Lower bounds for essential dimensions via orthogonal representations

Vladimir Chernousov *
Department of Mathematics
University of Alberta
Edmonton, Alberta T6G 2G1

Jean–Pierre Serre
Collège de France
3, rue d'Ulm
75231 Paris, Cedex 05

§ 1 Introduction

Let us first recall what is the *essential dimension* of a functor, cf. [?] and [?]. Let k be a field, and let $\mathcal{F}$ be a functor from the category of field extensions of k into the category of sets. Let F/k be an extension and let ξ be an element of $\mathcal{F}(F)$. If E is a field with $k \subset E \subset F$ we say that ξ *comes from* E if it belongs to the image of $\mathcal{F}(E) \to \mathcal{F}(F)$. The *essential dimension* $\mathrm{ed}\,(\xi)$ of ξ is the minimum of the transcendence degrees E/k, for all E with $k \subset E \subset F$ such that ξ comes from E. One has $\mathrm{ed}(\xi) \leq \mathrm{tr.\,deg.}\, F$. If there is equality, we say that ξ is *incompressible*. The *essential dimension* $\mathrm{ed}\,(\mathcal{F})$ *of* $\mathcal{F}$ is

$$\mathrm{ed}\,(\mathcal{F}) = \max\,\{\mathrm{ed}\,(\xi)\},$$

the maximum being taken over all pairs (F, ξ) with $k \subset F$ and $\xi \in \mathcal{F}(F)$.

*Supported by the Canada Research Chairs Program, and by NSERC's Grant G121210944

Along similar lines, the *essential dimension* $\mathrm{ed}(\xi;p)$ *of* $\xi \in \mathcal{F}(F)$ *at a prime number* p is

$$\mathrm{ed}(\xi;p) = \min\{\mathrm{ed}(\xi_K)\},$$

where ξ_K is the image of ξ in $\mathcal{F}(K)$, and the minimum is taken over all extensions K/F with $[K:F]$ finite and prime to p. The *essential dimension of* $\mathcal{F}$ *at* p is

$$\mathrm{ed}(\mathcal{F};p) = \max\{\mathrm{ed}(\xi;p)\}$$

the maximum being taken over all pairs (F,ξ) with $\xi \in \mathcal{F}(F)$. It is clear that $\mathrm{ed}(\mathcal{F}) \geq \mathrm{ed}(\mathcal{F};p)$.

We will apply this to the functor $\mathcal{F}$ defined by:

$$\mathcal{F}(F) = H^1(F,G) = \{\text{ isomorphism classes of } G\text{-torsors over } \ F\},$$

where G is a smooth linear algebraic group over k. The *essential dimension* $\mathrm{ed}(G)$ of G (resp. the *essential dimension* $\mathrm{ed}(G;p)$ *at* p) is $\mathrm{ed}(\mathcal{F})$ (resp. $\mathrm{ed}(\mathcal{F};p)$). If ξ is a versal G-torsor, in the sense of [**?**], p.13, one has

$$\mathrm{ed}(G) = \mathrm{ed}(\xi) \text{ and } \mathrm{ed}(G;p) = \mathrm{ed}(\xi;p).$$

In case we feel the need to be precise about F, we write ed_F instead of just ed.

If $\mathrm{char}(k) = 0$, Reichstein and Youssin have given a very efficient lower bound for $\mathrm{ed}(G;p)$, namely:

If G is connected and contains a finite abelian p-group A whose centralizer is finite, then one has $\mathrm{ed}(G;p) \geq \mathrm{rk}(A)$*, where* $\mathrm{rk}(A)$ *denotes the minimum number of generators of A* ([**?**], th. 7.8).

The proof of Reichstein-Youssin uses resolution of singularities, hence does not apply (for the time being) when $\mathrm{char}(k) > 0$. What we do in the present paper is to prove most of their results relative to $p = 2$ in arbitrary characteristic (except[1] characteristic 2) by using orthogonal groups and quadratic forms (especially "monomial" quadratic forms, cf. **??**). For instance :

(1.1) *If G is semisimple of adjoint type, and -1 belongs to the Weyl group, then*

$$\mathrm{ed}(G;2) \geq \mathrm{rank}(G) + 1.$$

[1]It seems likely that a similar method can also be applied in characteristic 2, but we have not checked all the necessary steps.

This is the case $G = G^\circ$ of th. **??** of **??**. Note that it implies

$$\mathrm{ed}(E_8; 2) \geq 9 \quad \text{and} \quad \mathrm{ed}(E_7; 2) \geq 8.$$

(1.2) $\mathrm{ed}\,(\mathbf{Spin}_n; 2) \geq [n/2]$ *for* $n > 6,\ n \neq 10$, *the inequality being strict if* $n \equiv -1, 0$ *or* $1 \pmod 8$, cf. th. **??** and th. **??**.

(1.3) $\mathrm{ed}\,(\mathbf{HSpin}_n; 2) > n/2$ *if* $n \geq 8$, $n \equiv 0 \pmod 8$, cf. th. 13.

Of course, these results give lower bounds for $\mathrm{ed}(G)$ itself, for instance $\mathrm{ed}(E_8) \geq 9$.

§ 2 The Main Theorem

In what follows, we assume $\mathrm{char}(k) \neq 2$ and k algebraically closed.

Let G° be a simple algebraic group over k of adjoint type, and let T be a maximal torus of G°. Let $c \in \mathrm{Aut}(G^\circ)$ be such that $c^2 = 1$ and $c(t) = t^{-1}$ for every $t \in T$ (it is known that such an automorphism exists, see e.g. [**?**], Exp. XXIV, Prop. 3.16.2, p. 355). This automorphism is inner (i.e. belongs to G°) if and only if -1 belongs to the Weyl group of (G, T). When this is the case, we put $G = G^\circ$. If not, we define G to be the subgroup of $\mathrm{Aut}(G^\circ)$ generated by G° and c. We have

- $G = G^\circ$ for types A_1, B_r, C_r, D_r (r even), G_2, F_4, E_7, E_8 ;
- $(G : G^\circ) = 2$ and $G = \mathrm{Aut}(G^\circ)$ for types A_r ($r \geq 2$), D_r (r odd), E_6.

Let $r = \dim\,(T)$ be the rank of G.

Theorem 1 *If G is as above, we have* $\mathrm{ed}\,(G; 2) \geq r + 1$.

The proof of Theorem **??** consists in:

a) construction of a G-torsor θ_G over a suitable extension K/k with $\mathrm{tr.deg}_k(K) = r + 1$, see below;

b) proof that the image of θ_G in a suitable $H^1(K, \mathbf{O}_N)$ (cf. **??**) is incompressible (§**??**–6); this implies that θ_G itself is incompressible, and th. **??** follows.

