GEOMETRY OF NUMBERS

ISHAN LEVY

1. Minkowski

Lemma 1.1. *An additive subgroup of $\mathbb{R}^n$ is discrete iff it is freely generated by $\leq n$ $\mathbb{R}$-linearly independent elements. For elements of a discrete subgroup, being $\mathbb{Q}$-linearly independent and $\mathbb{R}$-linearly independent is the same.*

Proof. If it is freely generated by $\mathbb{R}$-linearly independent things, it is clearly discrete. If it is discrete, we can assume that the $\mathbb{R}$-span of the elements is everything. Take the subgroup generated by by some $\mathbb{R}$-basis in the subgroup to get a torus. By discreteness, the image of the subgroup in the quotient is finite, so the entire group must also be freely generated by $\mathbb{R}$-linearly independent elements. This also proves the second statement. □

A lattice is a discrete subgroup with full $\mathbb{R}$-rank. The area of a lattice L is the area of $\mathbb{R}^n/L$, which is a torus, so is finite. It will be denoted $A(L)$, and can be computed as the absolute value of the determinant of a basis.

Lemma 1.2. *If a measurable set S has area more than $A(L)$, then two points must be congruent mod L. If moreover it is compact, then we can require that it have area at least $A(L)$.*

Proof. Look at the image of the set in $\mathbb{R}^n/L$. □

Lemma 1.3. *If S is symmetric about the origin and convex, and has area at least $2^n A(L)$, then S contains a nonzero lattice point.*

Proof. There are $x \neq y$ congruent mod $2L$. Then $\frac{x-y}{2}$ is a nonzero lattice point. □

2. Finiteness of class group

Consider the r real embeddings of a number field K, and the s complex conjugate pair embeddings. The product of these is an embedding $K \to \mathbb{R}^r \times \mathbb{C}^s$. $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $r + 2s = n$.

Lemma 2.1. *$\mathcal{O}_K$ is a lattice in $\mathbb{R}^r \times \mathbb{C}^s$ of volume $2^{-s}\sqrt{|\operatorname{disc}(\mathcal{O}_K)|}$.*

Proof. Given a basis of $\mathcal{O}_K$, the discriminant is the determinant of the matrix of the conjugates of the basis. Note that $\mathrm{Re}(z) = \frac{z+\bar{z}}{2}$ and similarly $\mathrm{Im}(z) = \frac{z-\bar{z}}{2}$, so that we get that the square root of the absolute value of the discriminant of $\mathcal{O}_K$ is $2^s A(O_K)$. □

Lemma 2.2. *The region in* $(\sigma_i^{\mathbb{R}}, \sigma_j^{\mathbb{C}}) = \mathbb{R}^r \times \mathbb{C}^s$ *where* $\sum |\sigma_i^{\mathbb{R}}| + 2\sum |\sigma_j^{\mathbb{C}}| \leq x$ *has measure* $(\frac{\pi}{2})^s 2^r \frac{x^n}{n!}$

Proof. By scaling it is clear that the area should be cx^{r+2s}, where c is some constant. Adding one more real component gives area $\int_0^x cy^{r+2s} 2dy = \frac{2c}{r+2s+1} x^{(r+1)+2s}$. Adding a complex component gives area $\int_0^{\frac{x}{2}} c(x-2y)^{r+2s} 2\pi(\frac{x}{2} - y)dy$. Integrating by parts yields $\int_0^{\frac{x}{2}} c(x-2y)^{r+2s} = \frac{\pi}{2} \frac{cx^{r+2s+2}}{(r+2s+1)(r+2s+2)}$. By induction, we see that the measure is $(\frac{\pi}{2})^s 2^r \frac{x^{r+2s}}{(r+2s)!}$. □

Corollary 2.3. *Given a non-zero fractional ideal* I *in* $\mathcal{O}_K$*, there is a non-zero element of norm at most* $2^{r+s}\sqrt{|\operatorname{disc} K|}N(I)$.

Proof. Consider the convex symmetric region $\sum_1^r |\sigma_i^{\mathbb{R}}| + \sum_1^s 2|\sigma_i^{\mathbb{C}}| \leq x$, where $x^n = \frac{2^{n-r} n!}{\pi^s}\sqrt{|\operatorname{disc} K|}N(I)$. It is compact and has area 2^n times the area of $N(I)$, so there is a nonzero lattice point x. Then by AM-GM, $N(x) \leq (\frac{\sum_1^r |\sigma_i^{\mathbb{R}}| + \sum_1^s 2|\sigma_i^{\mathbb{C}}|}{n})^n = (\frac{4}{\pi})^s \frac{n!}{n^n}\sqrt{|\operatorname{disc} K|}N(I)$. □

Theorem 2.4. *Every ideal class contains an ideal of norm* $\leq (\frac{4}{\pi})^s \frac{n!}{n^n}\sqrt{|\operatorname{disc} K|}$.

