

BULLETIN DE LA S. M. F.

STEPHEN HOEL SCHANUEL

Heights in number fields

Bulletin de la S. M. F., tome 107 (1979), p. 433-449

[<http://www.numdam.org/item?id=BSMF_1979__107__433_0>](http://www.numdam.org/item?id=BSMF_1979__107__433_0)

© Bulletin de la S. M. F., 1979, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

HEIGHTS IN NUMBER FIELDS

BY

STEPHEN HOEL SCHANUEL (*)

[State University of New York, Buffalo]

RÉSUMÉ. — Soit K un corps de nombres de degré N sur les rationnels, et H_K la hauteur relative à K , des points de l'espace projectif de dimension $m - 1$. Soit $\lambda(B)$ le nombre de points dans cet espace projectif de hauteur $\leq B$. On démontre le comportement asymptotique $\lambda(B) \sim CB^m + O(B^{m-1/N})$ où C est une constante qu'on détermine explicitement en fonction des invariants classiques de K (discriminant, nombre de classes d'idéaux, régulateur, racines de l'unité). Dans le cas $m = 2$, $N = 1$, il faut remplacer le terme d'erreur par $O(B \log B)$. La démonstration se fait en comptant les points entiers dans l'espace affine et en divisant par l'action des unités, puis par l'action des idéaux principaux.

ABSTRACT. — Let K be a number field of degree N over $\mathbf{Q}$, and H_K the height relative to K of points in projective space of dimension $m - 1$. Let $\lambda(B)$ be the number of points in this projective space of height $\leq B$. We prove the asymptotic behavior $\lambda(B) \sim CB^m + O(B^{m-1/N})$, where C is a constant depending on the classical invariants of K (discriminant, class number, regulator, roots of unity). In the case $m = 2$, $N = 1$, one must replace the error term by $O(B \log B)$. The proof is done by counting integral points in affine space and by dividing by the action of units, followed by the action of principal ideals.

Introduction

In *Diophantine geometry* [5], LANG raises the problem of estimating the number of points in projective spaces, rational over a given number field K , of height at most B . The main result of this is Theorem 3, which asserts that the number of such points is $CB^m + O(B^{m-1/N})$ where $m - 1$ is the dimension of the projective space, N the degree of K over $\mathbf{Q}$, and C is a constant (depending on K and m) expressed in terms of classical invariants of K .

(*) Texte reçu le 16 mai 1978.

Stephen H. SCHANUEL, Mathematics Department, State University of New York Buffalo, N.Y. 14215 (États-Unis).

The basic idea is to study points with integral coordinates in affine m -space, and divide by the action of the units; then divide by the action of the principal integral ideals.

One counts integral points modulo units by an extension of the (DEDEKIND-WEBER) technique used to estimate the number of integral ideals of norm $\leq B$. The problem reduces to a geometric one: estimate the number of lattice points in $t\Delta$, where Δ is a bounded domain in Euclidean space, and t a large real number. The division by principal ideals is accomplished by an appropriate formulation of the Möbius inversion formula, coupled with some elementary estimates of partial sums of Dirichlet series.

This outline is oversimplified in two respects. One must count points with coordinates in a fixed ideal, modulo units; this differs only trivially from counting integral points modulo units. In the inversion, one inverts over all ideals, rather than just principal ideals. This has the advantage of rendering the inversion easier, and leading to a stronger result. Points in projective space are counted one class at a time, the class of a point being the ideal class of the ideal generated by the coordinates of the point.

I am indebted to Serge LANG, whose assistance and encouragement have been invaluable.

1. Integral points modulo units

Let K be a number field, i. e. a finite extension of the field $\mathbf{Q}$ of rational numbers, of degree N over $\mathbf{Q}$. A *divisor* $\mathfrak{d}$ on K is a pair $\mathfrak{d} = (\alpha, B)$, where α is a non-zero fractional ideal of K , and B a positive real number. The divisors form a group D under component-wise multiplication, and are partially ordered by: $(\alpha, B) \leq (\alpha', B')$ means $\alpha \subset \alpha'$ and $B \leq B'$. The *norm* of $\mathfrak{d}$, written $\|\mathfrak{d}\|$, is $BN\alpha^{-1}$, where $N\alpha$ denotes the ordinary norm of the fractional ideal α . S_∞ denotes the set of archimedean absolute values of K , normalized to extend the ordinary absolute value on $\mathbf{Q}$. For $v \in S_\infty$, N_v is the degree of the completion K_v over $\mathbf{R}$, and $|x|_v = v(x)$. To avoid numerous exponents, $\|x\|_v$ is used to abbreviate $|x|_v^{N_v}$, for x in K_v .

Let m be a positive integer, and K^m the cartesian product $K \times \dots \times K$. To any point X in $K^m - 0^m$ we associate a divisor

$$\mathfrak{d}_X = ([X], H_\infty X),$$

where:

$[X]$ is the ideal generated by the components of X , and

$$H_{\infty} X = \prod_{v \in S_{\infty}} \sup_i \|X_i\|_v.$$

For $m = 1$, the map $K^* \rightarrow D$ by $x \mapsto \mathfrak{d}_x$ is a homomorphism, with kernel U , the group of units of K , and image the *principal divisors*. Principal divisors have norm 1, so that $\|\mathfrak{d}\|$ depends only on the *class* of $\mathfrak{d}$ modulo principal divisors. The set of X in $K^m - 0^m$ satisfying $\mathfrak{d}_x \leq \mathfrak{d}$, for fixed $\mathfrak{d}$, is stable under componentwise multiplication by units; we denote the orbit set mod U by $L^m(\mathfrak{d})$, and the cardinality of $L^m(\mathfrak{d})$ by $\lambda^m(\mathfrak{d})$. Then $\lambda^m(\mathfrak{d})$ depends only on the class of $\mathfrak{d}$, since multiplication by $x \in K^*$ induces a bijection $L^m(\mathfrak{d}) \rightarrow L^m(\mathfrak{d}_x \mathfrak{d})$.

For $m = 1$, we have a classical estimate for λ . Namely $\lambda^1(a, B)$ is the number of principal ideals contained in a with norm at most B , and the Dedekind-Weber Theorem asserts that

$$\lambda^1(\mathfrak{d}) = \kappa \|\mathfrak{d}\| + O(\|\mathfrak{d}\|^{1-(1/N)}),$$

where κ is a constant depending only on K (cf. [8], [3]). Our first object is to extend this Theorem.

