. Let y be semisimple in G, and $G_{y0}=G'T'$ as in 3.6. By 3.1 there exists in G' a regular unipotent element z. Let $x=yz$. Then x is regular in G by 3.7 and $x_s=y$, whence *a)* holds. Let x and x' be regular elements of G. If x is conjugate to x', then clearly x_s is conjugate to x'_s. If x_s is conjugate to x'_s, we may assume $x_s=x'_s=y$, say. Then in G' (as above) the elements x_u and x'_u are regular by 3.7, hence conjugate by 3.3, whence x and x' are conjugate.

§ 4. The existence of regular unipotent elements

This section is devoted to the proof of 3.1. Throughout G is a semisimple group, T a maximal torus in G, and the notations of § 2 are used. In addition V denotes a real totally ordered vector space of rank r which extends the dual of T and its given ordering.

4.1. *Lemma.* — *Let the simple roots α_i be so labelled that the first q are mutually orthogonal as are the last $r-q$. Let $w=w_1w_2\dots w_r$.*

a) *The roots are permuted by w in r cycles.*

The space V *can be reordered so that*

b) *roots originally positive remain positive,*

and

c) *each cycle of roots under w contains exactly one relative maximum and one relative minimum.*

We observe that since the Dynkin graph has no circuits [9, p. 13-02] a labelling of the simple roots as above is always possible. In *c)* a root α is, for example, a maximum in its cycle under w if $\alpha > w\alpha$ and $\alpha > w^{-1}\alpha$ for the order on V. The proof of 4.1 depends on the following results proved in [16]. (These are not explicitly stated there, but see 3.2, 3.6, the proof of 4.2, and 6.3.)

4.2. *Lemma.* — *In* 4.1 *assume that* Σ *is indecomposable, that a positive definite inner product invariant under* W *is used in* V, *and that* n *denotes the order of* w.

a) *The roots of* Σ *are permuted by* w *in* r *cycles each of length* n.

If $\dim \Sigma > 1$, *there exists a plane* P *in* V *such that*

b) P *contains a vector* v *such that* $(v, \alpha) > 0$ *for every positive root* α,

and

c) w *fixes* P *and induces on* P *a rotation through the angle* $2\pi/n$.

For the proof of 4.1 we may assume that Σ is indecomposable, and, omitting a trivial case, that $\dim \Sigma > 1$. We choose P and v as in 4.2. Let α' denote the orthogonal projection on P of the root α. By 4.2 *b)* it is nonzero. Since by 4.2 *c)* the vectors $w^{-i}v$ $(1 \leq i \leq n)$ form the vertices a regular polygon, it can be arranged, by a slight change in v, that for each α these vectors make distinct angles with α'. It is then clear that there is one relative maximum and one relative minimum for the cycle of numbers $(w^{-i}v, \alpha')$. Since $(w^{-i}v, \alpha') = (w^{-i}v, \alpha) = (v, w^{i}\alpha)$, we can achieve *c)* by reordering V so that vectors v' for which $(v, v') > 0$ become positive. Then *a)* and *b)* also hold by 4.2 *a)* and 4.2 *b)*.

4.3. *Lemma.* — *Let* G *be simply connected, otherwise as above. Let* $\mathfrak{g}$ *be the Lie algebra of* G. *Let* $\mathfrak{t}$ *be the subalgebra corresponding to* T, *and* $\mathfrak{z}$ *the subalgebra of elements of* $\mathfrak{t}$ *which vanish at all roots on* T. *Let* w *be as in* 4.1. *Let* x *be an element of the double coset* $B\sigma_w B$, *and let* $\mathfrak{g}_x$ *denote the algebra of fixed points of* x *acting on* $\mathfrak{g}$ *via the adjoint representation. Then* $\dim \mathfrak{g}_x \leq \dim \mathfrak{z} + r$.

We identify $\mathfrak{g}$ with the tangent space to G at 1. Then by 2.3 we have a direct sum decomposition $\mathfrak{g} = \mathfrak{t} + \sum_{\alpha} K\mathfrak{x}_\alpha$ in which $K\mathfrak{x}_\alpha$ may be identified with the tangent space of X_α. We order the weights of the adjoint representation, that is, 0 and the roots, as in 4.1. By replacing x by a conjugate, we may assume $x = b\sigma_w$ $(b \in B)$.

1) *If* $\mathfrak{v}$ *in* $\mathfrak{g}$ *is a weight vector, then* $(1 - x)\mathfrak{v} = \mathfrak{v} - c\sigma_w \mathfrak{v} +$ *terms (corresponding to weights) higher than (that of)* $\sigma_w \mathfrak{v}$ $(c \in K^*)$. This follows from 7.15 *d)* below, which holds for any rational representation of G.

2) *If the root* α *is not maximal in its cycle under* w, *then* $(1 - x)\mathfrak{g}$ *contains a vector of the form* $c\mathfrak{x}_\alpha +$ *higher terms* $(c \in K^*)$. If $w\alpha > \alpha$ we apply 1) with $\mathfrak{v} = \mathfrak{x}_\alpha$, while if $w\alpha < \alpha$ we use $\mathfrak{v} = \sigma_w^{-1}\mathfrak{x}_\alpha$ instead.

3) *There exist* $r - \dim \mathfrak{z}$ *independent elements* $\mathfrak{t}_i$ *of* $\mathfrak{t}$ *such that for every* i *the space* $(1 - x)\mathfrak{g}$ *contains a vector of the form* $\mathfrak{t}_i +$ *higher terms.* Because of 1), in which $c = 1$ if $\mathfrak{v}$ is in $\mathfrak{t}$, this follows from:

4) *The kernel of* $1 - \sigma_w$ *on* $\mathfrak{t}$ *is* $\mathfrak{z}$. Because the adjoint action of σ_w on $\mathfrak{t}$ stems from the action of w on T by conjugation, we may write w in place of σ_w, on $\mathfrak{t}$. Assume

$(1-w)t_0=0$ with t_0 in t. Then $(1-w_1)t_0=(1-w_2\dots w_r)t_0$. If we evaluate the left side at the functions $\omega_2, \dots, \omega_r$ of 2.6 or the right side at ω_1 then by 2.6 we always get 0, whence both sides are 0. By an obvious induction we get that $(1-w_i)t_0=0$ for all i, and on evaluation at ω_i, that $t_0(\alpha_i)=t_0((1-w_i)\omega_i)=0$. Thus t_0 is in 3. One may reverse the steps to show that 3 is contained in the kernel of $1-\sigma_w$, whence 4).

Lemma 4.3 is a consequence of 2) and 3).

4.4. *Remark.* — One can show that 3 in 4.3 is the centre of g.

4.5. *Lemma. — Let the notation be as in* 4.1. *Let w_0 be the element of* W *which maps each positive root onto a negative one, and π the permutation defined by* $-w_0\alpha_i=\alpha_{\pi i}$ $(1\leq i\leq r)$. *Let σ_0 be an element of the normalizer of* T *which represents w_0. For each i let u_i be an element of $X_{\pi i}$ different from* 1 *and let* $x=u_1u_2\dots u_r$. *Then $\sigma_0x\sigma_0^{-1}$ is in* $B\sigma_wB$.

We have $\sigma_0u_i\sigma_0^{-1}$ in G_i-B, hence in $B\sigma_iB$ by 2.5. Since

$$B\sigma_1\dots\sigma_{i-1}B\sigma_iB=B\sigma_1\dots\sigma_{i-1}X_i\sigma_iB=B\sigma_1\dots\sigma_iB,$$

because w_i permutes the positive roots other than α_i by [8, p. 14-04, Cor. 3], and each root $w_1w_2\dots w_{i-1}\alpha_i$ is positive (cf. 7.2 *a)*) we get 4.5.

4.6. *Theorem. — The element x of* 4.5 *is regular.*

By going to the simply connected covering group, we may assume that G is simply connected. For any subalgebra $\mathfrak{a}$ of $\mathfrak{g}$ we write $\mathfrak{a}_x$ for the subalgebra of elements fixed by x. Let $\mathfrak{b}$ and $\mathfrak{u}$ denote the subalgebras corresponding to B and U. By 4.3 and 4.5 we have $\dim \mathfrak{b}_x\leq\dim \mathfrak{g}_x\leq\dim \mathfrak{z}+r$. An infinitesimal analogue of 2.1 yields $x_\alpha(c)t_0=t_0+c'ct_0(\alpha)\dot{x}_\alpha$ for all t_0 in t and some c' in K, whence $\mathfrak{t}_x$ contains $\mathfrak{z}$, and $\dim \mathfrak{b}_x\geq\dim \mathfrak{z}+\dim \mathfrak{u}_x$. Combined with the previous inequality this yields $\dim \mathfrak{u}_x\leq r$, whence $\dim U_x\leq r$. From the form of x we see that B is the unique Borel subgroup containing x. Each element of G_x normalizes B, hence belongs to B by [8, p. 9-03, Th. 1], or else by 2.4. Now if ut $(t\in T, u\in U)$ is in B_x then, working in B modulo the commutator subgroup of U, and using the fact that each X_i component of x is different from 1, we get $\alpha_i(t)=1$ for all i, whence t is in the centre of G, a finite group. Hence $\dim G_x=\dim U_x\leq r$, as required.

4.7. *Remarks. — a)* The condition $\dim U_x=r$ on x in U is not enough to make x regular, as one sees by examples in a group of type A_2. The added condition that all X_i components are different from 1 is essential.

b) If the characteristic of K is 0, or, more generally, if $\dim \mathfrak{z}\leq 1$ in 4.3, we may conclude from 4.3 and 3.4 as extended in 3.9 that all elements of $B\sigma_wB$ are regular, and then (cf. 7.3) that all elements of N in 1.4 are regular. There is, however, an exception: $\dim \mathfrak{z}=2$ if G is of type D_r (r even) and of characteristic 2. It is nevertheless true that all elements of $B\sigma_wB$ are regular (cf. 8.8). By 4.5 this implies that if x is the regular element of 4.6 and t in T is arbitrary, then tx is regular. If u is an arbitrary regular element of U, however, tu need not be regular: consider in SL(3) the superdiagonal matrix with diagonal entries -1, 1, -1 and superdiagonal entries all 2. In contrast if t is regular and u is arbitrary, then tu is regular by 2.13.

c) In characteristic 0 one may, in the simply connected case, imbed the element x of 4.6 in a subgroup isomorphic to SL(2) and then use the theory of the representations of this latter group to prove that x is regular. This is the method of Kostant, worked out in [3] for Lie algebras over the complex field. In the general case, however, a regular unipotent element can not be imbedded in the group SL(2), or even in the $ax+b$ group: in characteristic $p \neq 0$, a unipotent element of either of these groups has order at most p, while in a group G of type A_r, for example, a regular unipotent element has order at least $r+1$, so that if $r+1>p$ the imbedding is impossible.

d) Springer has studied U_x (x as in 4.6) by a method depending on a knowledge of the structural constants of the Lie algebra of U. His methods yield a proof of the regularity of x only if

(*) p does not divide any coefficient in the highest root of any component of G,

but it yields also that U_x is connected if and only if (*) holds, a result which quite likely has cohomological applications, since (*) is necessary and quite close to sufficient for the existence of p-torsion in the simply connected compact Lie group of the same type as G (see [1]).

e) The group G of type B_2 and characteristic 2 yields the simplest example in which U_x is not connected (it has 2 pieces). In this group every sufficiently general element of the centre of U is an irregular unipotent element whose centralizer is unipotent. Hence not every unipotent element is the unipotent part of a regular element (cf. 1.2 *a)*).

§ 5. Irregular elements

Our aim is to prove 1.3. The assumptions of § 4 continue. We write T_i for the kernel of α_i on T, U_i for the group generated by all X_α for which $\alpha>0$ and $\alpha \neq \alpha_i$, B_i for $T_i U_i$ ($1 \leq i \leq r$). The latter is a departure from the notation of 2.5.

5.1. *Lemma. — An element of* G *is irregular if and only if it is conjugate to an element of some* B_i.

For the proof we may restrict attention to elements of the form $x=yz$ ($y \in T$, $z \in U \cap G_y$) by 2.12. Let G′ be as in 3.6. The root system Σ' for G′ consists of all roots α such that $\alpha(y)=1$. It inherits an ordering from that of Σ. Assume first that x is in B_i. Then α_i is in Σ', and the X_i component of z is 1. Thus z is irregular in G′ by 3.2 and 3.3, whence x is irregular in G by 3.7. Assume now that x is irregular in G so that z is irregular in G′. If we write $z=\prod_\alpha u_\alpha$ ($u_\alpha \in X_\alpha$, $\alpha>0$, $\alpha \in \Sigma'$), we have $u_\alpha=1$ for some root α simple in Σ', by 3.2 and 3.3. We prove by induction on the height of α (this is $\sum_i n_i$ if $\alpha=\sum_i n_i \alpha_i$) that x may be replaced by a conjugate such that α above is simple in Σ. This conjugate will be in some B_i, and 5.1 will follow. We assume the height to be greater than 1. We have $(\alpha, \alpha_i)>0$ for some i, and α_i is not in Σ' since otherwise $\alpha-\alpha_i$ would be in Σ' in contradiction to the simplicity of α in Σ'. Thus $\sigma_i z \sigma_i^{-1}$ is

in U. Since $w_i\alpha = \alpha - 2\alpha_i(\alpha, \alpha_i)/(\alpha_i, \alpha_i)$ has smaller height than α, we may apply our inductive assumption to $\sigma_i x \sigma_i^{-1}$ to complete the proof of the assertion and of 5.1.

5.2. *Lemma. — If B_i' is an irreducible component of B_i, the union of the conjugates of B_i' is closed, irreducible, and of codimension 3 in G.*

The normalizer P_i of B_i has the form $P_i = G_i B_i$ and is a parabolic subgroup of G, since it contains the Borel subgroup B. The number of components of T_i, hence of B_i, is either 1 or 2: if $\alpha_i = n\alpha_i'$ with α_i' a primitive character on T, then $(2\alpha_i', \alpha_i)/(\alpha_i, \alpha_i)$ is an integer [8, p. 16-09, Cor. 1], whence $n = 1$ or 2. Thus P_i also normalizes B_i', whence if easily follows that P_i is the normalizer of B_i'. Since G/P_i is complete (because P_i is parabolic) by [8, p. 6-09, Th. 4], it follows by a standard argument (cf. [8, p. 6-12] or 2.14 above) that the union of the conjugates of B_i' is closed and irreducible and of codimension in G at least $\dim(P_i/B_i') = 3$, with equality if and only if there is an element contained in only a finite, nonzero number of conjugates of B_i'. Thus 5.2 follows from:

5.3. *Lemma.* — a) *There exists in $B_i' \cap T_i$ an element t such that $\alpha(t) \neq 1$ for every root $\alpha \neq \pm\alpha_i$.*

b) *If t is as in* a) *it is contained in only a finite number of conjugates of B_i' (or B_i).*

For *a)* we choose the notation so that $i = 1$. Then for some number $c_1 = \pm 1$, the set $B_i' \cap T_1$ consists of all t for which $\alpha_1'(t) = c_1$. That values c_j may be assigned for $\alpha_j(t)$ $(2 \leq j \leq r)$ so that *a)* holds then follows by induction: having chosen $c_2, \ldots, c_j$ so that $\alpha(t) \neq 1$ if α is a combination of $\alpha_1, \alpha_2, \ldots, \alpha_j$ and $\alpha \neq \pm\alpha_1$, one has only a finite set of numbers to avoid in the choice of c_{j+1}. For *b)* let C be either B_i' or B_i, and let t be as in *a)*. Let yCy^{-1} be a conjugate of C containing t. Since B normalizes C we may take y in the form $u\sigma_w$ of 2.4. Writing $u^{-1}tu = tu'$, the inclusion $y^{-1}ty \in C$ yields

$$(*) \qquad \sigma_w^{-1} t \sigma_w . \sigma_w^{-1} u' \sigma_w \in C.$$

Since $\sigma_w^{-1} u \sigma_w$ is in U^-, so is $\sigma_w^{-1} u' \sigma_w$, whence $u' = 1$. Thus u commutes with t, hence it is in X_i because of the choice of t. By $(*)$ we have $\sigma_w^{-1} t \sigma_w \in C$, hence $(w\alpha_i)(t) = 1$, and $w\alpha_i = \pm\alpha_i$. Thus $\sigma_w^{-1} u \sigma_w$ is in G_i and normalizes C, whence using $y = \sigma_w . \sigma_w^{-1} u \sigma_w$ we get $yCy^{-1} = \sigma_w C \sigma_w^{-1}$. The number in *b)* is thus finite and in fact equal to the number of elements of the Weyl group which fix α_i.

We now turn to the proof of Theorem 1.3. Parts *a)* and *b)* follow from 5.1 and 5.2. If $i \neq j$ the independence of α_i and α_j implies that each component of B_i meets each component of B_j. Thus by 5.2 the set Q is connected if $r > 1$. If $r = 1$, the irregular elements form the centre of G, whence *c)* follows.

5.4. *Corollary. — The set of regular elements is dense and open in* G.

This is clear.

5.5. *Corollary. — In the set of irregular elements the semisimple ones are dense.*

The set of elements of B_i of the form tu with t as in 5.3 *a)* and u in U_i is open in B_i, dense in B_i by 5.3 *a)*, and consists of semisimple elements: by 2.12 the last assertion need only be proved when u commutes with t and in that case $u = 1$ by 2.1 and 2.2 *b)*. By 5.1 this yields 5.5.

By combining 5.1, 5.5 and the considerations of 5.2 we may determine the number of components of Q. We state the result in the simplest case, omitting the proof, which is easy. We recall that G is an adjoint group if the roots generate the character group of T.