Proof. Choose an element x satisfying the norm bound in the previous result. Then $(x)I^{-1}$ is a proper ideal in the inverse class with the desired norm bound. □

Corollary 2.5. *The class group is finite.*

Proof. There are finitely many ideals of a given norm. □

3. Unit theorem

To study the units of $\mathcal{O}_K$, we will consider the **log embedding** $\mathcal{O}_K \to \mathbb{R}^{r+s}, x \mapsto [F_i : \mathbb{R}] \log(|\sigma_i(x)|) = l_i(x)$, where F_i is the field σ_i is an embedding into.

Lemma 3.1. *The kernel of the log embedding consists of roots of unity.*

Proof. Certainly they are in the kernel. Conversely, note that anything in the kernel has bounded coefficients of the characteristic polynomial, so that there are finitely many possibilities. But its powers are in the kernel, so it must be a root of unity. □

Lemma 3.2. *The image of the units via the log embedding is discrete.*

Proof. Any thing whose image is near zero has bounded coefficients of the characteristic polynomial, so there are only finitely many such things. □

The units lie in the hyperplane $\sum l_i = 0$. It turns out that they are full rank, and hence free of rank $r + s - 1$.

Theorem 3.3. *The units form a lattice in the hyperplane* $\sum l_i = 0$.

Proof. Suppose that we have a nonzero linear form on $\sum_i c_i l_i = 0$ on $\sum l_i = 0$. We will show there is a unit such that the form on that unit is nonzero. We can assume WLOG that $c_n = 0, c_1 > 0$. Consider the region in $\mathbb{R}^r \times \mathbb{C}^s$ defined by $|\sigma_i| \leq b_i$. For fixed b_i, $r + s > i$, we want to choose b_{r+s} large enough such that the region has area contains a lattice point. This will happen when $c = 2^r \pi^{-s} \sqrt{|\operatorname{disc}(K)|} \leq \prod b_i^{\mathbb{R}} \times \prod (b_i^{\mathbb{C}})^2$. Now choose any values of $b_1, \ldots, b_{r+s-1}$, and a sufficiently large b_{r+s} will make this an equality. Now if x is a nonzero lattice point in the region, then $1 \leq |N(x)| \leq \prod_i b_i^{\mathbb{R}} \times \prod_i (b_i^{\mathbb{C}})^2$. On the other hand, for $i < r + s$, $|\sigma_i| = \frac{N(\sigma_i)}{\prod_{j \neq i} \sigma_j} \geq \frac{b_i}{c}$. Thus l_i is between $[F_i : \mathbb{R}] \log(b_i) - \log(c)$ and $[F_i : \mathbb{R}] \log(b_i)$. Thus we can manufacture each l_i to be in any interval of our choosing of a fixed size, so we can produce infinitely many x such with norm at most c such that the $\sum_i c_i l_i$ takes distinct values on each. Since there are finitely many ideals of a given norm, two must differ by a unit on which the linear form doesn't vanish. □

4. Distribution of ideals

We would like to count the ideals of norm $\leq n$ in a number field. To do this, we will fix an ideal class, and let I be a representative of the inverse class. Then ideals of norm $\leq n$ are the same as principle ideals inside I with norm $\leq nN(I)$. To count principle ideals, we only have to count generators. Unfortunately in general, there can be a lot of units. To deal with this problem, let A be a fundamental parallelogram for a fundamental system of units u_i in the hyperplane they lie in for the log embedding, and let v be the vector that is $[F_i : \mathbb{R}]$ in each corresponding direction, i.e. the normal vector of the hyperplane A lies in. Now $A + \mathbb{R}v$ are representatives of a coset of the units in the log embedding, and so the preimage D under the log embedding up to roots of unity has a unique generator of every principle ideal. Moreover, because of how v was chosen, this region is scaling invariant.

Let N_n be the region of $\mathbb{R}^r \times \mathbb{C}^s$ with $N(x) \leq n$. Then the number of ideals in the ideal class is equal to the number of lattice points in $N_{nN(I)} \cap D$ divided by the number of roots of unity. Note that $N_a = a^{\frac{1}{n}} N_1$, so that $D_a = N_a \cap D = a^{\frac{1}{n}} (N_1 \cap D)$. We would like to prove that the number of lattice points of a lattice L in aD_1 is $\frac{A(D_1)}{A(L)} a^n + O(a^{n-1})$, but this is true for any region with reasonable boundary.