Let us start with part a). Let R be the root system of G with respect to T, and let R_{sh} be the (sub) root system formed by the short roots of R.

Let $\Delta = \{\alpha_1, \dots, \alpha_r\}$ be a basis of R_{sh}. The root lattices of R and R_{sh} are the same; hence Δ is a basis of the character group $X(T)$. This allows us to identify T with $\mathbf{G}_m \times \cdots \times \mathbf{G}_m$ using the basis Δ.

Call A_0 the kernel of "multiplication by 2" on T. Let $A = A_0 \times \{1, c\}$ be the subgroup of G generated by A_0 and by the element c defined above. The group A is isomorphic to $(\pm 1)^{r+1}$.

Take $K = k(t_1, \dots, t_r, u)$ where $t_1, \dots, t_r$ and u are independent indeterminates. We have $H^1(K, A) = H^1(K, \mathbf{Z}/2\mathbf{Z}) \times \ldots \times H^1(K, \mathbf{Z}/2\mathbf{Z})$. Identify $H^1(K, \mathbf{Z}/2\mathbf{Z})$ with $K^\times/(K^\times)^2$ as usual. Then u and the t_i's define elements (u) and (t_i) of $H^1(K, \mathbf{Z}/2\mathbf{Z})$. Let θ_A be the element of $H^1(K, A)$ with components $((t_1), \dots, (t_r), (u))$. Let θ_G be the image of θ_A in $H^1(K, G)$. We will prove in **??** :

Theorem 2 *(K, θ_G) is incompressible, and remains so after any field extension of K of odd degree.*

Note that Theorem **??** implies Theorem **??** since $\mathrm{tr.deg.}\, K = r + 1$.

Remarks. (i) It would not be useful to take A_0 instead of A. Indeed, A_0 is a subgroup of T and $H^1(K, T) = 1$ by Hilbert Theorem 90. Hence the image in $H^1(K, G)$ of any element of $H^1(K, A_0)$ is trivial. In particular, the class θ_G defined above is killed by the quadratic extension $K(\sqrt{u})/K$.
(ii) Suppose that $G = G^\circ$, i.e. that c belongs to G°. The subgroup A constructed above is the same as the one described in [**?**], p.139, for compact Lie groups. It is also the same one (with the same θ_G) as in Reichstein-Youssin theory [**?**].

§ 3 An orthogonal representation

Proposition 3 *There exists a quadratic space (V, q) over K, and an orthogonal irreducible linear representation*

$$\rho : G \longrightarrow \mathbf{O}\,(V, q)$$

with the following property:

$(*)$ *the nonzero weights of T on V are the short roots and they have multiplicity* 1.

Proof. Let B be a Borel subgroup containing T. This defines an order on the root system R. Let β be the highest root of R_{sh} with respect to that order. It is a dominant weight. We choose for V an irreducible representation $L(\beta)$ of G° with highest weight β. By a well-known criterion ([**?**], Lemmas 78, 79, p. 226), $L(\beta)$ is an orthogonal representation of G°. Since $R_{sh} \cup \{0\}$ is R-saturated in the sense of [**?**], VIII. § 7.2, the nonzero weights of $L(\beta)$ belong to R_{sh}, hence are conjugate to β by the Weyl group. This implies that they have multiplicity 1, so that $(*)$ is fulfilled.

It remains to show that this orthogonal representation of G° extends to an orthogonal representation of $\mathrm{Aut}\,(G^\circ)$, and hence of G. This can be done in the following way:

If $\mathrm{Aut}\,(G^\circ) = G^\circ$, there is nothing to prove.

If $\mathrm{Aut}\,(G^\circ) \neq G^\circ$, the roots have the same length, so that β is the highest root of R, and $V = L(\beta)$ is essentially the adjoint representation of G°. More precisely, if $\widetilde{G^\circ}$ denotes the universal covering of G°, one can take for V the image of $\mathrm{Lie}\,(\widetilde{G^\circ})$ in $\mathrm{Lie}\,(G^\circ)$, with the obvious action of $\mathrm{Aut}(G^\circ)$. One puts on V the "normalized Killing form" $q(x, y)$. That form is defined first over $\mathbf{Z}$, in which case it is equal to $\mathrm{Tr}\,(\mathrm{ad}(x) \cdot \mathrm{ad}(y))/2h$ where h is the Coxeter number (see [**?**], [**?**], [**?**]); it is then defined by base change for every simple group scheme, and the computation of its discriminant done in the references above shows that it is nondegenerate. □

Examples. a) When the roots of R have the same length, we have $V = \mathrm{Lie}\,(G^\circ)$, except for :

- type A_n when p divides $n+1$;
- type E_6 when $p = 3$.

In both cases, V has codimension 1 in $\mathrm{Lie}\, G^\circ$.

b) When the roots have different length, then:

- If G is of type G_2, then $V = L(\omega_1)$, where ω_1 is the first fundamental weight (in Bourbaki's notation); its dimension is 7.
- If G is of type F_4, then $V = L(\omega_4)$; its dimension is 26 if $p \neq 3$ and 25 if $p = 3$.
- If G is of type B_r, $r > 1$, then $V = L(\omega_1)$ is the standard representation of $G = \mathbf{SO}_{2r+1}$ of dimension $2r + 1$.

- If G is of type C_r, $r > 1$, then $V = L(\omega_2)$. When $p \nmid r$, one has $V \oplus 1 = \bigwedge^2(V_1)$ where $V_1 = L(\omega_1)$ is the standard representation of $\widetilde{G} = \mathbf{Sp}_{2r}$; one has $\dim V = 2r^2 - r - 1$. When $p \mid r$, V is a subquotient of $\bigwedge^2(V_1)$ of dimension $2r^2 - r - 2$.

§ 4 Monomial quadratic forms

Consider the following general situation. Let A be an abelian group of type $(2, \ldots, 2)$ and rank s and let $\lambda : A \to \mathbf{O}(V, q)$ be an orthogonal representation of A. As above, take $K = k(t_1, ..., t_s)$, where $t_1, \ldots, t_s$ are independent indeterminates, and define $\theta_A \in H^1(K, A)$ as in **??**. Let $\theta_O = \lambda(\theta_A)$ be the image of θ_A in $H^1(K, \mathbf{O}\,(V, q))$. Let $X(A) = \mathrm{Hom}\,(A, \mathbf{Z}/2\mathbf{Z})$ be the character group of A. Let X_λ be the subset of $X(A)$ made up of the characters whose multiplicity in λ is odd.