5.6. *Corollary.* — *If* G *is a simple adjoint group, the number of irreducible components of* Q *is just the number of conjugacy classes of roots under the Weyl group, except that when* G *is of type* C_r $(r \geq 2)$ *and of characteristic not* 2 *the number of components is* 3 *rather than* 2.

The method of the first part of the proof of 5.2 yields the following result, to be used in 6.11.

5.7. *Lemma.* — *The union of the conjugates of* U_i *is of codimension at least* $r+2$ *in* G.

§ 6. Class functions and the variety of regular classes

G, T, etc. are as before. By a function on G (or any variety over K) we mean a rational function with values in K. Each function is assumed to be given its maximum domain of definition. A function which is everywhere defined is called regular. A function f on G which satisfies the condition $f(x)=f(y)$ whenever x and y are conjugate points of definition of f, is called a class function. As is easily seen, the domain of definition of a class function consists of complete conjugacy classes.

6.1. *Theorem.* — *Let* C[G] *denote the algebra (over* K) *of regular class functions on* G.

a) C[G] *is freely generated as a vector space over* K *by the irreducible characters of* G.

b) *If* G *is simply connected,* C[G] *is freely generated as a commutative algebra over* K *by the fundamental characters* χ_i $(1 \leq i \leq r)$ *of* G.

Let C[T/W] denote the algebra of regular functions on T invariant under W. Since two elements of T are conjugate in G if and only if they are conjugate under W (this follows easily from 2.4), there is a natural map β from C[G] to C[T/W].

6.2. *Lemma.* — *The map* β *is injective.*

For if f in C[G] is such that $\beta f = 0$, then $f = 0$ on the set of semisimple elements, a dense set in G by 2.14, e.g., whence $f = 0$.

6.3. *Lemma.* — *If in* 6.1 *we replace* C[G] *by* C[T/W] *and the irreducible characters by their restrictions to* T, *the resulting statements are true.*

Let X, the character group of T, be endowed with a positive definite inner product invariant under W, and let D consist of the elements δ of X such that $(\delta, \alpha_i) \geq 0$ for all i. We wish to be able to add characters as functions on T. Thus we switch to a multiplicative notation for the group X. For each δ in D we write sym δ for the sum of the distinct images of δ under W. We write $\delta_1 < \delta_2$ if $\delta_1^{-1}\delta_2$ is a product of positive roots. Now the elements of X freely generate the vector space of regular functions on T [8, p. 4-05, Th. 2], and each element of X is conjugate under W to a unique element of D [8, p. 14-11, Prop. 6]. Thus the functions sym δ $(\delta \in D)$ freely generate C[T/W]. Now there is a 1—1 correspondence between the elements of D and the irreducible characters of G, say $\delta \leftrightarrow \chi_\delta$, such that one has $\chi_\delta|_T = \text{sym}\,\delta + \sum_{\delta'} c(\delta')\text{sym}\,\delta'$ $(\delta' < \delta, c(\delta') \in K)$

(see 7.15). Thus *a)* holds. Now if G is simply connected, the characters ω_i of 2.6 form a basis for D as a free commutative semigroup, and the corresponding irreducible characters on G are the χ_i. If $\delta = \prod_i \omega_i^{n(i)}$ is arbitrary in D, then on T we have $\chi_\delta = \prod_i \chi_i^{n(i)} + \sum_{\delta'} c(\delta')\chi_{\delta'}$ $(\delta' < \delta)$, whence by induction, the $\chi_i|_T$ generate the algebra C[T/W]. Using the above order one sees that the only polynomial in the $\chi_i|_T$ which is o is o. Thus *b)* holds.

6.4. *Corollary. — The map* β *is surjective. Hence it is an isomorphism.*

The first statement follows from 6.3 *a)*, the second from 6.2.

Theorem 6.1 is now an immediate consequence of 6.3 and 6.4.

6.5. *Corollary. — For all* f *in* C[G] *and* x *in* G, *we have* $f(x) = f(x_s)$.

For this equation holds when f is a character on G.

6.6. *Corollary. — Assume that the elements* x *and* y *of* G *are both semisimple or both regular. Then the following conditions are equivalent.*

a) x *and* y *are conjugate.*

b) $f(x) = f(y)$ *for every* f *in* C[G].

c) $\chi(x) = \chi(y)$ *for every character* χ *on* G.

d) $\rho(x)$ *and* $\rho(y)$ *are conjugate for every representation* ρ *of* G.

If G *is simply connected,* c) *and* d) *need only hold for the fundamental characters and representations of* G.

Here *a)* implies *d)*, which implies *c)*, which implies *b)* by 6.1 *a)*; and the modified implications when G is simply connected also hold by 6.1 *b)*. To prove *b)* implies *a)* we may by 1.2 and 6.5 assume that x and y are semisimple, and then that they are in T and that $f(x) = f(y)$ for every f in C[T/W] by 6.4. Since W is a finite group of automorphisms of the variety T, it follows, among other things, by [10, p. 57, Prop. 18] that C[T/W] separates the orbits of T under W. Thus x and y are conjugate under W, and *a)* holds. This proves 6.6.

6.7. *Corollary. — If* x *is in* G, *the following are equivalent.*

a) x *is unipotent.*

b) *Either* b) *or* c) *of* 6.6, *or its modification when* G *is simply connected, holds with* $y = 1$.

Since x is unipotent if and only if $x_s = 1$, this follows from 6.5 and the equivalence of *a)*, *b)* and *c)* in 6.6.

6.8. *Corollary. — The set* S *of regular semisimple elements has codimension* 1 *in* G.

By 6.4 the function $\prod_\alpha (\alpha - 1)$ (α root) on T has an extension to an element f of C[G]. It is then a consequence of 2.11 (see *a)* and *e)*), 2.12, 6.5 and 2.13 that S is defined by $f \neq 0$, whence 6.8.

6.9. *Theorem. — Every element of* C(G), *the algebra of class functions on* G, *is the ratio of elements of* C[G].

Each element of C(G) is defined at semisimple elements of G by 2.14, hence at a dense open set in T, whence by the argument of the proof of 6.4, the natural map

from C(G) to C(T/W) is an isomorphism. Now if f is in C(T/W), then $f=g/h$ with g and h regular on T, and because W is finite it can be arranged that h is in C[T/W], whence g is also, and 6.9 follows.

The class functions lead to a quotient structure on G which we now study. We say that the elements x and y of G are *in the same fibre* if $f(x)=f(y)$ for every regular class function f. We observe that if G is simply connected the fibres are the inverse images of points for the map p from G to affine r-space V defined thus:

6.10 $$p(x)=(\chi_1(x),\ \chi_2(x),\ \ldots,\ \chi_r(x)).$$

This is because of 6.1 *b)* and the surjectivity of p (see proof of 6.16). As the next result shows, the fibres are identical with the closures of the regular classes.

6.11. *Theorem. — Let* F *be a fibre.*

a) F *is a closed irreducible set of codimension* r *in* G.

b) F *is a union of classes of* G.

c) *The regular elements of* F *form a single class, which is open and has a complement of codimension at least* 2 *in* F.

d) *The semisimple elements of* F *form a single class, which is the unique closed class in* F *and the unique class of minimum dimension in* F, *and which is in the closure of every class in* F.

Clearly F is closed in G and a union of classes. By 1.2, 6.5 and 6.6 the fibre F contains a unique class R of regular elements and a unique class S of semisimple elements. Fix y in S and write $G_{y0}=G'T'$ as in 3.6. By 3.2 and 3.3 the regular unipotent elements are dense in U, hence also in the set of all unipotent elements. Applying this to G', and using 3.7, we see that among the elements x of F for which $x_s=y$ the regular ones, that is, the ones in R, are dense. Thus R is dense in F, which, being closed, is the closure of R. Since R is irreducible and of codimension r in G, the same is true of F. By 5.4 the class R is open in F. Applying 3.2, 3.3 and 5.7 to the group G' above, we see that the part of F—R for which $x_s=y$ has codimension at least $r+2$ in G_{y0}. Thus F—R itself has codimension at least $r+2$ in G, and at least 2 in F. It remains to prove that S is in the closure of every class in F, since the other parts of *d)* then follow, and by a shift to the group G' it suffices to prove this when $S=\{1\}$, that is, when F is the set of unipotent elements. Thus *d)* follows from:

6.12. *Lemma. — A nonempty closed subset* A *of* U *normalized by* T *contains the element* 1.

Let u in A be written $\prod_\alpha x_\alpha(c_\alpha)$ as in 2.2 *b)*. Let $n(\alpha)$ denote the height of α, and for each c in K let $u_c=\prod_\alpha x_\alpha(c^{n(\alpha)}c_\alpha)$. If $c\neq 0$, then u_c is conjugate to u via an element of T, whence it belongs to A. If f is a regular function on U vanishing on A, then $f(u_c)$ is a polynomial in c (by 2.2 *b)*) vanishing for $c\neq 0$, hence also for $c=0$. Thus u_0 is in A, which proves 6.12.

From 6.11 *d)* we get the known result.

6.13. *Corollary. — In a semisimple group a class is closed if and only if it is semisimple.*

More generally we have:

6.14. *Proposition. — In a connected linear group* G′ *each class which meets a Cartan subgroup is closed.*

Let B′ be a Borel subgroup of G′. Since G′/B′ is complete [8, p. 6-09, Th. 4], it is enough to prove 6.14 with B′ in place of G′. Let x be an element of a Cartan subgroup of B′. Then x centralizes some maximal torus T′ in B′ [8, p. 7-01, Th. 1], whence if $B'=T'U'$ as usual then the class of x in B′ is an orbit under U′ acting by conjugation on B′. Because U′ is unipotent it follows from [7] that this class is closed.

6.15. *Remarks. — a)* Almost all fibres in 6.11 consist of a single class which is regular, semisimple, and isomorphic to G/T. This follows from 2.15.

b) Almost all of the remaining fibres consist of exactly 2 classes R and S with $\dim R = \dim S + 2$.

c) It is natural to conjecture that every fibre is the union of a finite number of classes, or, equivalently, that the number of unipotent classes is finite. In characteristic 0 the finiteness follows from the corresponding result for Lie algebras [4, p. 359, Th. 1]. In characteristic $p \neq 0$ one may assume that G is over the field k of p elements and make the stronger conjecture that each unipotent class has a point over k, or equivalently, by 1.10, that each unipotent class is over k. The last result would follow from the plausible statement: if γ is an automorphism of K, the element $\prod_{\alpha>0} x_\alpha(c_\alpha)$ of U is conjugate to $\prod_{\alpha} x_\alpha(\gamma c_\alpha)$.

d) It should be observed that for a given type of group the number of unipotent classes can change with the characteristic. Thus for the group of type B_2 the number is 5 in characteristic 2 but only 4 otherwise.

e) The converse of 6.14 is false.

6.16. *Theorem. — Assume that* G *is simply connected and that* p *is the map* 6.10 *from* G *to affine r-space* V. *Then* G/p *exists as a variety, isomorphic to* V.

The points to be proved are 1), 2) and 3) below.

1) p *is regular and surjective.* Clearly p is regular. The algebra of regular functions on T is integral over the subalgebra fixed by W. Thus any homomorphism of the latter into K extends to one of the former [2, p. 420, Th. 5.5]. Applying this to the homomorphism for which $\chi_i|_T \to c_i$ $(c_i \in K, i \leq i \leq r)$ (see 6.1 and 6.4), we get the existence of t in T such that $\chi_i(t) = c_i$ for all i, whence p is surjective.

2) *Let* f *be a function on* V *and* x *an element of* G. *Then* f *is defined at* $p(x)$ *if and only if* $f \circ p$ *is defined at* x. Write $f = g/h$, the ratio of relatively prime polynomials in the natural coordinates on V. Then the restrictions to T of $g \circ p$ and $h \circ p$, as linear combinations of characters on T, are also relatively prime: otherwise suitable powers of these functions would have a nontrivial common factor invariant under W, which by 6.1 and 6.4 would contradict the fact that g and h are relatively prime. If $h(p(x)) \neq 0$, then clearly f is defined at $p(x)$ and $f \circ p$ at x. Assume $h(p(x)) = 0$. Because g and h are relatively prime, f is not defined at $p(x)$. We may take x in B and write $x = tu$ with t in T and u in U. Let A be an open set in G containing x. Then $Au^{-1} \cap T$ is an open

subset of T containing t, and because $g \circ p$ and $h \circ p$ are relatively prime on T and $h(p(t)) = h(p(x)) = 0$ by 2.12 and 6.5, it also contains a point t' at which $h \circ p = 0$ and $g \circ p \neq 0$. Then A contains the point $t'u$ at which the same equations hold, at which $f \circ p$ is not defined. Since A is arbitrary, $f \circ p$ is not defined at x, whence 2). From this discussion we see that

(*) *the domain of definition of a class function on* G *consists of complete fibres relative to* p.

3) *Under the map* $f \to f \circ p$ *the field of functions on* V *is mapped (isomorphically) onto the field of functions on* G *constant on the fibres of* p. The latter field consists of class functions, so that 3) follows from 6.1 *b)* and 6.9.

We recall that the regular elements form an open subvariety G^r of G.

6.17. *Corollary. — If* G *is simply connected, the set of regular classes of* G *has a structure of variety, that of* V, *given by the restriction of* p *to* G^r.

This means that the restriction of p to G^r has as its fibres the regular classes of G, and that 1), 2) and 3) above hold with G^r in place of G. All of this is clear.

To close this section we describe the situation when G is not simply connected. The proofs, being similar to those above, are omitted. Let $\pi : G' \to G$ be the simply connected covering of G, and let F be the kernel of π. An element f of F acts on the i^{th} fundamental representation of G' as a scalar $\omega_i(f)$. We define an action of F on V thus: $f.(c_i) = (\omega_i(f)c_i)$.

6.18. *Theorem. — Assume* G *semisimple but not necessarily simply connected. Then the set of regular classes of* G *has a structure of variety, isomorphic to that of the quotient variety* V/F.

§ 7. Structure of N

In this section G, N, etc. are as in 1.4. Our aim is to prove that N is isomorphic to affine r-space V, under the map p of 6.10 when G is simply connected.

7.1. *Theorem. — The set* N *of* 1.4 *is closed and irreducible in* G. *It is isomorphic as a variety to affine* r*-space* V *under the map* $(c_i) \to \prod_i (x_i(c_i)\sigma_i)$. *In particular, an element of* N *uniquely determines its components in the product that defines* N.

7.2. *Lemma. — Let* $\beta_i = w_1 w_2 \dots w_{i-1}\alpha_i \ (1 \leq i \leq r)$ *and* $w = w_1 w_2 \dots w_r$.

a) *The roots* β_i *are positive, distinct and independent.*

b) *They form the set of positive roots which become negative under* w^{-1}.

c) *The sum of two* β*'s is never a root.*

Since β_i is α_i increased by a combination of roots $\alpha_j \ (j<i)$, we have *a)*. The roots $w^{-1}\beta_i = -w_r w_{r-1} \dots w_{i+1}\alpha_i$ are all negative by *a)* applied with $\alpha_r, \dots, \alpha_1$ in place of $\alpha_1, \dots, \alpha_r$. Since w^{-1} is a product of r reflections corresponding to simple roots, no more than r positive roots can change sign under w^{-1} by [8, p. 14-04, Cor. 3], whence *b)*. If the sum of two β's were a root, this root would be a β by *b)*, which is impossible by *a)*.

7.3. *Lemma. — If* β_i *and* w *are as in* 7.2 *the product* $\prod_i X_{\beta_i}$ *in* U *is direct, and if* X_w *denotes this product and* $\sigma_w = \sigma_1 \sigma_2 \dots \sigma_r$, *then* $N = X_w \sigma_w$.

The first part follows from *a)* and *c)* of 7.2, and the second from the equation $X_{\beta_i} = \sigma_1 \dots \sigma_{i-1} X_i \sigma_{i-1}^{-1} \dots \sigma_1^{-1}$.

Consider now 7.1. By 2.2 *b)* the set $X_w \sigma_w$ is closed, irreducible, and isomorphic to V via the map $(c_i) \to \prod_i x_{\beta_i}(c_i)\sigma_w = \prod_i (x_i(a_i c_i)\sigma_i)$ (a_i fixed element of K^*), whence 7.1 follows.

7.4. *Examples of* N. — *a)* Assume $r = 1$ and $G = SL(2, K)$. Here we may choose X_1 as the group of superdiagonal unipotent matrices and σ_1 as the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Then N consists of all matrices of the form $y(c) = \begin{pmatrix} c & -1 \\ 1 & 0 \end{pmatrix}$.

b) Assume $r > 1$ and $G = SL(r+1, K)$. Here we may choose for $x_i(c)\sigma_i$ the matrix $1_{i-1} \overset{\circ}{+} y(c) \overset{\circ}{+} 1_{r-i}$, with $y(c)$ as in *a)* and 1_j the identity matrix of rank j. Then the element $\prod_i (x_i(c_i)\sigma_i)$ of N has the entries $c_1, -c_2, \dots, (-1)^{r-1}c_r, (-1)^r$ across the first row, 1 in all positions just below the main diagonal, and 0 elsewhere. We thus have one of the classical normal forms for a matrix which is regular in the sense that its minimal and characteristic polynomials are equal. We observe that the parameters c in this form are just the values of the characters χ_i at the element considered. A similar situation exists in the general case. The group X_w of 7.3 in the present case consists of all unipotent matrices which agree with the identity in all rows below the first.

Next we show (7.5 and 7.8 below) that N does not depend essentially on the choice of the σ_i and the labelling of the simple roots, or equivalently, the order of the factors in the product for N. The other choices necessary to define N, namely the maximal torus T and a corresponding system of simple roots, are immaterial because of well known conjugacy theorems.

