Class Number Formula

Devang Agarwal

Mathematics Department
University of British Columbia

Notation

Let K be a number field of degree n. We denote by r_1 the number of **real embeddings** of K, i.e. embeddings of K into $\mathbb{R}$ and by $2r_2$ the number of **complex embeddings** of K, i.e. embeddings of K into $\mathbb{C}$ which are not contained inside $\mathbb{R}$. These are necessarily even in number since they can be paired up via complex conjugation.
Since the total number of embeddings of K into $\mathbb{C}$ is n, we have $r_1 + 2r_2 = n$.
We denote by $\{\sigma_i\}_{i=1}^n$ the set of all embeddings of K into $\mathbb{C}$, where the indexing is such that,

- For $1 \leq i \leq r_1$, σ_i is a real embedding.
- For $r_1 + 1 \leq i \leq r_1 + r_2$, σ_i is a complex embedding, with

$$\sigma_{i+r_2} = \overline{\sigma_i}$$

For any $\alpha \in K$, we denote by $\alpha^{(i)}$, the image of α under σ_i.
We use N to denote both the element norm $N(\alpha) = \prod_{i=1}^n \alpha^{(i)}$ and the ideal norm $N\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}|$, and note that $N(\alpha\mathcal{O}_K) = |N(\alpha)|$

Ideal Classes

Definition

We call two ideals I and J of $\mathcal{O}_K$ **equivalent**, if there exist $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha I = \beta J$. Ideal multiplication is well defined upto equivalence classes of this relation, and turns the set of equivalence classes into a group, called the **ideal class group**.

If the ideal class group is trivial, then every ideal in the ring of integers $\mathcal{O}_K$ is principal, which in turn implies that it has unique factorization. It can be shown that a Dedekind domain (in particular $\mathcal{O}_K$) has unique factorization iff every ideal in it is principal. Therefore, the ideal class group measures how far is the ring of integers from having unique factorization. The ideal class group turns out to be finite, and we denote by h_K the **class number**, the size of the ideal class group.

Minkowski's Embedding and Finiteness of Ideal Class Group

Consider the embedding,

$$\sigma : K \to K_{\mathbb{R}} := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$$
$$\alpha \mapsto (\alpha^{(i)})_{i=1}^{r_1+r_2}$$

Under this embedding, $\mathcal{O}_K$ and all its ideals form a full rank lattice in $\mathbb{R}^n$. For any lattice Λ, let $cov(\Lambda)$ be the volume of its fundamental domain. Then we can compute that for an ideal $\mathfrak{a}$, $cov(\sigma(\mathfrak{a})) = 2^{-r_2} N\mathfrak{a}\sqrt{|d_K|}$, where d_K is the discriminant of K.
We extend the norm map $N : K \to \mathbb{Q}$ to $K_{\mathbb{R}}$ as,

$$N : K_{\mathbb{R}} \to \mathbb{R}$$
$$(x_i)_{i=1}^{r_1+r_2} \mapsto (\prod_{i=1}^{r_1} x_i) \cdot (\prod_{i=r_1+1}^{r_1+r_2} |x_i|^2)$$

Minkowski's Embedding and Finiteness of Ideal Class Group

Let $\mathfrak{a}$ be any ideal, and $\alpha \in \mathfrak{a}$. Then $\alpha\mathcal{O}_K = \mathfrak{a}\mathfrak{b}$ for some ideal $\mathfrak{b}$ in the inverse of the ideal class of $\mathfrak{a}$. Then $N\mathfrak{b} = (N\mathfrak{a})^{-1}|N(\alpha)|$. Since every ideal class has an inverse, if we can control $|N(\alpha)|$, then we can show that every ideal class has an ideal of bounded norm.

Theorem (Minkowski)

Every convex symmetric set in $\mathbb{R}^n$ of volume greater than $2^n cov(\Lambda)$ intersects Λ.

Choosing a suitable set and working with the lattice $\sigma(\mathfrak{b})$, Minkowski proved:

Theorem (Minkowski's bound)

Every ideal class contains an ideal $\mathfrak{a}$ such that,

$$N\mathfrak{a} \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}$$

Since number of ideals with a given norm is finite, we get the finiteness of the ideal class group.

