

A BOUND FOR THE TORSION IN THE K -THEORY
OF ALGEBRAIC INTEGERS

CHRISTOPHE SOULÉ

Received: November 6, 2002

Revised: May 30, 2003

A Kazuya Kato, qui
marche sous la lune.

ABSTRACT. Let m be an integer bigger than one, A a ring of algebraic integers, F its fraction field, and $K_m(A)$ the m -th Quillen K -group of A . We give a (huge) explicit bound for the order of the torsion subgroup of $K_m(A)$ (up to small primes), in terms of m , the degree of F over \mathbf{Q} , and its absolute discriminant.

Let F be a number field, A its ring of integers and $K_m(A)$ the m -th Quillen K -group of A . It was shown by Quillen that $K_m(A)$ is finitely generated. In this paper we shall give a (huge) explicit bound for the order of the torsion subgroup of $K_m(A)$ (up to small primes), in terms of m , the degree of F over \mathbf{Q} , and its absolute discriminant.

Our method is similar to the one developed in [13] for $F = \mathbf{Q}$. Namely, we reduce the problem to a bound on the torsion in the homology of the general linear group $\mathrm{GL}_N(A)$. Thanks to a result of Gabber, such a bound can be obtained by estimating the number of cells of given dimension in any complex of free abelian groups computing the homology of $\mathrm{GL}_N(A)$. Such a complex is derived from a contractible CW -complex \widetilde{W} on which $\mathrm{GL}_N(A)$ with compact quotient. We shall use the construction of \widetilde{W} given by Ash in [1]. It consists of those hermitian metrics h on A^N which have minimum equal to one and are such that their set $M(h)$ of minimal vectors has rank equal to N in F^N . To count cells in $\widetilde{W}/\mathrm{GL}_N(A)$, one will exhibit an explicit compact subset of $A^N \otimes_{\mathbf{Z}} \mathbf{R}$ which, for every $h \in \widetilde{W}$, contains a translate of $M(h)$ by some matrix of $\mathrm{GL}_N(A)$ (Proposition 2). The proof of this result relies on several arguments from the geometry of numbers using, among other things, the number field analog of Hermite's constant [4].

The bound on the K -theory of A implies a similar upper bound for the étale cohomology of $\mathrm{Spec}(A[1/p])$ with coefficients in the positive Tate twists of \mathbf{Z}_p , for any (big enough) prime number p .

However, this bound is quite large since it is doubly exponential both in m and, in general, the discriminant of F . We expect the correct answer to be polynomial in the discriminant and exponential in m (see 5.1).

The paper is organized as follows. In Section 1 we prove a few facts on the geometry of numbers for A , including a result about the image of A^* by the regulator map (Lemma 3), which was shown to us by H. Lenstra. Using these, we study in Section 2 hermitian lattices over A , and we get a bound on $M(h)$ when h lies in \widetilde{W} . The cell structure of \widetilde{W} is described in Section 3. The main Theorems are proved in Section 4. Finally, we discuss these results in Section 5, where we notice that, because of the Lichtenbaum conjectures, a lower bound for higher regulators of number fields would probably provide much better upper bounds for the étale cohomology of $\mathrm{Spec}(A[1/p])$. We conclude with the example of $K_8(\mathbf{Z})$ and its relation to the Vandiver conjecture.

1 GEOMETRY OF ALGEBRAIC NUMBERS

1.1

Let F be a number field, and A its ring of integers. We denote by $r = [F : \mathbf{Q}]$ the degree of F over \mathbf{Q} and by $D = |\mathrm{disc}(K/\mathbf{Q})|$ the absolute value of the discriminant of F over \mathbf{Q} . Let r_1 (resp. r_2) be the number of real (resp. complex) places of F . We have $r = r_1 + 2r_2$. We let $\Sigma = \mathrm{Hom}(F, \mathbf{C})$ be the set of complex embeddings of F . These notations will be used throughout. Given a finite set X we let $\#(X)$ denote its cardinal.

1.2

We first need a few facts from the geometry of numbers applied to A and A^* . The first one is the following classical result of Minkowski:

LEMMA 1. *Let L be a rank one torsion-free A -module. There exists a non zero element $x \in L$ such that the submodule spanned by x in L has index*

$$\#(L/Ax) \leq C_1,$$

where

$$C_1 = \frac{r!}{r^r} \cdot 4^{r_2} \pi^{-r_2} \sqrt{D}$$

in general, and $C_1 = 1$ when A is principal.

PROOF. The A -module L is isomorphic to an ideal I in A . According to [7], V §4, p. 119, Minkowski's first theorem implies that there exists $x \in I$ the norm of which satisfies

$$|N(x)| \leq C_1 N(I).$$

Here $|N(x)| = \#(A/Ax)$ and $N(I) = \#(A/I)$, therefore $\#(I/Ax) \leq C_1$. The case where A is principal is clear. q.e.d.

1.3

The family of complex embeddings $\sigma : F \rightarrow \mathbf{C}$, $\sigma \in \Sigma$, gives rise to a canonical isomorphism of real vector spaces of dimension r

$$F \otimes_{\mathbf{Q}} \mathbf{R} = (\mathbf{C}^{\Sigma})^+,$$

where $(\cdot)^+$ denotes the subspace invariant under complex conjugation. Given $\alpha \in F$ we shall write sometimes $|\alpha|_{\sigma}$ instead of $|\sigma(\alpha)|$.

LEMMA 2. *Given any element $x = (x_{\sigma}) \in F \otimes_{\mathbf{Q}} \mathbf{R}$, there exists $a \in A$ such that*

$$\sum_{\sigma \in \Sigma} |x_{\sigma} - \sigma(a)| \leq C_2,$$

with

$$C_2 = \frac{4^{r_1} \pi^{r_2}}{r^{r-2} r!} \sqrt{D}$$

in general, and

$$C_2 = 1/2 \quad \text{if} \quad F = \mathbf{Q}.$$

PROOF. Define a norm on $F \otimes_{\mathbf{Q}} \mathbf{R}$ by the formula

$$\|x\| = \sum_{\sigma \in \Sigma} |x_{\sigma}|.$$

The additive group A is a lattice in $F \otimes_{\mathbf{Q}} \mathbf{R}$, and we let μ_1, \dots, μ_r be its successive minima. In particular, there exist $a_1, \dots, a_r \in A$ such that $\|a_i\| = \mu_i$, $1 \leq i \leq r$, and $\{a_1, \dots, a_r\}$ are linearly independent over \mathbf{Z} . Any $x \in F \otimes_{\mathbf{Q}} \mathbf{R}$ can be written

$$x = \sum_{i=1}^r \lambda_i a_i, \quad \lambda_i \in \mathbf{R}.$$

Let $n_i \in \mathbf{Z}$ be such that $|n_i - \lambda_i| \leq 1/2$, for all $i = 1, \dots, r$, and

$$a = \sum_{i=1}^r n_i a_i.$$

Clearly

$$\|x - a\| \leq \sum_{i=1}^r |\lambda_i - n_i| \|a_i\| \leq \frac{1}{2} (\mu_1 + \dots + \mu_r) \leq \frac{r}{2} \mu_r. \tag{1}$$

On the other hand, we know from the product formula that, given any $a \in A - \{0\}$,

$$\prod_{\sigma \in \Sigma} |\sigma(a)| \geq 1. \quad (2)$$

By the inequality between arithmetic and geometric means this implies

$$\|a\| = \sum_{\sigma \in \Sigma} |\sigma(a)| \geq r,$$

hence

$$\mu_i \geq r \quad \text{for all } i = 1, \dots, r. \quad (3)$$

Minkowski's second theorem tells us that

$$\mu_1 \dots \mu_r \leq 2^r W 2^{-r_2} \sqrt{D} \quad (4)$$

([7], Lemma 2, p. 115), where W is the euclidean volume of the unit ball for $\|\cdot\|$ in $F \otimes_{\mathbf{Q}} \mathbf{R}$. (Note that the covolume of A is \sqrt{D} .) The volume W is the euclidean volume of those elements $(x_i, z_j) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ such that

$$\sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq 1.$$

One finds ([7], Lemma 3, p. 117)

$$W = 2^{r_1} 4^{-r_2} (2\pi)^{r_2} / r!. \quad (5)$$

From (3) and (4) we get

$$\mu_r \leq 2^r W \sqrt{D} 2^{-r_2} r^{-(r-1)}. \quad (6)$$

The lemma follows from (1), (5) and (6). q.e.d.

