Algebraic Number Theory, Math 421
Instructor: Sreekar M. Shastry
Notes on the distribution of ideals in number fields ([Mar77, Ch.6])

We use the usual notation, $K, L/K, G, \mathcal{O}_K, \mathcal{O}_L, P, Q, \ldots$

1. Roughly speaking, the idea is to show that the ideals of $\mathcal{O}_K$ are approximately equidistributed among the ideal classes and that the number of ideals with $\|I\| \leq t$ is approximately proportional to t.

Definition 2. Write $n = [K : \mathbb{Q}]$ and for each $t \geq 0$ put

$$i(t) := \#\{\text{ideals } I \subset \mathcal{O}_K : \|I\| \leq t\}$$

and for $C \in \mathrm{Cl}(K)$, put

$$i_C(t) := \#\{\text{ideals } I \in C : \|I\| \leq t\}$$

so that we have

$$i(t) = \sum_{C \in \mathrm{Cl}(K)} i_C(t).$$

This is a finite sum since the class group is finite.

Theorem 3. *There is a number κ depending only on $\mathcal{O}_K$ such that*

$$i_C(t) = \kappa t + \varepsilon_C(t)$$

where the error term is[1]

$$\varepsilon_C(t) = O(t^{1-1/n}).$$

Remark 4. We will determine κ later. This theorem is a refinement of and implies the statement

$$\frac{i_C(t)}{t} \to \kappa \text{ as } t \to \infty.$$

Summing over C we obtain the

Corollary 5. $i(t) = \kappa h_K t + \varepsilon(t)$ *where* $h_K := \#\mathrm{Cl}(K)$ *and* $\varepsilon(t) = O(t^{1-1/n})$.

Remarks 6. (a) This corollary will lead to the class number formula.

(b) Let us note that in the case $K = \mathbb{Q}$, $i(t) = [t]$ is the greatest integer $\leq t$ so that $\kappa = 1$ and $\varepsilon(t) = [t] - t$. The condition $\varepsilon(t) = O(t^{1-1/n}) = O(1)$ just expresses the fact that $\varepsilon(t)$ is bounded.

Proof of the Theorem. The idea is to count ideals in C by counting elements in a certain ideal. Let us fix an ideal $J \in C^{-1}$. Then there is a bijection

$$\left\{ \begin{array}{c} \text{ideals } I \in C \\ \text{s.t. } \|I\| \leq t \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{principal ideals } (\alpha) \subset J \\ \text{s.t. } \|(\alpha)\| \leq t\|J\| \end{array} \right\}$$

in which I corresponds to $IJ = (\alpha)$. Counting principal ideals $(\alpha) \subset J$ amounts to counting orbits of J under the action of $U := \mathcal{O}_K^\times$.

(We may rephrase the above as follows. Put

$$J_t := \{\alpha \in J : \|(\alpha)\| \leq t\|J\|\}.$$

Then the U action on J restricts to an action on J_t; the latter is a finite set because of what we know about the geometry of numbers and we have

$$i_C(t) = \#(U \backslash J_t).$$

It is this set that we shall count.)

[1]Recall that $f = O(g)$ iff $\limsup_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| < \infty$ or equivalently, $\frac{f(x)}{g(x)}$ is bounded as $x \to \infty$.

If K contained only finitely many units then we would have that $\#U.i_C(t)$ coincides with the number of elements $\alpha \in J$ such that $\|(\alpha)\| \leq t\|J\|$ and we might use geometric arguments with lattices to attack the problem.

There is one nontrivial case in which $\#U$ is finite, namely when K is imaginary quadratic. Let us consider this case first as it will give us some insight for the general case. Thus, until further notice, K is assumed to be imaginary quadratic.

We know that $\mathscr{O}_K$ is a lattice in $\mathbb{C}$ and therefore so is J. Moreover, $\|(\alpha)\| = \mathrm{N}_{K/\mathbb{Q}}(\alpha) = |\alpha|^2$ for $\alpha \neq 0$. Therefore we seek to count the number of nonzero elements of J in the circle of radius $\sqrt{t\|J\|}$ centered at 0. Let F be a fundamental domain for $J \subset \mathbb{C}$ and consider the translates of F centered at the various points of J; the number of points of J in a circle of radius ρ is approximately the number of these translates which are contained in the circle, and the latter is approximately $\pi\rho^2/\mathrm{vol}(F)$.