Dirichlet's Unit Theorem

For a unit $\alpha \in \mathcal{O}_K^*$, $N(\alpha)$ is a unit and an integer, and hence must be ± 1. Meanwhile if α is an integer with $N(\alpha) = \pm 1$, then considering its characteristic polynomial, we get,

$$\alpha^n + a_{n-1}\alpha^{n-1} \cdots + a_1\alpha \pm 1 = 0$$

which in turn tells us α^{-1} is a linear combination of powers of α, hence an integer, i.e. $\alpha \in \mathcal{O}_K^*$. So we have $\alpha \in \mathcal{O}_K$ is a unit iff $|N(\alpha)| = 1$.
Set $r = r_1 + r_2 - 1$ and consider the embedding,

$$\begin{aligned} L : \mathcal{O}_K^* &\to \mathbb{R}^{r_1} \times \mathbb{R}^{r_2} = \mathbb{R}^{r+1} \\ \alpha &\mapsto ((\log|\alpha^{(i)}|)_{i=1}^{r_1}, (2\log|\alpha^{(i)}|)_{i=r_1+1}^{r+1}) \end{aligned}$$

Dirichlet's Unit Theorem

Consider $L^{-1}([-M,M]^{r_1} \times [-2M,2M]^{r_2})$. These is the set of $\alpha \in \mathcal{O}_K^*$ such that $-M \leq \log|\alpha^{(i)}| \leq M$ or equivalently $e^{-M} \leq |\alpha^{(i)}| \leq e^M$ for all i. But that means that the coefficients of the characteristic polynomial of α which are symmetric functions of $\alpha^{(i)}$ are integers in a bounded region. This shows that $L^{-1}([-M,M]^{r+1}])$ is finite. In particular, the kernel of L is a finite subgroup containing the roots of unity in K and hence it must be the group of roots of unity in K. We also get that the image is a discrete subgroup of $\mathbb{R}^{r+1}$. Since $|N(\alpha)| = |\prod_{i=1}^{n} \alpha^{(i)}| = 1$, the image lies in the hyperplane $\sum_{i=1}^{r+1} x_i = 0$. It can be shown that the image is a lattice of rank r in this hyperplane, and hence we get,

Theorem (Dirichlet's Unit Theorem)

$\mathcal{O}_K^* \cong W_K \oplus \mathbb{Z}^r$, where W_K is the finite cyclic group of roots of unity in K, and if $\{\epsilon_j\}_{j=1}^{r}$ is a basis for the free part of $\mathcal{O}_K$, then their images under the map L form a lattice of full rank in the hyperplane $\sum_{i=1}^{r+1} x_i = 0$.

Regulator

We call a basis $\{\epsilon_j\}_{j=1}^r$ of the free part, a **fundamental system of units**.

Let $\mathbf{x} = (x_i)_{i=1}^r \in \mathbb{R}^r$ and set x_{r+1} such that $\sum_{i=1}^{r+1} x_i = 0$, then via the unit theorem, there exist unique $c_j \in \mathbb{R}$ such that

$$x_i = e_i \sum_{j=1}^{r} c_j \log|\epsilon_j^{(i)}|, \quad 1 \leq i \leq r+1$$

where $e_i = 1$ for $1 \leq i \leq r_1$ and $e_i = 2$ for $r_1 + 1 \leq i \leq r+1.$ Writing this as a matrix,

$$(x_i)_{i=1}^r = [e_i \log|\epsilon_j^{(i)}|]_{1 \leq i,j \leq r} (c_j)_{j=1}^r$$

Definition

We define the **regulator** R_K of K to be absolute value of the determinant of the matrix $[e_i \log|\epsilon_j^{(i)}|]_{1 \leq i,j \leq r}$.