THEOREM 1:

$$\lambda^m(\mathfrak{d}) = \kappa_m \|\mathfrak{d}\|^m + O(\|\mathfrak{d}\|^{m-(1/N)})$$

where the constant κ_m is given by

$$\kappa_m = \left(\frac{2^{r_1} (2\pi)^{r_2}}{\sqrt{d}} \right)^m m^{\frac{r}{w}}.$$

The notations are classical:

r_i is the number of $v \in S_{\infty}$ with $N_v = i$;

$r = r_1 + r_2 - 1$;

d = the absolute value of discriminant of K ,

R = the regulator of K ,

w = the order of the group of roots of unity in K ,

N = degree of K over $\mathbb{Q}$.

The $O(\)$ is to be interpreted for $\|\mathfrak{d}\| \rightarrow \infty$. More explicitly, there exists constants $C^i = C_{K,m}^i$ such that for $\|\mathfrak{d}\| > C^1$:

$$|\lambda^m(\mathfrak{d}) - \kappa_m \|\mathfrak{d}\|^m| < C^2 \|\mathfrak{d}\|^{m-(1/N)}.$$

Let $\alpha_1, \dots, \alpha_h$ be a set of representatives for the ideal classes. Then any divisor can be adjusted, by multiplication by a principal divisor, to the form (α_i, B) for some i . Since $\lambda^m(\mathfrak{d})$ and $\|\mathfrak{d}\|$ depend only on the class of $\mathfrak{d}$, we see that it will be enough to prove :

For a fixed integral ideal

$$\lambda^m(\alpha, B) = \kappa_m \left(\frac{B^m}{N\alpha} \right) + O(B^{m-(1/N)}).$$

We shall prove the Theorem in this form. First we reduce it to a problem of counting lattice points in a certain bounded domain in the Euclidean space $\mathbf{R}^{mN}$. We estimate this by parametrizing implicitly the boundary of the domain. Portions of the proof carry over almost verbatim from the known case $m = 1$.

The following agreements will be in force for the remainder of this section: K, m and α are fixed; $(\alpha)^m$ denotes m -tuples of elements in α . The index v ranges over S_∞ the index i over the set $\{1, \dots, m\}$. Thus K_v is identifiable with $\mathbf{R}$ or $\mathbf{C}$, with ambiguity only up to complex conjugation; we fix an identification. Whenever convenient we identify $\mathbf{C}$ with the Euclidean space $\mathbf{R}^2$ in the usual way. U is the group of units, W the group of roots of unity. $\mathbf{R}^+$ is the multiplicative group of positive real numbers; $\overline{\mathbf{R}^+} = \mathbf{R}^+ \cup \{0\}$.

Let A be a set, G an abelian group operating on A ; H is a subgroup of G . We say G is *effective mod H* (on A) if $ga = a$ implies $g \in H$. A subset S of A is *fundamental mod H* (in A) if:

1° S is H -stable ($hs \in S$ for $h \in H, s \in S$),

2° $GS = A$,

3° $gS \cap S$ is empty for $g \notin H$.

If G operates on both A and A' , then a map $\Phi: A \rightarrow A'$ is called a G -map if it commutes with the action of G . The following Lemma is immediate from the definitions.

LEMMA 1. — Let $\Phi: A \rightarrow A'$ be a G -map, H a subgroup of G . If G is *effective mod H* on A' , then it is *effective mod H* on A . If $\Delta \subset A'$ is *fundamental mod H* , then so is $\Phi^{-1}\Delta \subset A$.

In particular, if A is a commutative semigroup with unit, any homomorphism $\alpha: G \rightarrow A$ induces an operation of G on A by $ga = \alpha(g)a$; G is *effective mod H* if the kernel of α is contained in H . If $\Phi: A \rightarrow A'$

is a semigroup homomorphism such that $\Phi\alpha = \alpha'$, then it is a G -map. In our applications, G will always be the group U of units of K , and H will be the subgroup W of roots of unity.

Embed K in $\prod_{v \in S_\infty} K_v$ by $x \mapsto (x, \dots, x)$; the image of $\mathfrak{a}$ is a lattice in $\mathbf{R}^N$ of determinant $N\mathfrak{a} \sqrt{d/2^{r_2}}$.

The diagonal embedding of U in $\prod_v K_v^m$ is a semigroup homomorphism, so U operates on $\prod_v K_v^m$. We want to choose a fundamental set mod W for the U -stable subset $\prod_v (K_v^m - 0^m)$. For this we need the following Theorem.

UNIT THEOREM. — *Map*

$$U \rightarrow \prod_v \mathbf{R}_v = \mathbf{R}^{r_1+r_2} \quad \text{by } u \mapsto (\log \|u\|_v).$$

This is a homomorphism, with kernel W and image a lattice of maximal rank r_1+r_2-1 in the hyperplane H defined by $\sum y_v = 0$.

Define

$$\eta : \prod_v (K_v^m - 0^m) \rightarrow \prod_v \mathbf{R}_v \quad \text{by } \eta = (\eta_v),$$

where $\eta_v : K_v^m - 0^m \rightarrow \mathbf{R}$ is given $\eta_v(X) = \log \sup_i \|X_i\|_v$. This is a U -map (but not a semigroup homomorphism because of the sup). Let $\text{pr} : \prod \mathbf{R}_v^+ \rightarrow H$ be the projection along the vector (N_v) , also a U -map. More explicitly

$$(\text{pr } y)_v = y_v - \left(\frac{1}{N} \sum_{w \in S_\infty} y_w \right) N_v.$$

(The reason for this particular projection will be apparent shortly.)

LEMMA 2. — *Let F be a fundamental set mod W for H . Then $\Delta = (\text{pr } \eta)^{-1} F$ is a fundamental set mod W for $\prod_v (K_v^m - 0^m)$. Also, U is effective on $\prod_v (K_v^m - 0^m)$.*

Proof. — The first assertion follows from Lemma 1, and the second is clear.