These estimates are good for large ρ; specifically, let $n^-(\rho)$ be the number of translates of F which are centered at points of J and which are entirely contained within a circle of radius ρ centered at 0 and let $n^+(\rho)$ be the number of such translates which intersect the interior of the circle. Then, writing $n(\rho)$ for the number of points of J inside the circle, we have

$$n^-(\rho) \leq n(\rho) \leq n^+(\rho).$$

Now, writing δ for the length of the longer diagonal of the parallelogram F, we have

$$n^+(\rho) \leq n^-(\rho + \delta) \text{ for all } \rho$$

and thus

$$n^+(\rho - \delta) \leq n(\rho) \leq n^-(\rho + \delta).$$

Multiplying by $\mathrm{vol}(F)$ we obtain

$$\pi(\rho - \delta)^2 \leq n(\rho)\mathrm{vol}(F) \leq \pi(\rho + \delta)^2.$$

We have used the fact that $n^-(r)\mathrm{vol}(F) \leq \pi r^2 \leq n^+(r)\mathrm{vol}(F)$. Hence $n(\rho)\mathrm{vol}(F) = \pi\rho^2 + \gamma(\rho)$ where

$$|\gamma(\rho)| \leq \pi(2\rho\delta + \delta^2).$$

Using

$$\#U.i_C(t) = n\left(\sqrt{t\|J\|}\right) - 1$$

(where the -1 comes from the fact that we are only counting the nonzero points of J; the notation refers to the function $n(\cdot)$ defined above, not to the degree $n = [K : \mathbb{Q}] = 2$) we find that

$$i_C(t) = \frac{\pi t\|J\|}{\#U.\mathrm{vol}(F)} + \varepsilon(t)$$

with $\frac{\varepsilon(t)}{\sqrt{t}}$ bounded as $t \to \infty$. (Verify the details.) In other words, $\varepsilon(t) = O(\sqrt{t})$.

From what we know about the geometry of numbers[2], we have

$$\mathrm{vol}(F) = \mathrm{vol}(\mathbb{C}/\mathscr{O}_K)\|J\| = \frac{1}{2}\|J\|\sqrt{|\mathrm{disc}(\mathscr{O}_K)}.$$

Thus the theorem holds for imaginary quadratic fields with

$$\kappa = \frac{2\pi}{\#U.\sqrt{|\mathrm{disc}(\mathscr{O}_K)|}}$$

which simplifies to

$$\frac{\pi}{\sqrt{|\mathrm{disc}(\mathscr{O}_K)|}}$$

unless $K = \mathbb{Q}[i], \mathbb{Q}[\sqrt{-3}]$ in which case there is an extra factor of 2, resp. 3 in the denominator.

Returning to the general case...

Recall that $i_C(t) =$ the number of principal ideals $(\alpha) \subset J$ with $\|(\alpha)\| \leq t\|J\|$. Let $S \subset \mathscr{O}_K$ be a set of representatives for the orbit space $U\backslash(\mathscr{O}_K - \{0\})$. We will count the number of elements of $J \cap S$ such that $\|\cdot\| \leq t\|J\|$.

It will suffice to construct representatives for a free abelian subgroup $V := U_{\mathrm{free}}$ of rank $r + s - 1$. In other words, thus we are no longer counting $i_C(t)$ itself, but rather the quantity obtained from the representatives of the action on $\mathscr{O}_K - \{0\}$ of V where $U/V = U_{\mathrm{tors}}$ is a finite group. The proof that it is sufficient to count w.r.t V instead of w.r.t. U will be given below.

We have the mappings

$$V \subset U \subset \mathscr{O}_K - \{0\} \to \Lambda_{\mathscr{O}_K} - \{0\} \xrightarrow{\log} \mathbb{R}^{r+s}$$

from earlier. U maps onto a lattice $\Lambda_U \subset H \subset \mathbb{R}^{r+s}$ where H is the trace zero hyperplane. The kernel of $U \to \Lambda_U$ is the set of roots of unity and the restriction $V \to \Lambda_U$ is an isomorphism.

Replace $\mathbb{R}^n$ with $\mathbb{R}^r \times \mathbb{C}^s$; recall that $n = r+2s$. We may then regard $\Lambda_{\mathscr{O}_K} \subset \mathbb{R}^n$ as a subset of $\mathbb{R}^r \times \mathbb{C}^s$, and thence regard $\Lambda_{\mathscr{O}_K} \subset (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$. We extend the log map to all of $(\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$ in the obvious manner:

$$\log(x_1, \ldots, x_r, z_1, \ldots, z_s) := (\log|x_1|, \ldots, 2\log|z_1|, \ldots).$$

(The factor of 2 is to ensure compatibility with our earlier definition of log). Therefore we have

$$V \subset U \subset \mathscr{O}_K - \{0\} \hookrightarrow (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \xrightarrow{\log} \mathbb{R}^{r+s}.$$

Moreover the map $\hookrightarrow$ is a homomorphism of groups w.r.t multiplication of K on the source and componentwise multiplication on the target;

$$\mathscr{O}_K - \{0\} \ni \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \tau_1(\alpha), \ldots, \tau_s(\alpha)) \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s.$$

Write V' for the image of V in $(\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$.

