Available online at www.sciencedirect.com
ScienceDirect

Expo. Math. 25 (2007) 53–66

EXPOSITIONES MATHEMATICAE

www.elsevier.de/exmath

Counting integral ideals in a number field

M. Ram Murty[a,*,1], Jeanine Van Order[b]

[a] *Department of Mathematics and Statistics, Queen's University, Kingston, Ont., Canada K7L 3N6*
[b] *DPMMS Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, CB3 0WA Cambridge, UK*

Received 3 November 2005

Abstract

Let K be an algebraic number field. We discuss the problem of counting the number of integral ideals below a given norm and obtain effective error estimates. The approach is elementary and follows a classical line of argument of Dedekind and Weber. The novelty here is that explicit error estimates can be obtained by fine tuning this classical argument without too much difficulty. The error estimate is sufficiently strong to give the analytic continuation of the Dedekind zeta function to the left of the line $\Re(s) = 1$ as well as explicit bounds for the residue of the zeta function at $s = 1$.

MSC 2000: primary 11R45; secondary 11R42

Keywords: Algebraic number theory; Dedekind zeta function; Density theorems; Global fields

1. Introduction

In any introductory course in algebraic number theory, one finds that beyond the rudimentary theory of Dedekind domains and Dirichlet's unit theorem, there is not sufficient time to cover the deeper aspects of the analytic theory of algebraic numbers. More precisely, in a single semester course, it seems almost impossible to acquaint students with the theory of the Dedekind zeta function, the distribution of ideals in ideal classes, and the prime

[*] Corresponding author. Tel.: +1 613 533 2413; fax: +1 613 533 2964.
E-mail addresses: murty@mast.queensu.ca (M.R. Murty), J.M.Van-Order@dpmms.cam.ac.uk (J. Van Order).

[1] Research partially supported by an NSERC grant.

0723-0869/$ - see front matter © 2006 Elsevier GmbH. All rights reserved.
doi:10.1016/j.exmath.2006.08.001

ideal theorem. The purpose of this article is to show that once the basic theory of algebraic number fields is in place, the analytic theory can be treated in one or two lectures along the lines indicated below. This approach is not new. It has its origins in the work of Dedekind and his student Weber [9]. It is also the approach taken in [5] through its problem solving format. In this note, we amplify the technique and at the same time derive effective results with explicit constants. This will have applications to computational questions as well as certain questions arising in mathematical logic.

We begin by fixing notation. Let K be an algebraic number field, and let $n=[K:\mathbb{Q}]$. Let $\mathcal{O}_K$ denote the ring of integers of K. As is well-known, the ideals of $\mathcal{O}_K$ can be partitioned into equivalence classes as follows. We say $\mathfrak{a}\equiv\mathfrak{b}$ if there are α, $\beta\in\mathcal{O}_K$ so that $(\alpha)\mathfrak{a}=(\beta)\mathfrak{b}$. By a celebrated theorem of Minkowski, this equivalence relation partitions the ideals of $\mathcal{O}_K$ into a finite number of classes. This finite number is called the class number of K, and is denoted h_K. In fact, the equivalence classes can be given the structure of a group as follows. For two classes C_1, C_2 choose $\mathfrak{a}\in C_1$ and $\mathfrak{b}\in C_2$. Define the product of C_1 and C_2 as the class to which $\mathfrak{ab}$ belongs. One can show this is well-defined, with the class of principal ideals acting as the identity element. Moreover, one can prove that given any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, there is an ideal $\mathfrak{a}'$ of $\mathcal{O}_K$ so that $\mathfrak{aa}'$ is principal. This gives the structure of a finite abelian group (called the ideal class group) to the equivalence classes of ideals in $\mathcal{O}_K$.

Now let C be an ideal class of $\mathcal{O}_K$, and choose an ideal $\mathfrak{b}$ in C^{-1}. If $\mathfrak{a}$ is an ideal of norm $\leqslant x$ in C, then $\mathfrak{ab}=(\alpha)$ is principal with $\alpha\in\mathfrak{b}$ and $|N(\alpha)|\leqslant xN(\mathfrak{b})$. Conversely, if $\alpha\in\mathfrak{b}$ and $|N(\alpha)|\leqslant xN(\mathfrak{b})$, then $\mathfrak{a}=(\alpha)\beta^{-1}$ is an integral ideal in C of norm $\leqslant x$. Thus, if we let $N(x,C)$ be the number of ideals of norm $\leqslant x$ in C, then the above remark shows that this is the same as counting the number of principal ideals (α), with $\alpha\in\mathfrak{b}$ and $|N(\alpha)|\leqslant xN(\mathfrak{b})$.