1.4

We also need a multiplicative analog of Lemma 2. Let $R(F)$ be the regulator of F , as defined in [7] V, § 1, p. 109. Let $s = r_1 + r_2 - 1$.

LEMMA 3. *Let (λ_σ) , $\sigma \in \Sigma$ be a family of positive real numbers such that $\lambda_{\bar{\sigma}} = \lambda_\sigma$ when $\bar{\sigma}$ is the complex conjugate of σ . There exists a unit $u \in A^*$ such that*

$$\sup_{\sigma \in \Sigma} (\lambda_\sigma |u|_\sigma) \leq C_3 \left(\prod_{\sigma \in \Sigma} \lambda_\sigma \right)^{1/r},$$

with

$$C_3 = \exp(s(4r(\log 3r)^3)^{s-1} 2^{r_2-1} R(F)).$$

PROOF. We follow an argument of H. Lenstra. Let $H \subset \mathbf{R}^{r_1+r_2}$ be the s -dimensional hyperplane consisting of vectors $(x_1, \dots, x_{r_1+r_2})$ such that $x_1 + x_2 + \dots + x_{r_1+r_2} = 0$. Choose a subset $\{\sigma_1, \dots, \sigma_{r_1+r_2}\} \subset \Sigma$ such that $\sigma_1, \dots, \sigma_{r_1}$ are the real embeddings of Σ and $\sigma_i \neq \bar{\sigma}_j$ if $i \neq j$. Given $\lambda = (\lambda_\sigma)_{\sigma \in \Sigma}$ as in the lemma, we let

$$\rho(\lambda) = (\log(\lambda_{\sigma_1}), \dots, \log(\lambda_{\sigma_{r_1}}), 2\log(\lambda_{\sigma_{r_1+1}}), \dots, 2\log(\lambda_{\sigma_{r_1+r_2}})).$$

If $u \in A^*$ is a unit, and $\lambda = (|u|_\sigma)$, we have $\rho(\lambda) \in H$. We get this way a lattice

$$L = \{\rho(|u|_\sigma), u \in A^*\}$$

in H .

Define a norm $\|\cdot\|$ on H by the formula

$$\|(x_i)\| = \text{Sup} \left(\text{Sup}_{1 \leq i \leq r_1} |x_i|, \text{Sup}_{r_1+1 \leq i \leq r_1+r_2} |x_i|/2 \right).$$

It is enough to show that, for any vector $x \in H$ there exists $a \in L$ such that

$$\|x - a\| \leq \log(C_3).$$

According to [14], Cor. 2, p. 84, we have (when $r \geq 2$)

$$\|a\| \geq \varepsilon$$

where

$$\varepsilon = r^{-1}(\log(3r))^{-3},$$

for any $a \in L - \{0\}$. Therefore, using Minkowski's second theorem as in the proof of Lemma 2 we get that, for any $x \in H$ there exists $a \in L$ with

$$\|x - a\| \leq s 2^{s-1} \varepsilon^{1-s} W \text{vol}(H/L),$$

where W is the euclidean volume of the unit ball for $\|\cdot\|$, where we identify H with \mathbf{R}^s by projecting on the first s coordinates. Clearly $W \leq 2^{s+r_2-1}$ when, by definition (loc.cit.), $\text{vol}(H/L)$ is equal to $R(F)$. The lemma follows.

1.5

We now give an upper bound for the constant C_3 of Lemma 3.

LEMMA 4. *The following inequality holds*

$$R \leq 11 r^2 \sqrt{D} \log(D)^{r-1}.$$

PROOF. Let κ be the residue at $s = 1$ of the zeta function of F . According to [11], Cor. 3, p. 333, we have

$$\kappa \leq 2^{r+1} D^a a^{1-r}$$

whenever $0 < a \leq 1$. Taking $a = \log(D)^{-1}$ we get

$$\kappa \leq e 2^{r+1} \log(D)^{r-1}. \quad (7)$$

On the other hand

$$\kappa = 2^{r_1} (2\pi)^{r_2} \frac{h(F) R(F)}{w(F) \sqrt{D}}, \quad (8)$$

where $h(F)$ is the class number of F and $w(F)$ the number of roots of unity in F ([7], Prop. 13, p. 300). Since $h(F) \geq 1$ we get

$$R(F) \leq w(F) 2^{-(r_1+r_2)} \pi^{-r_2} e 2^{r+1} \sqrt{D} \log(D)^{r-1}.$$

Since the degree over \mathbf{Q} of $\mathbf{Q}(\sqrt[r]{1})$ is $\varphi(n)$, where φ is the Euler function, we must have

$$\varphi(w(F)) \leq r.$$

When $n = p^t$ is an odd prime power we have

$$\varphi(p^t) = (p-1)p^{t-1} \geq p^{t/2}.$$

Therefore

$$w(F) \leq 2r^2.$$

Since

$$2^{-(r_1+r_2)} \pi^{-r_2} 2^r = \left(\frac{2}{\pi}\right)^{r_2} \leq 1$$

and $4e \leq 11$, the lemma follows.

2 HERMITIAN LATTICES

2.1

An *hermitian lattice* $\overline{M} = (M, h)$ is a torsion free A -module M of finite rank, equipped with an hermitian scalar product h on $M \otimes_{\mathbf{Z}} \mathbf{C}$ which is invariant under complex conjugation. In other words, if we let $M_{\sigma} = M \otimes_A \mathbf{C}$ be the complex vector space obtained from M by extension of scalars via $\sigma \in \Sigma$, h is given by a collection of hermitian scalar products h_{σ} on M_{σ} , $\sigma \in \Sigma$, such that $h_{\overline{\sigma}}(x, y) = h_{\sigma}(x, y)$ whenever x and y are in M .

We shall also write

$$h_{\sigma}(x) = h_{\sigma}(x, x)$$

and

$$\|x\|_\sigma = \sqrt{h_\sigma(x)}.$$

LEMMA 5. Let \overline{M} be an hermitian lattice of rank N . Assume that M contains N vectors e_1, \dots, e_N which are F -linearly independent in $M \otimes_A F$ and such that

$$\|e_i\| \leq 1$$

for all $i = 1, \dots, N$. Then there exist a direct sum decomposition

$$M = L_1 \oplus \dots \oplus L_N$$

where each L_i has rank one and contains a vector f_i such that

$$\#(L_i/A f_i) \leq C_1$$

and

$$\|f_i\| \leq (i-1) C_1 C_2 + C_1^{1/r} C_3.$$

Here C_1, C_2, C_3 are the constants defined in Lemmas 1, 2, 3 respectively.

PROOF. We proceed by induction on N . When $N = 1$, Lemma 1 tells us that $L_1 = M$ contains x_1 such that

$$\#(L_1/A x_1) \leq C_1.$$

Let us write

$$x_1 = \alpha e_1$$

with $\alpha \in F^*$. Using Lemma 3, we can choose $u \in A^*$ such that

$$\sup_{\sigma \in \Sigma} |u \alpha|_\sigma \leq C_3 \left(\prod_{\sigma} |\alpha|_\sigma \right)^{1/r} = C_3 N(\alpha)^{1/r} \leq C_3 C_1^{1/r}.$$

The lemma follows with $f_1 = u x_1$.