7.5. *Lemma.* — *Let each σ_i be replaced by an element σ_i' equivalent to it* mod T, *and let* $N' = \prod_i (X_i \sigma_i')$. *Then there exist t and t' in* T *such that* $N' = t'N = tNt^{-1}$.

Because T normalizes each X_i and is itself normalized by each σ_i, the first equality holds. We may write $tNt^{-1} = tw(t^{-1})N$, with w as in 7.3. Thus the second equality follows from:

7.6. *Lemma.* — *If w is as in* 7.2, *the endomorphism* $1 - w$ *of* $T\ (t \to tw(t^{-1}))$ *is surjective, or equivalently, its transpose* $1 - w'$ *on the dual* X *of* T *is injective.*

Suppose $(1 - w')x = 0$ with x in X. Then $(1 - w_1)x = (1 - w_2 \dots w_r)x$. The left side being a multiple of α_1 and the right side a combination of $\alpha_2, \dots, \alpha_r$, both sides are 0. Since x is fixed by w_1 it is orthogonal to α_1. Similarly it is orthogonal to $\alpha_2, \dots, \alpha_r$, hence is 0. Thus $1 - w'$ is injective.

7.7. *Remarks.* — *a)* The argument shows that the conclusion of 7.6 holds if w is the product of reflections corresponding to any r independent roots.

b) If G is simply connected, one can show by an argument like that in 4) of 4.3 that the kernel of $1 - w$ on T is just the centre of G.

7.8. *Proposition. — For each i let y_i be an element of $X_i\sigma_i$. Then the products obtained by multiplying the y_i in the $r!$ possible orders are conjugate.*

This result is not used in the sequel. Consider the Dynkin graph in which the nodes are the simple roots and the relation is nonorthogonality. Since the graph has no circuits [9, p. 13-02], it is a purely combinatorial fact that any cyclic arrangement of the simple roots can be obtained from any other by a sequence of moves each consisting of the interchange of 2 roots adjacent in the arrangement and not related in the graph (see [16, Lemma 2.3]). Now if α_i and α_j are not related in the graph, that is, orthogonal, then G_i and G_j commute elementwise (because $\alpha_i \pm \alpha_j$ are not roots), so that in case y_i is in G_i for each i our result follows. In the general case, if one interchanges y_i and y_j in the above situation, a factor from T appears, but this can be eliminated by conjugation by a suitable element of T, whence 7.8 follows.

7.9. *Theorem. — Let G be simply connected and let p be the map* 6.10 *from G to affine r-space V. Then p maps N, as a variety, isomorphically onto V.*

As in § 6, D denotes the set of characters on T of the form $\omega = \sum_i n_i\omega_i$ ($n_i \geq 0$, ω_i as in 2.6). We write $n_i = n_i(\omega)$ in this situation.

7.10. *Definition. —* $\omega_j \prec \omega_i$ means that *a)* $i \neq j$, and *b)* there exists ω in D such that $\omega_i - \omega$ is a sum of positive roots and $n_j(\omega) > 0$.

7.11. *Lemma. — The relation $\prec$ of* 7.10 *is a relation of strict partial order.*

If $\omega_k \prec \omega_j$ and $\omega_j \prec \omega_i$, then $k \neq i$ since a sum of positive roots and nonzero elements of D can not be 0 unless it is vacuous. Thus 7.11 follows.

7.12. *Remark.* — For simple groups of type A_r, B_2, or D_4 the relation $\prec$ is vacuous; for the other simple groups it is nonvacuous.

7.13. *Lemma. — Assume that σ_i is in G_i, and let $T_i = G_i \cap T$. Then there exists a bijection β from T_i to $X_i - \{1\}$ such that $x = \beta t$ if and only if $(xt\sigma_i)^3 = 1$.*

The group G_i is isomorphic to SL(2) by [8, p. 23-02, Prop. 2]. Identifying T_i (resp. X_i) with the subgroup of diagonal (resp. unipotent superdiagonal) matrices of SL(2), we get 7.13 by a simple calculation.

7.14. *Lemma. — Assume that G is simply connected, and that σ_i is chosen in G_i for each i, in the definition of N. Let the isomorphisms $x_i : K \to X_i$ be so normalized that $x_i(-1) = \beta(1)$ if β is as in* 7.13. *Let ψ_i be the function on N defined by $\prod_j (x_j(c_j)\sigma_j) \to c_i$. Then there exist functions f_i and g_i ($1 \leq i \leq r$) such that:*

a) *f_i (resp. g_i) is a polynomial with integral coefficients in those ψ_j (resp. χ_j) such that $\omega_j \prec \omega_i$ (see* 7.10).

b) *On N we have $\chi_i = \psi_i + f_i$ and $\psi_i = \chi_i + g_i$.*

Let i be fixed and let V_i be the space of the i^{th} fundamental representation of G. For each weight (character on T) ω, let V_ω be the subspace of vectors which transform according to ω. We recall, in the form of a lemma, the properties of irreducible representations needed for our proof.

7.15. *Lemma. —* a) $\sum_\omega V_\omega = V_i$, *the total space.*

b) *If* $\omega = \omega_i$, *the highest weight, then* $\dim V_\omega = 1$.

c) *If* $\omega_i - \omega$ *is not a sum of positive roots,* $V_\omega = 0$.

d) *If* v *is in* V_ω, *if* $1 \leq j \leq r$, *and if we set* $\omega(n) = \omega + n\alpha_j$ *for* $n \geq 1$, *then there exist vectors* v_n *in* $V_{\omega(n)}$ *such that* $x_j(c)v = v + \sum_n c^n v_n$ *for all* c *in* K.

The proofs may be found in [8, Exp. 15 and p. 21-01, Lemme 1].

Now let x be an element of N. We write $x = \prod_j y_j$ and $y_j = x_j(c_j)\sigma_j$, and proceed to calculate $\chi_i(x)$, in several steps:

1) *If* v *is in* V_ω *and* $\omega(n) = \omega + (n - n_j(\omega))\alpha_j$ *for* $n \geq 1$, *there exist vectors* v_n *in* $V_{\omega(n)}$ *such that* $y_j v = \sigma_j v + \sum_n \psi_j(x)^n v_n$. This follows from 7.15 *d)* because $\sigma_j v$ corresponds to the weight $w_j\omega = \omega - n_j(\omega)\alpha_j$.

2) *Let* π_ω *be the projection on* V_ω *determined by* 7.15 a). *Then* $\pi_\omega x \pi_\omega = \prod_j (\pi_\omega y_j \pi_\omega)$. This follows from 1) and the independence of the roots α_j.

3) $\chi_i(x) = \sum_\omega \operatorname{tr} \pi_\omega x \pi_\omega$. This follows from the orthogonal decomposition $1 = \sum_\omega \pi_\omega$, which holds by 7.15 *a)*.

4) *If* $\omega = \omega_i$, *the highest weight, then* $\operatorname{tr} \pi_\omega x \pi_\omega = \psi_i(x)$. Let v be a basis for V_ω (see 7.15 *b)*), and let $v' = -\sigma_i v$. Then $y_i = x_i(c_i)\sigma_i$ fixes the space V′ generated by v and v', by 7.15 *c)* and *d)*, and maps these vectors onto $-v' + ac_i v$ and bv $(a, b \in K)$, respectively. A simple calculation shows that $y_i^2 = 1$ on V′ if and only if $b = 1$ and $ac_i = -1$. Because of our normalization of x_i, this is true only if $c_i = -1$, so that $a = 1$. Thus $\pi_\omega y_i \pi_\omega v = c_i v$. If $j \neq i$, then $w_j\omega = \omega$ by 2.6, so that X_j and σ_j, and hence also the group G_j they generate, fix the line of v, and then v itself because G_j is equal to its commutator group. By 2) we conclude that $\pi_\omega x \pi_\omega v = c_i v$, whence 4) follows.

5) *If* ω *is in* D *and* $\omega \neq \omega_i$, *then* $\operatorname{tr} \pi_\omega x \pi_\omega$ *depends only on those* $\psi_j(x)$ *for which* $\omega_j \prec \omega_i$. We may assume $V_\omega \neq 0$. It follows from 1) and 2) that $\pi_\omega x \pi_\omega$ depends only on those $\psi_j(x)$ for which $n_j(\omega)$ is positive. Because $\omega_i - \omega$ is a sum of positive roots by 7.15 *c)*, this yields 5).

6) *If* ω *is not in* D, *then* $\pi_\omega x \pi_\omega = 0$. If j is such that $n_j(\omega) < 0$, then $\pi_\omega y_j \pi_\omega = 0$ by 1), whence 6) follows from 2).

7) *In terms of the* ψ_j *the function* χ_i *is a polynomial with integral coefficients.* That we have a polynomial follows from 1). The integrality follows from the fact, proved in [17] when the characteristic is not 0 and in [14] when the characteristic is 0, that there exists a basis of V_i relative to which each σ_j acts integrally and each $x_j(c_j)$ is a polynomial with integral coefficients.

To prove 7.14 now, we need only combine 3), 4), 5), 6) and 7) above to get the assertions concerning f_i and then solve the equations $\chi_i = \psi_i + f_i$ recursively for the ψ_i to get the assertions concerning g_i.

Now we can prove Theorem 7.9. By 7.5 we may assume σ_i is in G_i for each i. Then by 7.1 the functions ψ_i of 7.14 are affine coordinates on N, so that 7.9 follows from 7.14.

7.16. *Corollary.* — a) N *is a cross-section of the fibres of p in* 7.9.

b) *The corresponding retraction q from* G *to* N, *given by* $q(x) = \prod_i x_i(\chi_i(x) + g_i(x))\sigma_i$ *if the normalization of* 7.14 *is used, yields on* G *a quotient structure isomorphic to that for p.*

c) *The set* s(N) *made up of the semisimple parts of the elements of* N *is a cross-section of the semisimple classes of* G.

The formula for q follows from 7.14, and the other parts of *a)* and *b)* from 7.9. Then *c)* follows from 6.11 *d)*. We observe that s(N) is never closed or connected, only constructible.

§ 8. Proof of 1.4 and 1.5

It follows from 7.9 that if G is simply connected distinct elements of N lie in distinct conjugacy classes. Thus 1.4 and 1.5 are consequences of the following result.

8.1. *Theorem.* — *Let* G *be simply connected (and semisimple),* x *an element of* G, *and* N *as in* 1.4. *Then the following are equivalent.*

a) x *is regular.*

b) x *is conjugate to an element of* N.

c) *The differentials* $d\chi_i$ *are independent at* x.

First we prove some lemmas.

8.2. *Lemma.* — *Under the assumptions of* 8.1 *let* ψ_i *denote the restriction of* χ_i *to* T, *let* ω_0 *denote the product* $\prod_i \omega_i$ *of the fundamental weights, and let the function f on* T *be defined by* $\prod_i (d\psi_i) = f \prod_i (\omega_i^{-1} d\omega_i)$, *the products being exterior products of differential forms. Then* $f = \sum_w (\det w) w\omega_0 = \omega_0 \prod_\alpha (1 - \alpha^{-1})$, *the sum over w in* W *and the product over the positive roots* α.

We will deduce this from $\psi_i = \operatorname{sym} \omega_i + \sum_\delta c_i(\delta) \operatorname{sym} \delta$ ($\delta \in$ D, $\delta < \omega_i$, $c_i(\delta) \in$ K, notation of 6.3). Replacing the c's by indeterminates, we may view the equations to be proved as formal identities with integral coefficients in the group algebra of the dual of T, thus need only prove them in characteristic 0. First f is skew: $wf = (\det w)^{-1} f$ for every w in W. We have $w d\psi_i = d\psi_i$, and if $w\omega_i = \prod_j \omega_j^{n(i,j)}$, then $w(\omega_i^{-1} d\omega_i) = \sum_j n(i,j) \omega_j^{-1} d\omega_j$, which, because $\prod_i \omega_i^{-1} d\omega_i \neq 0$, yields $f = wf . \det(n(i,j)) = wf . \det w$. Because f is skew and the characteristic is 0, we have

$$(*) \qquad f = \sum_\delta c(\delta) \sum_w (\det w) w\delta \quad (\delta \in \mathrm{D},\ c(\delta) \in \mathrm{K}),$$

the inner sum being over W and the outer over D. From the expression for ψ_i, we have $d\psi_i = \omega_i(\omega_i^{-1} d\omega_i) +$ a combination of terms $\omega(\omega_j^{-1} d\omega_j)$, with ω lower (by a product of positive roots) than ω_i, whence $f = \omega_0 +$ lower terms. Thus in $(*)$ above $c(\omega_0) = 1$ and $c(\delta) = 0$ when δ is not lower than ω_0. If δ is lower than, and different from, ω_0, then δ is orthogonal to some α_i (if $\delta = \prod_i \omega_i^{n(i)}$, then some $n(i)$ is less than the corresponding

object for ω_0, hence is o), whence $\sum_w (\det w) w\delta = 0$. Thus (*) becomes $f = \sum_w (\det w) w\omega_0$. The final equality in 8.2 is a well known identity of Weyl [18, p. 386].

8.3. *Remark.* — $\prod_i (\omega_i^{-1} d\omega_i)$ above is, to within a constant factor, the unique differential r-form on T invariant under translations, that is, the " volume element " of T.

8.4. *Lemma.* — *Let* G′ *denote the neighborhood* U^-TU *of* T (*see* 2.3), *and let* π *denote the natural projection from* G′ *to* T. *For each* α *let* y_α *be the composition of the projection from* G′ *to* X_α *and an isomorphism from* X_α *to* K.

a) *If* f *is a regular function on* G, *its restriction to* G′ *is a combination of monomials in the functions* y_α *and* $\omega_i^{\pm 1} \circ \pi$.

b) *If* f *is also a class function and the combination is irredundant, then each monomial has a total degree in the* y_α*'s which is either* o *or at least* 2.

Here *a)* follows from 2.3. In *b)* no monomial could involve exactly one y_α (to the first degree), because then conjugation by t in T and use of 2.1 would yield $\alpha(t) = 1$ for all t in T, a contradiction.

8.5. *Lemma.* — *Let* ψ_i *be as in* 8.2 *and* π *as in* 8.4. *Then* $d\chi_i = d\psi_i \circ d\pi$ *at all points of* T.

Here the tangent space at t as an element of G is being identified with its tangent space as an element of G′. By 8.4 *b)* we have on G′ an equation $\chi_i = \psi_i \circ \pi +$ terms of degree at least 2 in the y_α. Since each y_α is o on T, we have there $d\chi_i = d\psi_i \circ d\pi$.

8.6. *Lemma.* — *If* x *is semisimple,* a) *and* c) *of* 8.1 *are equivalent.*

We may take x in T. By 8.5 and the surjectivity of $d\pi$ (from the tangent space of x in G′ to its tangent space in T), the $d\chi_i$ are independent at x if and only if the $d\psi_i$ are, and by 8.2 this is so if and only if $\alpha(x) \neq 1$ for every root α, that is, if and only if x is regular, by 2.11.

We can now prove 8.1. From 7.9 it follows that *b)* implies *c)*, and from 5.5 and 8.6 that *c)* implies *a)*. Now assume x is regular. By 7.9 there is a unique element y in both N and the fibre of p which contains x. Then y is regular because *b)* $\rightarrow$ *a)* has already been shown, whence x is conjugate to y by 6.11 *c)*. Thus *a)* implies *b)*, and 8.1 is proved.

Using the above methods one can also show:

8.7. *Theorem.* — *Without the assumption of simple connectedness in* 8.1, *conditions* a) *and* b) *are equivalent and are implied by*

c′) *there exist* r *regular class functions on* G *whose differentials are independent at* x.

One can also show that the elements of N conjugate to a given one $\prod_i x_i(c_i)\sigma_i$ are those of the form $\prod_i x_i(\omega_i(f)c_i)\sigma_i$ ($f \in F$), in the notation of the paragraph before 6.18.

8.8. *Remark.* — If $w = w_1 w_2 \ldots w_r$, all elements of the double coset $B\sigma_w B$ are regular, not just those of N. This depends on 7.3, 7.5 and the following result, whose proof is omitted.

8.9. *Proposition.* — *If* w *is as above, then the map from the Cartesian product of* $\sigma_w U^- \sigma_w^{-1} \cap U$ *and* $\sigma_w^{-1} U \sigma_w \cap U$ *to* U *given by* $(u_1, u_2) \rightarrow u_2^{-1}.u_1.\sigma_w u_2 \sigma_w^{-1}$ *is bijective.*

§ 9. Rationality of N

Henceforth k denotes a perfect subfield of our universal field K, which for convenience is assumed to be an algebraic closure of k, and Γ denotes the Galois group of K over k. In this section G is a simply connected semisimple group. If G is (defined) over k, it is natural to ask whether N or a suitable analogue thereof can be constructed over k. As the following result shows, the answer is in general no.

9.1. *Theorem. — If* G *is over* k, *then a necessary condition for the existence over* k *of a cross-section* C *of the regular classes is the existence of a Borel subgroup over* k.

For the unique unipotent element of C is clearly over k, and so is the unique Borel subgroup that contains it (see 3.2 and 3.3).

As we now show, this necessary condition comes quite close to being sufficient. First we consider a more restrictive situation, that in which G splits over k, that is, is over k and contains a maximal torus which with all of its characters is over k.

9.2. *Theorem. — If* G *splits over* k, *then* N *in* 1.4 (*and hence also* s(N) *in* 7.16 c)) *can be constructed over* k.

