On short representations of orders and number fields

Johannes Buchmann
Oliver van Sprang

FB 14-Informatik
Universität des Saarlandes
D-6600 Saarbrücken
West Germany

e-mail: buchmann@cs.uni-sb.de
e-mail: oliver@cs.uni-sb.de

January 15, 1992

Abstract

We discuss the problem of transforming representations of number fields by generating polynomials and by $\mathbb{Q}$-basis into each other. We prove that for a number field or an order of discriminant Δ one can determine in polynomial time a representation whose size is polynomially bounded in $\log |\Delta|$.

1 Introduction

In the literature the time bounds for computing invariants of an algebraic number field $\mathbf{K}$ such as the *class group* or the *regulator* never depend on the specific representation of the field but only on its discriminant Δ (see [1] and [5]). The algorithms for computing those invariants must therefore receive as input a representation of $\mathbf{K}$ whose size is polynomially bounded in $\log |\Delta|$. In this paper we prove that such a representation can be obtained in polynomial time from any representation of $\mathbf{K}$ by a generating polynomial or by means of the multiplication table of a $\mathbb{Q}$-basis.

We use the notions of algorithms and complexity in a similar way as in [5]. An algorithm takes as *input* a finite sequence of non-negative integers and produces another such sequence called the *output*. The *norm* of a finite sequence of non-negative integers $\mathrm{N} = (n_1, n_2, \ldots, n_t)$ is defined to be $|\mathrm{N}| = \max\{n_i : 1 \leq i \leq t\}$.

The *size* of that sequence is $2 + t\log(|N|+2)$. Hence from an upper bound for the norm we immediately obtain an upper bound for the size of N. An algorithm is said to be *polynomial-time* or *good* if its running time is $l^{O(1)}$, where l is the size of the input.

Mathematical objects are encoded by finite sequences of non-negative integers. If the method of encoding is clear we will say that the object is input for an algorithm rather than the encoding. Also the norm of an object M is defined to be the norm of its encoding sequence; it is denoted by |M|. Analogously, the size of an object is defined to be the size of its encoding sequence. Adding a sign bit we can use non-negative integers to represent all integers. Vectors and matrices of integers are represented in the obvious way. Polynomials are encoded by the sequence of their coefficients.

In the second section of this paper we describe how to find a generating polynomial of a number field if we are given a $\mathbb{Q}$-basis and vice versa. In the third section we will prove that there exist small representations of number fields and orders whose size is polynomially bounded in the discriminant of the number field or the order respectively.

2 Representation of number fields and orders

We assume that, an *algebraic number field* $\mathbf{K}$ of degree n is represented by a *generating polynomial* which is a monic, irreducible polynomial in $\mathbb{Z}[x]$ such that $\mathbf{K} \cong \mathbb{Q}[x]/p(x)\mathbb{Q}[x]$. If we set $\rho = x + p(x)\mathbb{Q}[x]$, then we can write $\mathbf{K} = \mathbb{Q}(\rho)$. The number ρ is called a *primitive element* of $\mathbf{K}$.

An order of $\mathbf{K}$ is represented by a $\mathbb{Z}$-basis $\Omega = (\omega_1, \ldots, \omega_n)$, which, in turn, is given by its *multiplication table* $\mathrm{MT}(\Omega) = (w_{ijk}) \in \mathbb{Q}^{n\times n\times n}$ which is defined by the equations

$$\omega_i\omega_j = \sum_{k=1}^{n} w_{ijk}\omega_k \qquad 1 \le i,j \le n \quad .$$

The first goal of this section is to prove that given an order we can find its quotient field in polynomial time. In order to construct a primitive element from a $\mathbb{Z}$-basis of the order, we need to be able to compute minimal polynomials.