Assume now that $N \geq 2$, and let $L_1 = M \cap F e_1$ in $M \otimes_A F$. As above, we choose $f_1 = a_{11} e_1$ in L_1 with $[L_1 : A f_1] \leq C_1$ and

$$\sup_{\sigma \in \Sigma} |a_{11}|_\sigma \leq C_3 C_1^{1/r}.$$

The quotient $M' = L/L_1$ is torsion free of rank $N - 1$. We equip M' with the quotient metric induced by h , we let $p : M \rightarrow M'$ be the projection, and $e'_i = p(e_i)$, $i = 2, \dots, N$. Clearly

$$\|e'_i\| \leq 1$$

for all $i = 2, \dots, N$.

We assume by induction that M' can be written

$$M' = L'_2 \oplus \cdots \oplus L'_N$$

and that L'_i contains a vector f'_i such that

$$n_i = \#(L'_i / A f'_i) \leq C_1$$

with

$$f'_i = \sum_{2 \leq j \leq i} a_{ij} e'_j, \quad (9)$$

$a_{ij} \in F$, and, for all $\sigma \in \Sigma$,

$$|a_{ij}|_\sigma \leq C_1 C_2 \quad \text{if } 2 \leq j < i \leq N,$$

and

$$|a_{ii}|_\sigma \leq C_1^{1/r} C_3, \quad 2 \leq i \leq N.$$

Let $s : M' \rightarrow M$ be any section of the projection p . From (9) it follows that there exists $\mu_i \in F$ such that

$$s(f'_i) - \sum_{2 \leq j < i} a_{ij} e_j = \mu_i e_1.$$

Applying Lemma 2, we can choose $b_i \in A$ such that

$$\sum_{\sigma \in \Sigma} \left| \frac{\mu_i}{n_i} - b_i \right|_\sigma \leq C_2.$$

Define $t : M' \rightarrow M$ by the formulae

$$t(x) = s(x) - a(x) b_i e_1$$

whenever $x \in L'_i$, hence

$$n_i x = a(x) f'_i,$$

for some $a(x) \in A$, $2 \leq i \leq N$. If we take $f_i = t(f'_i)$, we get

$$f_i = s(f'_i) - n_i b_i e_1 = \sum_{2 \leq j < i} a_{ij} e_j + (\mu_i - n_i b_i) e_1$$

and, for all $\sigma \in \Sigma$,

$$|\mu_i - n_i b_i|_\sigma \leq n_i C_2 \leq C_1 C_2.$$

We define $a_{i1} = \mu_i - n_i b_i$ and $L_i = t(L'_i)$. Then

$$M = L_1 \oplus \cdots \oplus L_N$$

satisfies our induction hypothesis:

$$\begin{aligned} \#(L_i/A f_i) &\leq C_1 \\ f_i &= \sum_{1 \leq j \leq i} a_{ij} e_j, \\ |a_{ij}|_\sigma &\leq C_1 C_2 \quad \text{when } j < i, \end{aligned}$$

and

$$|a_{ii}|_\sigma \leq C_1^{1/r} C_3, \quad \text{for all } \sigma \in \Sigma, i = 1, \dots, N.$$

Since

$$\|e_i\| \leq 1 \quad \text{for all } i = 1, \dots, N,$$

this implies

$$\|f_i\| \leq (i - 1) C_1 C_2 + C_1^{1/r} C_3.$$

q.e.d.

2.2

LEMMA 6. *Let $I \subset A$ be a nontrivial ideal. There exists a set of representatives $\mathcal{R} \subset A$ of A modulo I such that, for any x in \mathcal{R} ,*

$$\sum_{\sigma \in \Sigma} |x|_\sigma \leq C_2 \left(\frac{r+3}{4} \right) N(I),$$

where $N(I) = \#(A/I)$ and C_2 is the constant in Lemma 2.

PROOF. According to the proof of Lemma 2, the \mathbf{Z} -module A contains a basis of r elements e_1, \dots, e_r such that

$$\sum_{\sigma} |e_i|_\sigma \leq \mu_r \leq \frac{2}{r} C_2.$$

Therefore, by Lemma 5 applied to the field \mathbf{Q} , in which case $C_1 = C_3 = 1$ and $C_2 = 1/2$, there exists a basis (f_i) of A over \mathbf{Z} such that,

$$\sum_{\sigma \in \Sigma} |f_i|_\sigma \leq \frac{2}{r} C_2 \left(\frac{i-1}{2} + 1 \right).$$

Since the integer $n = N(I)$ belongs to I , the map $A/I \rightarrow A/nA$ is injective and we can choose \mathcal{R} among those

$$x = \sum_{i=1}^r x_i f_i$$

such that $x_i \in \mathbf{Z}$ and $|x_i| \leq n/2$. In that case, if $x \in \mathcal{R}$, we have

$$\sum_{\sigma \in \Sigma} |x|_\sigma \leq \frac{n}{2} \sum_{\sigma, i} |f_i|_\sigma \leq n C_2 \frac{r+3}{4}.$$

q.e.d.

2.3

LEMMA 7. Let \overline{M} be an hermitian lattice and assume that $M = L_1 \oplus L_2$ is the direct sum of two lattices of rank one. Let $f_i \in L_i$ be a non zero vector, and $n_i = \#(L_i/A f_i)$, $i = 1, 2$. Then there exists a vector $e_1 \in M$, and an isomorphism

$$\psi : A e_1 \oplus L \rightarrow M$$

such that L contains a vector e_2 with

$$\#(L/A e_2) \leq n_1 n_2,$$

$$\|e_1\| \leq n_2 C_2 \|f_1\| + \left(1 + C_2^2 \frac{r+3}{4} n_1^r\right) \|f_2\|,$$

and

$$\|\psi(e_2)\| \leq n_2 \|f_1\| + C_2 \frac{r+3}{4} n_1^r \|f_2\|.$$

PROOF. The algebraic content of this lemma is [9], Lemma 1.7, p. 12. To control the norms in this proof we first define an isomorphism

$$u_i : L_i \rightarrow I_i$$

where I_i is an ideal of A . If $x \in L_i$, $u_i(x) \in A$ is the unique element such that

$$n_i x = u_i(x) f_i, \quad i = 1, 2.$$

In particular $n_i = u_i(f_i)$.

Next, we choose an ideal J_1 in the class of I_1 which is prime to I_2 . According to [9], proof of Lemma 1.8, we can choose

$$J_1 = \frac{x_0}{a_0} I_1,$$

where a_0 is any element of $I_1 - \{0\}$ and x_0 belongs to a set of representatives of A modulo $I_1 J$, where $I_1 J = a_0 A$.

According to Lemma 6 we can assume that

$$\sum_{\sigma \in \Sigma} |x_0|_{\sigma} \leq C_2 \left(\frac{r+3}{4}\right) N(I_1 J) = C_2 \left(\frac{r+3}{4}\right) N(a_0).$$

The composite isomorphism

$$v_1 : L_1 \rightarrow J_1 \rightarrow I_1$$

maps f_1 to $n_1 x_0/a_0$. We choose $a_0 = n_1$, hence $v_1(f_1) = x_0$ and

$$\sum_{\sigma \in \Sigma} |x_0|_{\sigma} \leq C_2 \left(\frac{r+3}{4}\right) n_1^r.$$

The direct sum of the inverses of v_1 and u_2 is an isomorphism

$$\varphi : J_1 \oplus I_2 \xrightarrow{\sim} L_1 \oplus L_2 = M .$$

Since J_1 and I_2 are prime to each other we have an exact sequence (as in [9] loc.cit.)