Let G split relative to the maximal torus T. Since the simple root α_i is over k, so is X_i, and it remains to choose each σ_i over k. We start with an arbitrary choice for σ_i. Then the map $\gamma \to \sigma_i^{-1}\gamma(\sigma_i) = x_\gamma$ is a cocycle from Γ to a group isomorphic to K^*, namely, $G_i \cap T$. In other words:

9.3. a) $x_{\gamma\delta} = x_\gamma \gamma(x_\delta)$ *for all* γ *and* δ *in* Γ.

b) *There exists a subgroup* Γ_1 *of finite index in* Γ *such that* $x_\gamma = 1$ *if* γ *is in* Γ_1.

By a famous theorem of Hilbert (see, e.g., [11, p. 159]), this cocycle is trivial, that is, there exists t_i in T such that $x_\gamma = t_i \gamma(t_i^{-1})$ for all γ in Γ. Then $\sigma_i t_i$ is over k, as required.

9.4. *Theorem. — Assume that* G *is over* k, *and contains a Borel subgroup over* k. *Assume further that* G *contains no simple component of type* A_n (n *even*). *Then the set* N *of* 1.4 *can be constructed over* k.

Let B be a Borel subgroup over k. It contains a maximal torus T over k. If k is infinite, this follows from 2.14 and Rosenlicht's theorem [6, p. 44] that G_k is dense in G, while if k is finite with q elements and β is the q^{th} power automorphism, one picks an arbitrary maximal torus T', then x in B so that $x\beta(T')x^{-1} = T'$ (conjugacy theorem), then y in B so that $x = y^{-1}\beta(y)$ (Lang's theorem [5]), and then $T = yT'y^{-1}$. We order the roots so that B corresponds to the set of positive roots. Γ permutes the simple roots α_i in orbits. We order the α_i so that those in each orbit come together. If for each orbit we can construct over k the corresponding part of the product for N, then we can construct N over k. Thus we may (and shall) assume that there is a single orbit. Let Γ_1 be the stabilizer of α_1 in Γ, and k_1 the corresponding subfield of K. Then α_1 is over k_1, whence G_1 (the corresponding group of rank 1) is also, so that by 9.2 applied with G_1 in place of G the set $X_1\sigma_1$ can be constructed over k_1. Then Γ operates on this set to produce, in an unambiguous way, sets $X_i\sigma_i$ ($1 \leq i \leq r$). But these sets commute

pairwise: the roots (in each orbit) are orthogonal because of the exclusion of the type A_n (n even). Their product is thus fixed by all of Γ, hence is over k, as required.

Observe that 9.2 and 9.4 yield 1.6.

9.5. *Corollary. — Under the assumptions of* 9.2 *or* 9.4 *the natural map (inclusion) from the set of regular elements over k to the set of regular classes over k is surjective. In other words, each regular class over k contains an element over k.*

Let C be a regular class over k. Then $C \cap N$ is over k by 9.2 or 9.4, and it consists of one element by 1.4, whence 9.5.

9.6. *Remark.* — For the group of type A_n (n even) we do not know whether there exists over k a global closed irreducible cross-section of the regular classes of G, or even of the fibres of the map p of 6.10 (which can be taken over k if V is suitably defined over k), although a study of the group of type A_2 casts some doubt on these possibilities. All that we can show, 9.7 *c)* below, is that there exists a local cross-section (covering a dense open set in V) with the above properties.

9.7. *Theorem. — Assume that* G *is over k, and contains a Borel subgroup over k. Assume that every simple component of* G *is of type* A_n *(n even). Then there exists in* G *a set* N′ *with the following properties.*

a) N′ *is a disjoint union of a finite number of closed irreducible subsets of* G.

b) N′ *is a cross-section of the fibres of p in* 6.10.

c) *p maps each component of* N′ *isomorphically onto a subvariety of* V, *and one component consisting of regular elements onto a dense open subvariety of* V.

d) $s(N')$ *is a cross-section of the semisimple classes of* G.

e) *Each component of* N′ *is over k.*

In order to continue our main development, we postpone the construction of N′ to the end of the section.

9.8. *Theorem. — If* G *(with or without components of type* A_n *(n even)) is over k and contains a Borel subgroup over k, the natural map from the set of semisimple elements over k to the set of semisimple classes over k is surjective.*

Observe that this is Theorem 1.7 of the introduction. As is easily seen, we may assume either that no components of G are of type A_n (n even) or that all are. In the first case we replace N by $s(N)$ and 1.4 by 7.16 *c)* in the proof of 9.5, while in the second case we use $s(N')$ and 9.7 *d)* instead.

9.9. *Remark.* — G need not be semisimple for the validity of 9.8. For let A be a connected linear group satisfying the other assumptions. If R is the unipotent radical, then A/R is a connected reductive group, hence the direct product of a torus and a simply connected semisimple group because A is simply connected, whence the result to be proved holds for A/R. A semisimple class of A over k thus contains an element x over k mod R. The map $\gamma \to x^{-1}\gamma(x)$ then defines a cocycle into R which is trivial because R is unipotent (see [12, Prop. 3.1.1]), whence 9.9.

Theorem 9.8 admits a converse.

9.10. *Theorem. — If* G *is over* k *and the map of* 9.8 *is surjective, then* G *contains a Borel subgroup over* k.

If k is finite, this follows from Lang's theorem (see the proof of 9.4), even without the assumption of surjectivity. Henceforth let k be infinite. Let F be the centre of G, n the order of F, h the height of the highest root, and c and c' elements of k^* such that $c=c'^n$ and c has order greater than $h+1$. Let T be a maximal torus over k (for the existence, see the proof of 9.4), and t' an element of T such that $\alpha_i(t')=c'$ for every α_i in some system of simple roots. Set $t=t'^n$, so that $\alpha_i(t)=c$.

1) t *is regular.* If α is a root of height m, then $\alpha(t)=c^m\neq 1$, whence 1). Since $c^m=c$ only if $m=1$ we also have:

2) *If* α *is a root such that* $\alpha(t)=c$, *then* α *is simple.*

3) *The class of* t *is over* k. Each element γ of the Galois group Γ acts as an automorphism on the root system, hence determines a unique element w_γ of the Weyl group such that $w_\gamma\circ\gamma$ permutes the simple roots. Since $\alpha_i(t')$ is independent of i and is in k, we have $\alpha_i((w_\gamma\circ\gamma)(t'))=((w_\gamma\circ\gamma)^{-1}(\alpha_i))(t')=\alpha_i(t')$, whence $(w_\gamma\circ\gamma)(t')=ft'$ for some f in F. Thus $(w_\gamma\circ\gamma)(t)=f^n t=t$, which yields 3).

4) *One can normalize the pair* T, t *above so that* 1) *and* 2) *hold and also* t *is over* k. By the surjectivity assumption in 9.10 there exists t'' over k and conjugate to t. Any inner automorphism which maps t to t'' maps T onto a maximal torus T'' which must be over k because it is the unique maximal torus containing t'' by 1) and 2.11, and also maps the simple system relative to T into one relative to T'' so that the equations $\alpha_i(t)=c$ are preserved. On replacing T, t by T'', t'', we get 4).

Now by 4) we have $(\gamma\alpha_i)(t)=(\gamma\alpha_i)(\gamma t)=\gamma(\alpha_i(t))=\gamma(c)=c$, whence $\gamma\alpha_i$ is simple by 2). Thus each γ preserves the set of positive roots, hence also the corresponding Borel subgroup, which is thus over k, as required.

It remains to construct the set N' of 9.7. If G is a group of type A_n (n even) in which T, etc. are given, the following notation is used. The simple roots are labelled $\alpha_1, \alpha_2, \ldots, \alpha_n$ from one end of the Dynkin graph to the other (see [8, p. 19-03]). We write $n=2m$, set $\alpha=\alpha_m+\alpha_{m+1}$, a root, let G_α denote the group of rank 1 generated by X_α and $X_{-\alpha}$, write T_α for $T\cap G_\alpha$, and σ_α for an element normalizing T according to the reflection relative to α. The group of automorphisms of the system of simple roots pairs α_i with α_{2m+1-i}, which is orthogonal to α_i unless $i=m$. Hence (see the proof of 9.4) only the part of N corresponding to α_m and α_{m+1} need be modified.

9.11. *Theorem. — Let* G *be as in* 9.7. *If* G *contains a single component, assume (in the above notation) that the choices* σ_i *and* σ_α *are normalized to be in* G_i *and* G_α $(i\neq m, m+1)$, *that* u_m *and* u_{m+1} *are elements of* X_m *and* X_{m+1} *and different from* 1, *that* N'' (*resp.* N''') *is the product of* $X_\alpha\sigma_\alpha$ (*resp.* $u_{m+1}u_m X_\alpha\sigma_\alpha T_\alpha$) *and* $\prod_j X_j\sigma_j$ $(j\neq m, m+1)$, *and that* N' *is the union of* N'' *and* N'''. *If* G *is a product of several components, assume that* N' *is constructed as a product accordingly. Then one has* a) *to* e) *of* 9.7.

We proceed to study N'' and N''' as we did N in § 7. The following observation will be useful.

9.12. *Lemma.* — a) *The sequence of roots* $S=\{\alpha_1, \ldots, \alpha_{m-1}, \alpha, \alpha_{m+2}, \ldots, \alpha_{2m}\}$ *yields a simple system of type* A_{2m-1}.

b) *If* G' *is the corresponding semisimple subgroup of* G, *then* N'' *as constructed in* G' *fulfills the rules of construction of* N *in* G.

The verification of *a)* is easy, while *b)* is obvious.

9.13. *Lemma.* — *The sets* N'' *and* N''' *are closed and irreducible in* G. *The natural maps from the Cartesian products* $X_\alpha \times \prod_j X_j$ *and* $X_\alpha \times T_\alpha \times \prod_j X_j$ *to* N'' *and* N''', *respectively, are isomorphisms of varieties. In particular each element of* N'' *or* N''' *uniquely determines its components.*

The assertions about N'' follow from 7.1 and 9.12. Those concerning N''' are proved similarly.

9.14. *Lemma.* — *If* u_m *and* u_{m+1} *in* 9.11 *are replaced by alternates* u'_m *and* u'_{m+1}, *then* N''' *is replaced by a conjugate, under* T.

We can find t in T to transform u_m and u_{m+1} into u'_m and u'_{m+1}, and, because only the values $\alpha_m(t)$ and $\alpha_{m+1}(t)$ are relevant (see 2.1), so that also $\alpha_j(t)=1$ if $j \neq m, m+1$; we are using the independence of the simple roots here. By conjugating N''' by t, we get 9.14.

9.15. *Lemma.* — *Let the functions* $\psi_i\,(i \neq m, m+1)$ *and* ψ_α *be defined on* N'' *as the functions* ψ_i *of* 7.14 *are defined on* N. *Further, set* $\chi_0=\chi_{2m+1}=1$ *and* $\psi_0=\psi_{2m+1}=1$. *Then on* N'' *on has*

a) $\chi_i=\psi_i+\psi_{i-1}$ *if* $1 \leq i \leq m-1$.

b) $\chi_i=\psi_i+\psi_{i+1}$ *if* $m+2 \leq i \leq 2m$.

c) $\chi_m=\psi_\alpha+\psi_{m-1}$.

d) $\chi_{m+1}=\psi_\alpha+\psi_{m+2}$.

1) *Let* ρ_i *be the* i^{th} *fundamental representation of* G *and* ρ'_i *that of* G' (*according to the sequence* S *in* 9.12). *Then the restriction of* ρ_i *to* G' *is isomorphic to the direct sum of* ρ'_i *and* ρ'_{i-1}. Here ρ'_0 is the trivial representation. We may identify G with SL(L) and G' with the subgroup $SL(L')\times SL(L'')$, if L' and L'' are vector spaces of rank $2m$ and 1 and L is their direct sum. Then ρ_i is realized by the action of G on the space $\wedge^i L$ of skew tensors of rank i over L. Combining this with the canonical decomposition $\wedge^i L=\wedge^i L' \dot{+} \wedge^{i-1} L' \otimes L''$, we get 1).

We will use the notation D, V_ω, π_ω, etc. of 7.14.

2) *If* G *in* 7.14 *is of type* A_r, *then one has*:

a) *The only weight* ω *in* D *such that* $V_\omega \neq 0$ *if* $\omega=\omega_i$.

b) *The function* f_i *is* 0.

Using the realization of ρ_i as in 1), we see that the transforms of V_{ω_i} under the Weyl group W generate V_i. Since D is a fundamental domain for the action of W, this proves *a)*. Referring to the proof of 7.14, the contribution to $\chi_i(x)$ coming from step 5) is 0, by *a)*, whence *b)* follows.

3) *Proof of* 9.15. — Writing 1) in terms of characters, $\chi_i = \chi'_i + \chi'_{i-1}$, and then using 9.12 and 7.14 as refined in 2 *b)* above, for the group G', we get 9.15.

9.16. *Lemma. — Let* ψ_i *and* ψ_α *be as in* 9.15, *but on* N''' *instead of* N''. *Let* u_m *and* u_{m+1} *be so chosen that the final stage of* ψ_α (*isomorphism from* X_α *to* K) *maps the commutator* (u_{m+1}, u_m) *onto* 1. *Let* φ_α *denote the composition of the projection* $N''' \to T_\alpha$ *and the evaluation* $t \to \alpha_m(t)$ (*or* $\alpha_{m+1}(t)$). *Then on* N''' *one has* a) *and* b) *of* 9.15 *and also*

c) $\chi_m = \varphi_\alpha \psi_\alpha + \psi_{m-1}$,

d) $\chi_{m+1} = \varphi_\alpha + \varphi_\alpha \psi_\alpha + \psi_{m+2}$.

1) *Assume that* $1 \leq i \leq m$. *Then there exist exactly two weights* ω *such that* $(\omega, \beta) \geq 0$ *for all* β *in the sequence* S *of* 9.12, *and* $V_\omega \neq 0$. *For both,* $\dim V_\omega = 1$. *One is the highest weight* ω_i *and the other, say* ω'_i, *is orthogonal to all terms of* S *but the* $(i-1)^{\text{th}}$. The highest weights of the representations ρ'_i and ρ'_{i-1} in 1) of 9.15 satisfy the first two statements by 2 *a)* of 9.15 and 7.15 *b)*. Finally ω_i must correspond to ρ'_i rather than ρ'_{i-1} because ω_i is not orthogonal to the i^{th} term of S.

Now let $x = y_\alpha \prod_j y_j = y_\alpha y$ be an element of N''' with y_α in $u_{m+1} u_m X_\alpha \sigma_\alpha T_\alpha$ and y_j in $X_j \sigma_j$ $(j \neq m, m+1)$.

2) $\pi_\omega x \pi_\omega = \pi_\omega y_\alpha \pi_\omega \prod_j (\pi_\omega y_j \pi_\omega) = \pi_\omega y_\alpha \pi_\omega \cdot \pi_\omega y \pi_\omega$.

The proof is like that of 2) in the proof of 7.14.

3) $\chi_i(x) = \sum_\omega \operatorname{tr} \pi_\omega x \pi_\omega$ $(\omega = \omega_i, \omega'_i)$. This follows from 1) above, by a proof like that of 6) of 7.14.

4) *Proof of* a). — Since $1 \leq i \leq m-1$, both ω_i and ω'_i in 1) are orthogonal to α_m, α_{m+1} and α. Thus if $\omega = \omega_i$ or ω'_i and z is any element of the group generated by G_m and G_{m+1}, then $\pi_\omega z \pi_\omega = 1$ on V_ω, whence $\pi_\omega x \pi_\omega = \pi_\omega \sigma_\alpha y \pi_\omega$, and by a slight extension of 3) we get $\chi_i(x) = \chi_i(\sigma_\alpha y)$. Here $\sigma_\alpha y$ is in N'', so that 9.15 *a)* may be applied. The result is *a)*.

5) *Proof of* c). — Here $i = m$. If $\omega = \omega'_m$, then ω is orthogonal to α, whence $\pi_\omega x \pi_\omega = \pi_\omega \sigma_\alpha y \pi_\omega$ as in 4). Now applying 7.14 as refined in 2 *b)* of the proof of 9.15 to the representation ρ'_{m-1} of G' (see step 1) of 9.15), we get

$$(*) \qquad \operatorname{tr} \pi_\omega x \pi_\omega = \psi_{m-1}(x).$$

Assume now that $\omega = \omega_n$. We write $y_\alpha = u_{m+1} u_m u_\alpha \sigma_\alpha t_\alpha$ as in 9.11, and normalize the choices σ_m and σ_{m+1} so that they are in G_m and G_{m+1} and $\sigma_\alpha = \sigma_{m+1} \sigma_m \sigma_{m+1}^{-1}$, and then write $y_\alpha = z_1 z_2 z_3 t_\alpha$ with $z_1 = u_{m+1} \sigma_{m+1}$, and $z_2 = \sigma_{m+1}^{-1} u_\alpha \sigma_\alpha \sigma_{m+1}$, and $z_3 = \sigma_{m+1}^{-1} \sigma_\alpha^{-1} u_m \sigma_\alpha$. Here z_1 and z_3 are in G_{m+1}, while z_2 is in G_m. The factor t_α acts on V_ω as the scalar $\alpha_m(t_\alpha) = \varphi_\alpha(x)$. Then because ω is orthogonal to α_{m+1} the factor z_3 may be suppressed. By the independence of α_m and α_{m+1} (see 7.15 *d)*) we may also suppress z_1. Thus $\pi_\omega x \pi_\omega = \varphi_\alpha(x) \pi_\omega z_2 \pi_\omega = \varphi_\alpha(x) \psi_\alpha(x)$ on V_ω, by 4) of 7.14. Combining this with (*) above, we get *c)*.

6) *Proof of* b) *and* d). — By applying to G an automorphism which fixes T and interchanges the roots α_i and α_{2n+1-i} $(1 \leq i \leq m)$, we get *b)* from *a)* and *d)* from *c)*, if we observe that in the latter case we must take the product of u_m and u_{m+1} in the opposite order, so that u_α in 5) above must be replaced by $(u_{m+1}, u_m)u_\alpha$, which because of the original assumption on this commutator yields the extra term φ_α.