Theorem 4 *The integers* $\mathrm{ed}(\theta_O)$ *and* $\mathrm{ed}(\theta_O; 2)$ *are both equal to the rank* r_λ *of the subgroup of* $X(A)$ *generated by* X_λ*.*

Note that $\theta_O \in H^1(K, \mathbf{O}\,(V, q))$ may be interpreted as a quadratic form (namely, the twist of q by θ_O); we will denote this form by q_O; it is well defined up to K-isomorphism. To prove Theorem **??**, we first need to compute explicitly q_O.

Computation of q_O

If $\alpha \in X(A)$, let V_α be the corresponding weight subspace of V. We have an orthogonal decomposition $V = \bigoplus_\alpha V_\alpha$; put $m_\alpha = \dim V_\alpha$.

Let $\alpha_1, \ldots, \alpha_s$ be the canonical basis of $X(A)$ corresponding to the projections $A = \mathbf{Z}/2\mathbf{Z} \times \cdots \times \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$. Any element $a \in A$ acts by multiplication by $\alpha(a)$ on V_α. Hence twisting $q|_{V_\alpha}$ by θ_O we obtain a quadratic form $\langle t^\alpha, \ldots, t^\alpha \rangle$ of dimension m_α, where $t^\alpha = \alpha(t) = t_1^{n_1} \cdots t_s^{n_s} \in K^\times$ for $\alpha = n_1\alpha_1 + \cdots + n_s\alpha_s$. Hence q_O can be written as

$$q_O = \oplus\; m_\alpha \,\langle t^\alpha \rangle,$$

where $m_\alpha \langle t^\alpha \rangle$ means the direct sum of m_α copies of the 1-dimension form $\langle t^\alpha \rangle$. Note that, because -1 is a square, we have $\langle t^\alpha, t^\alpha \rangle = 0$ in the Witt group $W(K)$, so that the formula can also be written as

$$q_O = \bigoplus_{\alpha \in X_\lambda} \langle t^\alpha \rangle \quad \text{in} \;\; W(K),$$

where the sum is over the set X_λ defined above.

Examples. Let $\rho : G \to \mathbf{O}\,(V, q)$ be as in Proposition **??** and let λ denote the composition $A \to G \xrightarrow{\rho} \mathbf{O}\,(V, q)$.
a) If $G = G_2$ and V is as defined in **??**, then

$$q_O = \langle\, u, t_1, ut_1, t_2, ut_2, t_1t_2, ut_1t_2\,\rangle = \langle\langle\, u, t_1, t_2\,\rangle\rangle - \langle 1\rangle,$$

where $\langle\langle\, u, t_1, t_2\,\rangle\rangle$ is the generic 3-Pfister form.

b) Similarly, in the case of $G = F_4$ (and $p \neq 3$), q_O is

$$q_O = q_3 \otimes (q_2 - \langle 1\rangle) \oplus \langle 1, 1\rangle,$$

where q_2 (resp. q_3) is a generic 2-Pfister form (resp. 3-Pfister form). When $p = 3$, the term $\langle 1, 1\rangle$ is replaced by $\langle 1\rangle$.

c) In case $G = E_8$, q_0 can also be computed. One finds:

$$q_O = 8\,\langle 1\rangle \oplus \langle 1, u\rangle \otimes (\bigoplus_{(m)} \langle t_1^{m_1} \cdots t_8^{m_8}\rangle\,)$$

where $m = (m_1, \ldots, m_8)$ runs through the 120 octuples of $0, 1$'s such that

$$m_1m_2 + m_3m_4 + m_5m_6 + m_7m_8 \equiv 1 \pmod 2.$$

Monomial quadratic forms

A rank n quadratic form $f(X_1, \ldots, X_n)$ over $K = k(t_1, \ldots, t_s)$ is called *monomial* if it is a diagonal form

$$f(X) = \sum a_i X_i^2,$$

with $a_i \in K$ and if each coefficient a_i is a monomial in $t_1, \ldots, t_s$ with exponents in $\mathbf{Z}$ ("Laurent monomial"). As usual, we write such a form as $f = \langle a_1, \ldots, a_n\rangle$.

Examples. a) The generic 2-Pfister form $\langle 1, t_1, t_2, t_1t_2\rangle$ is monomial over $k(t_1, t_2)$.
b) The form $q_O = \bigoplus_{\alpha} \langle\, t^\alpha\rangle$ defined above is monomial.

Let $f = \langle a_1, \ldots, a_n \rangle$ be monomial. After dividing the a_i's by squares, we may assume that they are "square-free", i.e. for every i and j, the exponent of t_j in the monomial a_i is 0 or 1. We can then write f as:

$$f = \oplus\, m_f(\mu)\, \langle t^\mu \rangle,$$

where the exponent $\mu = (\mu_1, \ldots, \mu_s)$ belongs to $\{0,1\}^s = (\mathbf{F}_2)^s$, t^μ means $t_1^{\mu_1} \cdots t_s^{\mu_s}$, and $m_f(\mu)$ is ≥ 0. We say that f is *multiplicity free* if it is square-free and $m_f(\mu) = 0$ or 1 for every μ.

Proposition 5 *A multiplicity free monomial quadratic form f over $K = k(t_1, \ldots, t_s)$ is anisotropic.*

Proof. Let v be the valuation of K with value group $\mathbf{Z}^s$ (with lexicographic order) which is trivial on k and such that

$$v(t_1) = (1, 0, \ldots, 0), \ldots, v(t_s) = (0, \ldots, 0, 1)$$

(see [**?**], Chap. 6, § 10). If f represents 0 we get an equation

$$\sum t^\mu \phi_\mu(t)^2 = 0,$$

where the non-zero terms have different v-valuations (and even different valuations in $\Gamma/2\Gamma$). This is only possible if all the terms are 0.
Alternate proof: use the fact that f is a subform of a generic s-Pfister form, and that such a form is anisotropic, cf. [**?**], p. 111. □

Let f be a monomial square-free quadratic form over K, and let X_f be the subset of $(\mathbf{F}_2)^s$ made up of the μ's such that $m_f(\mu)$ is odd. Let $e = e_f$ be the rank of X_f, i.e. the dimension of the $\mathbf{F}_2$-subspace of $(\mathbf{F}_2)^s$ generated by X_f.

Proposition 6 *The integers* $\mathrm{ed}(f)$ *and* $\mathrm{ed}(f; 2)$ *are both equal to e.*

Note that for $f = q_O$ the rank of X_{q_O} is obviously equal to that of X_λ, hence Theorem **??** follows from Proposition **??**.