---

[2]In greater detail, we are using the facts

(i) a fundamental domain for the lattice $\iota(\mathscr{O}_K)$ has volume

$$\frac{1}{2^s}\sqrt{|\mathrm{disc}(\mathscr{O}_K)|},$$

and

(ii) for a sublattice $\Lambda' \subset \Lambda$, the group Λ/Λ' is finite and we have

$$\mathrm{vol}(\mathbb{R}^n/\Lambda') = \mathrm{vol}(\mathbb{R}^n/\Lambda)|\Lambda/\Lambda'|$$

so that for an ideal $I \subset \mathscr{O}_K$ we obtain

$$\mathrm{vol}(\mathbb{R}^n/\Lambda_I) = \mathrm{vol}(\mathbb{R}^n/\Lambda_{\mathscr{O}_K})|\Lambda_{\mathscr{O}_K}/\Lambda_I| = \frac{1}{2^s}(|\mathrm{disc}(\mathscr{O}_K)|)^{1/2}\|I\|$$

A set of coset reps for V in $\mathscr{O}_K - \{0\}$ may be obtained from a set of coset reps for V' in $(\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$ namely, a set of coset reps is the same thing as a fundamental domain for $V' \subset (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$. Counting elements of the ideal J in the desired subset of $\mathscr{O}_K - \{0\}$ is therefore the same as counting elements of the lattice Λ_J inside the fundamental domain. Moreover the condition

$$\|(\alpha)\| \leq t\|J\|$$

is equivalent to

$$|\mathrm{N}(\overline{\alpha})| \leq t\|J\|$$

where $\overline{\alpha}$ is the image of α in $(\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$ and N is the "norm" defined by

$$\mathrm{N}(x_1, \ldots, x_r, z_1, \ldots, z_s) = x_1 \cdots x_r |z_1|^2 \cdots |z_s|^2.$$

(Verify this.)

To summarize, it remains to

(1) find a set D of coset reps for $V' \subset (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$;

(2) count elements $x \in \Lambda_J \cap D$ s.t. $|\mathrm{N}(x)| \leq t\|J\|$.

Now let us show that it suffices to work with $V = U_{\text{free}}$ instead of all of U. The number of x in (2) is essentially the number of principal ideals $(\alpha) \subset J$ with $\|(\alpha)\| \leq t\|J\|$ except that each such ideal has been counted $w := \#U_{\text{tors}}$ times. Thus the number of x in (2) is $w.i_C(t)$.

To construct D we need the following obvious Lemma whose proof is left as an exercise.

Lemma A. Let $f : G' \to G$ be a homomorphism of abelian groups and let S' be a subgroup of G' which is carried isomorphically onto the subgroup $S \subset G$. Suppose that D is a set of coset reps for $S \subset G$. Then $D' := f^{-1}(D)$ is a set of coset reps for $S' \subset G'$.

Proof of Lemma A. This follows upon noting that, since S' is carried isomorphically onto S, $\ker(f) \cap S'$ is trivial. Thus we have a bijections between $\ker(f) \times D$, $D' = f^{-1}(D)$ and G'/S' which lift the bijections between $\{1\} \times D$, D and G/S. ///

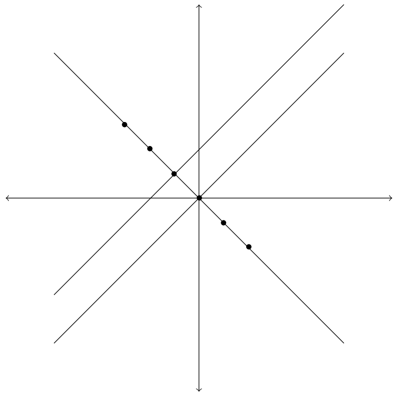
We apply Lemma A to the homomorphism $\log : (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \to \mathbb{R}^{r+s}$.[3] We know that V' maps isomorphically onto the lattice Λ_U so what we seek is a set D of coset reps for Λ_U in $\mathbb{R}^n$; then its preimage D' will be the sought fundamental domain.

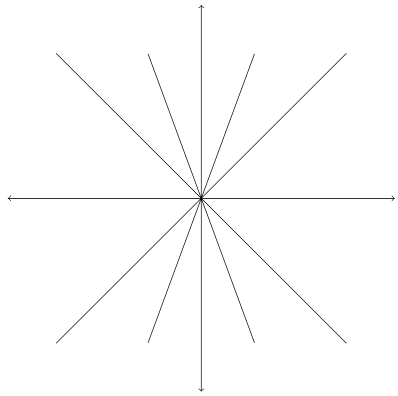
As an example, consider the real quadratic case, so that $r = 2, s = 0$ and Λ_U is a one dimensional lattice in the line $x + y = 0$. D can be taken to be the half-open infinite strip shown in the diagram on the left, and its preimage D' in $(\mathbb{R}^\times)^2$ is shown on the right.

---

[3]Recall the definition of log:

$$\mathbb{R}^{r+2s} \supset \Lambda_{\mathscr{O}_K} - \{0\} \ni (x_1, \ldots, x_n) \mapsto$$
$$(\log|x_1|, \ldots, \log|x_r|, \underbrace{\log(x_{r+1}^2 + x_{r+2}^2), \ldots, \log(x_{n-1}^2 + x_n^2)}_{s}) \in \mathbb{R}^{r+s}.$$





In general, let F be a fundamental domain F for $\Lambda_U \subset H$ and take D to be the direct product $F \times \mathbb{R}.v$ where $\mathbb{R}.v$ is any line through the origin not contained in H, i.e. $v \in \mathbb{R}^{r+s} - H$. Then

$$D' = \{x \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s : \log x \in F \times \mathbb{R}.v\}$$

is a fundamental domain for V'.

