Introduction to Algebraic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Lattices

Lattice in a Vector Space

Definition

Let V be an n-dimensional real vector space. A **lattice** in V is a subgroup of the form $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$, where $\{v_1, \ldots, v_m\}$ is a linearly independent set of vectors in V. The lattice is called **complete** if $m = n$. To Γ (or rather, to its generating set $\{v_1, \ldots, v_m\}$) is associated its **fundamental mesh** or **fundamental region**, Φ_Γ, defined as

$$\Phi_\Gamma = \{\alpha_1 v_1 + \cdots + \alpha_m v_m : 0 \leq \alpha_i < 1\}.$$

Claim: Completeness is equivalent to $V = \bigcup_{\gamma \in \Gamma}(\Phi_\Gamma + \gamma)$.

The right-hand side is easily seen to be equal to the real vector space spanned by $v_1, \ldots, v_m$.

- In order words, Γ is complete if every element of V is a translate of an element in the fundamental region by a lattice point.

Characterization of Lattices

Definition

A subset Γ of $\mathbb{R}^n$ is said to be **discrete** if, for any radius $r \geq 0$, Γ contains only finitely many points at a radius at most r from 0.

Proposition

A subgroup $\Gamma \subset V$ is a lattice if and only if it is discrete.

- Suppose, first, that Γ is a lattice.
  Choose a basis $v_1, \ldots, v_m$.
  Consider the vector space V_0 spanned by these vectors.
  By linear independence of the set, every vector $v \in V_0$ can be expressed uniquely as a linear combination of the basis.
  So we can define a continuous $\phi : \mathbb{R}^m \to \mathbb{R}^m$ by

$$\phi(a_1 v_1 + \cdots + a_m v_m) = (a_1, \ldots, a_m).$$

Characterization of Lattices (Cont'd)

- Pick some radius $r \geq 0$.

  Consider the closed ball B of radius r around 0.

  Since B is closed and bounded, it is compact.

  Thus, $\phi(B)$ is also compact.

  Thus, is a subset of the closed ball of some radius M, say.

  If $v = a_1 v_1 + \cdots + a_m v_m \in B$, then we must have $\|\phi(v)\| \leq M$.

  So $\|(a_1, \ldots, a_m)\| \leq M$.

  This implies that $|a_i| \leq M$, for all i.

  Thus, there are only finitely many points in Γ with this property.

  So Γ is discrete.

Characterization of Lattices (Converse)

- Conversely, suppose Γ is discrete.
  Let V_0 be the $\mathbb{R}$-span of Γ, of some dimension m.
  Let $\{u_1, \ldots, u_m\}$ be a basis of V_0 formed of elements in Γ.
  Let
  $$\Gamma_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subseteq \Gamma.$$
  Suppose
  $$\Gamma = \bigcup_{i \in I} (\Gamma_0 + \gamma_i),$$
  a (disjoint) union of cosets of Γ_0 in Γ.
  Now Γ_0 is complete in V_0, and $\gamma_i \in V_0$.
  So γ_i is the translate of some $\mu_i \in \Phi_{\Gamma_0}$ by an element of Γ_0.
  Then $\Gamma_0 + \gamma_i = \Gamma_0 + \mu_i$.
  So
  $$\Gamma = \bigcup_{i \in I} (\Gamma_0 + \mu_i).$$

Characterization of Lattices (Converse Cont'd)

- However, $\mu_i \in \Gamma$ as well as $\mu_i \in \Phi_{\Gamma_0}$.
  As Γ is discrete, $\Gamma \cap \Phi_{\Gamma_0}$ is finite, since Φ_{Γ_0} certainly lies inside some closed ball.
  It follows that I is finite.
  Thus, if q denotes the index of Γ_0 in Γ, we have $q\Gamma \subset \Gamma_0$.
  Then
  $$\Gamma \subset \mathbb{Z}\left(\frac{1}{q}u_1\right) + \cdots + \mathbb{Z}\left(\frac{1}{q}u_m\right).$$
  But now we can apply a previous proposition.
  Γ is a subset of a free abelian group of rank m.
  So Γ admits a $\mathbb{Z}$-basis. I.e., for some $r \leq m$,
  $$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r.$$
  The set $\{v_1, \ldots, v_r\}$ is linearly independent as the vectors span V_0 (so that in fact $r = m$).