Remark. One may wonder whether the equality $\mathrm{ed}(f) = \mathrm{ed}(f; 2)$ remains true for an arbitrary quadratic form f. It is not hard to see that it does if $\mathrm{ed}(f; 2) \leq 2$, but we do not know what happens for larger values of $\mathrm{ed}(f; 2)$.

§ 5 Proof of Proposition ??

We use induction on the number s of the indeterminates $t_1, \ldots, t_s$, the case $s = 0$ being obvious. Since -1 is a square in k, each pair $\langle t^\mu, t^\mu \rangle$ is hyperbolic, and can be replaced by $\langle 1, -1 \rangle = \langle 1, 1 \rangle$. Hence every monomial quadratic form f can be written as $f = \langle 1, \ldots, 1 \rangle \oplus q$, with q multiplicity free. Since $X_f = X_q$ or $X_q \cup \{0\}$, we have $e = \mathrm{rank}(X_f) = \mathrm{rank}(X_q)$.

We now make a further reduction on f. In order to state it, let us say that q is *e-reduced* if the set X_q contains the first e basic vectors

$$x_1 = (1, 0, \ldots, 0);\ x_2 = (0, 1, \ldots, 0);\ \ldots\ ;\ x_e = (0, \ldots, 1, \ldots, 0).$$

This amounts to saying that

$$q = \langle t_1, \ldots, t_e, a_{e+1}, \ldots, a_n \rangle,$$

where the a_i, for $i > e$, are pairwise distinct square-free monomials in $t_1, \ldots, t_e$ of total degree $\neq 1$.

Lemma 7 *There is an automorphism of the extension K/k which transforms q into an e-reduced form.*

Proof. Note that $\mathbf{GL}_s(\mathbf{Z})$ acts in a natural way on the set of monomials with exponents in $\mathbf{Z}$. This gives a natural embedding of $\mathbf{GL}_s(\mathbf{Z})$ into $\mathrm{Aut}(K/k)$. Moreover, the natural map

$$\mathbf{GL}_s(\mathbf{Z}) \longrightarrow \mathbf{GL}_s(\mathbf{F}_2)$$

is surjective, since $\mathbf{GL}_s(\mathbf{F}_2) = \mathbf{SL}_s(\mathbf{F}_2)$ and

$$\mathbf{SL}_s(\mathbf{Z}) \to \mathbf{SL}_s(\mathbf{Z}/m\mathbf{Z})$$

is well known to be surjective for any m. By the very definition of e, the set X_q contains e elements $z_1, \ldots, z_e$ which are linearly independent over $\mathbf{F}_2$. Hence there exists $\phi \in \mathbf{GL}_s(\mathbf{Z}) \subset \mathrm{Aut}(K/k)$ whose reduction mod 2 transforms the z_i into the first e basic vectors $x_1, \ldots, x_e$. It is clear that $\phi(q)$ is e-reduced. □

We now use the "residue operators" of the local theory of quadratic forms (see e.g. [**?**], Chap. VI, § 1.5). Recall that, if v is a discrete valuation of a field K, with residue field $\widetilde{K}$, one may write any quadratic form q over K in the form

$$q = \langle\, u_1, \ldots, u_m, \pi u_{m+1}, \ldots, \pi u_n \,\rangle,$$

where the u's are units, π is a uniformizing element and m is an integer with $0 \leq m \leq n$. One defines the first residue $\partial_1(q)$ of q as the class in the Witt group $W(\widetilde{K})$ of the quadratic form $\langle \tilde{u}_1, \ldots, \tilde{u}_m \,\rangle$, where $\tilde{u}_i$ denotes the image of u_i in $\widetilde{K}$; similarly, the second residue $\partial_2(q)$ of q is the class in $W(\widetilde{K})$ of $\langle\, \tilde{u}_{m+1}, \ldots, \tilde{u}_n \,\rangle$. It is known (*loc. cit.*) that the class of $\partial_1(q)$ does not depend on the choice of π, nor on the choice of the diagonalization of q; as for the class of $\partial_2(q)$, it is only defined up to similarity (i.e. up to multiplication by a 1-dimensional quadratic form).

Proposition 8 *Let v be a discrete valuation on an extension L of k trivial on k, let $\widetilde{L}$ be its residue field, and let ϕ be a quadratic form over L. Let e be a positive integer. Assume*:

a) $\partial_2(\phi) \neq 0$ *in* $W(\widetilde{L})$.

b) $\mathrm{ed}_{\widetilde{L}}(\psi; 2) \geq e - 1$ *for every quadratic form* ψ *over* $\widetilde{L}$ *belonging to the Witt class of* $\partial_1(\phi)$.

Then $\mathrm{ed}_L(\phi; 2) \geq e$.

(Both ed's are relative to k, viewed as a subfield of L and of $\widetilde{L}$.)

Proposition **??** *implies Proposition* **??**

We apply induction on e. The case $e = 0$ or 1 is trivial. Let us assume $e > 1$. We may suppose that f is of the form $f = \langle 1, \ldots, 1 \rangle \oplus q$, where q is e-reduced and multiplicity free. Since the exponents μ appearing in X_f are sums of the x_i $(1 \leq i \leq e)$, the t^μ appearing in q belong to the subfield $k(t_1, ..., t_e)$ of K. This shows that $\mathrm{ed}(f) \leq e$.

It remains to show that $\mathrm{ed}(f; 2) \geq e$. To do so, consider the valuation v on K associated to the indeterminate t_1. Such a valuation is characterized by the properties:

$$v(t_1) = 1;$$
$$v(x) = 0 \;\text{ if } x \in k(t_2, ..., t_s)^\times.$$

Moreover, we have $\widetilde{K} = k(t_2, ..., t_s)$.

Let us write f as $f = \phi \oplus \langle t_1 \rangle \otimes \phi'$, where ϕ, ϕ' are monomial quadratic forms over $k(t_2, \ldots, t_s)$. The second residue of f with respect to v is given by $\partial_2(f) = \partial_2(q) = \phi'$. Since q is multiplicity free, so is ϕ'. It is clear that $\phi' \neq 0$, and hence ϕ' is anisotropic, by Proposition **??**. Since the Witt class of ϕ' is $\partial_2(f)$, we have checked condition a) of Proposition **??**.