Since we have the fundamental domain D', we no longer need to keep track of what we called D above, and therefore to ease notation we will write $D = D'$ henceforth.

The best choice of v will turn out to be

$$v_0 := (\underbrace{1, \dots, 1}_{r}, \underbrace{2, \dots, 2}_{s}).$$

(In the real quadratic case, $v_0 = (1, 1)$.) With this choice of $v = v_0$, we have $D = aD$ for all $a \in \mathbb{R} - \{0\}$. (Verify this.)

Recall that we sought to count the number of points x in $\Lambda_J \cap D$ s.t. $|\mathrm{N}(x)| \leq t\|J\|$. For this purpose we define

$$D_a := \{x \in D : |\mathrm{N}(x)| \leq a\}$$

and note that we have

$$D_a = a^{1/n} D_1.$$

Thus we have reduced to counting the number of points in

$$\Lambda_J \cap (t\|J\|)^{1/n} D_1.$$

More precisely, we want an asymptotic estimate for this number as $t \to \infty$.

We will obtain such an estimate under rather general conditions. Let Λ be a lattice in $\mathbb{R}^n$ and let B be any bounded subset of $\mathbb{R}^n$. We seek to estimate $|\Lambda \cap aB|$ as $a \to \infty$.

Lemma B. If B has a sufficiently nice boundary (to be made precise later) then

$$|\Lambda \cap aB| = \frac{\mathrm{vol}(B)}{\mathrm{vol}(\mathbb{R}^n/\Lambda)} a^n + \gamma(a)$$

where $\gamma(a) = O(a^{n-1})$.

To apply this we consider $(\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$ to be contained in $\mathbb{R}^n$ in the obvious manner. Grant for the moment that D_1 is bounded and has sufficiently nice boundary. Then we obtain

$$|\Lambda_J \cap (t\|J\|)^{1/n} D_1| = \frac{\mathrm{vol}(D_1)\|J\|}{\mathrm{vol}(\mathbb{R}^n/\Lambda_J)} t + \delta(t)$$

where $\delta(t) = O(t^{1-1/n})$. The coefficient of t simplifies to
$$\frac{\operatorname{vol}(D_1)}{\operatorname{vol}(\mathbb{R}^n/\Lambda_{\mathscr{O}_K})}.$$
Thus we finally obtain
$$i_C(t) = \kappa t + \varepsilon(t)$$
with $\varepsilon(t) = O(t^{1-1/n})$ and
$$\kappa = \frac{\operatorname{vol}(D_1)}{w.\operatorname{vol}(\mathbb{R}^n/\Lambda_{\mathscr{O}_K})} = \frac{2^s \operatorname{vol}(D_1)}{w|\operatorname{disc}(\mathscr{O}_K)|^{1/2}}.$$

The proof will be complete after we
(a) define "sufficiently nice"
(b) prove Lemma B
(c) show that D_1 is bounded and has a sufficiently nice boundary

We do not need $\operatorname{vol}(D_1)$ for the proof of the theorem, but we will compute it later since it will lead to the class number formula.

"Sufficiently nice boundary" means $(n-1)$-Lipschitz parametrizable. This means that the boundary is covered by the images of finitely many Lipschitz functions $f : [0,1]^{n-1} \to \mathbb{R}^n$; the condition is that the ratio
$$\frac{|f(x) - f(y)|}{|x - y|}$$
is bounded as x, y range over $[0,1]^{n-1}$ and $|\cdot|$ is the metric in $\mathbb{R}^n, \mathbb{R}^{n-1}$ as appropriate.

Proof of Lemma B. Let us reduce the problem to $\Lambda = \mathbb{Z}^n$. Take $\varphi \in GL_n(\mathbb{R})$ which carries Λ to $\mathbb{Z}^n$. Since the Lipschitz condition is preserved by linear transformations, we have that $B' = \varphi(B)$ has a sufficiently nice boundary. Clearly
$$|\Lambda \cap aB| = |\mathbb{Z}^n \cap aB'|$$
so that it will suffice to show that the Lemma holds for $\mathbb{Z}^n$ and that
$$\operatorname{vol}(B') = \frac{\operatorname{vol}(B)}{\operatorname{vol}(\mathbb{R}^n/\Lambda)}.$$
The latter assertion follows from the calculation
$$\frac{\operatorname{vol}(\mathbb{R}^n/\Lambda)}{\operatorname{vol}(\mathbb{R}^n/\mathbb{Z}^n)} = \frac{\operatorname{vol}(B)}{\operatorname{vol}(B')} = |\det(\varphi)|.$$
This equation expresses the effect of a linear transformation on Lebesgue measure, namely that all volumes are scaled by the determinant. Noting that $\operatorname{vol}(\mathbb{R}^n/\mathbb{Z}^n) = 1$ gives the sought equality.