9.17. *Remark.* — Observe that the extra term φ_α, which turns out to be just the term we need, owes its existence directly to the noncommutativity of X_m and X_{m+1}. This is only fair, since the present development does also.

9.18. *Corollary.* — $\sum_0^{n+1} (-1)^i \chi_i$ *is* 0 *on* N″ *and* $(-1)^{m+1}\varphi_\alpha$ *on* N‴.

If we use 9.15 and 9.16, then in the first case all terms cancel while in the second the one term remains.

One may also express 9.18 thus: if G is represented as $SL(n+1)$, the elements of N″ have 1 as a characteristic value, those of N‴ do not.

9.19. *Corollary.* — *Let* p *and* V *be as in* 6.10. *Let* f *be the function* $(c_1, \ldots, c_n) \to \sum_0^{n+1} (-1)^i c_i$ $(c_0 = c_{n+1} = 1)$, *and* V″ *and* V‴ *the subvarieties of* V *defined by* $f = 0$ *and* $f \neq 0$, *respectively.*

a) p *maps* N″ *and* N‴ *isomorphically onto* V″ *and* V‴.

b) *All elements of* N‴ *are regular.*

The functions ψ_i $(i \neq m, m+1)$ and ψ_α may be used as coordinates on N″ by 9.12 and 7.1. So may the functions χ_i $(i \neq m)$, in terms of which the first set may be expressed by the recursive solution of *a)*, *b)* and *d)* of 9.15. The latter functions are the images under p of the canonical coordinates of V excluding the m^{th}, which may be taken as coordinates on V″. Thus p maps N″ isomorphically onto V″. The proof for N‴ and V‴ is similar: first we normalize u_m and u_{m+1} as in 9.16, which is permissible by 9.4, and then in 9.16 we solve in turn for φ_α (see 9.18), ψ_i and $\varphi_\alpha\psi_\alpha$. The second isomorphism in *a)* implies that the differentials $d\chi_i$ are independent at all points of N‴, whence 1.5 implies *b)*.

9.20. *Remark.* — One can show that the regular elements of N″ are those for which $\sum_0^{n+1} (-1)^j j\chi_j \neq 0$.

Now we can prove 9.7 and 9.11. By 9.13 we have *a)*, and by 9.19 we have *b)* and *c)*, thus by *b)* also *d)*. The argument using k_1 and Γ_1 in the proof of 9.4 may be used to reduce the proof of *e)* to the case in which G consists of a single component. Proceeding as in the proof of 9.4 we are reduced to proving that the part of N″ and N‴ corresponding to the indices m, $m+1$, and α can be constructed over k. Since α is over k, so are T_α and X_α, and we can form $X_\alpha\sigma_\alpha$ over k by 9.3. Finally, by Hilbert's theorem [11, p. 159] and the k_1, Γ_1 reduction referred to above, we can choose u_m and u_{m+1} in 9.11 so that the class of $u_m u_{m+1}$ in $X_m X_{m+1} X_\alpha / X_\alpha$ is over k, whence *e)*.

§ 10. Some cohomological applications

The convention in § 9 concerning k and K continues.

First we prove 1.8. We recall that $H^1(k, G)$ consists of all cocycles from the Galois group Γ to the group G, that is, functions $\gamma \to x_\gamma$ which satisfy 9.3, modulo the equivalence relation, $(x_\gamma) \sim (x'_\gamma)$ if $x'_\gamma = a^{-1} x_\gamma \gamma(a)$ for some a in G and all γ in Γ. For the significance of this concept, as well as its basic properties, the reader is referred to [11, 12, 13]. We start with an arbitrary cocycle (x_γ) and wish to construct an equivalent one with values in a torus over k. Assume first that k is finite. Let q be the order of k, and β the q^{th} power homomorphism. By Lang's theorem [5] there exists a in G such that $a^{-1} x_\beta \beta(a) = 1$. Since β and any subgroup Γ_1 of finite index generate Γ (in other words, the Galois group of any finite extension of k is generated by the restriction of β), it follows from 9.3 *b)* that $a^{-1} x_\gamma \gamma(a) = 1$ for all γ, whence $(x_\gamma) \sim (1)$. Assume now that k is infinite. We form $x(G)$, the group G twisted by the cocycle x (see, e.g., [13]). This is a group over k, isomorphic to G over K. If $x(G)$ is identified with G, then γ in Γ acts on $x(G)$ as $x(\gamma) = i(x_\gamma) \circ \gamma$; here $i(x_\gamma)$ denotes the inner automorphism by x_γ. By 2.15 and the Rosenlicht density theorem [6, p. 44] there exists in $x(G)$ an element y which is strongly regular and over k. Thus

(*) $i(x_\gamma)\gamma(y) = y$ for all γ in Γ.

Hence the conjugacy class of y in G is over k, whence by 1.7 it contains an element z over k. Writing $y = i(a)z$, with a in G, and substituting into (*), we conclude that $a^{-1} x_\gamma \gamma(a)$ is in the centralizer of z, a torus because z is strongly regular, and over k because z is, whence 1.8.

10.1. *Corollary. — The assumption of semisimplicity in* 1.8 *can be dropped. In other words,* G *can be any simply connected, connected linear group with a Borel subgroup over k.*

By applying the semisimple case to G divided by its radical, we are reduced to the case in which G is solvable, which we henceforth assume. As in 9.4 we can find a Cartan subgroup C over k, and then the unique maximal torus T of C is over k and maximal also in G (see [8, p. 7-01 to p. 7-04]), whence we have over k the decomposition $G = UT$, with U the unique maximal unipotent subgroup. Now let $\gamma \to x_\gamma = u_\gamma t_\gamma$ be a cocycle. Then (t_γ) is also a cocycle, and (u_γ) is a cocycle in the group U twisted by (t_γ). Since U is unipotent, the last cocycle is trivial: $u_\gamma = a t_\gamma \gamma(a)^{-1} t_\gamma^{-1}$ for some a in U, by [12, Prop. 3.11]. Then $(x_\gamma) = (a t_\gamma \gamma(a)^{-1}) \sim (t_\gamma)$, whence 10.1 follows.

Next we consider 1.9. Assume that *a)* holds. By [12, Prop. 3.1.2] we have $H^1(k, G) = 0$ in case G is a torus, hence, by 1.8, also in case G is simply connected, semisimple, and contains a Borel subgroup over k, and then, by [12, Prop. 3.1.4], in case " simply connected " is replaced by " adjoint ". Now if G is an arbitrary semisimple adjoint group (over k, of course), there exists a group G_0 split over k and isomorphic to G over K, and the argument of [13, p. III-12] together with $H^1(k, G_0) = 0$ shows that G contains a Borel subgroup over k, whence $H^1(k, G) = 0$ by the result above. By [12, Prop. 3.1.4 Cor.] it now follows that *b)* holds in general. Now a result of

Springer [13, p. III-16, Th. 3] asserts that if $\dim k \leq 1$ and G and S are as in *c)*, then there exists a principal homogeneous space P and a G-map from P to S, all over k. By *b)*, P has a point over k, hence so does S, whence *c)*.

10.2. *Corollary. — Let k be a perfect field of* $\dim \leq 1$, *and* G *a connected linear group over k.*

a) G *contains a Borel subgroup over k.*

b) *Each conjugacy class over k contains an element over k.*

Observe that *b)* is the same as 1.10. Both results follow from 1.9. In the first case we take as the homogeneous space the variety of Borel subgroups, in the second case the conjugacy class under consideration.

10.3. *Corollary. — If k is as above and* G *is simply connected, the natural map from the set of semisimple classes of G_k to the set of semisimple classes of* G *over k is bijective.*

By 10.2 *a)* and 9.9 the map is surjective. To prove injectivity we must show that if x and y are semisimple elements of G_k which are conjugate in G they are also conjugate in G_k. We have $axa^{-1}=y$ with a in G. Then for γ in Γ we have $\gamma(a)x\gamma(a)^{-1}=y$, whence $a^{-1}\gamma(a)$ is in G_x. Now $\gamma \to a^{-1}\gamma(a)$ is a cocycle and G_x is connected (cf. 2.10), and over k because x is. Thus by 1.9 there exists b in G_x such that $b^{-1}a^{-1}\gamma(a)\gamma(b)=1$ for all γ. Thus ab is over k, and x and y are conjugate in G_k, under ab in fact, whence 10.3.

10.4. *Remarks. — a)* For regular classes 10.3 is false, since regular elements of G_k conjugate in G need not be conjugate in G_k.

b) For the split adjoint group of type A_r over any field k one can show, by the usual normal forms, that any elements of G_k, semisimple or not, are conjugate in G_k if they are conjugate in G. Does the same result hold for the other simple types, and is it enough to assume a Borel subgroup over k?

§ 11. Added in proof

M. Kneser has informed me that in 1.8 the assumption that G is simply connected can be dropped. If k is finite, the proof is as before (see § 10). If k is infinite, the key point is that the group $x(G)$ of the proof of 1.8 can be constructed even if (x_γ) is only a cocycle modulo the centre of G, so that if G is simply connected such a " cocycle " is equivalent to one with values in a torus over k. By applying this to the simply connected covering group of a group which is as in 1.8 but not simply connected, we get the improved version of 1.8. Proceeding then as in the proof of 10.1 we can drop the assumption of semisimplicity. The result is:

11.1. *Theorem. — Let k be a perfect field and* G *a connected linear group which is over k and contains a Borel subgroup over k. Then each element of* $H^1(k, G)$ *can be represented by a cocycle whose values are in a torus over k.*

Using 11.1 we now give a simplified proof of the implication *a)* $\to$ *b)* of 1.9. The assumption $\dim k \leq 1$ is used only in the proof, for which we refer the

reader to [12, Prop. 3.1.2], that $H^1(k, G)=o$ if G is a torus over k, since we show:

11.2. *Theorem. — Let k be a perfect field and n a positive integer such that* $H^1(k, T)=o$ *for every torus* T *of rank n and over k. Then* $H^1(k, G)=o$ *for every connected linear group* G *of rank n and over k.*

By 11.1 and the assumption in 11.2 we have

(*) $H^1(k, G)=o$ if G in 11.2 contains a Borel subgroup over k.

In the general case let R be the radical of G and Z the centre of G/R. There exists a group G_0 (the split one, e.g.) which is over k and contains a Borel subgroup B over k, and an isomorphism φ over K of G_0 onto $(G/R)/Z$. Since G_0 is a centreless semisimple group, we have the split extension $\mathrm{Aut}\, G_0 = G_0 E$, in which E is a finite group which fixes B (see [8, p. 17-07, Prop. 1]). For $\gamma\in\Gamma$, write $\varphi^{-1}\gamma(\varphi)=g_\gamma e_\gamma (g_\gamma\in G_0, e_\gamma\in E)$. Then (e_γ) is a cocycle and (g_γ) is a cocycle in the group G_0 twisted by (e_γ). In this group (g_γ) is equivalent to the trivial cocycle by (*) because B is over k. Thus $(g_\gamma e_\gamma)$ is equivalent to (e_γ) in $H^1(k, \mathrm{Aut}\, G_0)$, whence φ may be normalized so that $\varphi^{-1}\gamma(\varphi)=e_\gamma$. Then φB is a Borel subgroup over k in $(G/R)/Z$, and its inverse image is one in G, whence $H^1(k, G)=o$ by (*).

BIBLIOGRAPHY

[1] A. Borel, Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes, *Tôhoku Math. J.*, 13 (1961), 216-240.

[2] S. Helgason, *Differential geometry and symmetric spaces*, Academic Press, New York (1962).

[3] B. Kostant, The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group, *Amer. J. Math.*, 81 (1959), 973-1032.

[4] —, Lie group representations on polynomial rings, *Amer. J. Math.*, 85 (1963), 327-404.

[5] S. Lang, Algebraic groups over finite fields, *Amer. J. Math.*, 78 (1956), 555-563.

[6] M. Rosenlicht, Some rationality questions on algebraic groups, *Ann. di Mat.*, 43 (1957), 25-50.

[7] —, On quotient varieties and the affine imbedding of certain homogeneous spaces, *Trans. Amer. Math. Soc.*, 101 (1961), 211-223.

[8] Séminaire C. Chevalley, *Classification des Groupes de Lie algébriques* (two volumes), Paris (1956-58).

[9] Séminaire « Sophus Lie », *Théorie des algèbres de Lie...*, Paris (1954-5).

[10] J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, Paris (1959).

[11] —, *Corps locaux*, Hermann, Paris (1962).

[12] —, Cohomologie galoisienne des groupes algébriques linéaires, *Colloque sur la théorie des groupes algébriques*, Bruxelles (1962), 53-68.

[13] —, *Cohomologie galoisienne*, Cours fait au Collège de France ((1962-3).

[14] D. A. Smith, *Dissertation*, Yale University (1963).

[15] T. A. Springer, Quelques résultats sur la cohomologie galoisienne, *Colloque sur la théorie des groupes algébriques*, Bruxelles (1962), 129-135.

[16] R. Steinberg, Finite reflection groups, *Trans. Amer. Math. Soc.*, 91 (1959), 493-504.

[17] —, Representations of algebraic groups, *Nagoya Math. J.*, 22 (1963), 33-56.

[18] H. Weyl, Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare Transformationen III, *Math. Zeit.* (1926), 377-395.

University of California, Los Angeles.

Reçu le 25-8-1964.

Appendix 2.
Complements on Galois cohomology

[The following text reproduces, with minor changes, the *résumé de cours* published in *l'Annuaire du Collège de France*, 1990–1991, pp. 111–121.]

The course was devoted to the same topic as that in 1962–1963: *Galois cohomology*. The emphasis was mainly on the problems raised by semisimple groups when no restrictions are placed upon the ground field.

§ 1. Notation

– k is a commutative field, assumed to be of characteristic $\neq 2$, for simplicity;

– k_s is a separable closure of k;

– $\mathrm{Gal}(k_s/k)$ is the Galois group of k_s/k; it is a profinite group. If L is an algebraic group over k, we denote by $H^1(k, L)$ the first cohomology set of $\mathrm{Gal}(k_s/k)$ with values in $L(k_s)$. It is a pointed set.

If C is a $\mathrm{Gal}(k_s/k)$-module, one defines, for any $n \geq 0$, the cohomology groups

$$H^n(k, C) = H^n(\mathrm{Gal}(k_s/k), C) \ .$$

For example, if $C = \mathbf{Z}/2\mathbf{Z}$, we have

$$H^1(k, \mathbf{Z}/2\mathbf{Z}) = k^*/k^{*2}$$

and

$$H^2(k, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Br}_2(k)$$

(the kernel of multiplication by 2 in the Brauer group of k).

One of the themes of the course was to make explicit the relations which exist (or which may exist) between the set $H^1(k, L)$ for semisimple L, and the groups $H^n(k, C)$ for $C = \mathbf{Z}/2\mathbf{Z}$ (or $\mathbf{Z}/3\mathbf{Z}$, or any other "small" module over $\mathrm{Gal}(k_s/k)$).

§ 2. The orthogonal case

This is the best understood case, thanks to its interpretation in terms of classes of quadratic forms:

Let q be a nondegenerate quadratic form of rank $n \geq 1$ over k, and let $\mathbf{O}(q)$ be the *orthogonal group* of q, considered as an algebraic group over k. If x is an element of $H^1(k, \mathbf{Q}(q))$, one may *twist* q by x and obtain from it another quadratic form q_x with the same rank n as q. The map $x \mapsto (q_x)$ defines a *bijection* of $H^1(k, \mathbf{O}(q))$ onto the set of *classes of nondegenerate quadratic forms of rank* n over k.

There is an analogous result for the identity component $\mathbf{SO}(q)$ of $\mathbf{O}(q)$, if one restricts oneself to quadratic forms having the same discriminant as q.

In this way, every *invariant* of classes of quadratic forms can be interpreted as a function on the cohomology set $H^1(k, \mathbf{O}(q))$, or on the set $H^1(k, \mathbf{SO}(q))$.

2.1. Examples of invariants: the Stiefel-Whitney classes

Let us write q as an orthogonal direct sum of forms of rank 1:

$$q = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \cdots \oplus \langle a_n \rangle = \langle a_1, a_2, \ldots, a_n \rangle \ , \quad \text{with } a_i \in k^* .$$

If m is an integer ≥ 0, one defines an element $w_m(q)$ of $H^m(k, \mathbf{Z}/2\mathbf{Z})$ by the formula

$$w_m(q) = \sum_{i_1 < \cdots < i_m} (a_{i_1}) \cdots (a_{i_m}) \ . \tag{2.1.1}$$

(We denote by (a) the element of $H^1(k, \mathbf{Z}/2\mathbf{Z})$ defined by $a \in k^*$: the product $(a_{i_1}) \cdots (a_{i_m})$ is a cup-product in the cohomology algebra $H^*(k, \mathbf{Z}/2\mathbf{Z})$.)

It can be shown (A. Delzant [40]) that $w_m(q)$ only depends on the class of q and not on the chosen decomposition; this comes from the well-known fact that relations between quadratic forms "follow from the relations in rank ≤ 2".

One says that $w_m(q)$ is the m-th *Stiefel-Whitney class* of q.

Remarks.

1) The classes $w_1(q)$ and $w_2(q)$ have standard interpretations: discriminant, Hasse-Witt invariant. The $w_m(q)$, for $m \geq 3$ are less interesting; it is better to replace them (as far as possible) with Milnor invariants, cf. §2.3 below.