Let us look at condition b). Of course ϕ is a representative of $\partial_1(f)$. Moreover, it is clear that ϕ can be written as $\phi = m\langle 1, 1 \rangle \oplus \psi$, where m is an integer ≥ 0 and ψ is a multiplicity free $(e-1)$-reduced monomial quadratic form over $\widetilde{K}$, hence is anisotropic, by Proposition **??**. Since $\langle 1, 1 \rangle = \langle 1, -1 \rangle$, this shows that any quadratic form ψ' over $\widetilde{K}$ which belongs to the Witt class $\partial_1(f)$ is isomorphic to $m'\langle 1, 1 \rangle \oplus \psi$, hence is $(e-1)$-reduced. We may thus apply the induction assumption to ψ', and deduce that $\mathrm{ed}_{\widetilde{K}}(\psi'; 2) \geq e - 1$. By Proposition **??**, we get $\mathrm{ed}_K(f; 2) \geq e$, as required.

Proof of Proposition **??**

Let L' be an odd-degree extension of L, and let F be a subfield of L', containing k, and such that ϕ is L'-isomorphic to a quadratic form ϕ_F over F. We have to show that $\mathrm{tr.deg}_k(F) \geq e$. We distinguish two cases:

i) *The case* $L' = L$. Let w be the restriction of v to the subfield F. There are three possibilities:

i_1) w is trivial on F (i.e. $v(x) = 0$ for every $x \in F^\times$). In that case, the coefficients of ϕ_F are v-units, and this implies that $\partial_2(\phi) = 0$, which we assumed is not true.

i_2) The value group $v(F^\times)$ is a subgroup of even index of $v(L^\times) = \mathbf{Z}$. The same argument as for i_1) shows that $\partial_2(\phi) = 0$.

i_3) The index of $v(F^\times)$ in $v(L^\times)$ is odd. In that case, $\partial_1(\phi) \in W(\widetilde{L})$ is the image of $\partial_1(\phi_F) \in W(\widetilde{F})$ under the natural map $W(\widetilde{F}) \to W(\widetilde{L})$. Here $\widetilde{F}$ is the residue field of F with respect to w. Choose any representative $\psi_{\widetilde{F}}$ of $\partial_1(\phi_F)$; it gives a representative $\psi_{\widetilde{L}}$ of $\partial_1(\phi)$, hence we have

$$\mathrm{ed}_{\widetilde{F}}(\psi_{\widetilde{F}}; 2) \geq \mathrm{ed}_{\widetilde{L}}(\psi_{\widetilde{L}}; 2) \geq e - 1$$

by hypothesis b). This implies that $\mathrm{tr.deg}_k(\widetilde{F}) \geq e - 1$, hence $\mathrm{tr.deg}_k(F) \geq e$ by a standard result of valuation theory, cf. [**?**], Chap. 6, § 10, no. 3.

ii) *The general case.* Let S be the set of extensions w of v to L'. For each $w \in S$, let $e(w/v)$ and $f(w/v)$ be the ramification index and the residue degree of w with respect to v.

Lemma 9 *There exists* $w \in S$ *such that both* $e(w/v)$ *and* $f(w/v)$ *are odd.*

Proof. By dévissage, it is enough to prove this in the following two cases.

a) The extension L'/L is separable. In that case, we have the standard formula (cf. [**?**], Chap. 6, § 8, no. 5)

$$\sum_{w \in S} e(w/v) f(w/v) = [L' : L].$$

Since $[L' : L]$ is odd, there is at least one $w \in S$ such that $e(w/v)f(w/v)$ is odd.

b) We have $\mathrm{char}(L) = p > 0$ and L'/L is purely inseparable. In that case, S is reduced to one element w, and one checks that $e(w/v)$ and $f(w/v)$ are powers of p, hence are odd. □

End of proof of ii). Select w as in Lemma **??**. We are going to apply case i) to (L', ϕ, w). Note first that the w-residues of ϕ are the images of its v-residues by the base change $\widetilde{L} \to \widetilde{L}'$. Since $[\widetilde{L}' : \widetilde{L}]$ is odd, the map $W(\widetilde{L}) \to W(\widetilde{L}')$ is injective. This shows that $\partial_2(\phi) \neq 0$ in $W(\widetilde{L}')$, so that condition a) is satisfied by (L', ϕ, w).

It remains to check condition b). Let ψ_0 be the unique anisotropic representative of $\partial_1(\phi)$; by a classical theorem of Springer (cf. [**?**], p.198), it remains anisotropic in $\widetilde{L}'$. Hence the representatives ψ of $\partial_1(\phi)$ over $\widetilde{L}'$ are the sums of ψ_0 and some hyperbolic forms; in particular they come from $\widetilde{L}$. Since an odd degree extension does not change $\mathrm{ed}(\ ;2)$ we have $\mathrm{ed}_{\widetilde{L}'}(\psi; 2) \geq e - 1$. We have thus checked conditions a) and b) over L', and we may apply part i) of the proof.

This concludes the proof of Proposition **??** and hence of Proposition **??** and of Theorem **??**. □

Remark. Let K/k be a field extension, with k algebraically closed. Let q and q' be quadratic forms over K which belong to the same Witt class. Is it true that $\mathrm{ed}(q) = \mathrm{ed}(q')$ and $\mathrm{ed}(q; 2) = \mathrm{ed}(q'; 2)$? It is so when $K = k(t_1, \ldots, t_e)$ and one of the forms q or q' is monomial. We do not know what happens in general.

§ 6 Proof of Theorem ??

Let $\rho : G \to \mathbf{O}\,(V, q)$ be as in Proposition **??**, and let $\theta_O = \rho(\theta_G)$ be the image of θ_G in $H^1(K, \mathbf{O}\,(V, q))$. If ρ_A denotes the composition $A \to G \xrightarrow{\rho} \mathbf{O}\,(V, q)$, we have $\theta_O = \rho_A(\theta_A)$. By Theorem **??**, it suffices to show that the rank of $\langle X_{\rho_A} \rangle$ is $r+1$. We need the following.

Lemma 10 *Let R be an irreducible root system, and R_{sh} the set of short roots. Let $Q(R)$ be the root lattice of R. If α and β are elements of R_{sh}, we have:*

$$\alpha = \beta \pmod{2Q(R)} \Longleftrightarrow \alpha = \pm\beta.$$

Proof. This can be checked by inspection of all possible root systems. □

Let us compute the weights of ρ_A and their multiplicities. For a short root $\alpha \in R_{sh}^+$ we denote by V_α the corresponding weight subspace of V for T. By construction, $\dim V_\alpha = 1$ and we have an orthogonal decomposition

$$V = V_0 \oplus \left\{ \bigoplus_\alpha (V_\alpha \oplus V_{-\alpha}) \right\},$$

where the sum is taken over all positive short roots.