Theorem 1 *There is a good algorithm that given an algebraic number field and an element α of that field computes the minimal polynomial of α.*

Proof: Let $\mathbf{K}$ be the given number field and let n be its degree. Consider the following linear map

$$\begin{array}{cccc} \varphi & : & \mathbb{Q}^{n+1} & \longrightarrow & \mathbf{K} \\ & & (a_0, a_1, \ldots, a_n) & \longmapsto & \sum_{i=0}^{n} a_i\alpha^i \end{array}$$

Let $(a_o, \ldots, a_n)$ be an element of the kernel of φ. Then α is a root of the polynomial $p(x) = \sum_{i=1}^{n} a_i x^i$. The minimal polynomial of α is the monic polynomial $p(x) \in \mathbb{Q}[x]$ of minimal degree such that $p(\alpha) = 0$. It can be obtained from a kernel element with a maximum number of tailing zeros. In order to find such an element one determines the matrix of φ by using the multiplication table of $\mathbf{K}$. Gaussian elimination yields the desired result. Clearly, this algorithm runs in polynomial time. $\square$

In order to continue our discussion we need to introduce some notation. Let

$$\begin{aligned} p(x) &= p_0 x^d + p_1 x^{d-1} + \cdots + p_{d-1} x + p_d \\ &= p_0 \prod_{i=1}^{d} (x - z_i) \end{aligned}$$

be a polynomial with complex coefficients and roots z_i, $1 \le i \le d$. We set $\mathbf{L}(p) = \sum_{k=0}^{d} |p_k|$, $\mathbf{Z}(p) = \max\{|z_k| : 1 \le k \le d\}$.

If α is an algebraic number with minimal polynomial $m_\alpha(x)$, then we set $\deg \alpha = \deg m_\alpha(x)$, $\mathbf{L}(\alpha) = \mathbf{L}(m_\alpha(x))$, $\mathbf{Z}(\alpha) = \mathbf{Z}(m_\alpha(x))$. The functions $\mathbf{L}$ and $\mathbf{Z}$ satisfy the following inequalities.

Lemma 1 *For $p \in \mathbb{C}[x]$ we have*

$$\boldsymbol{L}(p) \le p_0 \, (\, 2 \, \boldsymbol{Z}(p) \,)^d.$$

Proof: From [8] pp. 168 we know that $\mathbf{L}(p) \le 2^d \, p_0 \prod_{k=1}^{d} \max\{1, |z|\}$. This obviously implies the assertion. $\square$

We will also use representation matrices. Let $\mathbf{K}$ be an algebraic number field with $\mathbb{Q}$-basis $\Omega = (\omega_1, \ldots, \omega_n)$. For $\alpha \in \mathbf{K}$ the matrix $\mathrm{M}_\Omega(\alpha) = (a_{ij})$ which is defined by the equations

$$\alpha \, \omega_j = \sum_{i=1}^{n} a_{ij} \, \omega_i \qquad 1 \le j \le n$$

is called the *representation matrix* of α with respect to Ω. The map

$$\begin{aligned} \phi : \quad \mathbf{K} &\longrightarrow \mathbb{Q}^{n \times n} \\ \alpha &\longmapsto \mathrm{M}_\Omega(\alpha) \end{aligned}$$

is a field monomorphism.

Theorem 2 *There is a good algorithm that given an order $\mathcal{O}$ of an algebraic number field of degree n, finds its quotient field $\boldsymbol{K}$ such that $|\boldsymbol{K}| \le (\, 2n^3 (\log n) |\mathcal{O}|)^n$.*

Proof: Let $\mathcal{O}$ be given by the $\mathbb{Z}$-basis $\Omega = (\omega_1, \ldots, \omega_n)$. We use the standard primitive element construction to find ρ. To be more precise, we construct a sequence $\rho_1, \rho_2, \cdots \rho_n$ of algebraic integers such that $\mathbb{Q}(\rho_i) = \mathbb{Q}(\omega_1, \cdots, \omega_i)$. Then we can set $\rho = \rho_n$.

We start the construction by setting $\rho_1 = \omega_1$ and by computing $m_{\rho_1}(x)$ using the method from Theorem 1.

Now suppose that we know ρ_i for some $i \in \{1, \ldots, n-1\}$. If $\deg \rho_i = n$ then set $\rho_{i+1} = \rho_i$. If $\deg \rho_i < n$ then we need to construct ρ_{i+1} as a primitive element of $\mathbb{Q}(\rho_i, \omega_{i+1})$ over $\mathbb{Q}$. We determine the minimal polynomial of ω_{i+1}, and factor it over $\mathbb{Q}(\rho_i)$. By the result of [7] this can be done in polynomial time. This determines the degree $d = [\mathbb{Q}(\rho_i, \omega_{i+1}) : \mathbb{Q}(\rho_i)]$. If $d = 1$ then we set $\rho_{i+1} = \rho_i$. Now suppose that $d > 1$. For $t \in \{1, 2, \ldots, n^2\}$ we form the minimal polynomials of $\rho_i + t\omega_{i+1}$, until we find an element of degree $d \cdot \deg \rho_i(x)$. By the argument used in the proof of the primitve element theorem (see [4] pp. 280) such an element must exist. We denote it by ρ_{i+1}.