Counting Ideals in Ideal Classes

Fix an ideal class C, and let $N(x, C)$ be the number of ideals of norm $\leq x$ in C. Fixing an ideal $\mathfrak{b} \in C^{-1}$, Then we have,

$$\{\text{ideals in } C \text{ of norm} \leq x\} \leftrightarrow \{\text{principal ideals contained in } \mathfrak{b} \text{ of norm} \leq xN\mathfrak{b}\}$$

$$\mathfrak{a} \to \mathfrak{a}\mathfrak{b}$$

$$(\alpha\mathcal{O}_K)\mathfrak{b}^{-1} \leftarrow \alpha\mathcal{O}_K \subset \mathfrak{b}$$

So we try to count principal ideals in $\mathfrak{b}$.
Let $\{\beta_i\}_{i=1}^{n}$ be an integral basis for $\mathfrak{b}$. Then for every $\alpha \in \mathfrak{b}$,

$$\alpha = \sum_{j=1}^{n} t_j\beta_j$$

for integers t_i.

Counting Ideals in Ideal Classes

Moreover, the $N(\alpha\mathcal{O}_K) = |N(\alpha)| \leq xN\mathfrak{b}$ is equivalent to,

$$\left|\prod_{i=1}^{n} \alpha^{(i)}\right| \leq xN\mathfrak{b}$$

where,

$$\alpha^{(i)} = \sum_{j=1}^{n} t_j \beta_j^{(i)}$$

For $\mathbf{t} \in (t_j)_{j=1}^{n} \in \mathbb{R}^n$, define,

$$\alpha^{(i)}(\mathbf{t}) = \sum_{j=1}^{n} t_j \beta_j^{(i)}, \quad N(\alpha)(\mathbf{t}) = \prod_{i=1}^{n} \alpha^{(i)}(\mathbf{t})$$

Counting Ideals in Ideal Classes

Then elements $\alpha \in \mathfrak{b}$ with $|N(\alpha)| \leq xN\mathfrak{b}$ correspond exactly to lattice points in the region,

$$A_x = \{\mathbf{t} \in \mathbb{R}^n \mid |N(\alpha)(\mathbf{t})| \leq xN\mathfrak{b}\}$$

But we need to count principal ideals, so we need to account for multiple elements generating the same ideal.
For $\alpha \in \mathfrak{b}$, Set $x_i(\alpha) = e_i \log|\alpha^{(i)}(N(\alpha))^{-\frac{1}{n}}|$ for $1 \leq i \leq r+1$. Since $\alpha^{i+r_2} = \overline{\alpha^{(i)}}$ for $r_1 + 1 \leq i \leq r+1$, we have $\sum_{i=1}^{r+1} x_i(\alpha) = 0$. If we set, $(c_j(\alpha))_{j=1}^{r} = [e_i \log|\epsilon_j^{(i)}|]_{1 \leq i,j \leq r}^{-1}(x_i(\alpha))_{i=1}^{r}$, we have

$$\log|\alpha^{(i)}(N(\alpha))^{-\frac{1}{n}}| = \sum_{j=1}^{r} c_j(\alpha)\log|\epsilon_j^{(i)}| \quad 1 \leq i \leq n$$

Counting Ideals in Ideal Classes

All units of $\mathcal{O}_K$ are of the form $u = \zeta \prod_{i=1}^{r} \epsilon_j^{n_j}$ for integers n_j and root of unity ζ. Any other generator of $\alpha\mathcal{O}_K$ is of the form $u\alpha$ for some unit u. Note that,

$$c_j(u\alpha) = n_j + c_j(\alpha)$$

Therefore every principal ideal contained in $\mathfrak{b}$ has exactly $w = |W_K|$ generators α such that $0 \leq c_j(\alpha) < 1$, for all j.

Again for $\mathbf{t} \in \mathbb{R}^n$, set $x_i(\mathbf{t}) = e_i \log|\alpha^{(i)}(\mathbf{t})(N(\alpha)(\mathbf{t}))^{-\frac{1}{n}}|$ for $1 \leq i \leq r+1$. Since $\alpha^{i+r_2}(\mathbf{t}) = \overline{\alpha^{(i)}(\mathbf{t})}$ for $r_1 + 1 \leq i \leq r+1$, we have $\sum_{i=1}^{r+1} x_i(\mathbf{t}) = 0$. Define,

$$(c_j(\mathbf{t}))_{j=1}^{r} = [e_i \log|\epsilon_j^{(i)}|]^{-1}_{1 \leq i,j \leq r}(x_i(\mathbf{t}))_{i=1}^{r}$$