Any element $a \in A^\circ$ acts by multiplication by $\alpha(a)$ on $W_\alpha = V_\alpha \oplus V_{-\alpha}$, and acts trivially on V_0. The automorphism c of **??** preserves V_0 and permutes V_α and $V_{-\alpha}$. Since k is algebraically closed, there is a basis $\{u_\alpha, v_\alpha\}$ of W_α such that $c(u_\alpha) = u_\alpha$, and $c(v_\alpha) = -v_\alpha$. It follows that the weight subspaces for ρ_A belonging to $\bigoplus_\alpha (V_\alpha \oplus V_{-\alpha})$ correspond to characters $\alpha \in R_{sh}^+$ and $\alpha\gamma$, where $\gamma \in X(A) = \mathrm{Hom}(A, \pm 1)$ is given by $A^\circ \mapsto 1$ and $c \mapsto -1$. Furthermore, all these weights of ρ_A have multiplicity 1, by Lemma **??**. Depending on the action of c on V_0 the set X_{ρ_A} may contain additionally 0 and γ. In all cases the rank of $\langle X_{\rho_A} \rangle$ is $r+1$, as required. □

§ 7 Spin groups

We keep the notation of the previous §§. In particular, the ground field k is algebraically closed of characteristic $\neq 2$. If $n > 2$, we denote by $\mathbf{Spin}_n$ the universal covering of the group $\mathbf{SO}_n$ (relative to the unit quadratic form $\langle 1, ..., 1 \rangle$). For $n \leq 6$, this group is "special", which implies that $\mathrm{ed}(\mathbf{Spin}_n) = 0$, cf. [?]. The situation is different for $n > 6$. In order to state it precisely, let us define an integer $e(n)$ by :

$e(10) = 4$;
$e(n) = [n/2] = \text{rank } \mathbf{Spin}_n$ if $n > 6$ and $n \neq 10$.

Theorem 11 *We have* $\mathrm{ed}(\mathbf{Spin}_n;2) \geq e(n)$ *for every* $n > 6$.

Proof. Let us write $e = e(n)$, and put $K = k(t_1, ..., t_e)$, where $t_1, \ldots, t_e$ are independent indeterminates. We are going to construct a *monomial quadratic form* f_n of rank n over K with the following properties:

(i) the Stiefel-Whitney classes $w_1(f_n)$ and $w_2(f_n)$ are both zero. (For the definitions of the Stiefel-Whitney classes, see e.g. [**?**], § 17.)

(ii) $\mathrm{rank}(X_{f_n}) = e$, with the notation of the lines preceding Proposition **??**.

Such a form f_n corresponds to an element $[f_n]$ of $H^1(K, \mathbf{O}_n)$ which belongs to the image of $H^1(K, \mathbf{Spin}_n) \to H^1(K, \mathbf{O}_n)$ (because of (i)) and is such that $\mathrm{ed}([f_n];2) = e$ (because of (ii), cf. Proposition **??**). This shows that $H^1(K, \mathbf{Spin}_n)$ contains an element ξ_n with $\mathrm{ed}(\xi_n;2) \geq e$; hence the theorem.

Here is the construction of f_n. There are four cases, depending on the value of n modulo 4:

a) $n \equiv 0 \pmod 4$, $n \geq 8$. We have $e = n/2$, which is even. We define f_n by:

$$f_n = \langle t_1, \ldots, t_e \rangle \otimes \langle 1, t_1 \cdots t_e \rangle.$$

Condition (ii) is obvious (but would not be true in the excluded case $n = 4$). As for condition (i), it follows from the general formulae:

$$w_1(f \otimes f') = 0 \quad \text{and} \quad w_2(f \otimes f') = w_1(f) \cdot w_1(f')$$

if $\mathrm{rank}(f)$ and $\mathrm{rank}(f')$ are even. Indeed this shows that $w_1(f_n) = 0$ and that $w_2(f_n) = (t_1 \cdots t_e) \cdot (t_1 \cdots t_e) = (-1) \cdot (t_1 \cdots t_e) = 0$ since -1 is a square in k.

b) $n \equiv -1 \pmod 4$, $n \geq 7$. Here $e = (n-1)/2$, which is odd. We put:

$$f_n = \langle t_1, \ldots, t_e \rangle \otimes \langle 1, t_1 \cdots t_e \rangle \oplus \langle t_1 \cdots t_e \rangle.$$

Conditions (i) and (ii) are checked as in case a).

c) $n \equiv 1 \pmod 4$, $n \geq 9$. Here $e = (n-1)/2$, which is even. We put:

$$f_n = f_{n-1} \oplus \langle 1 \rangle = \langle t_1, \ldots, t_e \rangle \otimes \langle 1, t_1 \cdots t_e \rangle \oplus \langle 1 \rangle.$$

Conditions (i) and (ii) follow from case a).

d) $n \equiv 2 \pmod 4$. This case splits into four subcases:

d$_1$) $n = 10$. Here $e = 4$ and we put

$$f_{10} = f_8 \oplus \langle 1, 1\rangle = \langle t_1, \ldots, t_4\rangle \otimes \langle 1, t_1 ... t_4\rangle \oplus \langle 1, 1\rangle.$$

d$_2$) $n = 14$. Here $e = 7$. We put

$$f_{14} = \langle t_7\rangle \otimes (\langle\langle\, t_1, t_2, t_3\,\rangle\rangle_0 \oplus \langle\langle\, t_4, t_5, t_6\,\rangle\rangle_0)$$

where $\langle\langle a, b, c\rangle\rangle_0$ means $\langle\langle a, b, c\rangle\rangle - \langle 1\rangle$, i.e. $\langle a, b, c, ab, bc, ac, abc\rangle$. The simplest way to check condition (i) is to rewrite f_{14} in the Witt ring $W(K)$ as

$$f_{14} = \langle t_7\rangle \cdot (\langle\langle\, t_1, t_2, t_3\,\rangle\rangle + \langle\langle\, t_4, t_5, t_6\,\rangle\rangle).$$

This shows that f_{14} belongs to the cube I^3 of the augmentation ideal I of $W(K)$, and that implies condition (i). Condition (ii) is easy to check.

d$_3$) $n = 18$. Here $e = 9$. We put:

$$f_{18} = \langle t_1, t_2, t_1t_2\rangle \otimes \langle t_7, t_8\rangle \oplus \langle t_3, t_4, t_3t_4\rangle \otimes \langle t_8, t_9\rangle \oplus \langle t_5, t_6, t_5t_6\rangle \otimes \langle t_7, t_9\rangle.$$