To count the number of such principal ideals (α), we fix an integral basis $\beta_1,\ldots,\beta_n$ of $\mathfrak{b}$. Then as $\alpha\in\mathfrak{b}$, we may write

$$\alpha=x_1\beta_1+\cdots+x_n\beta_n \tag{1.1}$$

for some integers $x_1,\ldots,x_n$. Thus, any α of the form (1.1) satisfying $|N(\alpha)|\leqslant xN(\mathfrak{b})$ gives rise to a principal ideal, and consequently corresponds to a lattice point $(x_1,\ldots,x_n)\in\mathbb{R}^n$. However, this correspondence between the principal ideal (α) and the lattice point is not one-to-one, since for any associate α' of α, we have $(\alpha')=(\alpha)$. Thus, in order to translate the problem of determining $N(x,C)$ into a lattice point problem, we make a choice of generator for the principal ideal. To this end, we need to recall Dirichlet's unit theorem.

Proposition 1 (*Dirichlet, 1846*). *Let K be an algebraic number field of degree n over $\mathbb{Q}$. As usual, write $n=r_1+2r_2$ where r_1 is the number of real embeddings of K into $\mathbb{R}$ and $2r_2$ is the number of non-real embeddings of K into $\mathbb{C}$. Let $r=r_1+r_2-1$. Then, there exist fundamental units $\varepsilon_1,\ldots,\varepsilon_r$ such that every unit of $\mathcal{O}_K$ can be written uniquely as*

$$\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r},$$

where ζ is a root of unity in $\mathcal{O}_K$ and $n_1,\ldots,n_r\in\mathbb{Z}$. There are only finitely many roots of unity in K, and we denote this number by w.

Remark 1.1. For a proof, see [5, p. 99].

An important consequence of Dirichlet's unit theorem is that if $\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r} = 1$, then $n_1 = \cdots = n_r = 0$, since the units are independent (by virtue of the uniqueness of representation). Thus, following the usual convention concerning the ordering of the embeddings, with $K \to K^{(i)}$ real for $1 \leqslant i \leqslant r_1$, $K \to K^{(i)}$ non-real for $r_1 + 1 \leqslant i \leqslant r_1 + r_2$ arranged so that

$$\overline{K^{(i+r_2)}} = K^{(i)},$$

we see that the $r \times r$ matrix

$$(\log |\varepsilon_j^{(i)}|)$$

is non-singular. Consequently, for any given α, there exist unique real numbers $c_1, \ldots, c_r$ so that

$$\sum_{j=1}^{r} c_j \log |\varepsilon_j^{(i)}| = \log \left(|\alpha^{(i)}| |N(\alpha)|^{-1/n} \right) \tag{1.2}$$

for $1 \leqslant i \leqslant r$. If α and α' generate the same principal ideal, then $\alpha = \varepsilon\alpha'$ for some unit ε. By the unit theorem, we may write

$$\varepsilon = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}.$$

Thus, the corresponding c_j's for α' are simply $c_j - n_j$, $1 \leqslant j \leqslant r$. Therefore, we may isolate a generator for the principal ideal (α) by insisting (1.2) is satisfied with $0 \leqslant c_j < 1$ for $1 \leqslant j \leqslant r$. As there are w roots of unity, we derive that $wN(x, C)$ is equal to the number of lattice points $(x_1, \ldots, x_n)$ in $\mathbb{R}^n$ satisfying the "norm condition"

$$|N(\alpha)| = |\alpha^{(1)} \cdots \alpha^{(n)}| \leqslant xN(\mathrm{b}) \tag{1.3}$$

with $\alpha^{(i)} = x_1\beta_i^{(i)} + \cdots + x_n\beta_n^{(i)}$, and the "regulator condition": there exist real numbers $c_1, \ldots, c_r$ such that $0 \leqslant c_i < 1$ and

$$\sum_{j=1}^{r} c_j \log |\varepsilon_j^{(i)}| = \log \left(|\alpha^{(i)}| |N(\alpha)|^{-1/n} \right) \tag{1.4}$$

for $1 \leqslant i \leqslant r$.