2) The same method gives other invariants. Thus, if n is even ≥ 4 and if $q = \langle a_1, \ldots, a_n \rangle$ is such that $w_1(q) = 0$ (i.e., if $a_1 \cdots a_n$ is a square), one can show that the element $(a_1) \cdots (a_{n-1})$ in $H^{n-1}(k, \mathbf{Z}/2\mathbf{Z})$ is an *invariant* of the class of q. The case $n = 4$ is particularly interesting.

2.2. Behavior of $w_1(q)$ and $w_2(q)$ under torsion

Take $x \in H^1(k, \mathbf{O}(q))$. We associate to x some elements

$$\delta^1(x) \in H^1(k, \mathbf{Z}/2\mathbf{Z}) \qquad \text{and} \qquad \delta^2(x) \in H^2(k, \mathbf{Z}/2\mathbf{Z})$$

in the following way:

$\delta^1(x)$ is the image of x in $H^1(k, \mathbf{Z}/2\mathbf{Z})$ by the map deduced from the homomorphism $\det : \mathbf{O}(q) \to \{\pm 1\} = \mathbf{Z}/2\mathbf{Z}$;

$\delta^2(x)$ is the coboundary of x relative to the exact sequence of algebraic groups:

$$1 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow \widetilde{\mathbf{O}}(q) \longrightarrow \mathbf{O}(q) \longrightarrow 1 .$$

(The group $\widetilde{\mathbf{O}}(q)$ is a certain quadratic covering of $\mathbf{O}(q)$ which extends the spinor covering $\mathbf{Spin}(q) \to \mathbf{SO}(q)$. One can characterize it by the following property: a symmetry with respect to a vector whose square is a can be lifted to an element of order 2 in $\widetilde{\mathbf{O}}(q)$ which is rational over the field $k(\sqrt{a})$.)

The invariants $\delta^1(x)$ and $\delta^2(x)$ allow one to compute the classes w_1 and w_2 of the form q_x derived from q by twisting using x. Indeed one has:

$$w_1(q_x) = w_1(q) + \delta^1(x) \quad \text{in } H^1(k, \mathbf{Z}/2\mathbf{Z}), \tag{2.2.1}$$

$$w_2(q_x) = w_2(q) + \delta^1(x) \cdot w_1(q) + \delta^2(x) \quad \text{in } H^2(k, \mathbf{Z}/2\mathbf{Z}). \tag{2.2.2}$$

2.3. The Milnor conjectures

Let $\mathbf{k}^M(k) = \bigoplus \mathbf{k}_n^M(k)$ *be the Milnor ring* (mod 2) of k (defined using the multilinear symbols $(a_1, \ldots, a_n) = (a_1) \cdots (a_n)$, $a_i \in k^*$, with the relations $2(a) = 0$ and $(a, b) = 0$ if $a + b = 1$).

Let W_k be the Witt ring of k, and I_k its augmentation ideal (kernel of the canonical homomorphism $W_k \to \mathbf{Z}/2\mathbf{Z}$).

There are natural homomorphisms

$$\mathbf{k}_n^M(k) \longrightarrow I_k^n / I_k^{n+1} \tag{2.3.1}$$

and

$$\mathbf{k}_n^M(k) \longrightarrow H^n(k, \mathbf{Z}/2\mathbf{Z}) . \tag{2.3.2}$$

Milnor's conjectures [117] say that these homomorphisms are *isomorphisms*. This has been proved for $n \leq 3$ (Arason [3], [4], Jacob-Rost [78], Merkurjev-Suslin [111]) and there are partial results for $n \geq 4$.

§ 3. Applications and examples

3.1. Invariants with values in $H^3(k, \mathbf{Z}/2\mathbf{Z})$: the case of the spinor group

Let q be a nondegenerate quadratic form over k, and let x be an element of $H^1(k, \mathbf{Spin}(q))$. If one twists q by x, one obtains a quadratic form q_x with the same rank as q. From (2.2.1) and (2.2.2), the invariants w_1 and w_2 of q_x are the same as those of q. It follows that the element $q_x - q$ in the Witt ring W_k belongs to the cube I_k^3 of the augmentation ideal I_k. Using the homomorphism

$$I_k^3 / I_k^4 \longrightarrow H^3(k, \mathbf{Z}/2\mathbf{Z})$$

constructed by Arason [3] (which is actually an isomorphism, cf. §2.3), one obtains an element of $H^3(k, \mathbf{Z}/2\mathbf{Z})$ which we shall denote $i(x)$. We have:

$$i(x) = 0 \iff q_x \equiv q \pmod{I_k^4} . \tag{3.1.1}$$

Hence we have a canonical map

$$H^1(k, \mathbf{Spin}(q)) \longrightarrow H^3(k, \mathbf{Z}/2\mathbf{Z}) . \tag{3.1.2}$$

3.2. Invariants with values in $H^3(k, \mathbf{Z}/2\mathbf{Z})$: the general case

Let G be a split *simply connected* semisimple group, and choose an irreducible representation ϱ of G in a vector space V of dimension n. Assume ϱ orthogonal, which is the case, for instance, if G is type G_2, F_4 or E_8. Then there exists a nondegenerate quadratic form q over V which is invariant under $\varrho(G)$. Thus we obtain a homomorphism $G \to \mathbf{O}(q)$. In view of the hypotheses made on G, this homomorphism lifts to a homomorphism

$$\tilde{\varrho} : G \longrightarrow \mathbf{Spin}(q) .$$

Using (3.1.2) we deduce from it a map

$$i_\varrho : H^1(k, G) \longrightarrow H^3(k, \mathbf{Z}/2\mathbf{Z}) , \tag{3.2.1}$$

which is easily shown not to depend on the choice of q.

3.3. The group G_2

Suppose that G is the exceptional group G_2, and is split. It is well known that there are natural bijections between the following three sets:

$H^1(k, G_2)$;

classes of octonion algebras over k;

classes of 3-fold Pfister forms over k.

It follows from this, and from the theorems quoted above, that, if one takes for ϱ the fundamental representation of degree 7 of G_2, the corresponding map i_ϱ is a *bijection of* $H^1(k, G_2)$ *onto the subset of* $H^3(k, \mathbf{Z}/2\mathbf{Z})$ *consisting of the decomposable elements* (i.e. cup-products of three elements of $H^1(k, \mathbf{Z}/2\mathbf{Z})$). This gives an entirely satisfactory cohomological description of the set $H^1(k, G_2)$.

One can go further. Denote by i the injection of $H^1(k, G_2)$ into $H^3(k, \mathbf{Z}/2\mathbf{Z})$ which we have just defined. Let ϱ be an arbitrary irreducible representation of G_2; by (3.2.1) there is a corresponding map

$$i_\varrho : H^1(k, G_2) \longrightarrow H^3(k, \mathbf{Z}/2\mathbf{Z}) .$$

We want to compare i_ϱ with i. The result is as follows (here I restrict myself to the case where the ground field has characteristic 0):

(3.3.1) *Either* $i_\varrho = i$, *or* $i_\varrho = 0$.

More precisely, let $m_i\omega_1 + m_2\omega_2$ be the dominant weight of ϱ, written as a linear combination of the fundamental weights ω_1 and ω_2 (ω_1 corresponds to

the representation of degree 7, and ω_2 to the adjoint representation). One can determine (thanks to formulas which were communicated to me by J. Tits) in which case one has $i_\varrho = i$; one finds that this is so if and only if the pair (m_1, m_2) is congruent (mod 8) to one of the following twelve pairs:

$(0,2), (0,3), (1,0), (1,4), (2,0), (2,3), (4,3), (4,6), (5,2), (5,6), (6,3), (6,4)$.

Thus, for the adjoint representation, which corresponds to $(0,1)$, we have $i_\varrho = 0$. One can make this more precise by explicitly determining the Killing form Kill_x of the k-form of G_2 associated to a given element $x \in H^1(k, G_2)$. If $q_x = \langle 1 \rangle \oplus q_x^0$ is the 3-fold Pfister form associated to x (i.e. the *norm form* of the corresponding octonion algebra), one finds that Kill_x *is isomorphic to* $\langle -1, -3 \rangle \otimes q_x^0$.

3.4. The group F_4

Here again, we have a concrete description of the cohomology: the elements of $H^1(k, F_4)$ correspond to the classes of *exceptional simple Jordan algebras* of dimension 27 over k. Unfortunately, one is far from knowing how to classify such algebras, despite the numerous results already obtained by Albert, Jacobson, Tits, Springer, McCrimmon, Racine, Petersson (cf. [2], [80], [105], [122], [123], [161], [163]). These results suggest that the elements of $H^1(k, F_4)$ could be characterized by two types of invariants:

(*invariants* mod 2) — The class of the quadratic form $\mathrm{Tr}(x^2)$ associated to the Jordan algebra, itself determined by the pair consisting in a *3-fold Pfister form* and a *5-fold Pfister form* divisible by the former. From a cohomological point of view, this means a decomposable element $x_3 \in H^3(k, \mathbf{Z}/2\mathbf{Z})$ (obtained by (3.2.1) through the irreducible representation ϱ of F_4 of dimension 26), and an element x_5 of $H^5(k, \mathbf{Z}/2\mathbf{Z})$ of the form $x_5 = x_3 yz$, with $y, z \in H^1(k, \mathbf{Z}/2\mathbf{Z})$.

(*invariants* mod 3 — assuming the characteristic $\neq 3$) — An element of $H^3(k, \mathbf{Z}/3\mathbf{Z})$ for which I only have a conjectural definition, based on "Tits's first construction" (this definition has been justified later by Rost [131], [132]).

At present, the only case which has been treated completely is that of the Jordan algebras called "reduced" (those for which the invariant mod 3 is 0): one knows, by a theorem due to Springer [163], that the mod 2 invariant (i.e. the trace form) then determines the Jordan algebra up to isomorphism.

3.5. The group E_8

When k is a number field, the structure of $H^1(k, E_8)$ has just been determined by Chernousov and Premet (cf. [30], [125]): the Hasse principle holds, which implies, for example, that the number of elements in $H^1(k, E_8)$ is 3^r, where r is the number of real places of k. The proof of this result has been given in a joint seminar with J. Tits.

When k is an arbitrary field (or even, for example, the field $\mathbf{Q}(T)$), very little is known about $H^1(k, E_8)$. The general results of Grothendieck [60] and of Bruhat-Tits ([23], III) suggest that an element of this set can have as invariants cohomology classes (of dimension ≥ 3) mod 2, mod 3 and mod 5 (because 2,

3, 5 are the *torsion primes* of E_8, cf. A. Borel, *Oe.* II, p. 776). For this see Rost [132], and also [156], §7.3.

§ 4. Injectivity problems

The set $H^1(k, G)$ is functorial in k and G:

a) If k' is an extension of k, there is a natural map

$$H^1(k, G) \longrightarrow H^1(k', G) .$$

b) If $G \to G'$ is an algebraic group morphism, there is a natural map $H^1(k, G) \to H^1(k, G')$.

There are several cases where these maps are *injective*:

(4.1) — (Witt's cancellation theorem [187]) If $q = q_1 \oplus q_2$, where q_i are quadratic forms, the map $H^1(k, \mathbf{O}(q_1)) \to H^1(k, \mathbf{O}(q))$ is injective.

(4.2) — Same assertion for the *unitary groups* associated with algebras with involutions over k, cf. Scharlau [139], chap. 7.

(4.3) (Springer [159]) — Injectivity of $H^1(k, \mathbf{O}(q)) \to H^1(k', \mathbf{O}(q))$ when k' is a finite extension of k *of odd degree.*

(4.4) (Bayer-Lenstra [9]) — Same assertion as (4.3), for the *unitary groups* instead of the orthogonal groups.

(4.5) (Pfister [124]) — Injectivity of $H^1(k, \mathbf{O}(q)) \to H^1(k, \mathbf{O}(q \otimes q'))$ when the rank of q' is odd (the morphism $\mathbf{O}(q) \to \mathbf{O}(q \otimes q')$ being defined by the tensor product).

One would like to have other similar statements, for example, the following (which may be a bit too optimistic):

(4.6 ?) — If k' is a finite extension of k with degree prime to 2 and 3, the map $H^1(k, F_4) \to H^1(k', F_4)$ is injective.

(4.7 ?) — Same assertion for E_8, with $\{2, 3\}$ replaced by $\{2, 3, 5\}$.

Remark.

Let G be an algebraic group over k, and let x and y be two elements of $H^1(k, G)$. Suppose that x and y have the same images in $H^1(k', G)$ and in $H^1(k'', G)$ where k' and k'' are two finite extensions of k with mutually prime degrees (for example $[k' : k] = 2$ and $[k'' : k] = 3$). This *does not imply* $x = y$ contrary to what happens in the abelian case; one can construct examples of this by taking G not to be connected; I do not know what happens when G is connected.

§ 5. The trace form

We are interested in the structure of the quadratic form $\mathrm{Tr}(x^2)$ associated to a finite-dimensional k-algebra. Two special cases have been considered:

5.1. Central simple algebras

Let A be such an algebra, assumed to be of finite rank n^2 over k. We associate to it the quadratic form q_A defined by

$$q_A(x) = \mathrm{Trd}_{A/k}(x^2) \ .$$

Denote by q_A^0 the trace form associated to the algebra of matrices $\mathbf{M}_n(k)$ of the same rank as A; it is the direct sum of a hyperbolic form of rank $n(n-1)$ and the unit form $\langle 1, 1, \ldots, 1\rangle$ of rank n.

We wish to compare q_A and q_A^0. There are two cases to consider:

(5.1.1) *n is odd*

The forms q_A and q_A^0 are then isomorphic; this follows from the theorem of Springer quoted in (4.3).

(5.1.2) *n is even*

Let (A) be the class of A in the Brauer group of k. The product of (A) by the integer $n/2$ is an element a of $\mathrm{Br}_2(k) = H^2(k, \mathbf{Z}/2\mathbf{Z})$. We have:

$$w_1(q_A) = w_1(q_A^0) \quad \text{and} \quad w_2(q_A) = w_2(q_A^0) + a \ .$$

(The formula relative to w_1 is easy. That relative to w_2 can be obtained by considering the homomorphism $\mathbf{PGL}_n \to \mathbf{SO}_{n^2}$ given by the adjoint representation and by showing, by a weight computation, that this homomorphism does not lift to the group $\mathbf{Spin}_{n^2}$ if n is even.)

5.2. Etale commutative algebras

Let E be such an algebra, let n be its rank and let q_E be the corresponding trace form. The invariants w_1 and w_2 of q_E may be computed by a known formula (cf. [154]). The course gave a proof of this formula which is somewhat different from the original one, and applied the result to quintic equations à la Kronecker-Hermite-Klein.

The case $n = 6$ poses some interesting problems:

1) Denote by $e : \mathrm{Gal}(k_s/k) \to S_6$ the homomorphism corresponding to E by Galois theory; this homomorphism is defined up to conjugation. If one composes e with an outer automorphism of S_6, one obtains a homomorphism $e' : \mathrm{Gal}(k_s/k) \to S_6$ which corresponds to another étale algebra E' of rank 6 ("sextic resolvent"). *How does one determine $q_{E'}$ starting from q_E?* The recipe is as follows: if one writes q_E and $q_{E'}$ in the form

$$q_E = \langle 1, 2\rangle \oplus Q \ , \qquad q_{E'} = \langle 1, 2\rangle \oplus Q' \ ,$$

where Q and Q' are of rank 4 (this is possible according to [154], App. I), we have $Q' = \langle 2d \rangle \otimes Q$, where d is the discriminant of E (i.e. of q_E).

2) Suppose one has $w_1(q_E) = 0$ and $w_2(q_E) = 0$. One may ask whether q_E is isomorphic to the unit form $\langle 1, \ldots, 1 \rangle$ (as would be the case if the rank were < 6). This is true if k is a number field (or a rational function field over a number field). It is in general false.

§ 6. Bayer-Lenstra theory: self-dual normal bases

Let G be a finite group. We are interested in the *G-Galois algebras* over k, i.e. in the *G-torsors* over k, G being considered as an algebraic group of dimension 0 over k. Such an algebra L is determined, up to a nonunique isomorphism, by a continuous homomorphism

$$\varphi_L : \mathrm{Gal}(k_s/k) \longrightarrow G .$$

When φ_L is surjective, L is a field, and it is a Galois extension of k with Galois group isomorphic to G.

In [9], E. Bayer and H. Lenstra are interested in the case when L has a *self-dual normal basis* ("an SDNB"); this means that there exists an element x of L such that $q_L(x) = 1$ and that x is orthogonal (relative to q_L) to every gx, $g \in G$, $g \neq 1$. (Thus, the gx form a "normal basis" of L, and this basis is its own dual with respect to q_L.)

One can give a cohomological criterion for the existence of a SDNB: if U_G denotes the unitary group of the involutory algebra $k[G]$, there is a canonical embedding of G into $U_G(k)$; by composing φ_L with this embedding one obtains a homomorphism $\mathrm{Gal}(k_s/k) \to U_G(k)$, and this homomorphism may be viewed as a 1-cocycle of $\mathrm{Gal}(k_s/k)$ in $U_G(k_s)$. The class ε_L of this cocycle is an element of $H^1(k, U_G)$. One has $\varepsilon_L = 0$ *if and only if L has an* SDNB.

From this criterion, combined with (4.4), Bayer-Lenstra deduced the following theorem:

(6.1) — *If there exists an extension of k of odd degree over which L acquires an* SDNB, *then L has an* SDNB *over k.*

In particular:

(6.2) — *If G is of odd order, every Galois G-algebra has an* SDNB.