The selection of the set F is standard. Let $\bar{u}_1, \dots, \bar{u}_r$ be a basis for the image of U in H ; it is an $\mathbf{R}$ -basis for H . Let $\tau_1, \dots, \tau_r$ be the dual basis; i. e. $\tau_j : H \rightarrow \mathbf{R}$ is the linear functional satisfying $\tau_j(\bar{u}_k) = \delta_{jk}$. Then F is defined to be the set of $y \in H$ such that $0 \leq \tau_j(y) < 1$, $j = 1, \dots, r$.

Let $R(B) \subset \prod K_v^m$ be the subset defined by

$$\prod_v \sup_i \|Z_{iv}\|_v \leq B,$$

and put $\Delta(B) = \Delta R(B)$. Then $R(B)$ is clearly U -stable, since

$$\prod_v \sup_i \|u Z_{iv}\|_v = \prod_v \|u\|_v \cdot \prod_v \sup_i \|Z_{iv}\|_v = \prod_v \sup_i \|Z_{iv}\|_v.$$

We want to count the number of orbits under U in $((\mathfrak{a}^m - 0^m) \cap R(B)$. Since Δ is fundamental mod W for $\prod_v (K_v^m - 0^m)$, its intersection with any stable subset, in particular with $((\mathfrak{a}^m - 0^m) \cap R(B)$, is fundamental mod W . (Apply Lemma 1 to the inclusion map.) Hence we need only count the number of W -orbits in

$$((\mathfrak{a}^m - 0^m) \cap R(B) \cap \Delta = (\mathfrak{a}^m \cap \Delta(B).$$

Since W acts effectively, each W -orbit contains w points.

PROPOSITION 1. — $w \lambda^m(\mathfrak{a}, B)$ is the number of points of the lattice $(\mathfrak{a}^m \cap \Delta(B)$.

The choice of pr was made to ensure that $\Delta(B)$ depends homogeneously on B .

LEMMA 3. — We have $t \Delta = \Delta$ for $t \in \mathbf{R}^*$, $R(B) = B^{1/N} R(1)$, and $\Delta(B) = B^{1/N} \Delta(1)$ for $B > 0$.

Proof. — Let $Z \in \prod_v (K_v^m - 0^m)$, $t \in \mathbf{R}^*$. We have

$$\eta(tZ) = \log |t| (N_v) + \eta(Z).$$

Since pr is linear, and annihilates (N_v) , $\text{pr } \eta(tZ) = \text{pr } \eta(Z)$, hence the first assertion. If $\rho(Z) = \prod_v \sup_i \|Z_{iv}\|_v$, then

$$\rho(tZ) = |t|^{\sum N_v} \rho(Z);$$

but $\sum_v N_v = N$, hence the second assertion. The third is immediate from the first two.

The next Theorem will enable us to estimate the number of lattice points in $\Delta(B)$. Let I^l denote the closed cube $(0, 1)^l$ in $\mathbf{R}^l$. Call a subset of $\mathbf{R}^k$ *Lipschitz-parametrizable* if it is contained in a finite union of sets $\Phi_j(I^{k-1})$, the Φ satisfying a Lipschitz condition: $|\Phi_j x - \Phi_j y| < C_1 |x - y|$, where C_1 is a constant independent of j, x, y . Let μ denote Lebesgue measure, and $\bar{\Gamma}$ the closure of Γ .

THEOREM 2. — Let Γ be a bounded subset of $\mathbf{R}^k$, with Lipschitz-parametrizable boundary. Let Λ be a lattice in $\mathbf{R}^k$. Then the number of lattice points in $t \Gamma$ is given by

$$\#(\Lambda \cap t \Gamma) = t^k \frac{\mu(\bar{\Gamma})}{\det \Lambda} + O(t^{k-1}) \quad \text{for } t \rightarrow \infty.$$

This Lemma is standard (cf. for instance LANG [6], Theorem 2 of Chapter VI, § 2).

A subset of $\mathbf{R}^k$ is called C^1 -parametrizable (by $(k-1)$ -cubes) if it is contained in a finite union of sets $\Phi_j(I^{k-1})$, the Φ_j having continuous partials. Note that C^1 -parametrizations are Lipschitz by the mean value Theorem.

PROPOSITION 2. — The set $\Delta(1)$ is bounded, with C^1 -parametrizable boundary.

The proof is formulated as a sequence of Lemmas. For $\Gamma \subset \mathbf{R}^k$, $\partial\Gamma$ denotes the boundary of Γ in the usual topology on $\mathbf{R}^k$.

LEMMA 4. — $\Delta(1) = \Delta \cap R(1)$ is bounded.

Proof. — Let $Y \subset \prod_v \mathbf{R}_v$ be the subset defined by $\sum_{v \in S_\infty} y_v \leq 0$. Then y_v is bounded above for y in $Y \cap \text{pr}^{-1} F$, v in S_∞ ; since

$$y = \text{pr } y + \frac{1}{N} \sum y_w(N_v)$$

the first term having bounded components and the second negative components. But $\Delta(1) = \eta^{-1}(Y \cap \text{pr}^{-1} F)$, and the definition of η shows that if ηZ has components bounded above, then Z has bounded components.

LEMMA 5. — $\left| \frac{y_{v'}}{N_{v'}} - \frac{y_{v''}}{N_{v''}} \right|$ is uniformly bounded for $v', v'' \in S_\infty$, $y \in \text{pr}^{-1} F$.

Proof. — $(\text{pr } y)_v = y_v - (\sum_{w \in S_\infty} y_w)/N$ and division by N_v yields

$$\frac{(\text{pr } y)_v}{N_v} = \frac{y_v}{N_v} - \frac{\sum_{w \in S_\infty} y_w}{N}.$$

The left side is bounded, and the difference of the values on the right for $v = v'$, $v = v''$ is the number we wished to estimate.

LEMMA 6. — The closure in $\prod_v \mathbf{R}_v^+$ of $(\text{pr } \log)^{-1} F$ is contained in $\prod_v \mathbf{R}_v^+ \cup \{0\}$.

Proof. — Let $x^j \in (\text{pr } \log)^{-1} F$ such that $x_{v'}^j \rightarrow 0$. We must show $x_{v''}^j \rightarrow 0$ for all $v'' \in S$. Put $y^j = \log x^j$. We see that $y_{v'}^j \rightarrow -\infty$. Hence, by Lemma 5, $y_{v''}^j \rightarrow -\infty$, so $x_{v''}^j \rightarrow 0$.