Next we estimate $\boldsymbol{L}(\rho)$. This is done by proving an upper bound for $\boldsymbol{Z}(\rho_i)$, $1 \le i \le n$, and by applying Lemma 1. The algebraic conjugates of each ω_i are the eigenvalues of the representation matrix of ω_i with respect to Ω. All the entries of this matrix are also entries of the multiplication table $\mathrm{MT}(\Omega)$. Therefore it follows from Gershgorin's theorem ([9] p. 104) that

$$\boldsymbol{Z}(\omega_i) \le n \cdot |\mathrm{MT}(\Omega)| \quad 1 \le i \le n .$$

If $\rho_{i+1} \ne \rho_i$ then we have $\boldsymbol{Z}(\rho_{i+1}) = \boldsymbol{Z}(\rho_i + t\omega_{i+1})$, with $t \in \{1, 2, \ldots, n^2\}$. Thus

$$Z(\rho_{i+1}) \le \boldsymbol{Z}(\rho_i) + n^3 |\mathrm{MT}(\Omega)|$$

which implies that

$$\boldsymbol{Z}(\rho) \le n^3 \log n \, |\mathrm{MT}(\Omega)| .$$

□

Theorem 3 *There is a good algorithm that given an algebraic number field $\boldsymbol{K}$ of degree n finds an order $\mathcal{O}$ in that field such that $|\mathcal{O}| \le (\, 1 + |\boldsymbol{K}|\,)^{n-2} \, |\boldsymbol{K}|$.*

Proof: Let $p(x) = x^n + p_1 x^{n-1} + \cdots + p_{n-1} x + p_n$, and let ρ be a root of p. Then $1, \rho, \ldots, \rho^{n-1}$ is a $\mathbb{Z}$-basis of an order of $\mathbf{K}$. In order to find the multiplication table of that basis we have to determine the coefficients $r_{i,k}$ in the representation

$$\rho^{n+k-1} = \sum_{i=1}^{n} r_{i,k} \rho^{i-1} .$$

We have $r_{i,0} = -p_{n-i+1}\,(1 \le i \le n)$. For consistency reasons, we set $r_{0,k} = 0$. Then we obtain the recurrence relation

$$r_{i,k+1} = r_{i-1,k} - r_{n,k}\, p_{n-i+1} \quad (1 \le i \le n,\ 0 \le k \le n-2) .$$

Therefore it follows that

$$|r_{i,k}| \le (1 + \boldsymbol{L}(p))^k \, \boldsymbol{L}(p)$$

which implies the assertion. $\square$

Next we show that a $\mathbb{Z}$-basis $\Omega_1 = (\omega_1, \omega_2, \ldots, \omega_n)$ of an order of an algebraic number field can be transformed into another $\mathbb{Z}$-basis $\Omega_2 = (\omega_1^{'} = 1, \omega_2^{'}, \ldots, \omega_n^{'})$.

Theorem 4 *There is a good algorithm that given a $\mathbb{Z}$-basis $\Omega = (\omega_1, \ldots, \omega_n)$ of an order of an algebraic number field finds the representation of $1 = x_1\omega_1 + \cdots + x_n\omega_n$. For this representation we have $x_i \in \mathbb{Z}$ and $|x_i| \leq n^{\frac{n-1}{2}} \cdot |MT(\Omega)|^{n-1}$, $1 \leq i \leq n$.*

Proof: The coefficients $x_1, \ldots, x_n$ can be determined by solving the n^2 linear equations $x_1 \mathrm{M}_\Omega(\omega_1) + \cdots + x_n \mathrm{M}_\Omega(\omega_n) = I_n$, where I_n is the $n \times n$ identity matrix. The solution of this system is unique and can be found in polynomial time by using Gaussian elimination.