In the Witt ring $W(K)$, one has:

$$f_{18} = \langle\langle\, t_1, t_2\,\rangle\rangle \cdot \langle t_7, t_8\rangle + \langle\langle\, t_3, t_4\,\rangle\rangle \cdot \langle t_8, t_9\rangle + \langle\langle\, t_5, t_6\,\rangle\rangle \cdot \langle t_7, t_9\rangle,$$

and this shows that $f_{18} \in I^3$, hence condition (i). As for condition (ii), one checks that, if one makes the change of variables:

$$T_1 = t_1t_7,\ T_2 = t_2t_7,\ T_3 = t_1t_2t_7,\ T_4 = t_3t_8,\ T_5 = t_4t_8,$$
$$T_6 = t_3t_4t_8,\ T_7 = t_5t_9,\ T_8 = t_6t_9,\ T_9 = t_5t_6t_9,$$

then f_{18} becomes *e-reduced* (as a monomial quadratic form in the T_i). This implies (ii).

d$_4$) $n \equiv 2 \pmod 4$, $n > 18$. We define f_n by induction on n, as the sum of f_{n-8} and f_8 (with independent variables):

$$f_n = f_{n-8} \oplus \langle t_{e-3}, t_{e-2}, t_{e-1}, t_e\rangle \otimes \langle 1, t_{e-3}t_{e-2}t_{e-1}t_e\rangle.$$

Conditions (i) and (ii) are proved by induction on n. This concludes the proof. □

Remarks. 1) The reader may wonder whether the quadratic form f_n used above could have been defined via an abelian finite subgroup of $\mathbf{Spin}_n(k)$

whose image in $\mathbf{SO}_n(k)$ is of type $(2,\ldots,2)$. The answer is "yes"; this follows from the well known construction of abelian 2-subgroups of $\mathbf{Spin}_n$ from binary linear codes (see e.g. [**?**], pp. 1043–1044). Indeed, this is how we first obtained case d_3 above ($n = 18$).

2) When $n \equiv -1, 0$ or $1 \pmod 8$, the bound given by Theorem **??** can be slightly improved. This is due (in characteristic 0, at least) to Reichstein-Youssin ([**?**], Theorem 8.16). More precisely:

Theorem 12 *Assume* $n \equiv -1, 0$ *or* $1 \pmod 8$, $n \geq 7$. *Then*:

$$\mathrm{ed}(\mathbf{Spin}_n; 2) \geq [n/2] + 1.$$

Proof. We define a $(2,\ldots,2)$-subgroup A of $\mathbf{Spin}_n(k)$ as in **??**, namely as $A_0 \times \{1, \tilde{c}\}$, where A_0 is the 2-division subgroup of the maximal torus T, and $\tilde{c}$ is a lifting in $\mathbf{Spin}_n(k)$ of the element c of the adjoint group. The congruence condition on n implies that $\tilde{c}$ is of order 2. We have $\mathrm{rank}\, A = r+1 = [n/2]+1$. Let us suppose first that $n \equiv \pm 1 \pmod 8$. The spin representation is then orthogonal, and it gives a homomorphism

$$\rho : \mathbf{Spin}_n \to \mathbf{O}_N, \text{ with } N = 2^r = 2^{(n-1)/2}.$$

If $K = k(t_1, \ldots, t_r, u)$ we define $\theta_A \in H^1(K, A)$ as in **??**. The image of θ_A by ρ corresponds to a rank N quadratic form q, which is easily shown to be isomorphic (up to a change of variables) to $\langle u \rangle \otimes \langle\langle t_1, \ldots, t_r \rangle\rangle$. By Proposition **??**, we have $\mathrm{ed}(q; 2) \geq r + 1$. This shows that the image θ of θ_A in $H^1(K, \mathbf{Spin}_n)$ is such that $\mathrm{ed}(\theta; 2) \geq r + 1$, and the theorem follows. The case where $n \equiv 0 \pmod 8$ is analogous : one takes for ρ the direct sum of the two half-spin representations (which are orthogonal, because $n \equiv 0 \pmod 8$). □

§ 8 Other examples

Theorem 13 (i) $\mathrm{ed}(\mathbf{HSpin}_n; 2) \geq n/2 + 1$ *if* $n > 0$, $n \equiv 0 \pmod 8$.
(ii) $\mathrm{ed}(\mathbf{PSO}_n; 2) \geq n - 2$ *if* n *is even* ≥ 4.
(iii) $\mathrm{ed}(2.E_7; 2) \geq 7$.
(iv) $\mathrm{ed}(\mathbf{PGL}_n) \geq v_2(n)$ *if* $n > 0$.

(Undefined notation will be explained below.)

Proof (sketch). Let G be the group $\mathbf{HSpin}_n$ (resp. $\mathbf{PSO}_n$, resp. $2.E_7$, resp. $\mathbf{PGL}_n$) mentioned in the theorem. We apply the method of the previous sections to a suitable abelian subgroup A of $G(k)$, of rank $e = n/2+1$ (resp. $n-2$, resp. 7, resp. $v_2(n)$) and to a suitable orthogonal representation $\rho : G \to \mathbf{GL}(V)$. We thus get a monomial quadratic form q over $K = k(t_1, \ldots, t_e)$, and a routine computation, based on Theorem **??**, shows that $\mathrm{ed}(q; 2) = e$, hence the result.

Here are the definitions of A and ρ in each case (the "routine computation" is left to the reader):

Case (i). The group $G = \mathbf{HSpin}_n$ is the *half-spin group*, i.e. the quotient of $\mathbf{Spin}_n$ by a central subgroup of order 2 distinct from the kernel of $\mathbf{Spin}_n \to \mathbf{SO}_n$. This is well defined whenever $n \equiv 0 \pmod 4$, with a slight ambiguity for $n = 8$, since in that case $\mathbf{HSpin}_8$ is isomorphic to $\mathbf{SO}_8$ (and hence $\mathrm{ed}(\mathbf{HSpin}_8; 2) = 7$). The group G acts faithfully on the corresponding half-spin representation S. Since $n \equiv 0 \pmod 8$, this is an orthogonal representation. Let T be a maximal torus of G. As in **??** we define A to be the subgroup of $G(k)$ generated by the elements of order 2 of T and by an element c of order 2 of $N(T)$ such that $ctc = t^{-1}$ for every $t \in T$ (such an element exists because n is divisible by 8). The group A is an elementary abelian $(2, \ldots, 2)$-group of rank $e = n/2+1$. We choose for V the direct sum $S \oplus \mathrm{Lie}(G)$.