Let

$$\Phi: \prod_v K_v^m \rightarrow \mathbf{R}_v^+$$

be defined by

$$(\Phi Z)_v = \sup_i \|Z_{iv}\|_v.$$

Then we have the following diagram of continuous maps:

$$\begin{array}{ccccc} (K_v^m - 0^m) & \xrightarrow{\Phi_0} & \mathbf{R}_v^+ & \xrightarrow{\log} & \mathbf{R}_v \xrightarrow{\text{pr}} H \subset \mathbf{R}_v \\ \downarrow & & \downarrow & & \\ K_v^m & \xrightarrow{\Phi} & \overline{\mathbf{R}_v^+} & & \end{array}$$

where the vertical maps are inclusions, Φ_0 is the restriction of Φ , and the composite $\log \Phi_0 = \eta$.

LEMMA 7. — *The closure of Δ in $\prod_v K_v^m$ is contained in*

$$\prod_v (K_v^m - 0^m) \cup \{0\}.$$

Proof. — We have

$$\Delta = \Phi^{-1}(\text{pr log})^{-1}F.$$

Continuity of Φ gives

$$\overline{\Delta} \subset \Phi^{-1}(\overline{(\text{pr log})^{-1}F}) \subset \Phi^{-1}(\prod_v \mathbf{R}_v^+ \cup \{0\}) \subset \prod_v (K_v^m - 0^m) \cup \{0\},$$

the bar indicating closure in $\prod_v K_v^m$, $\prod_v \overline{\mathbf{R}_v^+}$, respectively.

For the next sequence of Lemmas, we borrow the letter “ D ” to use for the derivative of a map from an open subset of $\mathbf{R}^k$ to $\mathbf{R}^l$. *Differentiable* means *having continuous partial derivatives*.

LEMMA 8. — *Any compact subset of $\partial R(1)$ is C^1 -parametrizable.*

Proof. — Let $\rho: \prod_v K_v^m \rightarrow \overline{\mathbf{R}^+}$ be given by $\rho(Z) = \prod_v \sup_i \|Z_{iv}\|_v$. If σ is a map $S_\infty \rightarrow \{1, 2, \dots, m\}$, let

$$\rho_\sigma: \prod_v K_v^m \rightarrow \overline{\mathbf{R}^+} \quad \text{by} \quad \rho_\sigma(Z) = \prod_v \|Z_{\sigma v, v}\|_v.$$

Then ρ and ρ_σ are differentiable on $\rho_\sigma^{-1}(\mathbf{R}^+)$, with non-vanishing derivative. We have $R(1) = \rho^{-1}([0, 1])$, hence

$$\partial R(1) \subset \rho^{-1}(\partial_{\overline{\mathbf{R}^+}}([0, 1])) = \rho^{-1}(1) \subset \prod_\sigma \rho_\sigma^{-1}(1).$$

Let H_σ be the closed hypersurface $\rho_\sigma^{-1}(1)$. Choose for each $Z \in H_\sigma$ an open neighborhood $W_{Z, \sigma}$ and a differentiable map $\Psi_{Z, \sigma}: I^{mN-1} \rightarrow \mathbf{R}^{mN}$ satisfying

$$W_{Z, \sigma} \cap H_\sigma \subset \Psi_{Z, \sigma}(I^{mN-1}).$$

This is possible by the implicit function Theorem, since $D\rho_\sigma$ does not vanish on H_σ . Now if C compact, $C \subset \partial R(1)$, select for each σ a finite set of $W_{Z,\sigma}$ covering $C \cap H_\sigma$. Then

$$C = \bigcup_\sigma (C \cap H_\sigma) \subset \bigcup_\sigma \bigcup_{\text{finite}} (W_{Z,\sigma} \cap H_\sigma) \subset \bigcup_{\text{finite}} \Psi_{Z,\sigma}(I^{mN-1}).$$

The parametrization of subsets of $\partial\Delta$ is similar; but it requires more care, since the hypersurfaces used are not closed. We borrow “ S ” to denote the unit $(mN-1)$ -sphere in $\mathbf{R}^{mN} = \prod_v K_v^m$.

LEMMA 9. — *The intersection of $\partial\Delta$ with S is C^1 -parametrizable by $(mN-2)$ -cubes.*

Proof. — Taking our clue from the fact that Δ is defined by $0 \leq \tau_j \text{ pr } \eta(Z) < 1$, we construct finitely many hypersurfaces whose union contains $\partial\Delta - \{0\}$. Define, for

$$\sigma: S_\infty \rightarrow \{1, \dots, m\}, \quad \eta_\sigma: V_\sigma \rightarrow \prod_v \mathbf{R}_v \quad \text{by } \eta_\sigma(Z) = \log(\|Z_{\sigma v, v}\|_v),$$

where $V_\sigma \subset \prod_v (K_v^m - 0^m)$ is the open subset

$$\{Z; Z_{\sigma v, v} \neq 0 \text{ for } v \in S_\infty\}.$$

Then η_σ is differentiable, and $D\eta_\sigma(Z): \mathbf{R}^{mN} \rightarrow \prod_v \mathbf{R}_v$ is surjective at all Z . (This reduces immediately to the same assertion for $K_v^* \rightarrow \mathbf{R}$ by $Z \mapsto \log \|Z\|_v$; since $V_\sigma = \prod_v K_v^{m-1} \times \prod_v K_v^*$, and η_σ factors into: projection on the second factor, followed by a componentwise map $\prod_v K_v^* \rightarrow \prod_v \mathbf{R}_v$.) Now for

$$l_\alpha = (j, \sigma, \delta) (j = 1, \dots, r; \quad \sigma: S_\infty \rightarrow \{1, \dots, m\}; \quad \delta \in \{0, 1\}),$$