Thus we take $\Lambda = \mathbb{Z}^n$. Consider the translates of the unit cube $[0,1]^n$ centered at points of $\mathbb{Z}^n$. We will call any such translate a cube. The number of cubes inside aB is approximately $|\mathbb{Z}^n \cap aB|$ and likewise approximately $\operatorname{vol}(aB)$. In either case, the difference between the actual count of cubes and the approximate value is bounded by the number of cubes which meet the boundary of aB. Hence it will suffice to show that this last number is $O(a^{n-1})$ for then it will follow that
$$|\mathbb{Z}^n \cap aB| = \operatorname{vol}(aB) + \gamma(a) = a^n \operatorname{vol}(B) + \gamma(a)$$
with $\gamma(a) = O(a^{n-1})$. This will complete the proof of Lemma B for $\mathbb{Z}^n$.

∂B is covered by the sets $f([0,1]^{n-1})$ for finitely many Lipschitz functions f and thus the boundary of aB is covered by the sets
$$a.f([0,1]^{n-1}).$$
Fixing one such f, it is enough to show that the number of cubes intersecting $a.f([0,1]^{n-1})$ is $O(a^{n-1})$. (This is in a way a geometrically obvious statement. The

scale by a would produce the factor of a^{n-1} and the Lipschitz property produces a constant which is subsumed by the O-notation.)

We subdivide $[0,1]^{n-1}$ into $[a]^{n-1}$ smaller cubes in the obvious manner, where $[a]$ is the greatest integer $\leq a$. Without loss, $a \geq 1$ (we are interested in the asymptotics as $a \to \infty$). Each small cube S has diagonal $\sqrt{n-1}/[a]$ so that the diameter of $f(S)$ is at most $\lambda\sqrt{n-1}/[a]$ where λ is the Lipschitz bound for f. Then $a.f(S)$ has diameter at most $a\lambda\sqrt{n-1}/[a]$; this is at most $2\lambda\sqrt{n-1}$ since $a \geq 1$. Crucially, note that this last quantity, $2\lambda\sqrt{n-1}$, is independent of a.

We now make a gross estimate. Fix a point $x \in a.f(S)$ and take the open n-ball centered at that point of radius $2\lambda\sqrt{n-1}$, $B_x(2\lambda\sqrt{n-1}) \subset \mathbb{R}^n$. It is clear that this ball contains $a.f(S)$ and intersects at most

$$\mu = (4\lambda\sqrt{n-1} + 2)^n$$

cubes. Note that μ is independent of a. It follows that the number of cubes intersecting $a.f([0,1]^{n-1})$ is at most $\mu[a]^{n-1}$ since $[0,1]^{n-1}$ = the union of $[a]^{n-1}$ translates of the small cube S. Finally, to complete the proof of the lemma, we have

$$\mu[a]^{n-1} = O(a^{n-1}),$$

as required. ///

We have dispensed with (a) and (b) above. Now we must attend to (c) by showing that D_1 is bounded and has a sufficiently nice boundary.

Recall that D_1 consists of all $x = (x_1, \ldots, x_r, z_1, \ldots, z_s) \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$ s.t.

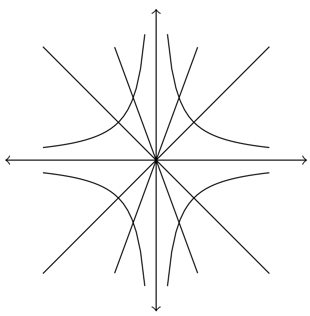
$$\log(x) = (\log|x_1|, \ldots, 2\log|z_1|, \ldots) \in F \oplus \mathbb{R}.v_0$$

and s.t. $|x_1 \cdots x_r z_1^2 \cdots z_s^2| \leq 1$. This last condition is equivalent to saying that $\log(x)$ has coordinate sum ≤ 0. It follows that

$$x \in D_1 \text{ iff } \log(x) \in F \times (-\infty, 0].v_0.$$

Using this let us see that D_1 is bounded: the fact that F is bounded places bounds on all coordinates of points of F and therefore the coordinates of the points of $F \times (-\infty, 0].v_0$ are bounded above. The points of D_1 are thus bounded by definition of log (namely, $\log^{-1}$ = exp of a negative number is in $[0,1]$). Thus $D_1 \subset (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$ is bounded.

This is what D_1 looks like in the real quadratic case.



From the figure, it is clear that the boundary of D_1 is 1-Lipschitz parametrizable, so the proof is complete for real quadratic fields.

Returning to the general case, we replace D_1 with the subset D_1^+ consisting of the points s.t. $x_1 \geq 0, \ldots, x_r \geq 0$. D_1 has a sufficiently nice boundary iff D_1^+ does and $\mathrm{vol}(D_1) = 2^r \mathrm{vol}(D_1^+)$ (in other words, to make D_1^+ we are choosing half of each real coordinate of D_1).