Example of a Non-Lattice

- Consider $\mathbb{Z}1 + \mathbb{Z}\sqrt{2}$ inside $\mathbb{R}$.

  This is a perfectly good subgroup of $\mathbb{R}$ (under addition).

  Each of the basis elements is a multiple of the other.

  So $\mathbb{Z}1 + \mathbb{Z}\sqrt{2}$ is not a lattice.

  Nor is it discrete.

  We can find $a, b \in \mathbb{Z}$, such that $a + b\sqrt{2}$ is arbitrarily close to 0.

Criterion for Completeness

Proposition

A lattice $\Gamma \subset V$ is complete if and only if there exists a bounded $B_V \subset V$, such that

$$V = \bigcup_{\gamma \in \Gamma} (B_V + \gamma).$$

- Suppose Γ is complete. Then we may take $B_V = \Phi_\Gamma$.

  Assume, conversely, that B_V is bounded, such that $V = \bigcup_{\gamma \in \Gamma}(B_V + \gamma)$.

  There exists a constant d, such that every point of B_V lies at a distance of at most d from 0.

  Then the collection of translates $\{B_V + \gamma : \gamma \in \Gamma\}$ contains no point which lies at a distance greater than d from some element of Γ.

  However, if V_0 denotes the span of Γ, and V_0 is not all of V, then it is of strictly smaller dimension.

  Thus, there exist points in V which lie arbitrarily far from V_0.

Volumes of Fundamental Domains

- We compute the volume of a fundamental domain for a lattice in $\mathbb{R}^n$.

  If Γ is a lattice, write $\mathrm{vol}(\Gamma)$ for $\mathrm{vol}(\Phi_\Gamma)$.

Proposition

Suppose that $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ is a lattice in $\mathbb{R}^n$. If $v_i = (a_{i1} \ \cdots \ a_{in})$, then

$$\mathrm{vol}(\Gamma) = |\det(a_{ij})|.$$

- Write $\{e_1, \ldots, e_n\}$ for the standard basis of $\mathbb{R}^n$, so that $v_i = \sum_{i=1}^n a_{ij} e_j$.

  Write $x_1, \ldots, x_n$ for the co-ordinates of a general point of $\mathbb{R}^n$ with respect to the standard basis.

  Then we have

$$\mathrm{vol}(\Gamma) = \int_{\Phi_\Gamma} 1 dx_1 dx_2 \ldots dx_n.$$

Volumes of Fundamental Domains (Cont'd)

- Φ_Γ is given very simply in co-ordinates with respect to $\{v_1, \ldots, v_n\}$.

  Φ_Γ is the set of points $\alpha_1 v_1 + \cdots + \alpha_n v_n$, with $0 \leq \alpha_i < 1$.

  So we want to change basis from the standard basis to $\{v_1, \ldots, v_n\}$.

  We have

$$v_i = \sum_{i=1}^{n} a_{ij} e_j, \quad 1 \leq i \leq n.$$

  So the change of basis matrix from $\{v_1, \ldots, v_n\}$ to $\{e_1, \ldots, e_n\}$ is given by $A = (a_{ij})$.

  Suppose $x \in \mathbb{R}^n$ is equal to

$$x = \sum_{i=1}^{n} x_i e_i \quad \text{and} \quad x = \sum_{i=1}^{n} y_i v_i.$$

  The coefficients are transformed by the matrix A.

Volumes of Fundamental Domains (Cont'd)

- The co-ordinates of Φ_Γ in $\{v_1, \ldots, v_n\}$ are $0 \leq y_i < 1$, by definition.

  The formula for changing the variable in multiple integrals involves the Jacobian of the transformation, which is just $|\det A|$.

  More precisely, we have

$$\begin{aligned} \mathrm{vol}(\Gamma) &= \int_{\Phi_\Gamma} 1 dx_1 dx_2 \cdots dx_n \\ &= \int_{\Phi_\Gamma} |\det A| dy_1 dy_2 \cdots dy_n \\ &= |\det A| \int_0^1 \cdots \int_0^1 1 dy_1 \cdots dy_n \\ &= |\det A|. \end{aligned}$$

Centrally Symmetric and Convex Regions

- Consider a vector space V, which we identify with $\mathbb{R}^n$ so that we can define a volume for subsets of V.