We claim that the regulator condition also holds for all i with $1 \leqslant i \leqslant n$. To see this, let us observe that if we replace i by $i + r_2$, the identity still holds for $1 \leqslant i \leqslant r$. Thus, we only need to show the condition holds for $i = r + 1$. To this end, let $e_i = 1$ if $K^{(i)}$ is real, and let $e_i = 2$ if $K^{(i)}$ is not real. Then,

$$\sum_{i=1}^{r+1} e_i \log |\varepsilon_j^{(i)}| = 0$$

since the norm of the unit has absolute value 1. We multiply this relation by c_j and sum over j from 1 to r to obtain

$$0 = \sum_{i=1}^{r+1} e_i \left(\sum_{j=1}^{r} c_j \log |\varepsilon_j^{(i)}| \right).$$

This is seen to be

$$0 = e_{r+1} \sum_{j=1}^{r} c_j \log |\varepsilon_j^{(r+1)}| + \sum_{i=1}^{r} e_i \log \left(|\alpha^{(i)}||N(\alpha)|^{-1/n} \right).$$

This last sum is

$$-e_{r+1} \log \left(|\alpha^{(r+1)}||N(\alpha)|^{-1/n} \right),$$

and so we deduce that (1.2) holds for $i = r+1$ also. Thus, (1.2) holds for all i with $1 \leqslant i \leqslant n$.

This motivates the following lattice point problem. The number $wN(x, C)$ is the number of lattice points $(x_1, \ldots, x_n)$ in the region B_x of $\mathbb{R}^n$ defined by the "norm condition" (1.3) and the "regulator" condition (1.4), with

$$\alpha^{(i)} = x_1 \beta_i^{(i)} + \cdots + x_n \beta_n^{(i)} \neq 0$$

for any i satisfying $1 \leqslant i \leqslant n$. For future reference, we note that the set of points $(x_1, \ldots, x_n)$ with $\alpha^{(i)} = 0$ lie in a subvariety of smaller dimension. We will also need to estimate the number of lattice points in this subvariety.

2. Upper bounds

We begin by showing that B_x is a bounded region in $\mathbb{R}^n$. This is seen as follows. Because the integral basis $\beta_1, \ldots, \beta_n$ of $\mathfrak{b}$ is linearly independent over $\mathbb{Q}$, we have

$$\det(\beta_i^{(j)}) \neq 0.$$

Thus, the linear map

$$\phi(x_1, \ldots, x_n) = (\alpha^{(1)}, \ldots, \alpha^{(n)})$$

is invertible. Let M be the largest of the values of $|\log |\varepsilon_j^{(i)}||$ for $1 \leqslant i,\ j \leqslant r$. Then, from (1.2), we deduce that

$$|\alpha^{(i)}| \leqslant e^{rM} |N(\alpha)|^{1/n}.$$

Since (1.1) implies that $|N(\alpha)| \leqslant xN(\mathfrak{b})$, we deduce that

$$|\alpha^{(i)}| \leqslant e^{rM} (xN(\mathfrak{b}))^{1/n}.$$

We can say more. If we write $(\gamma_{ij}) = (\beta_j^{(i)})^{-1}$, and let γ denote the largest absolute value of the γ_{ij}'s, then we find

$$|x_i| \leqslant \gamma n e^{rM} (xN(\mathfrak{b}))^{1/n}. \tag{2.1}$$

This clearly defines a bounded region of $\mathbb{R}^n$. From this bound, we can derive an upper boud of $N(x, C)$ by applying a classical result of Minkowski which we recall below.

Proposition 2 (*Minkowski*). *Let K be an algebraic number field of degree n over $\mathbb{Q}$. Then, each ideal class contains an ideal $\mathfrak{b}$ satisfying*

$$N(\mathfrak{b}) \leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |d_K|^{\frac{1}{2}} = \mathscr{M}_K \ (say),$$

where $|d_K|$ denotes the discriminant of the number field.

Applying Proposition 2, we deduce:

Theorem 1. *Let γ, M, r be as above. Then*

$$wN(x, C) \leqslant \left(2n\gamma e^{rM}\mathscr{M}_K^{1/n}x^{1/n} + 1\right)^n.$$

For the trivial class, we have the better bound

$$wN(x, 1) \leqslant (2n\gamma e^{rM}x^{1/n} + 1)^n.$$

3. An asymptotic formula for $N(x, C)$

The analysis of the previous section can be refined to derive an asymptotic formula for $N(x, C)$ with an effective error term. As explained earlier, $wN(x, C)$ is equal to the number of non-zero lattice points in the region B_x. Following Dedekind and Weber [9], we approximate this number by the volume of B_x.

To be precise, let I^n denote the unit cube in $\mathbb{R}^n$. To each lattice point P contained in B_x, we associate $P + I^n$, and we think of our region B_x as being “approximated” by these cubes. Each cube has volume 1 and the number of lattice points is thus expected to be approximated by the volume B_x. We make the argument effective via the following technical argument.