Here are some other results about SDNB, obtained in collaboration with E. Bayer, cf. [11]:

Let L be a Galois G-algebra, and let $\varphi_L : \mathrm{Gal}(k_s/k) \to G$ be the corresponding homomorphism. If x is an element of $H^n(G, \mathbf{Z}/2\mathbf{Z})$, its image under

$$\varphi_L^* : H^n(G, \mathbf{Z}/2\mathbf{Z}) \longrightarrow H^n(\mathrm{Gal}(k_s/k), \mathbf{Z}/2\mathbf{Z}) = H^n(k, \mathbf{Z}/2\mathbf{Z})$$

will be denoted by x_L.

(6.3) *In order that L have an* SDNB, *it is necessary that $x_L = 0$ for every $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$* (i. e., the image of $\mathrm{Gal}(k_s/k)$ in G is in all the index-2 subgroups of G). *This condition is sufficient if the cohomological 2-dimension of* $\mathrm{Gal}(k_s/k)$ *is* ≤ 1 (i. e., if the Sylow 2-groups of $\mathrm{Gal}(k_s/k)$ are free pro-2-groups).

(6.4) — *Suppose that k is a number field. In order that L have an* SDNB, *it is necessary that $\varphi_L(c_v) = 1$ for every real place v of k* (c_v denoting the complex conjugation with respect to an extension of v to k_s). *This condition is sufficient if $H^1(G, \mathbf{Z}/2\mathbf{Z}) = H^2(G, \mathbf{Z}/2\mathbf{Z}) = 0$.*

(6.5) *The case where a Sylow 2-group of G is elementary abelian.*

Let S be a Sylow 2-group of G. Suppose that S is an elementary abelian group of order 2^r, $r \geq 1$; the order of G is $2^r m$, with m odd.

(6.5.1) — *There exists an r-fold Pfister form q_L^1, and, up to isomorphism, only one, such that $\langle 2^r \rangle \otimes q_L \simeq m \otimes q_L^1$* (a direct sum of m copies of q_L^1).

This form is an *invariant* of the Galois algebra L. It is the unit form if L has an SDNB. Conversely:

(6.5.2) — *Suppose that the normalizer N of S acts transitively on $S - \{1\}$. The following are equivalent*:

(i) *L has an* SDNB.
(ii) *The form q_L is isomorphic to the unit form of rank $2^r m$.*
(iii) *The form q_L^1 is isomorphic to the unit form of rank 2^r.*

When r is small enough, this result can be translated into cohomological terms. Indeed, the hypothesis that N act transitively on $S - \{1\}$ implies that there exists an element x of $H^r(G, \mathbf{Z}/2\mathbf{Z})$ whose restriction to any subgroup of order 2 of G is $\neq 0$, and such an element is unique, up to the addition of a "negligible" cohomology class (cf. § 7 below). The corresponding element x_L of $H^r(k, \mathbf{Z}/2\mathbf{Z})$ is an invariant of the Galois algebra L.

(6.5.3) — *Suppose that $r \leq 4$. The conditions* (i), (ii), (iii) *in* (6.5.2) *are then equivalent to*:

(iv) *$x_L = 0$ in $H^r(k, \mathbf{Z}/2\mathbf{Z})$.*

The hypothesis $r \leq 4$ could be dropped if the conjectures in §2.3 were proved.

Examples.

1) Suppose that $r = 2$ and that N acts transitively on $S - \{1\}$; this is so when $G = A_4$, A_5 or $\mathbf{PSL}_2(\mathbf{F}_q)$ with $q \equiv 3 \pmod 8$. The group $H^2(G, \mathbf{Z}/2\mathbf{Z})$ contains a single element $x \neq 0$; let $\widetilde{G}$ be the corresponding extension of G by $\mathbf{Z}/2\mathbf{Z}$. It follows from (6.5.3) that L *has an* SDNB *if and only if the homomorphism* $\varphi_L : \mathrm{Gal}(k_s/k) \to G$ *lifts to a homomorphism in* $\widetilde{G}$. Such a lifting corresponds to a Galois $\widetilde{G}$-algebra $\widetilde{L}$; one can show it is possible to arrange that $\widetilde{L}$ also has an SDNB.

2) Take as G the group $\mathbf{SL}_2(\mathbf{F}_8)$ or the Janko group J_1. The hypotheses in (6.5.2) and (6.5.3) are then satisfied with $r = 3$. The group $H^3(G, \mathbf{Z}/2\mathbf{Z})$ contains a single element $x \neq 0$, and one sees that L *has an* SDNB *if and only if* $x_L = 0$ *in* $H^3(k, \mathbf{Z}/2\mathbf{Z})$.

Remark.

The property that a G-Galois algebra L have an SDNB can be translated into "Galois twisting" terms as follows:

Let V be a finite-dimensional vector space over k, equipped with a family $\mathbf{q} = (q_i)$ of *quadratic tensors* (of type $(2,0)$, $(1,1)$, or $(0,2)$, it doesn't matter which). Suppose that G acts on V and fixes every q_i. One may then *twist* $(V, \mathbf{q})$ by the G-torsor corresponding to L. In this way one obtains a *k-form* $(V, \mathbf{q})_L$ of $(V, \mathbf{q})$. One can prove:

(6.6) *If L has an* SDNB, $(V, \mathbf{q})_L$ *is isomorphic to* $(V, \mathbf{q})$.

Moreover, this property *characterizes* the Galois algebras which have an SDNB.

(Note that such a statement would be false for cubic tensors.)

§ 7. Negligible cohomology classes

Let G be a finite group and C a G-module. An element x in $H^q(G, C)$ is said to be *negligible* (from the Galois standpoint) if, for every field k, and every continuous homomorphism $\varphi : \mathrm{Gal}(k_s/k) \to G$, we have

$$\varphi^*(x) = 0 \qquad \text{in } H^q(k, C) \ .$$

(This amounts to saying that $x_L = 0$ for every G-Galois algebra L.)

Example.

If a and b are two elements of $H^1(G, \mathbf{Z}/2\mathbf{Z})$, the cup-product $ab(a+b)$ is a negligible element of $H^3(G, \mathbf{Z}/2\mathbf{Z})$.

Here are some results about these classes:

(7.0) — *If $q = 1$, no nonzero element of $H^q(G, C)$ is negligible. The same is true if $q = 2$ and G acts trivially on C.*

(7.1) — *For every finite group G there exists an integer $q(G)$ such that any cohomology class of G of odd order and dimension $q > q(G)$ is negligible.*

This result does not extend to classes of even order. Indeed, no cohomology class (other than 0) of a cyclic group of order 2 is negligible, as one sees by taking $k = \mathbf{R}$.

(7.2) — *Suppose that G is elementary abelian of order 2^r. If $x \in H^q(G, \mathbf{Z}/2\mathbf{Z})$, the following properties are equivalent:*

(a) *x is negligible.*
(b) *The restriction of x to any subgroup of order 2 is 0.*
(c) *x belongs to the ideal of the algebra $H^*(G, \mathbf{Z}/2\mathbf{Z})$ generated by the cup-products $ab(a+b)$, where a and b run over $H^1(G, \mathbf{Z}/2\mathbf{Z})$.*

(There are analogous results when G is elementary abelian of order p^r ($p \neq 2$), and $C = \mathbf{Z}/p\mathbf{Z}$.)

(7.3) — *Suppose that G is isomorphic to a symmetric group S_n. Then:*

(a) *If N is odd, every element of $H^q(G, \mathbf{Z}/N\mathbf{Z})$, $q \geq 1$, is negligible.*
(b) *In order that an element of $H^q(G, \mathbf{Z}/2\mathbf{Z})$ be negligible, it is necessary and sufficient that its restrictions to the subgroups of G of order 2 vanish.*

Bibliography

[1] A. Albert – *Structure of Algebras*, A.M.S. Colloquium Publ. 24, Providence, 1961.

[2] A. Albert and N. Jacobson – On reduced exceptional simple Jordan algebras, *Ann. of Math.* **66** (1957), 400–417.

[3] J. Arason – Cohomologische Invarianten quadratischer Formen, *J. Algebra* **36** (1975), 446–491.

[4] " " – A proof of Merkurjev's theorem, *Canadian Math. Soc. Conference Proc.* **4** (1984), 121–130.

[5] E. Artin and O. Schreier – Eine Kennzeichnung der reell abgeschlossenen Körper, *Hamb. Abh.* **5** (1927), 225–231 (= E. Artin, *C.P.* 21).

[6] E. Artin and J. Tate – *Class Field Theory*, Benjamin Publ., New York, 1967.

[7] M. Artin, A. Grothendieck and J-L. Verdier – *Cohomologie Etale des Schémas* (SGA 4), Lect. Notes in Math. 269–270–305, Springer-Verlag, 1972–1973.

[8] J. Ax – Proof of some conjectures on cohomological dimension, *Proc. A.M.S.* **16** (1965), 1214–1221.

[9] E. Bayer-Fluckiger and H.W. Lenstra, Jr. – Forms in odd degree extensions and self-dual normal bases, *Amer. J. Math.* **112** (1990), 359–373.

[10] E. Bayer-Fluckiger and R. Parimala – Galois cohomology of classical groups over fields of cohomological dimension ≤ 2, *Invent. Math.* **122** (1995), 195–229.

[11] E. Bayer-Fluckiger and J-P. Serre – Torsions quadratiques et bases normales autoduales, *Amer. J. Math.* **116** (1994), 1–63.

[12] F. van der Blij and T.A. Springer – The arithmetics of octaves and of the group G_2, *Indag. Math.* **21** (1959), 406–418.

[13] A. Borel – Groupes linéaires algébriques, *Ann. of Math.* **64** (1956), 20–82 (= *Oe.* 39).

[14] " " – Some finiteness properties of adele groups over number fields, *Publ. Math. I.H.E.S.* **16** (1963), 5–30 (= *Oe.* 60).

[15] " " – Arithmetic properties of linear algebraic groups, *Proc. Int. Congress Math. Stockholm* (1962), 10–22 (= *Oe.* 61).

[16] " " – *Linear Algebraic Groups*, 2nd edition, Springer-Verlag, 1991.

[17] A. Borel and Harish-Chandra – Arithmetic subgroups of algebraic groups, *Ann. of Math.* **75** (1962) 485–535 (= A. Borel, *Oe.* 58).

[18] A. Borel and J-P. Serre – Théorèmes de finitude en cohomologie galoisienne, *Comm. Math. Helv.* **39** (1964), 111–164 (= A. Borel, *Oe.* 64).

[19] A. Borel and T.A. Springer – Rationality properties of linear algebraic groups, *Proc. Symp. Pure Math. A.M.S.* **9** (1966), 26–32 (= A. Borel, *Oe.* 76); II, *Tôhoku Math. J.* **20** (1968), 443–497 (= A. Borel, *Oe.* 80).

[20] A. Borel and J. Tits – Groupes réductifs, *Publ. Math. I.H.E.S.* **27** (1965), 55–150 (= A. Borel, *Oe.* 66); Compléments, *ibid.* **41** (1972), 253–276 (= A. Borel, *Oe.* 94).

[21] Z.I. Borevič and I.R. Šafarevič – *Number Theory* (in Russian), 3rd edition, Moscow, 1985.

[22] F. Bruhat and J. Tits – Groupes algébrique simples sur un corps local, *Proc. Conf. Local Fields*, Driebergen, 23–26, Springer-Verlag, 1967.

[23] F. Bruhat and J. Tits – Groupes réductifs sur un corps local, *Publ. Math. I.H.E.S.* **41** (1972), 5–252; II, *ibid.* **60** (1984), 5–184; III, *J. Fac. Sci. Univ. Tokyo* **34** (1987), 671–688.

[24] A. Brumer – Pseudocompact algebras, profinite groups and class formations, *J. Algebra* **4** (1966), 442–470.

[25] H. Cartan and S. Eilenberg – *Homological Algebra*, Princeton Math. Ser. 19, Princeton, 1956.

[26] J.W.S. Cassels – Arithmetic on an elliptic curve, *Proc. Int. Congress Math. Stockholm* (1962), 234–246.

[27] J.W.S. Cassels and A. Fröhlich (edit.) – *Algebraic Number Theory*, Acad. Press, New York, 1967.

[28] F. Châtelet – Variations sur un thème de H. Poincaré, *Ann. Sci. E.N.S.* **61** (1944), 249–300.

[29] " " – Méthodes galoisiennes et courbes de genre 1, *Ann. Univ. Lyon*, sect. A–IX (1946), 40–49.

[30] V.I. Chernousov – The Hasse principle for groups of type E_8, *Math. U.S.S.R. Izv.* **34** (1990), 409–423.

[31] C. Chevalley – Démonstration d'une hypothèse de M. Artin, *Hamb. Abh.* **11** (1934), 73–75.

[32] " " – *Theory of Lie Groups*, Princeton Univ. Press, Princeton, 1946.

[33] " " – Sur certains groupes simples, *Tôhoku Math. J.* **7** (1955), 14–66.

[34] " " – *Classification des groupes de Lie algébriques*, Sém. E.N.S., I.H.P., Paris, 1956–1958.

[35] " " – Certains schémas de groupes semi-simples, *Sém. Bourbaki* 1960/61, exposé 219.

[36] J-L. Colliot-Thélène and J-J. Sansuc – Sur le principe de Hasse et sur l'approximation faible, et sur une hypothèse de Schinzel, *Acta Arith.* **41** (1982), 33–53.

[37] J-L. Colliot-Thélène and Sir Peter Swinnerton-Dyer – Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties, *J. Crelle* **453** (1994), 49–112.

[38] P. Dedecker – Sur la cohomologie non abélienne I, *Can. J. Math.* **12** (1960), 231–251; II, *ibid.* **15** (1963), 84–93.

[39] " " – Three dimensional non-abelian cohomology for groups, *Lect. Notes in Math.* **92**, Springer-Verlag, 1969, 32–64.
[40] A. Delzant – Définition des classes de Stiefel-Whitney d'un module quadratique sur un corps de caractéristique différente de 2, *C.R. Acad. Sci. Paris* **255** (1962), 1366–1368.
[41] M. Demazure and P. Gabriel – *Groupes Algébriques*, Masson, Paris, 1970.
[42] M. Demazure and A. Grothendieck – *Schémas en Groupes* (SGA 3), Lect. Notes in Math. 151–152–153, Springer-Verlag, 1970.
[43] S.P. Demuškin – The group of the maximum p-extension of a local field (in Russian), *Dokl. Akad. Nauk S.S.S.R.* **128** (1959), 657–660.
[44] " " – On 2-extensions of a local field (in Russian), *Math. Sibirsk.* **4** (1963), 951–955.
[45] " " – Topological 2-groups with an even number of generators and a complete defining relation (in Russian), *Izv. Akad. Nauk S.S.S.R.* **29** (1965), 3–10.
[46] J. Dieudonné – *La Géométrie des Groupes Classiques*, Ergebn. der Math. 5, Springer-Verlag, 1955.
[47] A. Douady – Cohomologie des groupes compacts totalement discontinus, *Sém. Bourbaki* 1959/60, exposé 189.
[48] D. Dummit and J.P. Labute – On a new characterization of Demuškin groups, *Invent. Math.* **73** (1983), 413–418.
[49] R.S. Elman – On Arason's theory of Galois cohomology, *Comm. Algebra* **10** (1982), 1449–1474.
[50] D.K. Faddeev – Simple algebras over a field of algebraic functions of one variable (in Russian), *Trud. Math. Inst. Steklov* **38** (1951), 321–344 (English translation: *A.M.S. Transl. Series* 2, vol. 3, 15–38).
[51] M. Fried and M. Jarden – *Field Arithmetic*, Ergebn. der Math. 11, Springer-Verlag, 1986.
[52] P. Gabriel – Des catégories abéliennes, *Bull. Soc. math. France* **90** (1962), 323–448.
[53] I. Giorgiutti – Groupes de Grothendieck, *Ann. Fac. Sci. Toulouse* **26** (1962), 151–207.
[54] J. Giraud – *Cohomologie Non Abélienne*, Springer-Verlag, 1971.
[55] R. Godement – Groupes linéaires algébriques sur un corps parfait, *Sém. Bourbaki*, 1960/61, exposé 206.
[56] E.S. Golod and I.R. Šafarevič – On class field towers (in Russian), *Izv. Akad. Nauk S.S.S.R.* **28** (1964), 261–272 (English translation: I.R. Shafarevich, *C.P.* 317–328).
[57] M.J. Greenberg – *Lectures on Forms in Many Variables*, Benjamin Publ., New York, 1969.
[58] A. Grothendieck – A general theory of fibre spaces with structure sheaf, *Univ. Kansas*, Report 4, 1955.
[59] " " – Sur quelques points d'algèbre homologique, *Tôhoku Math. J.* **9** (1957), 119–221.

[60] " " – Torsion homologique et sections rationnelles, *Sém. Chevalley* (1958), Anneaux de Chow et Applications, exposé 5.

[61] " " – Technique de descente et théorèmes d'existence en géométrie algébrique. II: le théorème d'existence en théorie formelle des modules, *Sém. Bourbaki*, 1959/60, exposé 195.

[62] " " – Eléments de Géométrie Algébrique (EGA), rédigés avec la collaboration de J. Dieudonné, *Publ. Math. I.H.E.S.* **4**, **8**, **11**, **17**, **20**, **24**, **28**, **32**, Paris, 1960–1967.

[63] " " – Le groupe de Brauer I–II–III, *Dix exposés sur la cohomologie des schémas*, 46–188, North Holland, Paris, 1968.

[64] " " – *Revêtements Etales et Groupe Fondamental* (SGA 1), Lect. Notes in Math. 224, Springer-Verlag, 1971.

[65] K. Haberland – *Galois Cohomology of Algebraic Number Fields*, VEB, Deutscher Verlag der Wiss., Berlin, 1978.

[66] D. Haran – A proof of Serre's theorem, *J. Indian Math. Soc.* **55** (1990), 213–234.