Definition

A region $X \subset V$ is **centrally symmetric** if

$$x \in X \quad \text{implies} \quad -x \in X.$$

Definition

A region $X \subset V$ is **convex** if given $x, y \in X$, and $t \in [0,1]$, then

$$tx + (1-t)y \in X.$$

That is, if x and y lie in X, so does the line joining them.

Minkowski's Theorem

Theorem (Minkowski)

Let Γ be a complete lattice in V. Let X be a centrally symmetric convex subset of V. Suppose

$$\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma).$$

Then X contains at least one non-zero lattice point of V.

- It suffices to prove that there exist distinct $\gamma_1, \gamma_2 \in \Gamma$ such that

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset.$$

In fact, suppose $\gamma_1 + \frac{1}{2}x_1 = \gamma_2 + \frac{1}{2}x_2$.
Then $\gamma_1 - \gamma_2 = \frac{1}{2}x_2 + \frac{1}{2}(-x_1)$.
By central symmetry, $-x_1 \in X$.
By convexity, $\gamma_1 - \gamma_2 \in X$.
Hence, $\gamma_1 - \gamma_2 \in X \cap \Gamma$.

Proof of Minkowski's Theorem

- Suppose, to the contrary, $\{\frac{1}{2}X+\gamma\}_{\gamma\in\Gamma}$ are pairwise disjoint.
  The same holds for the intersections $\{\Phi_\Gamma \cap (\frac{1}{2}X+\gamma)\}_{\gamma\in\Gamma}$ with Φ_Γ.
  These sets are all contained in Φ_Γ.
  So we have

$$\mathrm{vol}(\Gamma) \geq \sum_{\gamma\in\Gamma} \mathrm{vol}\left(\Phi_\Gamma \cap \left(\frac{1}{2}X+\gamma\right)\right).$$

  $(\Phi_\Gamma-\gamma)\cap\frac{1}{2}X$ is a translation of $\Phi_\Gamma\cap(\frac{1}{2}X+\gamma)$ by $-\gamma$.
  So $\Phi_\Gamma\cap(\frac{1}{2}X+\gamma)$ and $(\Phi_\Gamma-\gamma)\cap\frac{1}{2}X$ have the same volume.
  The set $\{\Phi_\Gamma-\gamma\}_{\gamma\in\Gamma}$ covers V.
  So $\{(\Phi_\Gamma-\gamma)\cap\frac{1}{2}X\}_{\gamma\in\Gamma}$ covers $\frac{1}{2}X$.
  Then

$$\mathrm{vol}(\Gamma) \geq \sum_{\gamma\in\Gamma} \mathrm{vol}\left((\Phi_\Gamma-\gamma)\cap\frac{1}{2}X\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\mathrm{vol}(X).$$

  This contradicts the hypothesis on $\mathrm{vol}(X)$.

Subsection 2

Geometry of Number Fields

Embeddings Revisited

- Let K be a number field.
- Inside $\mathbb{Z}_K$, we have the units $\mathbb{Z}_K^\times$.
- Recall that:
  - An element $\epsilon \in \mathbb{Z}_K$ is a unit if and only if $N_{K/\mathbb{Q}}(\epsilon) = \pm 1$;
  - Non-zero elements $x_1, x_2 \in \mathbb{Z}_K$ are associates if $\frac{x_1}{x_2} \in \mathbb{Z}_K^\times$.
- By a previous proposition, if $[K : \mathbb{Q}] = n$, there are n embeddings of K into $\mathbb{C}$.

Real and Complex Embeddings

Definition

If $\sigma : K \hookrightarrow \mathbb{C}$ has $\sigma(K) \subset \mathbb{R}$, then σ is said to be **real**.
Otherwise σ is said to be **complex**.
In the complex case, the conjugate, $\overline{\sigma}$, defined by

$$\overline{\sigma}(k) = \overline{\sigma(k)},$$

is also an embedding.

- Thus, if there are r_1 real embeddings and r_2 conjugate pairs of complex embeddings, one has $r_1 + 2r_2 = n$.
- We will tend to write ρ for a real embedding, σ and $\overline{\sigma}$ for complex pairs, and τ when discussing an arbitrary embedding.
- Using this notation, the real embeddings are $\{\rho_1, \ldots, \rho_{r_1}\}$, and the complex embeddings will be $\{\sigma_1, \overline{\sigma}_1, \ldots, \sigma_{r_2}, \overline{\sigma}_{r_2}\}$.