Lemma 3.1. *With notation as above, let*

$$\begin{aligned} N(x_1, \ldots, x_n) &= \sum_{k=1}^{n}\left(\sum_{i=1}^{n} x_i\beta_i^{(k)}\right) \\ &= \sum_{\substack{i_1,\ldots,i_n \\ i_1+\ldots+i_n=n}} a_{i_1,\ldots,i_n}x_1^{i_1}\cdots x_n^{i_n} \ (say). \end{aligned}$$

Then, for $|t_i| \leqslant 1$, we have

$$|N(u_1 + t_1, \ldots, u_n + t_n) - N(u_1, \ldots, u_n)| \leqslant n^{n+1}\tilde{\beta}^n(U + 1)^{n-1},$$

where $\tilde{\beta}$ is the largest absolute value of the $\beta_i^{(j)}$, and $U = \max_{1\leqslant i\leqslant n}|u_i|$.

Proof. We see that

$$\begin{aligned}|N(u_1+t_1,\ldots,u_n+t_n)-N(u_1,\ldots,u_n)|\\ =\left|\sum_{\substack{1_1,\ldots,i_n\\ i_1+\cdots+1_n=n}} a_{i_1,\ldots,i_n}[(u_1+t_1)^{i_1}\cdots(u_n+t_n)^{i_n}-u_1^{i_1}\cdots u_n^{i_n}]\right|.\end{aligned}$$

Letting

$$f(\lambda):=(u_1+\lambda t_1)^{i_1}\cdots(u_n+\lambda t_n)^{i_n},$$

we have by the mean-value theorem that the expression in square brackets is

$$f(1)-f(0)=f'(\xi)$$

for some $\xi\in[0,1]$. A simple calculation shows that

$$|f'(\xi)|\leqslant n(U+1)^{n-1},$$

where

$$U=\max_{1\leqslant i\leqslant n}|u_i|.$$

Clearly,

$$|a_{i_1,\ldots,i_n}|\leqslant\binom{n}{i_1\cdots i_n}\tilde{\beta}^n,$$

so putting these inequalities together gives us the stated inequality.

Lemma 3.2. *There is a $\delta>0$ such that for any non-zero lattice point P contained in $B_{(t-\delta)^n}$, the translate $P+I^n$ is also contained in B_{t^n}.*

Proof. Let $P=(u_1,\ldots,u_n)$. By the previous lemma,

$$\begin{aligned}|N(u_1+t_1,\ldots,u_n+t_n)-N(u_1,\ldots,u_n)|&\leqslant n^{n+1}\tilde{\beta}^n(U+1)^{n-1}\\ &\leqslant 2^{n-1}n^{n+1}\tilde{\beta}^n U^{n-1},\end{aligned}$$

since P is a non-zero lattice point and $U+1\leqslant 2U$. By (2.1), we know

$$U\leqslant n\gamma e^{rM}N(\mathfrak{b})^{\frac{1}{n}}(t-\delta).$$

Let

$$\Phi(\mathfrak{b})=2^{n-1}n^{2n}\gamma^{n-1}e^{rM}N(\mathfrak{b})^{(n-1)/n}.$$

Then, by the triangle inequality, we obtain

$$\begin{aligned}|N(u_1+t_1,\ldots,u_n+t_n)|&\leqslant(t-\delta)^n N(\mathfrak{b})+\Phi(\mathfrak{b})(t-\delta)^{n-1}\\ &\leqslant(t-\delta)^{n-1}N(\mathfrak{b})[t-\delta+\Phi_0]\end{aligned}$$

where

$$\Phi_0 = 2^{n-1} n^{2n} \gamma^{n-1} e^{rM(n-1)}. \tag{3.1}$$

If we choose $\delta = \Phi_0$, we see that the lemma holds with this choice of δ.

Remark 3.1. In the proof of the lemma, we used only the fact that $|t_i| \leqslant 1$. Thus, the argument also shows that for any non-zero lattice point P contained in B_{t^n}, $P - I^n$ is also contained in $B_{(t-\delta)^n}$.

We can now deduce our main theorem.