Let us construct a Lipschitz parametrization of ∂D_1^+. We need some notation. The fundamental domain F is of the form

$$\left\{ \sum_{k=1}^{r+s-1} t_k v_k : 0 \le t_k \le 1 \right\}$$

where $\{v_1, \ldots, v_{r+s-1}\}$ is a $\mathbb{Z}$-basis for the lattice Λ_U. For each k, write

$$v_k = (v_k^1, \ldots, v_k^{r+s})$$

(recall that $v_k \in \Lambda_U \subset H \subset \mathbb{R}^{r+s}$; H is the trace zero hyperplane in $\mathbb{R}^{r+s}$, not $\mathbb{R}^{r+2s}$). A point $(x_1, \ldots, x_r, z_1, \ldots, z_s) \in D_1^+$ is characterized by the equations

$$\log(x_j) = \sum_{k=1}^{r+s-1} t_k v_r^j + u \qquad 1 \le j \le r$$

$$2\log|z_j| = \sum_{k=1}^{r+s-1} t_k v_r^j + 2u \qquad r+1 \le j \le r+s.$$

Here, $x_j > 0, t_k \in [0,1), u \in (-\infty, 0]$. Write $t_{r+s} = e^u$ and introduce polar coordinates (ρ_j, θ_j) for each z_j so that we may write D_1^+ as the set of

$$(x_1, \ldots, x_r, \rho_1 e^{i\theta_1}, \ldots, \rho_s e^{i\theta_s})$$

s.t.

$$x_j = t_{r+s} \exp\left\{ \sum_{k=1}^{r+s-1} t_k v_k^j \right\}$$

$$\rho_j = t_{r+s} \exp\left\{ \frac{1}{2} \sum_{k=1}^{r+s-1} t_k v_k^{r+j} \right\}$$

$$\theta_j = 2\pi t_{r+s+j}$$

with $t_{r+s} \in (0,1]$ and the other $t_k \in [0,1)$. This gives a parametrization of D_1^+ by a half-open n-cube. Letting all the t_k take on their boundary values, we obtain a parametrization of the closure $\overline{D_1^+}$. In other words, we have a function

$$f : [0,1]^n \to \mathbb{R}^r \times \mathbb{C}^s$$

mapping the cube onto $\overline{D_1^+}$. (To prove that the image is $\overline{D_1^+}$, note that since $[0,1]^n$ is compact and f is continuous, the image is a compact hence closed set containing D_1^+. On the other hand, the half open cube is dense in the cube, hence D_1^+ is dense in the image. Therefore the image is exactly $\overline{D_1^+}$.)

The closure $\overline{D_1^+}$ is the disjoint union of the interior I and the boundary $B := \partial\overline{D_1^+}$. We shall show that the interior of the cube is sent to I and hence that the boundary of the cube is mapped onto a set containing B. The boundary of the cube is the union of $2n$ $(n-1)$-cubes, hence B is covered by the images of the $2n$ mappings from $(n-1)$-cubes. Each of these mappings is Lipschitz because f is (a fact which we will prove below) and hence B is $(n-1)$-Lipschitz parametrizable. This is what we had to show.

It remains to prove that f is Lipschitz and that the interior $(0,1)^n \subset [0,1]^n$ is mapped into the interior I of D_1^+.

To show that f is Lipschitz, note that all of its partial derivatives exist and are continuous and therefore all partial derivatives are bounded on $[0,1]^n$ (a continuous function on a compact set is bounded). This implies that f is Lipschitz (note well the intervention of the polar coordinates ρ_j, θ_j.)

Finally, we must show that $(0,1)^n$ is sent to I. We claim that the restriction

$$f : (0,1)^n \to \mathbb{R}^r \times \mathbb{C}^s$$

is the composite of four maps

$$(0,1)^n \xrightarrow{f_1} \mathbb{R}^n \xrightarrow{f_2} \mathbb{R}^n \xrightarrow{f_3} \mathbb{R}^r \times (0,\infty)^s \times \mathbb{R}^s \xrightarrow{f_4} \mathbb{R}^r \times \mathbb{C}^s$$

each of which preseves open sets. Granting this assertion, it follows that $(0,1)^n$ is mapped onto an open set by f and therefore is sent into I.

The f_i are defined as follows.

$$f_1(t_1,\ldots,t_n) := (t_1,\ldots,\log(t_{r+s}),\ldots,t_n),$$

where the log is applied only to the $(r+s)$th coordinate. f_2 is the linear transformation

$$f_2(u_1,\ldots,u_n) := (u_1,\ldots,u_n)M$$

where M is the $n \times n$ matrix

$$\left(\begin{array}{c|c} \begin{matrix} v_1 \\ \vdots \\ v_{r+s-1} \\ (1,\ldots,1,2,\ldots,2) \end{matrix} & \mbox{\Huge 0} \\ \hline \mbox{\Huge 0} & \begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix} \end{array}\right)$$

f_3 is defined by applying the function e^x to each of the first r (real, rectangular) coordinates x; applying $\frac{1}{2}e^x$ to each of the next s (radial) coordinates; multiplying each of the last s (angular) coordinates by 2π.