Also because of the uniqueness, this system contains n linearly independent equations. We denote the $n \times n$ subsystem by $\mathrm{A}\, x = b$, $\mathrm{A} \in \mathbb{Q}^{n \times n}$, $b \in \mathbb{Q}^n$. The entries of A belong to some $\mathrm{M}_\Omega(\omega_i)$ and the entries of the $\mathrm{M}_\Omega(\omega_i)$ belong to $\mathrm{MT}(\Omega)$. The entries of b are either one or zero. Applying Cramer's rule and Hadamard's inequality we obtain the stated bound. $\square$

Lemma 2 *There is good algorithm that given a vector $\underline{x} \in \mathbb{Z}^n$, $\underline{x} = (x_1, \ldots, x_n)$, $\gcd(x_1, \ldots, x_n) = 1$ finds a matrix $X \in \mathrm{GL}(n, \mathbb{Z})$ whose first column is $\underline{x}$. For this matrix X we have $|X| \leq (2|x|)^{n-1}$.*

Proof: Let $\underline{e}_i$ be the i-th column vector of the $n \times n$ indentity matrix I_n. Set

$$\underline{b}_i = \begin{cases} \underline{e}_i & \text{for} \ \ 1 \leq i \leq n \\ \underline{x} & \text{for} \ \ i = n+1\,. \end{cases}$$

Then $(\underline{b}_1, \ldots, \underline{b}_{n+1})$ is a generating system of the lattice $\mathbb{Z}^n$. We will transform that system into a new one with $\underline{b}_i = 0$ for some $i \leq n$ and $\underline{b}_{n+1} = \underline{x}$. Then the matrix we are looking for is $(\underline{x}, \underline{b}_1, \ldots, \underline{b}_{i-1}, \underline{b}_{i+1}, \underline{b}_n)$.

In the beginning we have $x_1\underline{b}_1 + \cdots + x_{n+1}\underline{b}_{n+1} = 0$, where $x_{n+1} = -1$. The vector $(x_1, \ldots, x_{n+1})$ is called a *relation* for the generating system. Whenever we compute a new generating system, we also compute a new relation. If we find a relation where for some $i \leq n$ we have $x_i = 1$, then we may replace $\underline{b}_i$ by 0 and we are done.

Let $d_i = \gcd(x_1, \ldots, x_i)\, 1 \leq i \leq n$. We describe an algorithm, which in the i-th iteration replaces $\underline{b}_i$ and $\underline{b}_{i+1}$ such that $(0, 0, \ldots, d_{i+1}, x_{i+2}, \ldots, x_{n+1})$ is a relation for $(\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_{n+1})$. Since $\gcd(x_1, \ldots, x_n) = 1$ this algorithm finds the desired system after at most n iterations.

Suppose that the algorithm has carried out $i-1$ iterations, $i \leq n$. If $i = 1$ then the algorithm has not done anything yet. We compute a,b such that $d_{i+1} = ad_i - bx_{i+1}$.

Then we know from [3] that $|a| \leq |x_{i+1}|$, $|b| \leq |d_i|$. Let $c = \frac{d_i}{d_{i+1}}$, $d = \frac{x_{i+1}}{d_i+1}$. Then we have $c, d \in \mathbb{Z}$ and $ad - bc = 1$, i.e.

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}).$$

Now we replace

$$(\underline{b}_i, \underline{b}_{i+1}) \text{ by } (\underline{b}_i, \underline{b}_{i+1}) \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Then the new system $(\underline{b}_1, \ldots, \underline{b}_{n+1})$ generates $\mathbb{Z}^n$ and $(0, \ldots, d_{i+1}, x_{i+2}, \ldots, x_{n+1})$ is a relation for that system.

In order to estimate the entries of X, we let $\underline{b}_j^{(i)}$ $(1 \leq j \leq n,\ 1 \leq i \leq n-1)$ be the j-th vector in the generating system after the i-th iteration.
Without loss of generality we assume that we carry out $n-1$ iterations. Let $\mathrm{B}_j = \max\{|\underline{b}_j^{(i)}| : 1 \leq j \leq n\}$, then $\mathrm{B}_j \leq 2\,|x|\,\mathrm{B}_{j-1}$. We also have $\mathrm{B}_0 = 1$. This implies $|\mathrm{X}| \leq (2|x|)^{n-1}$. □