Theorem 2. *With* δ *given by* (3.1) *and* $t = x^{\frac{1}{n}}$, *we have*

$$\mathrm{Vol}(B_{(t-\delta)^n}) \leqslant wN(x, C) \leqslant \mathrm{Vol}(B_{(t+\delta)^n}).$$

Proof. By Lemma 3.2, we deduce

$$wN((t-\delta)^n, C) \leqslant \mathrm{Vol}(B_x).$$

Replacing t by $t + \delta$, this gives

$$wN(x, C) \leqslant \mathrm{Vol}(B_{(t+\delta)^n}).$$

By the remark made after the lemma, we deduce

$$\mathrm{Vol}(B_{(t-\delta)^n}) \leqslant wN(x, C).$$

Putting these inequalities together gives us the theorem.

It is easy to see that the region B_x is a homogeneously expanding domain as x tends to infinity. Indeed, we have

$$B_{t^n} = tB_1.$$

Thus, $\mathrm{Vol}(B_{(t-\delta)^n}) = (t-\delta)^n \mathrm{Vol}(B_1)$ and $\mathrm{Vol}(B_{(t+\delta)^n}) = (t+\delta)^n \mathrm{Vol}(B_1)$. We therefore deduce:

Corollary 1.

$$(x^{1/n} - \delta)^n \mathrm{Vol}(B_1) \leqslant wN(x, C) \leqslant (x^{\frac{1}{n}} + \delta)^n \mathrm{Vol}(B_1)$$

From Corollary 1, we are able to deduce that

$$wN(x, C) = \mathrm{Vol}(B_1)x + O(x^{(n-1)/n}).$$

In particular, this implies that the ideal class zeta function

$$\zeta(s, C) = \sum_{\mathfrak{a} \in C} \frac{1}{N\mathfrak{a}^s}$$

can be extended analytically to $\Re(s) > 1 - (1/n)$ and with only a simple pole at $s = 1$ and residue equal to

$$\frac{\mathrm{Vol}(B_1)}{w}.$$

However, we have been careful to prove more than this. Since δ is explicitly given by (3.1), we have the important

Theorem 3.

$$|wN(x, C) - \mathrm{Vol}(B_1)x| \leqslant 2^n x^{\frac{n-1}{n}} \max(1, \Phi_0^n)\mathrm{Vol}(B_1),$$

where $\Phi_0 = 2^{n-1}n^{2n}\gamma^n e^{rM(n-1)}$.

Let $N(x; K)$ be the number of ideals in $\mathcal{O}_K$ with norm $\leqslant x$. Then

$$N(x; K) = \sum_C N(x, C),$$

the summation being over the finite ideal classes. From Theorem 3, we are able to deduce

Theorem 4. *Let* h_K *be the class number of* $\mathcal{O}_K$. *Then*,

$$|wN(x; K) - \mathrm{Vol}(B_1)h_K x| \leqslant h_K 2^n x^{\frac{n-1}{n}} \max(1, \Phi_0^n)\mathrm{Vol}(B_1).$$

We will indicate at the end of this paper how one may bound h_K in an elementary way. Thus, we may regard Theorem 4 as representing a completely effective estimate for the error term in Weber's theorem alluded to at the beginning of this paper.

4. The volume of B_1

The calculation of the volume of B_1 is easily done using the calculus of several variables. In this connection, we follow [5, pp. 142–144], and give a brief description of the derivation.

We let B_1^* be the domain described by

$$\alpha^{(i)} = \sum_{j=1}^{n} x_j \beta_j^{(i)}, \quad 1 \leqslant i \leqslant n$$

and

$$0 < |\alpha^{(1)} \cdots \alpha^{(n)}| \leqslant N(\mathfrak{b})$$

so that there exist c_j's for $1 \leqslant j \leqslant r$ satisfying $0 \leqslant c_j < 1$ and

$$\log\left(|\alpha^{(i)}||N(\alpha)|^{\frac{-1}{n}}\right) = \sum_{j=1}^{r} c_j \log|\varepsilon_j^{(i)}|$$

for $1 \leqslant i \leqslant n$, or

$$|\alpha^{(i)}| \leqslant e^{rM}(N(\mathfrak{b}))^{\frac{1}{n}}, \quad 1 \leqslant i \leqslant n$$

and at least one $\alpha^{(i)} = 0$. The difference between B_1 and B_1^* is in the last condition, allowing for $\alpha^{(i)} = 0$ for some i. Thus, B_1^* is a closed bounded region and

$$\mathrm{Vol}(B_1^*) = \int \cdots \int_{B_1^*} \mathrm{d}x_1 \cdots \mathrm{d}x_n.$$