$$0 \longrightarrow J_1 I_2 \longrightarrow J_1 \oplus I_2 \xrightarrow{p} A \longrightarrow 0$$

where p is the sum in A . Let

$$s : A \longrightarrow J_1 \oplus I_2$$

be any section of p and let $\alpha \in J_1$ be such that

$$s(1) = (\alpha, 1 - \alpha) .$$

Let $\alpha = \lambda n_2 x_0$ with $\lambda \in F$. Applying Lemma 2, we choose $a \in A$ such that

$$\sum_{\sigma \in \Sigma} |\lambda - a|_{\sigma} \leq C_2 .$$

Since $n_2 x_0$ lies in $J_1 I_2$ the element

$$\beta = \alpha - a n_2 x_0 = (\lambda - a) n_2 x_0$$

lies in J_1 , and $1 - \beta$ lies in I_2 . Since

$$\beta = v_1((\lambda - a) n_2 f_1)$$

and

$$1 - \beta = u_2 \left(\frac{1}{n_2} - (\lambda - a) x_0 f_2 \right)$$

we get

$$\begin{aligned} \|\varphi(\beta, 1 - \beta)\| &\leq \|(\lambda - a) n_2 f_1\| + \left\| \left(\frac{1}{n_2} - (\lambda - a) x_0 \right) f_2 \right\| \\ &\leq n_2 C_2 \|f_1\| + \left(1 + C_2^2 \left(\frac{r+3}{4} \right) n_1^r \right) \|f_2\| . \end{aligned}$$

We let $e_1 = \varphi(\beta, 1 - \beta)$. On the other hand we define

$$L = J_1 I_2 (\simeq L_1 \otimes L_2)$$

and map L to M by the composite map

$$L \xrightarrow{i} J_1 \oplus I_2 \xrightarrow{\varphi} M$$

where $i(x) = (x, -x)$. We choose

$$e_2 = n_2 x_0 \in L$$

so that $\varphi \circ i(e_2) = (n_2 v_1(f_1), x_0 u_2(f_2))$ has norm

$$\|\varphi \circ i(e_2)\| \leq n_2 \|f_1\| + C_2 \left(\frac{r+3}{4} \right) n_1^r \|f_2\|.$$

Furthermore we have isomorphisms

$$L \oplus A \xrightarrow{(i,s)} J_1 \oplus I_2 \xrightarrow{\varphi} M$$

and

$$\#(L/A e_2) = \#(J_1 I_2/A e_2) \leq \#(J_1/A x_0) \times \#(I_2/A n_2) = n_1 n_2.$$

q.e.d.

2.4

PROPOSITION 1. *Let \overline{M} be a rank N hermitian free A -module such that its unit ball contains a basis of $M \otimes_A F$. Then M has a basis (e_1, \dots, e_N) such that*

$$\|e_i\| \leq B_i$$

with $B_i = (i-1)C_2 + C_3$, $i = 1, \dots, N$, when A is principal and

$$B_i = (1 + C_1 C_2)(N C_2 + C_3) \left(1 + C_2 \frac{r+3}{4} \right)^{\log_2(N)+2} C_1^{2(r+1)N/i}$$

in general. Here $\log_2(N)$ is the logarithm of N in base 2.

PROOF. When A is principal, $C_1 = 1$ and Proposition 1 follows from Lemma 5.

In general Lemma 5 tells us that

$$M = L_1 \oplus \dots \oplus L_N$$

and L_i contains a vector f_i with $\#(L_i/A f_i) \leq C_1$ and

$$\|f_i\| \leq C_1((i-1)C_2 + C_3) \leq C_1(N C_2 + C_3).$$

Let $k > 1$ be an integer and $\lambda > 0$ be a real number. We shall prove by induction N that, if M has a decomposition as above with

$$\#(L_i/A f_i) \leq k$$

and

$$\|f_i\| \leq k \lambda,$$

then M has a basis (e_1, \dots, e_N) such that

$$\|e_i\| \leq \lambda \left(\frac{1}{k} + C_2 \right) \left(1 + C_2 \frac{r+3}{4} \right)^t k^{(r+1)(1+2+\dots+2^t)}, \quad (10)$$

for all $i = 1, \dots, N$, where $t \geq 1$ is such that

$$\frac{N}{2^t} < i \leq \frac{N}{2^{t-1}}.$$

The case $N \leq 2$ follows from Lemma 7. If $N > 2$, let N' be the integral part of $N/2$. Applying Lemma 7 to every direct sum $L_i \oplus L_{N-i}$, $N/2 < i \leq N$, we get

$$M = M' \oplus \left(\bigoplus_{i=N'+1}^N A e_i \right)$$

with

$$\begin{aligned} \|e_i\| &\leq k\lambda \left(1 + C_2 k + C_2^2 \frac{r+3}{4} k^r \right) \\ &\leq \lambda \left(\frac{1}{k} + C_2 \right) \left(1 + C_2 \frac{r+3}{4} \right) k^{r+1} \end{aligned}$$

and M' is free, $M' = \bigoplus_{i=0}^{N'} L'_i$, and each L'_i contains a vector f'_i such that

$$[L'_i : A f'_i] \leq k^2$$

and

$$\|f'_i\| \leq \lambda \left(1 + C_2 \frac{r+3}{4} \right) k^{r+1}.$$

By the induction hypothesis, M' has a basis (e_i) , $1 \leq i \leq N'$, such that

$$\|e_i\| \leq \left(1 + C_2 \frac{r+3}{4} \right) k^{(r+1)} \left(\frac{1}{k^2} + C_2 \right) \left(1 + C_2 \frac{r+3}{4} \right)^t (k^2)^{(r+1)(1+\dots+2^t)}$$

whenever

$$\frac{N'}{2^t} < i \leq \frac{N'}{2^{t-1}}.$$

If

$$\frac{N}{2^{t+1}} < i \leq \frac{N}{2^t},$$

this inequality implies

$$\|e_i\| \leq \lambda \left(\frac{1}{k} + C_2 \right) \left(1 + C_2 \frac{r+3}{4} \right)^{t+1} k^{(r+1)(1+\dots+2^{t+1})}.$$

Therefore M satisfies the induction hypothesis (10).

Since

$$1 + 2 + \dots + 2^t = 2^{t+1} - 1 \leq \frac{2N}{i}$$

and $t \leq \log_2(N) + 1$, Proposition 1 follows by taking $k = C_1$ and

$$\lambda = C_1(N C_2 + C_3)$$

in (10).

q.e.d.

2.5

Let \overline{M} be a rank N hermitian free A -module. We let

$$m(h) = \inf \{h(x), x \in M - \{0\}\}$$

be the minimum value of h on $M - \{0\}$ and

$$M(h) = \{x \in M / h(x) = m(h)\}$$

be the (finite) set of minimal vectors of M . Let ω_N be the standard volume of the unit ball in \mathbf{R}^N .

PROPOSITION 2. *Let $\overline{M} = (M, h)$ be as above. Assume that $m(h) = 1$ and that $M(h)$ spans the F -vector space $M \otimes_A F$. Then M has a basis f_1, \dots, f_N such that any $x \in M(h)$ is of the form*

$$x = \sum_{i=1}^N y_i f_i$$

with

$$\sum_{\sigma \in \Sigma} |y_i|_{\sigma}^2 \leq T_i,$$

$$T_i = r^{rN} C_3^{2rN+2} \gamma^N \prod_{j \neq i} B_j^2,$$

and

$$\gamma = 4^{r_1+r_2} \omega_N^{-2r_1/N} \omega_{2N}^{-2r_2/N} D.$$

PROOF. From Proposition 1 we know that M has a basis (e_1, \dots, e_N) with $\|e_i\| \leq B_i$. Let $x \in M(h)$ be a minimal vector and (x_i) its coordinates in the basis (e_i) .