Embedding K into $K_{\mathbb{R}}$

- Define a map

$$\begin{aligned} i : K &\hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}; \\ \alpha &\mapsto (\rho_1(\alpha), \ldots, \rho_{r_1}(\alpha), \sigma_1(\alpha), \ldots, \sigma_{r_2}(\alpha)). \end{aligned}$$

- Suppose addition and multiplication on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ are defined componentwise.
- Then i preserves the additive and multiplicative structure of K.
- Set $K_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.
- Note that, as $\mathbb{C} \cong \mathbb{R}^2$ and $r_1 + 2r_2 = n$, $K_{\mathbb{R}}$ is an n-dimensional real vector space.
- The map i embeds K into $K_{\mathbb{R}}$.

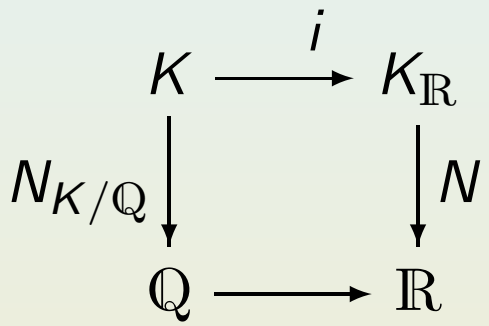
Embedding of K into $K_{\mathbb{R}}$ and a Norm

- One has the norm map $N_{K/\mathbb{Q}}$ on K, where $N_{K/\mathbb{Q}}(\alpha)$ was defined as the determinant of the map $m_\alpha : x \mapsto \alpha x$ on K (using any basis for K as a $\mathbb{Q}$-vector space).
- We can similarly define a map $N : K_{\mathbb{R}} \to \mathbb{R}$ so that if $\alpha \in K_{\mathbb{R}}$, then $N(\alpha)$ is defined as the determinant of the multiplication map $x \mapsto \alpha x$ on the space $K_{\mathbb{R}}$.
- It is easy to see that the map is given explicitly by

$$N : K_{\mathbb{R}} \to \mathbb{R}; \quad (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \mapsto \prod_{i=1}^{r_1} x_i \cdot \prod_{i=1}^{r_2} |z_i|^2.$$

The Two Norms

- We can see that the following diagram commutes



In other words, given $\alpha \in K$, there is an equality

$$N(i(\alpha)) = N_{K/\mathbb{Q}}(\alpha).$$

We have

$$\begin{aligned} N(i(\alpha)) &= N(\rho_1(\alpha),\ldots,\rho_{r_1}(\alpha),\sigma_1(\alpha),\ldots,\sigma_{r_2}(\alpha)) \\ &= \prod_{i=1}^{r_1}\rho_i(\alpha)\cdot\prod_{i=1}^{r_2}|\sigma_i(\alpha)|^2 \\ &= N_{K/\mathbb{Q}}(\alpha). \end{aligned}$$

An Embedding into $\mathbb{C}^n$

- Think of $K_{\mathbb{R}}$ as a subset of $\mathbb{C}^n$ by defining $i_{\mathbb{C}} : K_{\mathbb{R}} \hookrightarrow \mathbb{C}^n$ by

$$(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \mapsto (x_1, \ldots, x_{r_1}, z_1, \overline{z}_1, \ldots, z_{r_2}, \overline{z}_{r_2}).$$

- Notice that the map $K \hookrightarrow K_{\mathbb{R}} \hookrightarrow \mathbb{C}^n$ is then given by

$$x \mapsto (\rho_1(x), \ldots, \rho_{r_1}(x), \sigma_1(x), \overline{\sigma}_1(x), \ldots, \sigma_2(x), \overline{\sigma}_2(x)).$$

- Note that this is a ring homomorphism.

A Notion of Volume

- $\mathbb{C}^n$ has a natural inner product which, given two elements $z = (z_1, \ldots, z_n)$ and $z' = (z'_1, \ldots, z'_n)$, is defined by

$$(z, z') = \sum_{i=1}^{n} z_i \overline{z}'_i.$$

- This gives us a length on $\mathbb{C}^n$, where

$$\|z\| = (z, z)^{1/2}.$$

- As $K_{\mathbb{R}}$ is a subset, we get a length, distance, etc., on $K_{\mathbb{R}}$.
- In particular, we can define the volume

$$\mathrm{vol}(X)$$

of a subset X of $K_{\mathbb{R}}$.