Moreover, $\mathrm{Vol}(B_1^*) = \mathrm{Vol}(B_1)$ since the extra condition defines a manifold of lower dimension. To evaluate the integral, we change variables:

$$u_i := \alpha^{(i)} = \sum_{j=1}^{n} x_j \beta_j^{(i)}, \quad 1 \leqslant i \leqslant r_1$$

$$u_i + u_{i+r_2}\sqrt{-1} := \sum_{j=1}^{n} x_j \beta_j^{(i)}, \quad r_1 + 1 \leqslant i \leqslant r_1 + r_2.$$

Thus, for $r_1 + 1 \leqslant i \leqslant r_1 + r_2$, we have

$$u_i = \sum_{j=1}^{n} \left(\frac{\beta_j^{(i)} + \beta_j^{(i+r_2)}}{2} \right),$$

$$u_{i+r_2} = \sum_{j=1}^{n} \left(\frac{\beta_j^{(i)} + \beta_j^{(i+r_2)}}{2\sqrt{-1}} \right).$$

The absolute value of the Jacobian for this change of variables is easily computed to be

$$2^{-r_2} N(\mathfrak{b}) \sqrt{|d_K|}.$$

Hence,

$$\mathrm{Vol}(B_1) = \frac{2^{r_2}}{N(\mathfrak{b})\sqrt{|d_K|}} \int \cdots \int_{\tilde{B_1^*}} \mathrm{d}u_1 \cdots \mathrm{d}u_n,$$

where $\tilde{B_1^*}$ is the image of B_1^* under the change of variables. The variables $u_1, \ldots, u_{r_1}$ may take one of two signs and so, if we insist $u_i \geqslant 0$ for $i = 1, \ldots, r_1$, we must multiply our volume integral with this additional constraint by a factor of 2^{r_1}. Thus, we may switch to polar coordinates:

$$\rho_j = u_j, \quad 1 \leqslant j \leqslant r_1$$

and

$$\rho_j \cos\theta_j = u_j, \quad \rho_j \sin\theta_j = u_j + r_2$$

for $r_1+1 \leqslant j \leqslant r_1+r_2$; consequently, $\rho_j \geqslant 0$ and $0 \leqslant \theta_j < 2\pi$. The Jacobian of this transform is easily computed to be

$$\rho_{r_1+1} \cdots \rho_{r_1+r_2}.$$

Thus,

$$\mathrm{Vol}(B_1) = \frac{2^{r_1+r_2}(2\pi)^{r_2}}{N(\mathfrak{b})\sqrt{|d_K|}} \int \cdots \int_{C_1^*} \rho_{r_1+1} \cdots \rho_{r_1+r_2}\, \mathrm{d}\rho_1 \cdots \mathrm{d}\rho_{r_1+r_2}$$

where C_1^* is the domain described by

$$0 \leqslant \prod_{j=1}^{r_1+r_2} \rho_j^{e_j} \leqslant N(\mathfrak{b}),$$

$$\log \rho_i - \frac{1}{n} \sum_{j=1}^{r} e_j \log \rho_j = \sum_{j=1}^{r} c_j \log |\varepsilon_j^{(i)}|$$

for $1 \leqslant i \leqslant r_1 + r_2$. (Here, $e_1 = 1$ for $1 \leqslant i \leqslant r_1$ and 2 for $r_1 + 1 \leqslant i \leqslant r_1 + r_2$.) We make one more change of variables. Put

$$\tau_j = \rho_j^{e_j},\ 1 \leqslant j \leqslant r_1 + r_2.$$

The Jacobian of this transformation is easily seen to be

$$2^{-r_2} \rho_{r_1+1}^{-1} \cdots \rho_{r_1+r_2}^{-1},$$

so that the integral becomes

$$\frac{2^{r_1}(2\pi)^{r_2}}{N(\mathfrak{b})\sqrt{|d_K|}} \int \cdots \int_{D_1^*} \mathrm{d}\tau_1 \cdots \tau_{r_1+r_2},$$

where D_1^* is the region described by

$$\tau_1 \cdots \tau_{r_1+r_2} \leqslant N(\mathfrak{b}), \qquad \tau_i > 0$$

$$\log \tau_i - \frac{e_i}{n} \sum_{j=1}^{r} \log \tau_j = e_i \sum_{j=1}^{r} c_j \log |\varepsilon_j^{(i)}|.$$

We make one final change of variables; we write the c_i's in terms of the τ_i's and put

$$u = \tau_1 \cdots \tau_{r+1}.$$

The Jacobian of this transformation is now seen to be the regulator, defined as

$$R_K := \det\left(e_i \log |\varepsilon_j^{(i)}|\right)_{1 \leqslant i,j \leqslant r}.$$