Fix $i \in \{1, \dots, N\}$ and $\sigma \in \Sigma$. Consider the square matrix

$$H_i = (h_{\sigma}(v_k, v_{\ell})),$$

where $v_k = e_k$ if $k \neq i$ and $v_i = x$. Furthermore, let

$$H_{\sigma} = (h_{\sigma}(e_k, e_{\ell})).$$

Since

$$|x_i|_{\sigma}^2 = \det(H_i) \det(H_{\sigma})^{-1}$$

the Hadamard inequality implies

$$|x_i|_{\sigma}^2 \leq h_{\sigma}(x) \prod_{j \neq i} h_{\sigma}(e_j) \det(H_{\sigma})^{-1}.$$

For any unit $u \in A^*$ we can replace e_i by $u^{-1} e_i$, and x_i by $y_i = u x_i$. We then have

$$\sum_{\sigma \in \Sigma} |y_i|_{\sigma}^2 \leq \sum_{\sigma \in \Sigma} h_{\sigma}(x) \prod_{j \neq i} h_{\sigma}(e_j) |u|_{\sigma}^2 \det(H_{\sigma})^{-1}. \tag{11}$$

Applying Lemma 3 to $\lambda_{\sigma} = \det(H_{\sigma})^{-1/2}$ we find u such that, for all $\sigma \in \Sigma$,

$$|u|_{\sigma}^2 \det(H_{\sigma})^{-1} \leq C_3^2 \prod_{\sigma \in \Sigma} \det(H_{\sigma})^{-1}. \tag{12}$$

Since $\sum_{\sigma} h_{\sigma}(x) = 1$ and $h_{\sigma}(e_j) \leq \|e_j\|^2 \leq B_j^2$, we deduce from (11) and (12) that

$$\sum_{\sigma \in \Sigma} |y_i|_{\sigma}^2 \leq C_3^2 \cdot \prod_{j \neq i} B_j^2 \cdot \prod_{\sigma \in \Sigma} \det(H_{\sigma})^{-1}. \tag{13}$$

According to Icaza [4], Theorem 1, there exists $z \in L$ such that

$$\prod_{\sigma \in \Sigma} h_{\sigma}(z) \leq \gamma \prod_{\sigma \in \Sigma} \det(H_{\sigma})^{1/N}$$

with

$$\gamma = 4^{r_1+r_2} \omega_N^{-2r_1/N} \omega_{2N}^{-2r_2/N} D.$$

Using Lemma 3 again and the fact that $m(h) = 1$, we find $v \in A^*$ such that

$$\begin{aligned} 1 &\leq h(vz) \leq r C_3^2 \prod_{\sigma \in \Sigma} h_{\sigma}(z)^{1/r} \\ &\leq r C_3^2 \gamma^{1/r} \prod_{\sigma \in \Sigma} \det(H_{\sigma})^{1/rN}. \end{aligned}$$

From this it follows that

$$\prod_{\sigma \in \Sigma} \det(H_{\sigma})^{-1} \leq (r C_3^2)^{rN} \gamma^N \tag{14}$$

and Proposition 2 follows from (13) and (14).

2.6

To count the number of vectors in $M(h)$ using Proposition 2 we shall apply the following lemma :

LEMMA 8. *The number of elements a in A such that*

$$\sum_{\sigma \in \Sigma} |a|_{\sigma}^2 \leq T$$

is at most

$$B(T) = \text{Sup}(T^{r/2} 2^{r+3}, 1).$$

PROOF. When $r_2 > 0$, this follows from [7], V § 1, Theorem 0, p. 102, by noticing that one can take $C_3 = 2^{r+3}$ in loc.cit. When $r_2 = 0$, the argument is similar.

3 REDUCTION THEORY

3.1

Fix an integer $N \geq 2$. Let

$$\Gamma = \text{GL}_N(A)$$

and

$$G = \text{GL}_N(F \otimes_{\mathbf{Q}} \mathbf{R}).$$

On the standard lattice $L_0 = A^N$ consider the hermitian metric h_0 defined by

$$h_0(x, y) = \sum_{\sigma \in \Sigma} \sum_{i=1}^N x_{i\sigma} \overline{y_{i\sigma}}$$

for all vectors $x = (x_{i\sigma})$ and $y = (y_{i\sigma})$ in $L_0 \otimes_{\mathbf{Z}} \mathbf{C} = (\mathbf{C}^N)^{\Sigma}$. Any $g \in G$ defines an hermitian metric $h = g(h_0)$ on L_0 by the formula

$$g(h_0)(x, y) = h_0(g(x), g(y)).$$

Let K be the stabilizer of h_0 and G and $X = K \backslash G$. We can view each $h \in X$ as a metric on L_0 .

Following Ash [1], we say that a finite subset $M \subset L_0$ is *well-rounded* when it spans the F -vector space $L_0 \otimes_A F$. We let $\widetilde{W} \subset X$ be the space of metrics h such that $m(h) = 1$ and $M(h)$ is well-rounded. Given a well-rounded set $M \subset L_0$ we let $C(M) \subset \widetilde{W}$ be the set of metrics h such that

- $h(x) = 1$ for all $x \in M$
- $h(x) > 1$ for all $x \in L_0 - (M \cup \{0\})$.

As explained in [1], proof of (iv), pp. 466-467, $C(M)$ is either empty or topologically a cell, and the family of closed cells $\overline{C(M)}$ gives a Γ -invariant cellular decomposition of \widetilde{W} , such that

$$\overline{C(M)} = \coprod_{M' \supset M} C(M').$$

Furthermore \widetilde{W}/Γ is compact, of dimension $\dim(X) - N$.

3.2

PROPOSITION 3. i) For any integer $k \geq 0$, the number of cells of codimension k in \widetilde{W} is at most

$$c(k, N) = \binom{a(N)}{N+k}$$

where

$$a(N) = 2^{N(r+3)} \left(\prod_{i=1}^N T_i \right)^{r/2},$$

and T_i is as in Proposition 2.

ii) Given a cell in \widetilde{W} , its number of codimension one faces is at most $a(N)^{N+1}$.

PROOF. Let Φ be the set of vectors $x = (x_i)$ in A^N such that, for all $i = 1, \dots, N$,

$$\sum_{\sigma \in \Sigma} |x_i|_{\sigma}^2 \leq T_i.$$

Given $h \in \widetilde{W}$, Proposition 2 says that we can find a basis (f_i) of L_0 such that any x in $M(h)$ has its coordinates (x_i) bounded as above. If $\gamma \in \Gamma$ is the matrix mapping the standard basis of A^N to (f_i) , this means that $M(\gamma(h)) = \gamma^{-1}(M(h))$ is contained in Φ .

Let $\overline{C(M)}$ be a nonempty closed cell of codimension k in \widetilde{W} . For any $x \in L_0$, the equation $h(x) = 1$ defines a real affine hyperplane in the set of $N \times N$ hermitian matrices with coefficients in $(F \otimes_{\mathbf{Q}} \mathbf{C})^+$. The equations $h(x) = 1$, $x \in M$, may not be linearly independent, but, since $\overline{C(M)}$ has codimension k , M has at least $N+k$ elements. And since $M \subset M(h)$ for some $h \in \widetilde{W}$, there exists $\gamma \in \Gamma$ such that $\gamma^{-1}(M)$ is contained in Φ . Therefore, modulo the action of Γ , there are at most $\binom{\text{card}(\Phi)}{N+k}$ cells $\overline{C(M)}$ of codimension k . From Lemma 7 we know that

$$\text{card}(\Phi) \leq a(N),$$

therefore i) follows.

To prove ii), consider a cell $\overline{C(M)}$ and a codimension one face $\overline{C(M')}$ of $\overline{C(M)}$. We can write $M' = M \cup \{x\}$ for some vector x and there exists $\gamma \in \Gamma$ such that $\gamma(M') \subset \Phi$. Since M is well-rounded, the matrix γ is entirely determined by the set of vectors $\gamma(M)$, i.e. there are at most $\text{card}(\Phi)^N$ matrices γ such that $\gamma(M) \subset \Phi$. Since $\gamma(x) \in \Phi$, there are at most $\text{card}(\Phi)^{N+1}$ vectors x as above. q.e.d.