[67] G. Harder – Über die Galoiskohomologie halbeinfacher Matrizengruppen, I, *Math. Zeit.* **90** (1965), 404–428; II, *ibid.* **92** (1966), 396–415; III, *J. Crelle* **274/275** (1975), 125–138.

[68] " " – Bericht über neuere Resultate der Galoiskohomologie halbeinfacher Gruppen, *Jahr. D.M.V.* **70** (1968), 182–216.

[69] D. Hertzig – Forms of algebraic groups, *Proc. A.M.S.* **12** (1961), 657–660.

[70] G.P. Hochschild – Simple algebras with purely inseparable splitting fields of exponent 1, *Trans. A.M.S.* **79** (1955), 477–489.

[71] " " – Restricted Lie algebras and simple associative algebras of characteristic p, *Trans. A.M.S.* **80** (1955), 135–147.

[72] G.P. Hochschild and J-P. Serre – Cohomology of group extensions, *Trans. A.M.S.* **74** (1953), 110–134 (= J-P. Serre, *Oe.* 15)

[73] C. Hooley – On ternary quadratic forms that represent zero, *Glasgow Math. J.* **35** (1993), 13–23.

[74] B. Huppert – *Endliche Gruppen* I, Springer-Verlag, Berlin-Heidelberg, 1967.

[75] K. Iwasawa – On solvable extensions of algebraic number fields, *Ann. of Math.* **58** (1953), 548–572.

[76] " " – On Galois groups of local fields, *Trans. A.M.S.* **80** (1955), 448–469.

[77] K. Iwasawa – A note on the group of units of an algebraic number field, *J. Math. pures et appl.* **35** (1956), 189–192.

[78] B. Jacob and M. Rost – Degree four cohomological invariants for quadratic forms, *Invent. Math.* **96** (1989), 551–570.

[79] N. Jacobson – Composition algebras and their automorphisms, *Rend. Palermo* **7** (1958), 1–26.

[80] " " – *Structure and Representations of Jordan Algebras*, A.M.S. Colloquium Publ. 39, Providence, 1968.

[81] K. Kato – Galois cohomology of complete discrete valuation fields, *Lect. Notes in Math.* 967, 215–238, Springer-Verlag, 1982.

[82] Y. Kawada – Cohomology of group extensions, *J. Fac. Sci. Univ. Tokyo* **9** (1963), 417–431.
[83] " " – Class formations, *Proc. Symp. Pure Math.* 20, 96–114, A.M.S., Providence, 1969.
[84] M. Kneser – Schwache Approximation in algebraischen Gruppen, *Colloque de Bruxelles*, 1962, 41–52.
[85] " " – Einfach zusammenhängende Gruppen in der Arithmetik, *Proc. Int. Congress Math. Stockholm* (1962), 260–263.
[86] " " – Galoiskohomologie halbeinfacher algebraischer Gruppen über p-adischen Körpern, I, *Math. Zeit.* **88** (1965), 40–47; II, *ibid.* **89** (1965), 250–272.
[87] " " – *Lectures on Galois Cohomology of Classical Groups*, Tata Inst., Bombay, 1969.
[88] H. Koch – *Galoissche Theorie der p-Erweiterungen*, Math. Monogr. 10, VEB, Berlin, 1970.
[89] B. Kostant – The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group, *Amer. J. Math.* **81** (1959), 973–1032.
[90] R. Kottwitz – Tamagawa numbers, *Ann. of Math.* **127** (1988), 629–646.
[91] M. Krasner – Nombre des extensions d'un degré donné d'un corps p-adique, *Colloque C.N.R.S.* **143** (1966), 143–169.
[92] J.P. Labute – Classification of Demuškin groups, *Canad. J. Math.* **19** (1967), 106–132.
[93] " " – Algèbres de Lie et pro-p-groupes définis par une seule relation, *Invent. Math.* **4** (1967), 142–158.
[94] T.Y. Lam – *The Algebraic Theory of Quadratic Forms*, Benjamin, New York, 1973.
[95] S. Lang – On quasi-algebraic closure, *Ann. of Math.* **55** (1952), 373–390.
[96] " " – Algebraic groups over finite fields, *Amer. J. Math.* **78** (1956), 555–563.
[97] " " – Galois cohomology of abelian varieties over p-adic fields, *mimeographed notes*, May 1959.
[98] " " – *Topics in Cohomology of Groups*, Lect. Notes in Math. 1625, Springer-Verlag, 1996.
[99] " " – *Algebraic Number Theory*, Addison-Wesley, Reading, 1970.
[100] S. Lang and J. Tate – Principal homogeneous spaces over abelian varieties, *Amer. J. Math.* **80** (1958), 659–684.
[101] M. Lazard – Sur les groupes nilpotents et les anneaux de Lie, *Ann. Sci. E.N.S.* **71** (1954), 101–190.
[102] " " – Groupes analytiques p-adiques, *Publ. Math. I.H.E.S.* **26** (1965), 389–603.
[103] Y. Manin – Le groupe de Brauer-Grothendieck en géométrie diophantienne, *Actes Congrès Int. Nice* (1970), t. I, 401–411, Gauthier-Villars, Paris, 1971.
[104] " " – *Cubic Forms*: *Algebra, Geometry, Arithmetic*, North Holland, 1986.

[105] K. McCrimmon – The Freudenthal-Springer-Tits constructions of exceptional Jordan algebras, *Trans. A.M.S.* **139** (1969), 495–510.

[106] J. Mennicke – Einige endliche Gruppen mit drei Erzeugenden und drei Relationen, *Archiv der Math.* **10** (1959), 409–418.

[107] A.S. Merkurjev – On the norm residue symbol of degree 2 (in Russian), *Dokl. Akad. Nauk S.S.S.R.* **261** (1981), 542–547 (English translation: *Soviet Math. Dokl.* **24** (1981), 546–551).

[108] " " – Simple algebras and quadratic forms (in Russian), *Izv. Akad. Nauk S.S.S.R.* **55** (1991), 218–224 (English translation: *Math. U.S.S.R. Izv.* **38** (1992), 215–221).

[109] A.S. Merkurjev and A.A. Suslin – K-cohomology of Severi-Brauer varieties and the norm residue homomorphism (in Russian), *Izv. Akad. Nauk S.S.S.R.* **46** (1982), 1011–1046 (English translation: *Math. U.S.S.R. Izv.* **21** (1983), 307–340).

[110] " " – On the norm residue homomorphism of degree three, *LOMI preprint* E–9–86, Leningrad, 1986. (Norm residue homomorphism of degree three. (in Russian) *Izv. Akad. Nauk SSSR Ser. Mat.* **54** (1990), 339–356.)

[111] " " – The group K_3 for a field (in Russian), *Izv. Akad. Nauk S.S.S.R.* **54** (1990), 522–545 (English translation: *Math. U.S.S.R. Izv.* **36** (1991), 541–565).

[112] J-F. Mestre – Annulation, par changement de variable, d'éléments de $\mathrm{Br}_2(k(x))$ ayant quatre pôles, *C.R. Acad. Sci. Paris* **319** (1994), 529–532.

[113] " " – Construction d'extensions régulières de $\mathbf{Q}(T)$ à groupe de Galois $\mathbf{SL}_2(\mathbf{F}_7)$ et $\widetilde{M}_{12}$, *C.R. Acad. Sci. Paris* **319** (1994), 781–782.

[114] J. Milne – Duality in the flat cohomology of a surface, *Ann. Sci. E.N.S.* **9** (1976), 171–202.

[115] " " – *Etale Cohomology*, Princeton Univ. Press, Princeton, 1980.

[116] " " – *Arithmetic Duality Theorems*, Acad. Press, Boston, 1986.

[117] J. Milnor – Algebraic K-theory and quadratic forms, *Invent. Math.* **9** (1970), 318–344.

[118] M. Nagata – Note on a paper of Lang concerning quasi-algebraic closure, *Mem. Univ. Kyoto* **30** (1957), 237–241.

[119] J. Oesterlé – Nombres de Tamagawa et groupes unipotents en caractéristique p, *Invent. Math.* **78** (1984), 13–88.

[120] T. Ono – Arithmetic of algebraic tori, *Ann. of Math.* **74** (1961), 101–139.

[121] " " – On the Tamagawa number of algebraic tori, *Ann. of Math.* **78** (1963), 47–73.

[122] H.P. Petersson – Exceptional Jordan division algebras over a field with a discrete valuation, *J. Crelle* **274/275** (1975), 1–20.

[123] H.P. Petersson and M.L. Racine – On the invariants mod 2 of Albert algebras, *J. of Algebra* **174** (1995), 1049–1072.

[124] A. Pfister – Quadratische Formen in beliebigen Körpern, *Invent. Math.* **1** (1966), 116–132.

[125] V.P. Platonov and A.S. Rapinchuk – Алгебраические группы и теория чисел *Algebraic groups and number theory* (in Russian with an English summary) Izdat "Nauka", Moscow, 1991. (English translation: *Algebraic Groups and Number Fields*, Acad. Press, Boston, 1993).

[126] G. Poitou – *Cohomologie Galoisienne des Modules Finis*, Dunod, Paris, 1967.

[127] D. Quillen – The spectrum of an equivariant cohomology ring I, *Ann. of Math.* **94** (1971), 549–572; II, *ibid.*, 573–602.

[128] L. Ribes – *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure Math. 24, Kingston, Ontario, 1970.

[129] M. Rosenlicht – Some basic theorems on algebraic groups, *Amer. J. Math.* **78** (1956), 401–443.

[130] " " – Some rationality questions on algebraic groups, *Ann. Mat. Pura Appl.* **43** (1957), 25–50.

[131] M. Rost – A (mod 3) invariant for exceptional Jordan algebras, *C.R. Acad. Sci. Paris* **315** (1991), 823–827.

[132] " " – Cohomological invariants, in preparation.

[133] I.R. Šafarevič [Shafarevich]– On p-extensions (in Russian), Math. Sb. **20** (1947), 351–363 (English translation: *C.P.* 3–19).

[134] " " – Birational equivalence of elliptic curves (in Russian), *Dokl. Akad. Nauk S.S.S.R.* **114** (1957), 267–270. (English translation: *C.P.* 192–196).

[135] " " – Algebraic number fields (in Russian), *Proc. Int. Congress Math. Stockholm* (1962), 163–176 (English translation: *C.P.* 283–294).

[136] " " – Extensions with prescribed ramification points (in Russian, with a French summary), *Publ. Math. I.H.E.S.* **18** (1963), 295–319 (English translation: *C.P.* 295–316).

[137] J-J. Sansuc – Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, *J. Crelle* **327** (1981), 12–80.

[138] W. Scharlau – Über die Brauer-Gruppe eines algebraischen Funktionenkörpers in einer Variablen, *J. Crelle* **239–240** (1969), 1–6.

[139] " " – *Quadratic and Hermitian Forms*, Springer-Verlag, 1985.

[140] C. Scheiderer – *Real and Etale Cohomology*, Lect. Notes in Math. 1588, Springer-Verlag, 1994.

[141] A. Schinzel and W. Sierpinski – Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208; Errata, *ibid.* **5** (1959), 259.

[142] R. Schoof – Algebraic curves over $\mathbf{F}_2$ with many rational points, *J. Number Theory* **41** (1992), 6–14.

[143] J-P. Serre – Classes des corps cyclotomiques (d'après K. Iwasawa), *Sém. Bourbaki* 1958–1959, exposé 174 (= *Oe.* 41).

[144] " " – *Groupes Algébriques et Corps de Classes*, Hermann, Paris, 1959.

[145] " " – *Corps Locaux*, Hermann, Paris, 1962.

[146] " " – Cohomologie galoisienne des groupes algébriques linéaires, *Colloque de Bruxelles*, 1962, 53–67 (= *Oe.* 53).
[147] " " – Structure de certains pro-p-groupes (d'après Demuškin), *Sém. Bourbaki* 1962–1963, exposé 252 (= *Oe.* 58).
[148] " " – Sur les groupes de congruence des variétés abéliennes, *Izv. Akad. Nauk S.S.S.R.* **28** (1964), 1–20 (= *Oe.* 62); II, *ibid.* **35** (1971), 731–737 (= *Oe.* 89).
[149] " " – Sur la dimension cohomologique des groupes profinis, *Topology* **3** (1965), 413–420 (= *Oe.* 66).
[150] " " – *Représentations Linéaires des Groupes Finis*, Hermann, Paris, 1967.
[151] " " – Cohomologie des groupes discrets, *Ann. Math. Studies* 70, 77–169, Princeton Univ. Press, Princeton, 1971 (= *Oe.* 88).
[152] " " – Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local, *C.R. Acad. Sci. Paris* **287** (1978), 183–188 (= *Oe.* 115).
[153] " " – Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C.R. Acad. Sci. Paris* **296** (1983), 397–402 (= *Oe.* 128).
[154] " " – L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comm. Math. Helv.* **59** (1984), 651–676 (= *Oe.* 131).
[155] " " – Spécialisation des éléments de $\mathrm{Br}_2(\mathbf{Q}(T_1,\ldots,T_n))$, *C.R. Acad. Sci. Paris* **311** (1990), 397–402 (= *Oe.* 150).
[156] " " – Cohomologie galoisienne: progrès et problèmes, *Sém. Bourbaki* 1993–1994, exposé 783 (= *Oe.* 166).
[157] S.S. Shatz – *Profinite Groups, Arithmetic, and Geometry*, Ann. Math. Studies 67, Princeton Univ. Press, Princeton, 1972.
[158] C. Soulé – K_2 et le groupe de Brauer (d'après A.S. Merkurjev et A.A. Suslin), *Sém. Bourbaki* 1982–1983, exposé 601 (*Astérisque* **105–106**, S.M.F., 1983, 79–93).
[159] T.A. Springer – Sur les formes quadratiques d'indice zéro, *C.R. Acad. Sci. Paris* **234** (1952), 1517–1519.
[160] " " – On the equivalence of quadratic forms, *Proc. Acad. Amsterdam* **62** (1959), 241–253.
[161] " " – The classification of reduced exceptional simple Jordan algebras, *Proc. Acad. Amsterdam* **63** (1960), 414–422.
[162] " " – Quelques résultats sur la cohomologie galoisienne, *Colloque de Bruxelles*, 1962, 129–135.
[163] T.A. Springer and F.D. Veldkamp – *Octonions, Jordan Algebras and Exceptional Groups*, Springer-Verlag, 2000.
[164] R. Steinberg – Variations on a theme of Chevalley, *Pacific J. Math.* **9** (1959), 875–891 (= *C.P.* 8).
[165] " " – Regular elements of semisimple algebraic groups, *Publ. Math. I.H.E.S.* **25** (1965), 281–312 (= *C.P.* 20).
[166] " " – *Lectures on Chevalley Groups*, mimeographed notes, Yale, 1967.

[167] A.A. Suslin – Algebraic K-theory and the norm-residue homomorphism, *J. Soviet. Math.* **30** (1985), 2556–2611.
[168] R. Swan – Induced representations and projective modules, *Ann. of Math.* **71** (1960), 552–578.
[169] " " – The Grothendieck ring of a finite group, *Topology* **2** (1963), 85–110.
[170] J. Tate – WC-groups over p-adic fields, *Sém. Bourbaki* 1957–1958, exposé 156.
[171] " " – Duality theorems in Galois cohomology over number fields, *Proc. Int. Congress Math. Stockholm* (1962), 288–295.
[172] " " – The cohomology groups of tori in finite Galois extensions of number fields, *Nagoya Math. J.* **27** (1966), 709–719.
[173] " " – Relations between K_2 and Galois cohomology, *Invent. Math.* **36** (1976), 257–274.
[174] G. Terjanian – Un contre-exemple à une conjecture d'Artin, *C.R. Acad. Sci. Paris* **262** (1966), 612.
[175] J. Tits – Groupes semi-simples isotropes, *Colloque de Bruxelles*, 1962, 137–147.
[176] " " – Groupes simples et géométries associées, *Proc. Int. Congress Math. Stockholm* (1962), 197–221.
[177] " " – Classification of algebraic semisimple groups, *Proc. Symp. Pure Math.* 9, vol. I, 33–62, A.M.S., Providence, 1966.
[178] " " – Formes quadratiques, groupes orthogonaux et algèbres de Clifford, *Invent. Math.* **5** (1968), 19–41.
[179] " " – Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque, *J. Crelle* **247** (1971), 196–220.
[180] " " – Sur les degrés des extensions de corps déployant les groupes algébriques simples, *C.R. Acad. Sci. Paris* **315** (1992), 1131–1138.
[181] V.E. Voskresenskiĭ – *Algebraic Tori* (in Russian), Izdat "Nauka", Moscow, 1977.
[182] A. Weil – On algebraic groups and homogeneous spaces, *Amer. J. Math.* **77** (1955), 493–512 (= *Oe.* [1955b]).
[183] " " – The field of definition of a variety, *Amer. J. Math.* **78** (1956), 509–524 (= *Oe.* [1956]).
[184] " " – Algebras with involutions and the classical groups, *J. Indian Math. Soc.* **24** (1960), 589–623 (= *Oe.* [1960b]).
[185] " " – *Adeles and Algebraic Groups* (notes by M. Demazure and T. Ono), Inst. for Adv. Study, Princeton, 1961; Birkhäuser, Boston, 1982.
[186] " " – *Basic Number Theory*, Springer-Verlag, 1967.
[187] E. Witt – Theorie der quadratischen Formen in beliebigen Körpern, *J. Crelle* **176** (1937), 31–44.
[188] V.I. Yanchevskiĭ – K-unirationality of conic bundles and splitting fields of simple central algebras (in Russian), *Dokl. Akad. Nauk S.S.S.R.* **29** (1985), 1061–1064.
[189] H. Zassenhaus – *The Theory of Groups*, 2nd. ed., Chelsea, New York, 1949.

Index