Namely, let ∂B be **(n-1) Lipschitz parameterizable** if it is a finite union of images of cells under Lipschitz maps.

Lemma 4.1. *If $B \subset \mathbb{R}^n$ has $(n-1)$ Lipschitz parameterizable boundary, then $\#\{aB \cap L\} = \frac{A(B_1)}{A(L)}a^n + O(a^{n-1})$.*

Proof. First note that it suffices to assume L is the standard lattice. Let $\mathbb{Z}^n$ translates of $[0,1]^n$ be standard cubes. The difference between the number lattice points and the is bounded above by the number of standard cubes intersecting the boundary ∂B, so we need to show this is $O(a^{n-1})$. WLOG, ∂B can be the image of one $[0,1]^{n-1}$. To get a bound, break up each cube on the boundary into $\lfloor a \rfloor$ pieces in each direction, and note that if λ is the Lipschitz constant, then $\frac{\sqrt{n}\lambda}{\lfloor a \rfloor^{n-1}}$ is an upper bound on the maximum distance between any two points on the boundary of each subdivision, so the number of cubes hit by each subdivision is bounded above by a constant c, and so the total number of cubes hit is bounded above by ca^{n-1}. □

It suffices to see that D_1 has a Lipschitz parameterization, and compute its volume. We will replace D_1 by D_1^+, the subset where each real component is required to be positive. Clearly $A(D_1^+) = 2^{-r}A(D_1)$. If v_j are the coordinates in the log embedding of the fundmental system of units, then the fundamental domain is $\{\sum_{k=1}^{r+s-1} t_j v_j | 0 \leq t_j < 1\}$. let v_j^k be the components of v_j. If $x_1, \dots x_r, z_1, \dots z_s$ are coordinates in $\mathbb{R}^r \times \mathbb{C}^s$, then for every point $(x_1, \dots, x_r, z_1, \dots z_s)$ in D_1^+ we have $\log x_i = \sum_{k=1}^{r+s-1} t_k v_k^i + u$ and $2\log|z_i| = \sum_{k=1}^{r+s-1} t_k v_k^i + 2u$, where $u \leq 0$. Let $t_{r+s} = e^u$ so that it ranges in $(0,1]$. Now can write each nonzero z_i uniquely as $\rho_i e^{i\theta_i}$. The θ_i, t_k give a Lipschitz parameterization of the region.

Moreover, we can use the parameterization to compute the area. Using polar coordinates, we have $\int_{D_1^+} \prod \rho_i dx_j d\rho_i d\theta_k$. We will change coordinates from the x_j, ρ_i to t_j. for $t < r+s$, $\frac{dx_i}{dt_j}$ is $x_i v_j^i$, and similarly $\frac{d\rho_i}{dt_j}$ is $\frac{1}{2}\rho_i v_j^{r+i}$. $\frac{dx_i}{dt_{r+s}} = x_i$, $\frac{d\rho_i}{dt_{r+s}} = \rho_i$. The determinant of this Jacobian will be $2^{-s}\prod x_i \prod \rho_i$ times the determinant of the coordinates of the v_j and v. The determinant of v_j and v is defined to be n times the **regulator** of K denoted $\mathrm{reg}(K)$, so after the change of coordinates we have $\pi^s \int_{0 \leq t_i \leq 1} \prod \rho_i^2 \prod x_i dt_1 \dots dt_{r+s}$. The product in the integral is t_{r+s}^{n-1} since the v_i are units so their coordinates sum up to 0. We end up with $\pi^s \mathrm{reg}(K)$ as our volume.

Theorem 4.2. *Let $j_K^c(n)$ be the number of ideals of norm at most n in the ideal class c. Then $j_K^c(n) = \frac{2^{r+s}\pi^s \mathrm{reg}(K)}{\omega_K \sqrt{|\mathrm{disc}(K)|}} n + O(n^{1-\frac{1}{[K:\mathbb{Q}]}})$. If $j_K(n)$ is the number of ideals of norm at most n, then $j_K(n) = \frac{h_K 2^{r+s}\pi^s \mathrm{reg}(K)}{\omega_K \sqrt{|\mathrm{disc}(K)|}} n + O(n^{1-\frac{1}{[K:\mathbb{Q}]}})$, where h_K is the class number, and ω_K is the number of roots of unity.*

Proof. As argued before, $\omega_K j_K^c(n) = \frac{A(D_1)}{A(I)} N(I)n + O(n^{1-\frac{1}{[K:\mathbb{Q}]}})$, but we have computed $A(D_1)$, and we know $A(I)$, so putting everything together gives the formula. □