Then $wN(x, C)$ is number of lattice points in the region,

$$B_x = \{\mathbf{t} \in \mathbb{R}^n \mid |N(\alpha)(\mathbf{t})| \leq xN\mathfrak{b};\ \text{for all } j, 0 \leq c_j(\mathbf{t}) < 1\}$$

Counting Ideals in Ideal Classes

It can be easily verified that $tB_1 = B_{t^n}$.
By some more precise considerations about lattice points and the boundary of B_x we can obtain the estimate

$$wN(x, C) = \mu(B_x) + O(x^{1-\frac{1}{n}}) = \mu(B_1)x + O(x^{1-\frac{1}{n}})$$

where μ is the Lesbesgue measure.

Theorem (Dedekind)

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

So we have,

$$N(x, C) = \frac{2^{r_1}(2\pi)^{r_2}R_K}{w\sqrt{|d_K|}}x + O(x^{1-\frac{1}{n}})$$

Analytic Class Number Formula

Set $N(x, K)$ to be the number of ideals of norm $\leq x$. Then we have the estimate,

$$N(x, K) = \sum_{C} N(x, C) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w\sqrt{|d_K|}} x + O(x^{1-\frac{1}{n}})$$

Writing the Dedekind zeta function as a Dirichlet series,

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a(n, K)}{n^s}$$

where $a(n, K) =$ number of ideals of norm exactly n. Set,

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

Analytic Class Number Formula

Then we have that the partial sums for the coefficients of the Dirichlet series $\zeta_K(s) - \rho_K\zeta_K(s)$ are $O(x^{1-\frac{1}{n}})$. Therefore, $\zeta_K(s) - \rho_K\zeta_K(s)$ is analytic for $\mathrm{Re}(s) > 1 - \frac{1}{n}$, and

Theorem (Analytic Class Number Formula)

$\zeta_K(s)$ is analytic for $Re(s) > 1$ except a simple pole at $s = 1$. The residue of $\zeta_K(s)$ at $s = 1$ is given by,

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}R_K h_K}{w\sqrt{|d_K|}}$$

Dirichlet's Class Number Formula

Let $K = \mathbb{Q}(\sqrt{d})$ for a square free integer d. Then $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ has exactly two irreducible characters, the trivial character 1 and the character $\chi(1) = -1$, $\chi(0) = 1$. Then we have,

$$\zeta_K(s) = \zeta(s)L(s, \chi, K/\mathbb{Q})$$

Since the Artin symbol for this extension is given by the Kronecker symbol $\left(\frac{d_K}{p}\right)$,

$$L(s, \chi, K/\mathbb{Q}) = \sum_{i=1}^{\infty} \left(\frac{d_K}{n}\right) \frac{1}{n^s}$$

Taking residues at $s = 1$ on both sides,

$$\sum_{i=1}^{\infty} \left(\frac{d_K}{n}\right) \frac{1}{n} = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w\sqrt{|d_K|}}$$

Dirichlet's Class Number Formula

We know that $d_K = d$ if $d \equiv 1 \pmod 4$ and $d_K = 4d$ if $d \equiv 2, 3 \pmod 4$. Therefore d and d_K have the same sign.

If $d_K > 0$, K is a real quadratic field, so $r_1 = 2$, $r_2 = 0$, and $w = 2$. The unit group is isomorphic to $\{\pm 1\} \oplus \mathbb{Z}$. Therefore the ring of integers has a unique fundamental unit ϵ such that $\epsilon > 1$. Therefore $R_K = \log \epsilon$. Hence we get,

$$\sum_{i=1}^{\infty} \left(\frac{d_K}{n}\right) \frac{1}{n} = \frac{2 h_K \log \epsilon}{\sqrt{|d_K|}}$$

If $d_K < 0$. K is an imaginary quadratic field, so $r_1 = 0$, $r_2 = 1$. The unit group is just the finite group of roots of unity, and $R_K = 1$. So we get,

$$\sum_{i=1}^{\infty} \left(\frac{d_K}{n}\right) \frac{1}{n} = \frac{2\pi h_K}{w \sqrt{|d_K|}}$$