3.3

LEMMA 9. Let $\gamma \in \Gamma - \{1\}$ and p be a prime number such that $\gamma^p = 1$. Then

$$p \leq 1 + \text{Sup}(r, N).$$

PROOF. Since γ is non trivial we have $P(\gamma) = 0$ where P is the cyclotomic polynomial

$$P(x) = X^{p-1} + X^{p-2} + \cdots + 1.$$

If F does not contain the p -th roots of one, P is irreducible, and therefore it divides the characteristic polynomial of the matrix γ over F , hence $p - 1 \leq N$. Otherwise, F contains $Q(\mu_p)$, which is of degree $p - 1$, therefore $p - 1 \leq r$.

4 THE MAIN RESULTS

4.1

For any integer $n > 0$ and any finite abelian group A we let $\text{card}_n(A)$ be the largest divisor of the integer $\#(A)$ such that no prime $p \leq n$ divides $\text{card}_n(A)$. Let $N \geq 2$ be an integer. We keep the notation of § 3 and we let

$$\tilde{w} = \dim(X) - N = r_1 \frac{N(N+1)}{2} + r_2 N^2 - N$$

be the dimension of \widetilde{W} . For any $k \leq \tilde{w}$ we define

$$h(k, N) = a(N)^{(N+1)c(\tilde{w}-k-1, N)},$$

where $c(\cdot, N)$ and $a(N)$ are defined in Proposition 3.

THEOREM 1. *The torsion subgroup of the homology of $\text{GL}_N(A)$ is bounded as follows*

$$\text{card}_{1+\text{sup}(r, N)} H_k(\text{GL}_N(A), \mathbf{Z})_{\text{tors}} \leq h(k, N).$$

PROOF. We know from [1] that \widetilde{W} is contractible and the stabilizer of any $h \in \widetilde{W}$ is finite. From Lemma 9 it follows that, modulo $\mathcal{S}_{1+\text{sup}(r, N)}$, the homology of $\Gamma = \text{GL}_N(A)$ is the homology of a complex (C, ∂) , where C_k is the free abelian group generated by a set of Γ -representatives of those k -dimensional cells c in \widetilde{W} such that the stabilizer of c does not change its orientation ([2], VII). According to Proposition 3, the rank of C_k is at most $c(\tilde{w} - k, N)$ and any cell of \widetilde{W} has at most $a(N)^{N+1}$ faces. Theorem 1 then follows from a general result of Gabber ([13], Proposition 3 and equation (18)).

4.2

For any integer $m \geq 1$ let

$$k(m) = h(m, 2m + 1).$$

Denote by $K_m(A)$ the m -th algebraic K -group of A .

THEOREM 2. *The following inequality holds*

$$\text{card}_{\text{sup}(r+1, 2m+2)} K_m(A)_{\text{tors}} \leq k(m).$$

PROOF. As in [13], Theorem 2, we consider the Hurewicz map

$$H : K_m(A) \rightarrow H_m(\text{GL}(A), \mathbf{Z}),$$

the kernel of which lies in \mathcal{S}_n , $n \leq (m + 1)/2$. Since, according to Maazen and Van der Kallen,

$$H_m(\text{GL}(A), \mathbf{Z}) = H_m(\text{GL}_N(A), \mathbf{Z})$$

when $N \geq 2m + 1$, Theorem 2 is a consequence of Theorem 1.

4.3

Let p be an odd prime and $n \geq 2$ an integer. For any $\nu \geq 1$ denote by $\mathbf{Z}/p^\nu(n)$ the étale sheaf $\mu_{p^\nu}^{\otimes n}$ on $\text{Spec}(A[1/p])$, and let

$$H^2(\text{Spec}(A[1/p]), \mathbf{Z}_p(n)) = \varinjlim_{\nu} H^2(\text{Spec}(A[1/p]), \mathbf{Z}_{p^\nu}(n)).$$

From [12], we know that this group is finite and zero for almost all p .

THEOREM 3. *The following inequality holds*

$$\prod_{\substack{p \geq 4n-1 \\ p \geq r+2}} \text{card } H^2(\text{Spec}(A[1/p]), \mathbf{Z}_p(n)) \leq k(2n - 2).$$

PROOF. According to [12], the cokernel of the Chern class

$$c_{n,2} : K_{2n-2}(A) \rightarrow H^2(\text{Spec}(A[1/p]), \mathbf{Z}_p(n))$$

lies in \mathcal{S}_{n+1} for all p . Furthermore, Borel proved that $K_{2m-2}(A)$ is finite. Therefore Theorem 3 follows from Theorem 2.

4.4

By Lemmas 1 to 7 and Propositions 1 to 3, the constant $k(m)$ is explicitly bounded in terms of m, r and D . We shall now simplify this upper bound.

PROPOSITION 4. i) $\log \log k(m) \leq 220 m^4 \log(m) r^{4r} \sqrt{D} \log(D)^{r-1}$

ii) *If F has class number one,*

$$\log \log k(m) \leq 210 m^4 \log(m) r^{4r} \sqrt{D} \log(D)^{r-1}$$

iii) If $F = \mathbf{Q}(\sqrt{-D})$ is imaginary quadratic

$$\log \log k(m) \leq 1120 m^4 \log(m) \log(D);$$

if furthermore F has class number one

$$\log \log k(m) \leq 510 m^4 \log(m) \log(D).$$

iv) When $F = \mathbf{Q}$ and $m \geq 9$

$$\log \log k(m) \leq 8 m^4 \log(m);$$

furthermore

$$\log \log k(7) \leq 40\,545$$

and

$$\log \log k(8) \leq 70\,130.$$

PROOF. By definition

$$k(m) = h(m, 2m+1) = a(N)^{(N+1)c(\tilde{w}-m-1, N)}$$

with $N = 2m+1$ and

$$c(\tilde{w}-m-1, N) = \binom{a(N)}{N + \tilde{w} - m - 1}.$$

Since

$$\begin{aligned} N + \tilde{w} - m - 1 &= r_1 \frac{N(N+1)}{2} + r_2 N^2 - m - 1 \\ &\leq 2rm^2 + 3rm + r - 2m - 1 \end{aligned}$$

and since $a(2m+1)$ is very big, we get

$$\begin{aligned} \log \log k(m) &\leq (2rm^2 + 3rm + r - 2m - 1) \log a(2m+1) \\ &\quad + \log(2m+2) + \log \log a(2m+1) \\ &\leq r(2m^2 + 3m + 1) \log a(2m+1). \end{aligned} \tag{15}$$

From Proposition 3 and Proposition 2 we get

$$a(N) = 2^{N(r+3)} \left(\prod_{i=1}^N T_i \right)^{r/2}, \tag{16}$$

and

$$\prod_{i=1}^N T_i = (r^{rN} \gamma^N C_3^{2rN+2})^N \prod_{i=1}^N B_i^{N-1}. \tag{17}$$

According to Proposition 1

$$\prod_{i=1}^N B_i = \left[(1 + C_1 C_2)(N C_2 + C_3) \left(1 + C_2 \frac{r+3}{4} \right)^{\log_2(N)+2} \right]^N \cdot C_1^{2(r+1)N H_N}, \quad (18)$$

where

$$H_N = \sum_{i=1}^N \frac{1}{i} \leq 1 + \log(N).$$

Assume $s \neq 0$. Then the upper bound C_3^* we get from Lemmas 3 and 4 for C_3 is much bigger than C_2 . Therefore

$$\log(N C_2 + C_3) \leq \log(N) + \log(C_3^*). \quad (19)$$

We deduce from (15), (16), (17), (18), (19) that

$$\log \log k(m) \leq X_1 + X_2$$

with

$$X_1 = r(2m^2 + 3m + 1) \frac{r}{2} (N(2rN + 2) + N(N - 1)) \log(C_3^*)$$

and

$$\begin{aligned} X_2 = & r(2m^2 + 3m + 1) \left(N(r + 3) \log(2) \right. \\ & + \frac{r}{2} N \left(N \log(\gamma) + (N - 1) \left[\log(1 + C_1 C_2) + \log(N) \right. \right. \\ & + (\log_2(N) + 2) \log \left(1 + C_2 \frac{r+3}{4} \right) \\ & \left. \left. + 2(r + 1)(1 + \log(N)) \log(C_1) \right] \right) \Big). \end{aligned} \quad (20)$$

Since $s \leq r - 1$, Lemma 3 and Lemma 4 imply

$$\log(C_3^*) \leq 11r^2(r - 1)(4r(\log 3r)^3)^{r-2} 2^{r-1} \sqrt{D} \log(D)^{r-1},$$

from which it follows that

$$X_1 \leq 208 \log(m) m^4 r^{4r} \sqrt{D} \log(D)^{r-1}$$

when $m \geq 2$ and $r \geq 2$.