This proves

Proposition 3.

$$\mathrm{Vol}(B_1) = \frac{2^{r_1}(2\pi)^{r_2} R_K}{\sqrt{|d_K|}}.$$

Now let

$$\rho_K = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w\sqrt{|d_K|}}.$$

We have proved:

Theorem 5.

$$\left| N(x, C) - \frac{\rho_K x}{h_K} \right| \leqslant \frac{\rho_k}{w h_K} 2^n x^{\frac{n-1}{n}} \max(1, \Phi_0^n)$$

and

$$|N(x; K) - \rho_K x| \leqslant \frac{\rho_k}{w} 2^n x^{\frac{n-1}{n}} \max(1, \Phi_0^n),$$

where

$$\Phi_0 = 2^{n-1} n^{2n} \gamma^n e^{rM(n-1)}.$$

In the next section, we will combine this result with Theorem 1 to derive bounds for the regulator.

5. Bounds for the regulator

By Theorem 1 we have

$$wN(x, 1) \leqslant (2n\gamma e^{rM} x^{1/n} + 1)^n,$$

where γ, M, r are as in Theorem 1. By Theorem 5,

$$N(x, C) = \frac{\rho_K x}{h_K} + O(x^{(n-1)/n}).$$

Putting these facts together, we deduce immediately that

Theorem 6.

$$\frac{w\rho_K}{h_K} = \frac{2^{r_1}(2\pi)^{r_2} R_K}{\sqrt{|d_K|}} \leqslant (2n\gamma e^{rM})^n.$$

In particular, this theorem allows us to bound the regulator of the field in terms of the class number. In the next section, we will discuss elementary ways to bound the class number.

Before we conclude this section, we indicate one further application of Theorem 5. This is the problem of bounding the Euler constant of the number field.

Let us recall that this constant, denoted γ_K, is defined as

$$\gamma_K := \lim_{s\to\infty}\left(\zeta_K(s) - \frac{\rho_K}{s-1}\right),$$

where $\zeta_K(s)$ denotes the Dedekind zeta function of K. In the case $K=\mathbb{Q}$, $\gamma_{\mathbb{Q}}$ coincides with the classical Euler–Mascheroni constant defined as

$$\gamma = \lim_{x\to\infty}\left(\sum_{n\leqslant x}\frac{1}{n} - \log x\right).$$

By the well-known method of partial summation, we have

$$\zeta_K(s) = s\int_1^\infty \frac{N(x;K)\,\mathrm{d}x}{x^{s+1}}.$$

Writing

$$N(x,K) = \rho_K x + E(x),$$

we find easily that

$$\zeta_K = \frac{\rho_K}{s-1} + \rho_K + \int_1^\infty \frac{E(x)}{x^{s+1}} + (|s-1|).$$

Thus, we deduce that

$$\gamma_K = \rho_K + \int_1^\infty \frac{E(x)}{x^2}\,\mathrm{d}x.$$

By Theorem 4,

$$|E(x)| \leqslant \rho_K 2^n \max(1, \Phi_0^n) x^{(n-1)/n}.$$

Thus,

$$\left|\int_1^\infty \frac{E(x)}{x^2}\,\mathrm{d}x\right| \leqslant \rho_K 2^n \max(1,\Phi_0^n) n.$$

This proves:

Theorem 7.

$$|\gamma_K| \leqslant \rho_K(1 + 2^n \max(1, (\Phi_0^n)n).$$

6. Bounds for the class number

In this section, we will indicate an elementary estimate for h_K. This will enable us to assert that all of our bounds are completely effective.

By considering the Euler product of $\zeta_K(s)$, we deduce that the number of ideals of norm m is at most the number of factorizations of m as a product of n positive numbers. This latter quantity is the generalized division function $\tau_n(m)$. Thus, we have the crude bound

$$N(x;K)\leqslant \sum_{m\leqslant x}\tau_n(m).$$

Since the class number is at most the number of ideals with norm at most $\mathscr{M}_K$, we deduce

$$h_K\leqslant N(\mathscr{M}_K;K).$$

We can bound the latter quantity crudely by $\mathscr{M}_K^{n+1}$, since $\tau_n(m)\leqslant m^n$. This proves:

Proposition 4.

$$h_K\leqslant \mathscr{M}_K^{n+1}.$$

We remark that a final analysis will give better results. For example, one can show (see [3, Theorem 6.5]) in an elementary way

$$h_K\leqslant |d_K|^{\frac{1}{2}}\frac{(n-1+\log|d_K|)^{n-1}}{(n-1)!},$$

and we may replace $|d_K|$ above by $\mathscr{M}_K$. However, it is our purpose here to show that effective bounds can be obtained by the simplest of reasoning.