define $\rho_\alpha: V_\sigma \rightarrow \mathbf{R}$ by $\rho_\alpha(Z) = \tau_j \text{ pr } \eta_\sigma(Z) - \delta$. Let H_α be the hypersurface defined by $\rho_\alpha = 0$. Since ρ_α is continuous, H_α is closed in V_σ (but not in $\mathbf{R}^{mN}$). Furthermore $\rho_\alpha(tZ) = \rho_\alpha(Z)$ for $t \in \mathbf{R}^*$, by the same computation that showed $t\Delta = \Delta$, with η replaced by η_σ . Since τ_j , pr are linear and surjective, and $D\eta_\sigma(Z)$ is surjective, $D\rho_\alpha(Z)$ is surjective. This, together with the homogeneity of ρ_α , insures that the functionals $D\rho_\alpha(Z)$ and $D\xi(Z)$ are linearly independent (even orthogonal), where ξ is the momentary symbol for the Euclidean norm of a vector. Thus H_α and S intersect nicely; we apply the implicit function Theorem. For any $Z \in H_\alpha \cap S$, there exist a neighborhood $W_{Z,\alpha}$ of Z , and a differentiable function $\Psi_{Z,\alpha}: I^{mN-2} \rightarrow \mathbf{R}^{mN}$, such that $(W_{Z,\alpha} \cap H_\alpha \cap S) \subset \Psi_{Z,\alpha}(I^{mN-2})$.

We want to get $\partial\Delta \cap S$ inside a (finite) union of compact subsets $H'_\alpha \subset H_\alpha \cap S$; then we can finish the proof as in Lemma 8. Let

$$F_\sigma = \{Z \in \prod_v K_v^m \text{ such that } \|Z_{\sigma v, v}\|_v = \sup_i \|Z_{iv}\|_v \text{ for all } v\},$$

and $F'_\sigma = \partial\Delta \cap S \cap F_\sigma$. Then F'_σ is compact, since each of the three sets is closed, and S compact. Further, $F'_\sigma \subset V_\sigma$, since the only point of $\partial\Delta$ with some $\sup_i \|Z_{iv}\|_v = 0$ is the origin, by Lemma 7. Let $H'_\alpha = H_\alpha \cap F'_\sigma$, for $\alpha = (j, \sigma, \delta)$. Then H'_α is compact. Namely H_α and F'_σ are closed in V_σ , so $H_\alpha \cap F'_\sigma$ is closed in F'_σ . Finally, by Lemma 7, $\partial\Delta \cap S$ is contained in the boundary relative to $\prod_v (K_v^m - 0)$ of Δ . But any point Z of the latter boundary satisfies $\tau_j \text{ pr } \eta(Z) = \delta$ for some j, δ ; choosing σ to yield the sup at Z gives $Z \in H_{j, \sigma, \delta} \cap F_\sigma$. Thus

$$\partial\Delta \cap S \subset \bigcup_\alpha (H_\alpha \cap F_\alpha),$$

and intersecting with $\partial\Delta \cap S$ on the right is harmless: $\partial\Delta \cap S \subset \bigcup_\alpha H'_\alpha$, yielding the Lemma.

LEMMA 10. — *The boundary of $\Delta(1)$ is parametrizable.*

Proof. — We have $\Delta(1) = \Delta \cap R(1)$, hence $\partial\Delta(1) \subset \partial\Delta \cup \partial R(1)$. Since $\Delta(1)$ is bounded, it suffices to parametrize compact subsets of $\partial\Delta$, $\partial R(1)$. But $\partial\Delta = \mathbf{R}^+ (\partial\Delta \cap S) \cup \{0\}$, which gives an obvious way to parametrize compact subsets of $\partial\Delta$. Namely if $\Phi_j : I^{mN-2} \rightarrow \mathbf{R}^{mN}$ parametrize $\partial\Delta \cap S$, then

$$\Psi_j : I^{mN-1} \rightarrow \mathbf{R}^{mN} \text{ by } \Psi_j(X, t) = Ct\Phi_j(X)$$

will do to parametrize any bounded subset of $\partial\Delta - \{0\}$.

In case $\partial\Delta \cap S$ is empty ($r = 0$), we have missed the point 0; parametrize it separately.

The proof of Proposition 2 is complete, so that we may apply Theorem 2. Since $\Delta(B) = B^{1/N} \Delta(1)$, we have

$$\begin{aligned} w\lambda^m(\alpha, B) &= (B^{1/N})^{mN} \frac{\mu(\Delta(1))}{\det(\alpha)^m} \\ &+ O(B^{1/N(mN-1)}) = \frac{2^{r_2m}}{\sqrt{d^m}} \overline{(\Delta(1))} \left(\frac{B}{N\alpha} \right)^m + O(B^{m-1/N}), \end{aligned}$$

so that the proof of Theorem 1 will be complete with the following computation.

PROPOSITION. — $\mu(\overline{\Delta(1)}) = Rm^r (2^{r_1} \pi^{r_2})^m$.

Proof. — The computation closely parallels that for the case $m = 1$ (cf. HECKE [3]).

For $N_v = 2$, let ρ_{iv} , θ_{iv} be polar coordinates in K_v^m :

$$\rho_{iv} = |Z_{iv}|, \quad \theta_{iv} = \arg Z_{iv}.$$

For $N_v = 1$, put $\rho_{iv} = |Z_{iv}|$.

Then

$$\mu(\overline{\Delta(1)}) = 2^{mr_1} \int \prod' \rho_{iv} \prod d\rho_{iv} \prod' d\theta_{iv},$$

where the $\prod$ is over all $i = 1, \dots, m$, $v \in S_\infty$ and $\prod'$ over $i = 1, \dots, m$, v complex ($N_v = 2$), and the integration over $\rho_{iv} \geq 0$, $0 \leq \theta_{iv} < 2\pi$,

$$\prod_v \sup_i \rho_{iv}^{N_v} \leq 1, \\ \text{pr } \log \sup(\rho_{iv}^{N_v}) \in \bar{F}.$$

Integrating with respect to the θ_{iv} , we get

$$2^{mr_1} (2\pi)^{mr_2} \int \prod_{i,v} (\rho_{iv}^{N_v-1} d\rho_{iv}).$$

The domain of integration is the union of domains D_σ ,

$$\sigma: S_\infty \rightarrow \{1, \dots, m\}$$

specified by

$$D_\sigma = \{(\rho_{iv}) \text{ such that } \sup_i \rho_{iv} = \rho_{\sigma v, v}\},$$

meeting only on lower dimensional linear subspaces $\rho_{iv} = \rho_{jv}$.