Theorem 5 *There is a good algorithm that given a $\mathbb{Z}$-basis Ω of an order of an algebraic number field of degree n finds a new $\mathbb{Z}$-basis $\Omega' = \{\omega_1', \ldots, \omega_n'\}$ with $\omega_1' = 1$ and*

$$|MT(\Omega')| \leq n^{\frac{n+7}{2}}\, n^{(n-1)\frac{n^2-1}{2}}\, |MT(\Omega)|^{n(n^2-1)+1}.$$

Proof: Using the method of the previous theorem we find the representation $1 = x_1\omega_1 + \cdots + x_n\omega_n$. By virtue of Lemma 2 we can determine a matrix $\mathrm{X} \in \mathrm{GL}(n, \mathbb{Z})$ with first column $x = (x_1, \ldots, x_n)$ and $|\mathrm{X}| \leq 2(\,|x|\,)^{n-1}$. We put

$$(\omega_1', \ldots, \omega_n') = (\omega_1, \ldots, \omega_n)\mathrm{X}.$$

For every $\alpha \in \mathbf{K}$ we have,

$$\mathrm{M}_{\Omega'}(\alpha) = \mathrm{X}^{-1}\mathrm{M}_\Omega(\alpha)\mathrm{X}.$$

Hence it follows for $1 \leq i \leq n$

$$\begin{aligned} \mathrm{M}_{\Omega'}(\omega_i')| &\leq n^3|\mathrm{X}^{-1}|\,|\mathrm{M}_\Omega(\omega_i')|\,|X| \\ &\leq (n-1)^{\frac{n+5}{2}}(2|x|)^{(n-1)^2+n-1}n|X|\,|\mathrm{MT}(\Omega)| \\ &\leq (n-1)^{\frac{n+7}{2}}(2|x|)^{n^2-1}\,|\mathrm{MT}(\Omega)|. \end{aligned}$$

Clearly, the upper bound for the $|\mathrm{M}_{\Omega'}(\omega_i')|$ is also an upper bound for $\mathrm{MT}(\Omega')$. By Theorem 4 we have $|x| \leq n^{\frac{n-1}{2}}|\mathrm{MT}(\Omega)|^n$ so we finally find

$$|\mathrm{MT}(\Omega')| \leq n^{\frac{n+7}{2}}\, n^{(n-1)\frac{n^2-1}{2}}\, |\mathrm{MT}(\Omega)|^{n(n^2-1)+1}$$

□

3 Short representation of number fields and orders

We first show that short representations of orders can be computed in polynomial time. We use the following theorem which was proved in [2].

Theorem 6 *There is a good algorithm that given an order of discriminant Δ in an algebraic number field of degree n computes a $\mathbb{Z}$-basis $\Omega = (\omega_1, \ldots, \omega_n)$ of that order such that*

$$|\mathcal{O}| \leq n^{\frac{(n+1)^2}{2}} 2^{\frac{(n+1)(n^2+1)}{2}+n^2} |\Delta|^{\frac{n}{2}}$$

and for every element ω of that basis we have

$$\boldsymbol{Z}(\omega) \leq n^{\frac{(n+1)^2+1}{2}} 2^{\frac{(n+1)(n^2+1)}{2}+n^2} |\Delta|^{\frac{n}{2}}.$$

Proof: The construction of the new $\mathbb{Z}$-basis can be found in [2]. As in the proof of Theorem 2, the second inequality follows from Gershgorin's theorem (see for instance [9] p.104). $\square$

We conclude that short representations of number fields can be computed in polynomial time.

Corollary 1 *There is a good algorithm that given an order of discriminant Δ in an algebraic number field of degree n computes a $\mathbb{Z}$-basis Ω of that order with first element* 1 *and*

$$|MT(\Omega)| \leq n^{\frac{n^5}{2}+n^4+\frac{n^3}{2}-n^2+\frac{n}{2}+9/2} \cdot 2^{\frac{n^6}{2}+\frac{3n^5}{2}-\frac{n^3}{2}+n^2+1/2} \cdot |\Delta|^{\frac{n^4}{2}-\frac{n^2}{2}+\frac{n}{2}}.$$

Proof: From theorem 6 we know that we can construct a $\mathbb{Z}$-basis $\Omega = (\omega_1, \ldots, \omega_n)$ in polynomial time having the property

$$|\mathrm{MT}(\Omega)| \leq n^{\frac{(n+1)^2}{2}} 2^{\frac{(n+1)(n^2+1)}{2}+n^2} |\Delta|^{\frac{n}{2}}.$$