Case (ii). The group $G = \mathbf{PSO}_n$ is the quotient $\mathbf{SO}_n/\mu_2$, i.e. an adjoint group of type $D_{n/2}$. The group A is the image in $G(k)$ of the diagonal matrices of square 1 in $\mathbf{SO}_n$. It is a $(2, \ldots, 2)$-abelian group of rank $e = n-2$. One takes for V the Lie algebra of G, with the quadratic form defined by $\mathrm{Tr}(x \cdot y)$.

Case (iii). The group $G = 2.E_7$ is a simply connected group of type E_7. Choose a maximal torus T of G, and let $c \in N(T)$ be such that $ctc^{-1} = t^{-1}$ for every $t \in T$. We have $c^2 = z$, where z is the non trivial element of the center of G. Let A_0 be the kernel of $t \mapsto t^2$; it is an elementary group of type $(2, \ldots, 2)$ and of rank 7; it contains z. The subgroup A of G generated by A_0 and c is an abelian group of type $(4, 2, \ldots, 2)$ and of rank 7. The image of A in the adjoint group $G' = G/\{1, z\}$ is $A' = A/\{1, z\}$; it is elementary abelian of rank 7. If $K = k(t_1, \ldots, t_7)$, we have a canonical element $\theta_{A'}$ in $H^1(K, A')$; since -1 is a square in K, there exists an element $\theta_A \in H^1(K, A)$ whose image in $H^1(K, A')$ is $\theta_{A'}$. We choose for orthogonal representation of G the adjoint representation. The action of A on this representation factors through A', hence gives a monomial quadratic form q over $k(t_1, \dots, t_7)$ and one checks that q is 7-reduced.

Case (iv). Here $G = \mathbf{PGL}_n$ and $e = 2m$, where m is the 2-adic valuation of n. If we write n as $2^m N$, with N odd, there is a natural injection of $\mathbf{PGL}_2 \times \dots \times \mathbf{PGL}_2$ (m factors) in G. Let A_1 be a $(2,2)$-subgroup of $\mathbf{PGL}_2$, and let $A = A_1 \times \dots \times A_1$ (m factors). We have an embedding

$$A \longrightarrow \mathbf{PGL}_2 \times \dots \times \mathbf{PGL}_2 \longrightarrow \mathbf{PGL}_n = G,$$

and A is a $(2, \dots, 2)$-group of rank e. We select for V the space M_n of $n \times n$ matrices, with the scalar product $\mathrm{Tr}(x \cdot y)$. The group G acts by conjugation on M_n. (Here the monomial quadratic form q is the tensor product of a generic e-Pfister form by the unit form $\langle 1, \dots, 1 \rangle$ of rank N^2; since N is odd, Theorem **??** shows that the essential dimension of q at 2 is indeed equal to e.) □

Remarks. 1) We do not know how good are the lower bounds of Theorems **??**,**??**,**??** and **??**. Some are rather weak: for instance, th. **??** applied to type B_n gives roughly half the true value of $\mathrm{ed}(G; 2)$. What about those on $\mathbf{Spin}_n$, $\mathbf{HSpin}_n$, and E_8? These questions are related: an upper bound for $\mathbf{HSpin}_{16}$ would give one for E_8.

2) Applying Proposition **??** to the generic quadratic form $q = \langle t_1, \dots, t_n \rangle$ and the generic quadratic form $q' = \langle t_1, \dots, t_{n-1}, t_1 \cdots t_{n-1} \rangle$ of discriminant 1 one recovers the well known facts that $\mathrm{ed}(\mathbf{O}_n; 2) \geq n$ and $\mathrm{ed}(\mathbf{SO}_n; 2) \geq n-1$ (if $n \geq 2$), cf. e.g. [**?**], Theorems 10.3 and 10.4.

3) There are cases where the method "$A \to G \to \mathbf{O}(V, q)$" fails to give any result. For instance, let G be a group of type E_6 (adjoint, or simply connected, it does not matter). By using the relations of this group with G_2 (cf. [**?**], Exercise 22.9) it is not hard to see that $\mathrm{ed}(G; 2)$ is equal to 3. One can show that there is no way to prove this by the $A \to G \to \mathbf{O}(V, q)$ method: every orthogonal representation $G \to \mathbf{O}(V, q)$ gives a map $H^1(K, G) \to H^1(K, \mathbf{O}(V, q))$ which is *trivial*, hence gives no information on $\mathrm{ed}(G)$.

Acknowledgement

Work on the present paper started in 2002, at the Centre Bernoulli, E.P.F.L., Lausanne. We want to thank the Centre Bernoulli for its hospitality and its stimulating atmosphere.

References

[BS 53] A. Borel and J-P. Serre, Sur certains sous-groupes des groupes de Lie compacts, Comm. Math. Helv. **27** (1953), 128–139 (= A. Borel, Oe. 24).

[Bo 64] N. Bourbaki, Algèbre Commutative, Chap. V-VI, Hermann, Paris, 1964; English translation, Springer-Verlag, 1983.

[Bo 75] N. Bourbaki, Groupes et Algèbres de Lie, Chap. VII-VIII, Hermann, Paris, 1975; English translation, Springer-Verlag, 2005.

[BR 97] J. Buhler and Z. Reichstein, On the essential dimension of a finite group, Compositio Math. **126** (1997), 159–179.

[DG 70] M. Demazure and A. Grothendieck, Structure des Schémas en Groupes Réductifs, SGA 3 III, LN 153, Springer-Verlag, 1970.

[GMS 03] S. Garibaldi, A. Merkurjev and J.-P. Serre, Cohomological Invariants in Galois Cohomology, A.M.S. Univ. Lectures Series 28, Providence, R.I., 2003.

[GN 04] B. H. Gross and G. Nebe, Globally maximal arithmetic groups, J. Algebra **272** (2004), 625-642.

[L 73] T.-Y. Lam, The Algebraic Theory of Quadratic Forms, Benjamin, MA, 1973.

[Pf 95] A.Pfister, Quadratic Forms with Applications to Geometry and Topology, Cambidge Univ. Press, Cambridge 1995.

[R 00] Z. Reichstein, On the notion of essential dimension for algebraic groups, Transform. Groups **5** (2000), 265–304.

[RY 00] Z. Reichstein and B. Youssin, Essential dimensions of algebraic groups and a resolution theorem for G-varieties (with an appendix by János Kollár and Endre Szabó), Canad. J. Math. **52** (2000), 1018–1056.

[Sel 57] G. B. Seligman, Some remarks on classical Lie algebras, J.Math. Mech. **6** (1957), 549-558.

[SpSt 70] T. Springer and R. Steinberg, Conjugacy classes, LN 131 (1970), 167-266 (= R. Steinberg, C.P., no 25, 293-394).

[St 67] R. Steinberg, Lectures on Chevalley groups, Yale University, 1967.