There are $m^{r_1+r_2}$ of these, and by symmetry we get

$$m^{r_1+r_2} 2^{mr_1} (2\pi)^{mr_2} \int \prod_{i,v} (\rho_{iv}^{N_v-1} d\theta_{iv}),$$

over the domain, $\rho_{1v} \geq \rho_{iv} \geq 0$,

$$\prod_v \rho_{iv}^{N_v} \leq 1, \\ \text{pr } \log(\rho_{iv}^{N_v}) \in \bar{F}.$$

Let $t_{iv} = \rho_{iv}^{N_v}$, so $dt_{iv} = N_v \rho_{iv}^{N_v-1} d\rho_{iv}$. Then we have

$$m^{r_1+r_2} 2^{mr_1} (2\pi)^{mr_2} \int \prod_{i,v} \left(\frac{1}{N_v} dt_{iv} \right) = m^{r_1+r_2} 2^{mr_1} \pi^{mr_2} \int \prod_{i,v} dt_{iv}.$$

Integrate over all t_{iv} with $i \neq 1$. We get

$$m^{r_1+r_2} 2^{mr_1} \pi^{mr_2} \int \prod_v (t_{1v}^{m-1} dt_{1v})$$

Put

$$u = \prod_v t_{iv} \\ \xi_j = \tau_j \operatorname{pr} \log(t_{iv}), j = 1, \dots, r.$$

The jacobian is $\pm R$, and we get

$$m^{r_1+r_2} 2^{mr_1} \pi^{mr_2} R \int u^{m-1} du \prod_j d\xi_j,$$

with the integration over the cube $0 \leq u \leq 1$, $0 \leq \xi_j \leq 1$, so the integral equals $1/m$, which gives the result.

2. The inversion

We recall that $\|\mathfrak{d}\|$ depends only on the class of $\mathfrak{d}$ modulo principal divisors, so that the map $K^m - 0^m \rightarrow \mathbf{R}^+$ given by $X \rightarrow \|\mathfrak{d}_X\|$ induces a map from the projective space $P^{m-1}(K)$ to $\mathbf{R}^+$, associating to any point K^*X its *height*, $\|\mathfrak{d}_X\|$. Theorem 1 can be applied to gives an estimate for the number of points in $P^{m-1}(K)$ of height at most B . The technique is parallel to that used to handle the case $K = \mathbf{Q}$, $m = 2$ (cf. [2], Chap. 16-18). We need only the most elementary facts about the zeta-function of K , namely convergence of the Dirichlet series

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N \mathfrak{a}^s}$$

and the product formula:

$$\prod_{\mathfrak{p}} (1 - N \mathfrak{p}^{-s})^{-1} = \zeta_K(s),$$

for real $s > 1$. (The sum extends over all integral ideals, the product over all prime ideals.)

Let I be the multiplicative semigroup of non-zero integral ideals of K , $\mathbf{R}(I)$ the set of functions $I \rightarrow \mathbf{R}$. Then $\mathbf{R}(I)$ is a commutative ring with unit, addition being pointwise and multiplication by convolution

$$(\chi_1 \chi_2)(\mathfrak{a}) = \sum_{\mathfrak{a}_1 \mathfrak{a}_2 = \mathfrak{a}} \chi_1(\mathfrak{a}_1) \chi_2(\mathfrak{a}_2).$$

Let $\mathbf{R}(D)$ be the set of functions $D \rightarrow \mathbf{R}$, vanishing on divisors of norm < 1 . Then $\mathbf{R}(D)$ is a module over $\mathbf{R}(I)$, if we define, for $\chi \in \mathbf{R}(I)$, $f \in \mathbf{R}(D)$,

$$\chi f(\mathfrak{a}, \frac{1}{N\mathfrak{a}}B) = \sum_{\mathfrak{b}} \chi(\mathfrak{b}) f(\mathfrak{b}\mathfrak{a}, B),$$

the sum extending over all integral ideals $\mathfrak{b}$. (The sums in both convolutions are finite.) Let $\mu \in \mathbf{R}(I)$ be the Möbius function:

$$\mu(\mathfrak{p}) = -1, \mu(\mathfrak{p}^v) = 0 \quad \text{for } v > 1, \mu(1) = 1 \quad \text{and} \quad \mu(\mathfrak{a})\mu(\mathfrak{b}) = \mu(\mathfrak{a}\mathfrak{b})$$

for $\mathfrak{a}, \mathfrak{b}$ relatively prime. Let χ_0 be the constant function $\chi_0(\mathfrak{a}) = 1$, all $\mathfrak{a}$. Then the Möbius inversion formula asserts that μ, χ_0 are inverses.

To estimate μf , for f in $\mathbf{R}(D)$, we will need the following Lemmas.

LEMMA 11. — For real $s > 1$:

$$\sum \frac{\mu(\mathfrak{a})}{N\mathfrak{a}^s} = \frac{1}{\zeta_K(s)},$$

the sum extending over all integral ideals $\mathfrak{a}$.

The Lemma is immediate from the fact that μ and χ_0 are inverses.

LEMMA 12. — Let $f, g \in \mathbf{R}(D)$. If $f(\mathfrak{b}) = \alpha \|\mathfrak{b}\|^s$ for s real > 1 , and $\|\mathfrak{b}\| \geq 1$, then

$$\mu f(\mathfrak{b}) = \frac{\alpha}{\zeta_K(s)} \|\mathfrak{b}\|^s + O(\|\mathfrak{b}\|).$$

If $g(\mathfrak{b}) = O(\|\mathfrak{b}\|^t)$ with t real ≥ 1 , then

$$\mu g(\mathfrak{b}) = O(\|\mathfrak{b}\|^t) \quad \text{for } t > 1,$$

and

$$\mu g(\mathfrak{b}) = O(\|\mathfrak{b}\| \log \|\mathfrak{b}\|) \quad \text{for } t = 1.$$

Proof. — Let $\mathfrak{b} = (\mathfrak{a}, B)$. Then

$$\mu f(\mathfrak{b}) = \sum_{N\mathfrak{a}\mathfrak{b} \leq B} \alpha \mu(\mathfrak{b}) (B/N\mathfrak{a}\mathfrak{b})^s = \alpha \|\mathfrak{b}\|^s \sum \frac{\mu(\mathfrak{b})}{N\mathfrak{b}^s}.$$