By virtue of theorem 5 we can compute a $\mathbb{Z}$-basis Ω' with the property required. Combining these two results we get the stated bound. $\square$

Corollary 2 *There is a good algorithm that given the maximal order of an algebraic number field of degree n and discriminant Δ computes a representatition of that field satisfying*

$$|\boldsymbol{K}| \leq 2^{n(1+\log\log n+3\log n+\log n\frac{(n+1)^2}{2}+\frac{(n+1)(n^2+1)}{2}+n^2)} |\Delta|^{\frac{n^2}{2}}$$

Proof: According to Theorem 2 we can find a representation of $\mathbf{K}$ with

$$|\mathbf{K}| \leq (2n^3(\log n)|\mathcal{O}|)^n.$$

Using the representation of $\mathcal{O}$ from Theorem 6 we obtain the stated bound. $\square$

In order to see that the size of representations and the generating polynomial constructed in the proofs can be estimated by a function that only depends on the discriminant and not on the degree of the field, we prove:

Theorem 7 *If Δ is the discriminant of an order in an algebraic number field of degree n, then* $\log|\Delta| \geq n$.

Proof: We know from [10] p. 70

$$|\Delta| \geq \left(\frac{11}{12}\right)^2 \left(\frac{\pi e^2}{4}\right)^n (2\pi n)^{-1} .$$

A close look at the last equation reveals the correctness of our theorem for all $n \geq 5$, since we have in this case

$$\log|\Delta| \geq n\log(\frac{\pi e^2}{4}) + 2\log(\frac{11}{12}) - \log(2\pi n) .$$

To complete the proof, we use a result of A.M. Odlyzko [11]. Using table 1 and 2 p.133 [11], we can verify the assertion for $n < 5$. $\square$

Using this result, we can find the following two corollaries.

Corollary 3 *There is a good algorithm that given an order of discriminant Δ in an algebraic number field of degree n computes a basis of that order of size* $0.5164\,(\log|\Delta|)^6$.

Proof: Straightforward computations using Theorem 6 and the fact that $log(2 + n) \leq 2 + log(n)$, for $n \in \mathbb{N}$ lead us to this result. $\square$

Corollary 4 *There is a good algorithm that given an algebraic number field of degree n and discriminant Δ computes a generating polynomial of that field of size* $2.6041\,(\log|\Delta|)^5$.

Proof: The assertion is an immediate consequence of Corollary 1. $\square$

References

[1] JOHANNES BUCHMANN Complexity of algorithms in algebraic number theory, in Number Theory, Proceedings of the First Conference of the Canadian Number Theory Association held at the Banff Center, pp. 37 - 53, Banff, Alberta, April 17-27, 1988

[2] J. BUCHMANN, V. KESSLER Computing a reduced lattice basis from a generating system, to appear.

[3] HENRI COHEN A course in computational algebraic number theory, Springer Verlag to appear 1992

[4] LARRY JOEL GOLDSTEIN Abstract Algebra. Prentice Hall, 1973

[5] H.W. LENSTRA, JR. Algorithms in algebraic number theory, preliminary version, May 20, 1991

[6] A.K. LENSTRA, H.W. LENSTRA, JR. AND L. LOVÁSZ Factoring polynomials with rational coefficients, Math. Annalen 261 (1982), pp. 515–534.

[7] A.K. LENSTRA Factoring polynomials over algebraic number fields, Lecture Notes in Computer Science 162, Proc. EUROCAL '83 pp. 245, London 1983

[8] M. MIGNOTTE Mathématiques pour le calcul formel. Presses Universitaires de France, 1989

[9] K. HAINER, F. STUMMEL Praktische Mathematik. Teubner Studienbücher Stuttgart, 1982

[10] W. NARKIEWICZ Elementary and Analytic Theory of Algebraic Numbers. Polish Scientific Publishers. Warszawa 1974

[11] A. M. ODLYZKO Bounds for discriminants and reletated estimates for class numbers, regulators and zeros of zeta function - A survey of recent results. Séminaire de Théorie des Nombres de Bordeaux vol.**2** (1990), Seriés 2, 119-141