Another Notion of Volume

- We can identify $K_{\mathbb{R}}$ with $\mathbb{R}^n$ using the isomorphism

$$i_{\mathbb{R}} : (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \mapsto (x_1, \ldots, x_{r_1}, u_1, v_1, \ldots, u_{r_2}, v_{r_2}),$$

  where $z_k = u_k + iv_k$, for $k = 1, \ldots, r_2$.
- Notice that $i_{\mathbb{R}}$ is a linear map.
- However, the multiplicative structure of $K_{\mathbb{R}}$ is not preserved.
- The space $\mathbb{R}^n$ has a natural inner product, the usual dot product, which, given two elements $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ in $\mathbb{R}^n$, is given by

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i.$$

Another Notion of Volume (Cont'd)

- This gives a notion of the usual Euclidean length of a vector $x \in \mathbb{R}^n$,

$$\|x\| = \sqrt{\langle x, x \rangle}.$$

- Then we get the usual notions of distances, areas, volumes etc.
- We write

$$\mathrm{vol}_{\mathbb{R}}(X)$$

for the volume of a subset $X \subset K_{\mathbb{R}}$ using this definition.

- We will make computations of volumes of lattices in $K_{\mathbb{R}}$ by mapping them to $\mathbb{R}^n$ using $i_{\mathbb{R}}$ and then using the previous definition.

Relation Between $\mathrm{vol}(\Gamma)$ and $\mathrm{vol}_{\mathbb{R}}(\Gamma)$

Proposition

If Γ is a lattice in $K_{\mathbb{R}}$, then $\mathrm{vol}(\Gamma) = 2^{r_2}\mathrm{vol}_{\mathbb{R}}(\Gamma)$.

- We illustrate the proof with a short example.
- Suppose $[K:\mathbb{Q}] = 3$, and we have one real embedding ρ, and one pair of complex embeddings σ and $\overline{\sigma}$.

  Let ω_1, ω_2 and ω_3 be 3 elements in K.

  The volume of the lattice Γ they generate in $K_{\mathbb{R}}$ is obtained by taking the embedding $i_{\mathbb{C}} : K_{\mathbb{R}} \hookrightarrow \mathbb{C}^n$ and computing

$$\mathrm{vol}(\Gamma) = \begin{vmatrix} \rho(\omega_1) & \sigma(\omega_1) & \overline{\sigma}(\omega_1) \\ \rho(\omega_2) & \sigma(\omega_2) & \overline{\sigma}(\omega_2) \\ \rho(\omega_3) & \sigma(\omega_3) & \overline{\sigma}(\omega_3) \end{vmatrix}.$$

Relation Between $\mathrm{vol}(\Gamma)$ and $\mathrm{vol}_{\mathbb{R}}(\Gamma)$ (Cont'd)

- On the other hand, suppose we use $i_{\mathbb{R}}$ to regard $K_{\mathbb{R}}$ as a subset of $\mathbb{R}^n$. Then the relevant determinant is computed as

$$\mathrm{vol}_{\mathbb{R}}(\Gamma) = \begin{vmatrix} \rho(\omega_1) & \mathrm{Re}(\sigma(\omega_1)) & \mathrm{Im}(\sigma(\omega_1)) \\ \rho(\omega_1) & \mathrm{Re}(\sigma(\omega_1)) & \mathrm{Im}(\sigma(\omega_1)) \\ \rho(\omega_1) & \mathrm{Re}(\sigma(\omega_1)) & \mathrm{Im}(\sigma(\omega_1)) \end{vmatrix}.$$

Let us write $\sigma(\omega_j) = u_j + iv_j$.