Finally f_4 sends

$$(x_1,\ldots,x_r,\rho_1,\ldots,\rho_s,\theta_1,\ldots,\theta_s)$$

to

$$(x_1,\ldots,x_r,\rho_1 e^{i\theta_1},\ldots,\rho_s e^{i\theta_s}) \in \mathbb{R}^r \times \mathbb{C}^s.$$

One checks that $f = f_1; f_2; f_3; f_4$. (Please do so!) Now, f_1, f_3, f_4 are defined in terms of log, exp, and scalar multiplication, each of which are local diffeomorphisms, and therefore f_1, f_3, f_4 take open sets to open sets. It remains to prove that the linear transformation f_2 takes open sets to open sets, or in other words, that it has rank n. This is clear from the shape of the matrix since since the v_k and $v_0 := (1,\ldots,1,2,\ldots,2)$ are linearly independent in $\mathbb{R}^{r+s}$. (Recall that $\{v_i\}$ is a $\mathbb{Z}$-basis for a lattice contained in the trace zero hyperplane; (1,...,1,2,...,2) is not in this hyperplane.)

This completes the proof of the theorem. ■

7. Our next objective is to give a formula for κ. This requires that we calculate

$$\mathrm{vol}(D_1) = 2^r \mathrm{vol}(D_1^+).$$

In polar coordinates, we have

$$\mathrm{vol}(D_1^+) = \int_{D_1^+} \rho_1 \cdots \rho_s dx_1 \cdots dx_r d\rho_1 \cdots d\rho_s d\theta_1 \cdots d\theta_s$$

(we may figuratively write $\mathrm{vol}(D_1^+) = \int_{D_1^+} \rho \, dx \, d\rho \, d\theta$.)

Changing coordinates, this integral becomes

$$\int_{[0,1]^n} \rho_1 \cdots \rho_s |J(t_1, \ldots, t_n)| dt_1 \cdots dt_n$$

where J is the Jacobian matrix of f. J is the matrix having as its entries the partial derivatives of the functions x_j, ρ_j, θ_j w.r.t. t_k. If we write

$$w_1, \ldots, w_n := x_1, \ldots, x_r, \rho_1, \ldots, \rho_s, \theta_1, \ldots, \theta_s$$

then we have $J = (a_{jk})$ with

$$a_{jk} = \frac{\partial w_j}{\partial t_k}.$$

(There is a typo in [Mar77] at this point. . .)

We have, for $k < r + s$,

$$\frac{\partial w_j}{\partial t_k} = \begin{cases} v_k^j w_j & j \leq r \\ \frac{1}{2} v_k^j w_j & r < j \leq r + s \\ 0 & j > r + s \end{cases}$$

$$\frac{\partial w_j}{\partial t_{r+s}} = \begin{cases} w_j / t_{r+s} & j \leq r + s \\ 0 & j > r + s \end{cases}$$

and for $k > r + s$,

$$\frac{\partial w_j}{\partial t_k} = \begin{cases} 2\pi & j = k \\ 0 & \text{otherwise.} \end{cases}$$

One must verify these computations (please do so!) and check that the determinant is given by

$$\det J = \frac{\pi^s x_1 \cdots x_r \rho_1 \cdots \rho_s}{t_{r+s}} \det(M)$$

where M is the matrix from the proof of the previous theorem. Thus we obtain

$$\text{vol}(D_1^+) = \pi^s |\det(M)| \int_{[0,1]^n} \frac{x_1 \cdots x_r \rho_1^2 \cdots \rho_s^2}{t_{r+s}} dt_1 \cdots dt_n.$$

Using the expressions for the parametrization, we have

$$x_1 \cdots x_r \rho_1^2 \cdots \rho_s^2 = t_{r+s}^n.$$

In greater detail, we have

$$\begin{aligned} x_1 \cdots x_r \rho_1^2 \cdots \rho_s^2 &= \prod_{j=1}^{r} t_{r+s} \exp\left\{ \sum_{k=1}^{r+s-1} t_k v_k^j \right\} \times \prod_{j=1}^{s} \left[t_{r+s} \exp\left\{ \frac{1}{2} \sum_{k=1}^{r+s-1} t_k v_k^{r+j} \right\} \right]^2 \\ &= t_{r+s}^{r+2s} \exp\left\{ \sum_{k=1}^{r+s-1} t_k v_k^j + \sum_{k=1}^{r+s-1} t_k v_k^{r+j} \right\} \\ &= t_{r+s}^n \end{aligned}$$

because $r + 2s = n$ and the v_k are in the trace zero hyperplane. Therefore

$$\text{vol}(D_1^+) = \pi^s |\det(M)| \int_{[0,1]^n} t_{r+s}^{n-1} dt_1 \cdots dt_n = \frac{1}{n} \pi^s |\det(M)|.$$