The sum is

$$\zeta_K(s)^{-1} - \sum_{N\mathfrak{b} \geq \mathfrak{b}} \frac{\mu(\mathfrak{b})}{N\mathfrak{b}^s},$$

with the latter term bounded by $\sum_{N\mathfrak{b} \geq \|\mathfrak{b}\|} 1/N \mathfrak{b}^s$, which is $O(\|\mathfrak{b}\|^{1-s})$, by an easy estimate, using the fact that the number of ideals of norm at most B is $O(B)$ ([4], Satz 203). On the other hand,

$$\mu g(\mathfrak{b}) = O\left(\|\mathfrak{b}\|^t \sum_{N\mathfrak{b} \leq \|\mathfrak{b}\|} \frac{1}{N \mathfrak{b}^t}\right),$$

and the sum is bounded by $\zeta_K(t)$, hence $O(1)$, for $t > 1$. For $t = 1$, $\sum_{N\mathfrak{b} \leq \|\mathfrak{b}\|} 1/N \mathfrak{b}$ is $O(\log \|\mathfrak{b}\|)$, again by [4] (Satz 203).

Let $Cl(\mathfrak{a})$ denote the class of $\mathfrak{a}$ modulo principal ideals. As before, $[X]$ is the ideal generated by $X_1, \dots, X_m$, and

$$H_\infty X = \prod_v \sup_i \|X_i\|_v.$$

Let $\tilde{L}^m(\mathfrak{b}) = \tilde{L}^m(\mathfrak{a}, B)$ be the set of points $K^* X$ in $P^{m-1}(K)$ of class $Cl[X] = Cl(\mathfrak{a})$, height at most $\|\mathfrak{b}\| = B N \mathfrak{a}^{-1}$. Let $\tilde{\lambda}^m(\mathfrak{b})$ denote the cardinality of $\tilde{L}^m(\mathfrak{b})$.

Note that for $\|\mathfrak{b}\| < 1$, both $\lambda^m(\mathfrak{b})$ and $\tilde{\lambda}^m(\mathfrak{b})$ are zero, since $\mathfrak{d}_X$ has norm at least 1; hence $\lambda^m, \tilde{\lambda}^m$ are in $\mathbf{R}(D)$.

THEOREM 3:

$$\tilde{\lambda}^m(\mathfrak{b}) = \frac{\chi_m}{\zeta_K(m)} \|\mathfrak{b}\|^m + O(\|\mathfrak{b}\|^{m-1/N}),$$

for $m = 2, 3, \dots$ and $N = 1, 2, \dots$ (except that, for $m = 2, N = 1$, the error term is to be replaced by $O(\|\mathfrak{b}\| \log \|\mathfrak{b}\|)$).

Proof. — Let

$$\bar{L}^m(\mathfrak{a}, B) = \{UX \in (K^m - 0^m)/U \text{ such that } [X] = \mathfrak{a}, H_\infty X \leq B\}.$$

Then

$$L^m(\mathfrak{a}, B) = \bigcup_{\mathfrak{b}} \bar{L}(\mathfrak{a}\mathfrak{b}, B),$$

the (disjoint) union extending over all integral ideals $\mathfrak{b}$. (For $N\mathfrak{b} > B/N \mathfrak{a}$, $\bar{L}(\mathfrak{a}\mathfrak{b}, B)$ is empty, so that the union is actually finite.) The map

$$\bar{L}^m(\mathfrak{c}, B) \rightarrow \tilde{L}^m(\mathfrak{c}, B) \text{ by } UX \rightarrow K^* X,$$

is easily verified to be a bijection, hence

$$\lambda^m(\mathfrak{a}, B) = \sum_{\mathfrak{b}} \tilde{\lambda}^m(\mathfrak{a}\mathfrak{b}, B).$$

Thus $\lambda^m = \chi_0 \tilde{\lambda}^m$, so $\mu \lambda^m = \mu \chi_0 \tilde{\lambda}^m = \tilde{\lambda}^m$. By Theorem 1, $\lambda^m = f + g$, where

$$f(\mathfrak{d}) = \kappa_m \|\mathfrak{d}\|^m \quad \text{and} \quad g(\mathfrak{d}) = O(\|\mathfrak{d}\|^{m-1/N}).$$

Hence $\mu \lambda^m = \mu f + \mu g$, and Lemma 12 yields the Theorem.

COROLLARY. — *The number of points in $P^{m-1}(K)$, of height at most B , is*

$$h \frac{\kappa_m}{\zeta_K(m)} B^m + O(B^{m-(1/N)}),$$

where h is the number of ideal classes. (For $m = 2$, $N = 1$, replace the error term by $O(B \log B)$.)

Proof. — If α_i are representatives for the ideal classes ($i = 1, \dots, k$), then the number of points of class $Cl(\alpha_i)$, height at most B , is $\lambda^m(\alpha_i, B \mathbf{N} \alpha_i)$ since this divisor has norm B . Summing over the ideal classes yields the Corollary.

The inversion in Theorem 3 can be copied verbatim to yield a more general result which interpolates between Theorems 1 and 3. Let S be any set of primes containing S_∞ . Then any ideal $\mathfrak{a}$ factors as $\mathfrak{a} = \alpha_S \alpha_{S'}$, where $(\alpha_S, \mathfrak{p}) = 1$ for $\mathfrak{p} \notin S$, and $(\alpha_{S'}, \mathfrak{p}) = 1$ for $\mathfrak{p} \in S - S_\infty$. The group of S -units, K_S , is the set of $x \in K^*$ for which $[x]_{S'} = 1$. Put

$$L_S^m(\mathfrak{a}, B) = \left\{ K_S X \in (K^m - 0^m)/K_{S'} \text{ such that } [X]_{S'} = \alpha_{S'}, \right. \\ \left. Cl[X]_S = Cl(\alpha_S), \mathbf{N}[X]^{-1} H_\infty X \leq \frac{B}{\mathbf{N} \alpha_S} \right\}$$

and let $\lambda_S^m(\mathfrak{d})$ be the cardinality of $L_S^m(\mathfrak{d})$. For $S = S_\infty$, $\lambda_{S_\infty}^m = \lambda^m$, and for S the set of all primes, $\lambda_S^m = \tilde{\lambda}^m$. Let $\mu_S, \chi_S \in \mathbf{R}(I)$ be multiplicative on relatively prime ideals, with $\mu_S(\mathfrak{p}^v) = 1$ if $\mathfrak{p} \in S - S_\infty$, $v = 1$, and zero otherwise; $\chi_S(\mathfrak{p}^v) = 1$ if $\mathfrak{p} \in S - S_\infty$, zero otherwise. Then μ_S, χ_S are inverses, and just as before we can conclude $\lambda^m = \chi_S \lambda_S^m$, so $\mu_S \lambda^m = \lambda_S^m$.