To evaluate X_2 first notice that

$$4\omega_N^{-2/N} \leq 1 + N/4$$

by [10], II, (1.5), Remark, hence

$$\begin{aligned} \log(\gamma) &\leq r_1 \log\left(1 + \frac{N}{4}\right) + 2r_2 \log\left(1 + \frac{N}{2}\right) + \log(D) \\ &\leq r \log(N) + \log(D) \end{aligned} \quad (21)$$

since $N \geq 5$.

By the Stirling formula and Lemma 1, if $r \geq 2$,

$$\begin{aligned} \log(C_1) &= \log(r!) - r \log(r) + r_2 \log\left(\frac{4}{\pi}\right) + \frac{1}{2} \log(D) \\ &\leq 1 + \frac{1}{2} \log(r) + \frac{1}{2} \log(D), \end{aligned} \quad (22)$$

$$\log\left(1 + C_2 \frac{r+3}{4}\right) \leq \text{Sup}\left(\log(C_2) + \log\left(\frac{r+3}{4}\right) + 1, \log(2)\right),$$

where

$$\begin{aligned} \log(C_2) + \log\left(\frac{r+3}{4}\right) &\leq r \log(4) - (r-2) \log(r) - \log(r!) \\ &\quad + \log\left(\frac{r+3}{4}\right) + \frac{1}{2} \log(D) \\ &\leq 2.4 + \frac{1}{2} \log(D), \end{aligned}$$

so that

$$\log\left(1 + C_2 \frac{r+3}{4}\right) \leq 3.4 + \frac{1}{2} \log(D). \quad (23)$$

We also have

$$\log(1 + C_1 C_2) \leq \text{Sup}(1 + \log(C_1) + \log(C_2), \log(2))$$

and

$$\begin{aligned} \log(C_1) + \log(C_2) &\leq -r \log(r) + r - (r-2) \log(r) + r \log(4) + \log(D) \\ &\leq 3.4 + \log(D), \end{aligned}$$

so that

$$\log(1 + C_1 C_2) \leq 4.4 + \log(D). \quad (24)$$

From (20), (21), (22), (23), (24) we get

$$X_2 \leq a \log(D) + b$$

with

$$a = r(2m^2 + 3m + 1)(2m + 1) \left(\frac{r}{2} ((2m + 1) + 2m + m \log_2(2m + 1) + m + 2m(r + 1)(1 + \log(2m + 1))) \right) \leq 75 r^3 m^4 \log(m)$$

if $r \geq 2$ and $m \geq 2$.

Finally

$$b = r(2m^2 + 3m + 1)(2m + 1) \left((r + 3) \log(2) + \frac{r}{2} (2m + 1) r (\log(r) + \log(2m + 1)) + \frac{r}{2} (2m) \left(4.4 + \log(2m + 1) + 3.4(\log_2(2m + 1) + 2) + 2(r + 1)(1 + \log(2m + 1)) \left(1 + \frac{1}{2} \log(r) \right) \right) \right) \leq 148 r^4 m^4 \log(m)$$

when $r \geq 2$ and $m \geq 2$.

Therefore

$$\begin{aligned} \log \log k(m) &\leq 208 \log(m) m^4 r^{4r} \sqrt{D} \log(D)^{r-1} + 75 r^3 m^4 \log(m) \log(D) \\ &\quad + 148 r^4 m^4 \log(m) \leq 220 m^4 \log(m) r^{4r} \sqrt{D} \log(D)^{r-1} \end{aligned}$$

when m , r and D are at least 2. This proves i).

If we assume that A is principal, we can take $C_1 = 1$ in Lemma 1 and $B_i = (i - 1)C_2 + C_3$ in Proposition 1. Since $C_2 < C_3$ we get

$$\log \left(\prod_{i=1}^N B_i \right) \leq \log(N!) + N \log(C_3)$$

and

$$\log \log k(m) \leq X_1 + X_3$$

where

$$\begin{aligned} X_3 &= r(2m^2 + 3m + 1) \left[(r + 3)(2m + 1) \log(2) + \frac{r^2}{2} (2m + 1)^2 \log(r) \right. \\ &\quad \left. + \frac{r}{2} (2m + 1)^2 \log(\gamma) + \frac{r}{2} (2m) \log((2m + 1)!) \right] \\ &\leq 6 m^4 r^2 \log(D) + 2 r^{4r} m^4 \log(m). \end{aligned}$$

Therefore

$$X_1 + X_3 \leq 210 m^4 \log(m) r^{4r} \sqrt{D} \log(D)^{r-1}.$$

Assume now that $r_1 + r_2 = 1$. Then $C_3 = 1$ and the term X_1 disappears from the above computation. Assume first that $F = \mathbf{Q}(\sqrt{-D})$. Since $r_2 = 1$ and $r_1 = 0$ we get

$$\log \log k(m) \leq (4m^2 + 3m + 1) \log a(2m + 1).$$

Furthermore (18) becomes

$$\prod_{i=1}^N B_i \leq \left[(1 + C_1 C_2)(1 + N C_2) \left(1 + \frac{5}{4} C_2\right)^{\log_2(N)+2} \right]^N \cdot C_1^{6N(1+\log(N))}.$$

Therefore

$$\begin{aligned} \log \log k(m) &\leq (4m^2 + 3m + 1) \left[5N \log(2) + 2N^2 \log(2) \right. \\ &\quad + N^2 \log(\gamma) + N(N-1) \left[\log(1 + C_1 C_2) \right. \\ &\quad + \log(1 + N C_2) + (\log_2(N) + 2) \log \left(1 + \frac{5}{4} C_2\right) \left. \right] \\ &\quad \left. + 6N(1 + \log N) \log(C_1) \right], \end{aligned}$$

with $N = 2m + 1$. We have now

$$\begin{aligned} \gamma &\leq \left(1 + \frac{N}{2}\right)^2 D, \\ C_1 &= \frac{2}{\pi} \sqrt{D} \quad \text{and} \quad C_2 = \frac{\pi}{2} \sqrt{D}. \end{aligned}$$

This implies

$$\log \log k(m) \leq 597 m^4 \log(m) + 256 m^4 \log(m) \log(D) \leq 1120 m^4 \log(m) \log(D).$$

If $F = \mathbf{Q}(\sqrt{-D})$ is principal we can take $C_1 = 1$ and $B_i = (i-1)C_2 + 1$. We get

$$\log \log k(m) \leq 510 m^4 \log(m) \log(D).$$

Finally, assume that $F = \mathbf{Q}$. Then

$$B_i = \frac{i+1}{2} \quad \text{since} \quad C_2 = \frac{1}{2}, \quad \text{and} \quad \gamma \leq 1 + \frac{N}{4}.$$

Therefore

$$\begin{aligned} \log \log k(m) &\leq (2m^2 + 2m + 1) \log a(2m + 1) \\ &\leq (2m^2 + 2m + 1) \left[4N \log(2) + \frac{N^2}{2} \log \left(1 + \frac{N}{4}\right) \right. \\ &\quad \left. + \frac{N-1}{2} \log \left(\prod_{i=1}^N \frac{i+1}{2} \right) \right] \\ &\leq 8m^4 \log(m) \end{aligned}$$

if $m \geq 9$. We can also estimate $k(7)$ and $k(8)$ from this inequality above. This proves iv).