The quantity

$$\frac{1}{n} |\det(M)|$$

is called the *regulator* of K, written as $\text{reg}(K)$. In fact, the regulator is equal to the absolute value of the determinant of the $(r + s) \times (r + s)$ matrix having as its first $r + s - 1$ rows $v_1, \ldots, v_{r+s-1}$ = the log vectors of a fundamental system of units and having for its final row the vector $\frac{1}{n}(1, \ldots, 1, 2, \ldots, 2)$. This quantity does not depend on the choice of basis $\{v_i\}$ (which we will see later on). Thus

$$\mathrm{vol}(D_1) = 2^r \pi^s \mathrm{reg}(K).$$

We have proven

Theorem 8.

$$\kappa = \frac{2^{r+s}\pi^s \mathrm{reg}(K)}{w|\mathrm{disc}(K)|^{1/2}}$$

where r is the number of real embeddings of K, s is half the number of non-real embeddings of K, and w is the number of roots of unity in K.

Let us give another characterization of the regulator. For this we will need the following lemma.

Lemma 9. *Let A be a square matrix, all of whose row sums are zero, except for the last row. Then the determinant of A is unchanged upon replacing the last row by any other vector with the same coordinate sum.*

Proof. Let B be the new matrix. Write v_A, v_B for the last row vector of A, B. Write C for the matrix whose last row is $v_A - v_B$, but which is otherwise the same as A and B. Then we have

$$\det(A) - \det(B) = \det(C).$$

But the columns of C add up to the zero vector, thus the columns of C are linearly dependent, and therefore $\det(C) = 0$. ∎

Recall that $\mathrm{reg}(K)$ is the absolute value of the determinant of the matrix with $v_1, \ldots, v_{r+s-1}$ in its first $r + s - 1$ rows and

$$(\underbrace{1/n, \ldots, 1/n}_{r}, \underbrace{2/n, \ldots, 2/n}_{s})$$

in its last row. The v_i are all in the trace zero hyperplane H, so that the last row may be replaced by any vector having coordinate sum 1 without affecting the regulator (recall that $r + 2s = n$). There are several candidates for the last row. If we put 1 in one entry and 0 in the others we see that $\mathrm{reg}(K)$ is the absolute value of an $(r+s-1) \times (r+s-1)$ subdeterminant. If we put $1/(r+s)$ everywhere along the last row we obtain a geometric intepretation.

Theorem 10.

$$\mathrm{reg}(K) = \frac{\mathrm{vol}(H/\Lambda_U)}{\sqrt{r+s}}$$

where Λ_U is the lattice associated to the unit group $U \subset \mathscr{O}_K - \{0\}$; moreover, if $v_1, \ldots, v_{r+s-1}$ is any $\mathbb{Z}$-basis for Λ_U then $\mathrm{reg}(K)$ is the absolute value of the determinant obtained by deleting any column from the matrix with rows $v_1, \ldots, v_{r+s-1}$.

Proof. Let Λ be the lattice in $\mathbb{R}^{r+s}$ with $\mathbb{Z}$-basis

$$\left\{ v_1, \ldots, v_{r+s-1}, \left(\frac{1}{r+s}, \ldots, \frac{1}{r+s}\right) \right\}.$$

Then by the lemma and the above discussion and what we know about the relationship between volumes and determinants, we have

$$\mathrm{reg}(K) = \mathrm{vol}(\mathbb{R}^{r+s}/\Lambda).$$

Since the last basis vector is orthogonal to H we find that $\mathrm{vol}(\mathbb{R}^{r+s}/\Lambda)$ is the product of $\mathrm{vol}(H/\Lambda_U)$ and the length of $(1/(r+s), \ldots, 1/(r+s))$. This length is $(r+s)^{-1/2}$.

Incidentally, this formula shows that $\operatorname{reg}(K)$ is independent of the choice of basis $\mathbb{Z}$-basis $\{v_i\}_{i=1}^{r+s-1}$.

The second statement follows by taking the last row vector to have 1 in one coordinate and 0 in the other coordinates, applying the Lemma, and expanding the determinant. ■

Remark 11. We remind the reader that a $\mathbb{Z}$-basis for Λ_U is gotten by taking the log vectors of any fundamental system of units of $\mathscr{O}_K$.

Example 12. Suppose that K is real quadratic and let u be *the* fundamental unit in $\mathscr{O}_K$(*the* indicates that we choose the uniquely determined u s.t. $u > 1$). Then

$$\operatorname{reg}(K) = \log u$$

where the vector $\log u$ reduces in this case to the log of a real number. Since $u > 1$, no absolute values are required. By the above, we have

$$\kappa = \frac{2 \log u}{\sqrt{\operatorname{disc}(\mathscr{O}_K)}}.$$

(See [Mar77, p.33] for the discriminant of a quadratic field, which in particular tells us that the discriminant of a real quadratic field is always positive.) In the imaginary quadratic case, we must *define* $\operatorname{reg}(K)$ to be 1. Then the earlier theorem gives the correct value of κ.

References

[Mar77] Daniel A. Marcus. *Number Fields.* Springer-Verlag, 1977. Universitext.