The estimates go as before, with $\zeta_K(s)$ replaced by

$$\zeta_S(s) = \sum \frac{\chi_S(\mathfrak{a})}{\mathbf{N} \alpha^s},$$

since the series

$$\sum \frac{\chi_S(\mathfrak{a})}{\mathbf{N} \alpha^s} \quad \text{and} \quad \sum \frac{\mu_S(\mathfrak{a})}{\mathbf{N} \alpha^s},$$

are still termwise dominated by $\sum 1/\mathbf{N} \alpha^s$.

In case S is finite, we can improve the estimates for the cases $m = 1$ or 2. Namely the Dirichlet series $\sum \mu_S(\mathfrak{b})/N \mathfrak{b}$ terminates, hence $\sum_{N \mathfrak{b} \leq \|\mathfrak{b}\|} \mu_S(\mathfrak{b})/N \mathfrak{b}^s$ is constant (equal to $\prod_{\mathfrak{p} \in S} (1 - N \mathfrak{p}^{-1})$) for large $\|\mathfrak{b}\|$.

Thus we obtain the following Theorem.

THEOREM 4. — For $m = 2, 3, \dots$ and $N = 1, 2, \dots$, we have

$$\lambda_S^m(\mathfrak{b}) = \frac{\kappa_m}{\zeta_S(m)} \|\mathfrak{b}\|^m + O(\|\mathfrak{b}\|^{m-(1/N)}),$$

For $m = 2$, $N = 1$, and S infinite, we have

$$\lambda_S^2(\mathfrak{b}) = \frac{\kappa_2}{\zeta_S(2)} \|\mathfrak{b}\|^2 + O(\|\mathfrak{b}\| \log \|\mathfrak{b}\|).$$

If S is finite, we have also

$$\lambda_S^1(\mathfrak{b}) = \prod_{\mathfrak{p} \in S} (1 - N \mathfrak{p}^{-s}) \kappa_1 \|\mathfrak{b}\| + O(\|\mathfrak{b}\|^{1-1/N}).$$

Let $\mathfrak{a}$ be prime to S , and $\alpha_1, \dots, \alpha_{h_S}$ be representatives for the subgroup of the ideal class group generated by the primes in $S - S_\infty$, with $\alpha_i = (\alpha_i)_S$. Then

$$\bigcup_i L_S^m(\alpha \alpha_i, B N \alpha_i) = \left\{ K_S X \in (K^m - 0^m)/K_S \text{ such that } [X]_{S'} \subset \alpha, \right. \\ \left. N[X]_S^{-1} H_\infty(X) \leq B \right\},$$

eliminating the condition on the classes. Hence the cardinality of this set is $\sum_{i=1}^{h_S} \lambda_S^m(\alpha \alpha_i, B N \alpha_i)$, which is just

$$h_S \frac{\kappa_m}{\zeta_S(m)} (B/N \mathfrak{a})^m + O((B/N \mathfrak{a})^{m-1/N}),$$

with the usual exception, since all the divisors in the sum have norm $B/N \mathfrak{a}$.

For $m = 1$, S finite, this estimates the number of principal S -ideals contained in a given S -ideal, with bounded norm (cf. [6]). Namely, the S -integers are those $x \in K^*$ with $[x]_{S'} \subset (1)$. Ideals in this ring are in norm-preserving correspondence with integral ideals of K , prime to S , and the units of the ring are just K_S .

Some possible extensions should be mentioned. For $m = 1$, LANDAU has improved the error term in Theorem 1 to $O(\|\mathfrak{b}\|^{1-2/(N+1)})$, by making

use of the analytic continuation of, and functional equation for, $\zeta_K(s)$ (see [4], Satz 210). A corresponding improvement for $m \neq 1$ would be inherited by all subsequent estimates.

Finally, one might extend in another direction, replacing the condition

$$\prod_{v \in S_\infty} \sup_i \|X_i\|_v \leq B,$$

in the definition of L^m by a set of conditions

$$\prod_{v \in S_j} \sup_i \|X_i\|_v \leq B_j,$$

where S_∞ is the disjoint union of S_j , and dividing by the appropriate unit group. For S_j consisting of singletons, $m = 1$, this would include the estimate of the number of points in parallelotopes. This should be followed by a variation on the inversion, based on a partition of the set of primes. So far I have been able to carry through only the first part of this program, obtaining necessary and sufficient conditions on the partition of S_∞ to yield finiteness, and yielding an estimate of the same type as in Theorem 1.

REFERENCE

- [1] DAVENPORT (H.). — On a principle of Lipschitz, *J. London math. Soc.*, t. 26, 1951, p. 179-183.
- [2] HARDY (G. H.) and WRIGHT (E. M.). — *An introduction to the theory of numbers*. — Oxford, Clarendon Press, 1938.
- [3] HECKE (H.). — *Vorlesungen über die Theorie der algebraischen Zahlen*. — Leipzig, Akademische Verlagsgesellschaft, 1923.
- [4] LANDAU (E.). — *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*. — Leipzig, Teubner, 1927.
- [5] LANG (S.). — *Diophantine geometry*. — New York, Interscience Publishers, 1962 (*Interscience Tracts in pure and applied Mathematics*, 11).
- [6] LANG (S.). — *Algebraic number theory*. — Reading, Addison-Wesley publishing Company, 1970 (*Addison-Wesley Series in Mathematics*).
- [7] SCHANUEL (S.). — On heights in number fields, *Bull. Amer. math. Soc.*, t. 70, 1964, p. 262-263.
- [8] WEBER (H.). — *Lehrbuch der Algebra*, Band 2, 2te Auflage. — Braunschweig, F. Vieweg, 1899.