5 DISCUSSION

5.1

The upper bound in Theorem 2 and Proposition 4 seems much too large. When $m = 0$, $\text{card } K_0(A)_{\text{tors}}$ is the class number $h(F)$, which is bounded as follows:

$$h(F) \leq \alpha \sqrt{D} \log(D)^{r-1}, \quad (25)$$

for some constant $\alpha(r)$ [11], Theorem 4.4, p. 153. Furthermore, when $F = \mathbf{Q}$, $m = 2n - 2$ and n is even, the Lichtenbaum conjecture predicts that $\text{card } K_{2n-2}(\mathbf{Z})$ is the order of the numerator of B_n/n , where B_n is the n -th Bernoulli number. The upper bound

$$B_n \leq n! \approx n^n$$

suggests, since the denominator of B_n/n is not very big, that $\text{card } K_m(\mathbf{Z})_{\text{tors}}$ should be exponential in m . We are thus led to the following:

CONJECTURE. *Fix $r \geq 1$. There exists positive constants α, β, γ such that, for any number field F of degree r on \mathbf{Q} ,*

$$\text{card } K_m(A)_{\text{tors}} \leq \alpha \exp(\beta m^\gamma \log D).$$

Furthermore, we expect that γ does not depend on r .

5.2

As suggested by A. Chambert-Loir, it is interesting to consider the analog in positive characteristic of the conjecture above. Let X be a smooth connected projective curve of genus g over the finite field with q elements, $\zeta_X(s)$ its zeta function and

$$P(t) = \prod_{i=1}^{2g} (1 - \alpha_i t),$$

where α_i are the roots of Frobenius acting on the first ℓ -adic cohomology group of X . When $n > 1$, it is expected that the finite group $K_{2n-2}(X)$ has order the numerator of $\zeta_X(1-n)$, i.e. $P(q^{n-1})$. Since $|\alpha_i| = q^{1/2}$ for all $i = 1 \cdots 2g$, we get

$$P(q^{n-1}) \leq (1 + q^{n-1/2})^{2g} \leq q^{2ng}.$$

In the analogy between number fields and function fields, the genus g is known to be an analog of $\log(D)$. Therefore the bound above is indeed analogous to the conjecture in §5.1.

5.3

The upper bound for $k(m)$ in Proposition 4 i) is twice exponential in D . One exponential is due to our use of Lemma 3, where C_3 is exponential in D . Maybe this can be improved in general, and not only when $s = 0$.

The exponential in D occurring in Proposition 4 ii) might be due to our use of the geometry of numbers. Indeed, if one evaluates the class number $h(F)$ by applying naively Minkowski's theorem (Lemma 1), the bound one gets is exponential in D ; see however [8], Theorem 6.5., for a better proof.

5.4

One method to prove (25) consists in combining the class number formula (see (7) and (8)) with a lower bound for the regulator $R(F)$. This suggests replacing the arguments of this paper by analytic number theory, to get good upper bounds for étale cohomology.

More precisely, let $n \geq 2$ be an integer, and let $\zeta_F(1-n)^*$ be the leading coefficient of the Taylor series of $\zeta_F(s)$ at $s = 1 - n$. Lichtenbaum conjectured that

$$\zeta_F(1-n)^* = \pm 2^{r_1} R_{2n-1}(F) \frac{\prod \text{card } H^2(\text{Spec}(A[1/p]), \mathbf{Z}_p(n))}{\prod_p \text{card } H^1(\text{Spec}(A[1/p]), \mathbf{Z}_p(n))_{\text{tors}}}, \quad (26)$$

where $R_{2n-1}(F)$ is the higher regulator for the group $K_{2n-1}(F)$. The equality (26) is known up a power of 2 when F is abelian over \mathbf{Q} [5], [6], [3].

The order of the denominator on the right-hand side of (26) is easy to evaluate, as well as $\zeta_F(1-n)^*$ (since it is related by the functional equation to $\zeta_F(n)$).

PROBLEM. *Can one find a lower bound for $R_{2n-1}(F)$?*

If such a problem could be solved, the equality (26) is likely to produce a much better upper bound for étale cohomology than Theorem 3. Zagier's conjecture suggests that this problem could be solved if one knew that the values of the n -logarithm on F are \mathbf{Q} -linearly independent.

5.5

To illustrate our discussion, let $F = \mathbf{Q}$ and $n = 5$. Then we have

$$H^2(\text{Spec}(\mathbf{Z}[1/p]), \mathbf{Z}_p(5))/p = C^{(p-5)},$$

where C is the class group of $\mathbf{Q}(\sqrt[p]{1})$ modulo p , and $C^{(i)}$ is the eigenspace of C of the i -th power of the Teichmüller character. Vandiver's conjecture predicts

that $C^{(p-5)} = 0$ when p is odd. It is true when $p \leq 4.10^6$. Theorem 3 and Proposition 4 tell us that

$$\prod_p H^2(\text{Spec}(\mathbf{Z}[1/p], \mathbf{Z}_p(5)) \leq k(8) \leq \exp \exp(70130).$$

If one could find either a better upper bound for the order of $K_8(\mathbf{Z})$ or a good lower bound for $R_9(\mathbf{Q})$, this would get us closer to the expected vanishing of $C^{(p-5)}$.

Notice that, using knowledge on $K_4(\mathbf{Z})$, Kurihara has proved that $C^{(p-3)} = 0$.

REFERENCES

- [1] A. Ash, Deformation retracts with lowest possible dimension of arithmetic quotients of self-adjoint homogeneous cones, *Math. Ann.* 225, no. 1, 69–76 (1977).
- [2] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, 87. Springer-Verlag, New York-Berlin, 1982. x+306 pp.
- [3] A. Huber, G. Kings, Bloch-Kato conjecture and main conjecture of Iwasawa theory for Dirichlet characters, preprint (2001).
- [4] M. I. Icaza, Hermite constant and extreme forms for algebraic number fields, *J. London Math. Soc.* (2) 55, no. 1, 11–22 (1997).
- [5] M. Kolster, T. Nguyen Quang Do, V. Fleckinger, Twisted S -units, p -adic class number formulas, and the Lichtenbaum conjectures, *Duke Math. J.* (3) 84, 679–717 (1996).
- [6] M. Kolster, T. Nguyen Quang Do, V. Fleckinger, Correction to “Twisted S -units, p -adic class number formulas, and the Lichtenbaum conjectures”, *Duke Math. J.* (3) 90, 641–643 (1997)
- [7] S. Lang, *Algebraic number theory*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont. 1970 xi+354 pp.
- [8] H. W. Lenstra, Jr., Algorithms in algebraic number theory, *Bull. AMS* 26, no. 2, 211–244 (1992).
- [9] J. Milnor, *Introduction to algebraic K-theory*, Annals of Mathematics Studies, No. 72. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971. xiii+184 pp.
- [10] J. Milnor and D. Husemoller: *Symmetric bilinear forms*, *Ergebnisse* 73, 1973, Springer-Verlag.
- [11] W. Narkiewicz, *Number theory*, Translated from the Polish by S. Kanemitsu. World Scientific Publishing Co., Singapore; distributed by Heyden & Son, Inc., Philadelphia, PA, 1983. xii+371 pp.

- [12] C. Soulé, *K*-théorie des anneaux d'entiers de corps de nombres et cohomologie étale, *Invent. Math.* 55, no. 3, 251–295 (1979).
- [13] C. Soulé, Perfect forms and the Vandiver conjecture, *J. Reine Angew. Math.* 517, 209–221 (1999).
- [14] P. Voutier, An effective bound for the height of algebraic numbers, *Acta Arith.* (1) 74, 81–95 (1996).

Christophe Soulé
CNRS and IHES
35 route de Chartres
91440 Bures-sur-Yvette
France
soule@ihes.fr