7. Concluding remarks

The value of these effective estimates is two-fold. First, they enable us to deduce the analytic continuation of the ideal class zeta functions

$$\zeta(s,C)=\sum_{\mathfrak{a}\in C}\frac{1}{N(\mathfrak{a})^s}$$

to the region $\Re(s)>1-(1/n)$. This enables one to deduce that ideals are uniformly distributed in the ideal classes. It also enables one to deduce the analytic continuation of the Hecke L-series attached to characters of the ideal class group. This, in turn, gives us (via the Tauberian theory), the uniform distribution of prime ideals in ideal classes, which in many ways should be viewed as the number field analogue of the classical theorem of Dirichlet concerning the infinitude of primes in arithmetic progressions. We refer the reader to Sections 11.2 and 11.3 of [5].

Secondly, we remark that in the elementary proof of the prime ideal theorem, extending the work of Erdös and Selberg to the number field case, Shapiro [7] makes essential use of the result

$$N(x;K)=\rho_K x+O\left(x^{\frac{n-1}{n}}\right).$$

It should be possible to extend his work further and combine it with some of the techniques of this paper to derive an elementary proof of the Chebotarev density theorem.

Finally, we re-iterate the elementary nature of our work and that the bounds we obtained for ρ_K and h_K are in no ways the best possible. There are many papers where better estimates are derived, for instance [4].

One may enquire as to the best error estimate one can derive for $E(x)$. It is doubtful if the methods of this paper can be fine tuned to yield better error terms. One can infer this in several ways. There is an interesting result of Erhart (see [8, p. 52] for details) which states the following. Let P be a convex d-dimensional polytope in $\mathbb{R}^n$ with vertices in $\mathbb{Z}^n$. If $i(P,t)$ is the number of lattice points in tP, then Erhart showed that $i(P,t)$ is a polynomial in t of degree d. In the case $d=n$, the coefficient of t^n is the volume of P, and the coefficient of t^{n-1} is one-half of the (relative) volume of the boundary of P. In the two-dimensional case, this is really the celebrated Pick's formula (see [6]). In the generic case, this second term is non-zero. With our normalization of $t=x^{1/n}$ this leads to the result that the error is asymptotically growing like $x^{(n-1)/n}$. Thus, to improve upon the error term $E(x)$ studied in this paper, one needs to exploit the specific context, most notably the analytic continuation of the zeta function and its functional equation.

Using such complex analytic methods, it is possible to show that for $n \geqslant 2$,

$$E(x) = O\left(x^{1-\frac{2}{n+1}}\right),$$

as in [1]. It is a famous open problem that one may take any exponent greater than $\frac{1}{2}-\frac{1}{2n}$. This problem can be viewed as a generalization of Gauss's circle problem, for if $K=\mathbb{Q}(\sqrt{-1})$, the estimation of $E(x)$ is identical with it. In this context, we indicate that the Generalized Riemann Hypothesis for $\zeta_K(s)$ would imply that any exponent greater than $\frac{1}{2}$ is permissible (see for example [2, p. 271]).

References

[1] E. Landau, Einführung in die Elementare und Theorie der Algebraischen Zahlen und der Ideale, 2. Aufl. Leipzig.

[2] S. Lang, Algebraic Number Theory, second ed., Springer, Berlin, 1994.

[3] H. Lenstra, Algorithms in Algebraic Number Theory, Bull. Amer. Math. Soc. New Series 26 (2) (1992) 211–244.

[4] S. Louboutin, Explicit bounds for residues of Dedekind zeta functions, values of L-functions at $s=1$, and relative class numbers, J. Number Theory (85) (2000) 263–282.

[5] R. Murty, J. Esmonde, Problems in Algebraic Number Theory, second ed., Springer, Berlin, 2005.

[6] R. Murty, N. Thain, Pick's Theorem via Minkowski's Theorem, to appear in the American Mathematical Monthly.

[7] H.N. Shapiro, Tauberian theorems and elementary prime number theory, Comm. Pure Appl. Math. (12) (1959) 579–610.

[8] R. Stanley, Combinatorics and Commutative Algebra, first ed., Birkhäuser, Basal, 1983.

[9] H. Weber, Lehrbuch der Algebra, Zweiter Band, third ed., Chelsea Publishing Co., New York, 1961.