Relation Between $\mathrm{vol}(\Gamma)$ and $\mathrm{vol}_{\mathbb{R}}(\Gamma)$ (Cont'd)

Simple column operations give

$$\begin{aligned}
\mathrm{vol}(\Gamma) &= \begin{vmatrix} \rho(\omega_1) & u_1+iv_1 & u_1-iv_1 \\ \rho(\omega_2) & u_2+iv_2 & u_1-iv_2 \\ \rho(\omega_3) & u_3+iv_3 & u_1-iv_3 \end{vmatrix} = \begin{vmatrix} \rho(\omega_1) & 2u_1 & u_1-iv_1 \\ \rho(\omega_2) & 2u_2 & u_2-iv_2 \\ \rho(\omega_3) & 2u_3 & u_3-iv_3 \end{vmatrix} \\
&= 2\begin{vmatrix} \rho(\omega_1) & u_1 & u_1-iv_1 \\ \rho(\omega_2) & u_2 & u_2-iv_2 \\ \rho(\omega_3) & u_3 & u_3-iv_3 \end{vmatrix} = 2\begin{vmatrix} \rho(\omega_1) & u_1 & -iv_1 \\ \rho(\omega_2) & u_2 & -iv_2 \\ \rho(\omega_3) & u_3 & -iv_3 \end{vmatrix} \\
&= |-2i|\begin{vmatrix} \rho(\omega_1) & u_1 & v_1 \\ \rho(\omega_2) & u_2 & v_2 \\ \rho(\omega_3) & u_3 & v_3 \end{vmatrix} = 2\mathrm{vol}_{\mathbb{R}}(\Gamma).
\end{aligned}$$

Exactly the same happens in the general case.

Every pair of complex conjugate embeddings gives an extra factor of 2 in the volume computation.

Lattice Property of $i(\mathbb{Z}_K)$

Proposition

$\Gamma = i(\mathbb{Z}_K)$ is a complete lattice in $K_{\mathbb{R}}$ and

$$\mathrm{vol}(\Gamma) = |D_K|^{1/2}.$$

- Let $\mathbb{Z}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$.

  Then $\Gamma = \mathbb{Z}i(\omega_1) + \cdots + \mathbb{Z}i(\omega_n) \subset K_{\mathbb{R}}$.

  Let M be the matrix $(\tau_i\omega_j)$ as τ_i runs over all embeddings $K \hookrightarrow \mathbb{C}$.

  By a previous definition, $D_K = \Delta\{\omega_1, \ldots, \omega_n\} = \det(M)^2$.

  So $|D_K|^{1/2} = |\det(M)|$.

  The same argument as in a previous proposition (this works in $\mathbb{C}^n$ rather than $\mathbb{R}^n$) shows that $\mathrm{vol}(\Gamma) = |\det(\tau_i\omega_j)|$.

  So we conclude that $\mathrm{vol}(\Gamma) = |D_K|^{1/2}$.

Discriminant of an Ideal

- Let $\mathfrak{a}$ be an integral ideal of K.
  Recall that, if $n = [K : \mathbb{Q}]$, then $\mathfrak{a}$ admits a $\mathbb{Z}$-basis,

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

- Define the **discriminant** of the ideal $\mathfrak{a}$ to be

$$D(\mathfrak{a}) = \Delta\{\alpha_1, \ldots, \alpha_n\} = \det(\tau_i \alpha_j)^2,$$

  where τ_i runs over all of the embeddings of K into $\mathbb{C}$.
- $D(\mathfrak{a})$ is independent of the choice of $\mathbb{Z}$-basis.
- By definition, $D_K = D(\mathbb{Z}_K)$.

Volume and Discriminant

Proposition

If $\mathfrak{a}$ is a non-zero ideal of $\mathbb{Z}_K$, then $\Gamma = i(\mathfrak{a})$ is a complete lattice in $K_{\mathbb{R}}$. Further, $D(\mathfrak{a}) = N_{K/\mathbb{Q}}(\mathfrak{a})^2 D_K$, and Φ_Γ has volume

$$\mathrm{vol}(\Gamma) = |D(\mathfrak{a})|^{1/2} = N_{K/\mathbb{Q}}(\mathfrak{a}) \cdot |D_K|^{1/2}.$$

- By definition of the ideal norm, $\mathbb{Z}_K$ is the (disjoint) union of $N_{K/\mathbb{Q}}(\mathfrak{a})$ cosets of $\mathfrak{a}$.

  Then $i(\mathfrak{a})$ has volume $N_{K/\mathbb{Q}}(\mathfrak{a}) \cdot \mathrm{vol}(i(\mathbb{Z}_K))$.

  By the preceding proposition, $\mathrm{vol}(i(\mathbb{Z}_K)) = |D_K|^{1/2}$.

  Therefore, $\mathrm{vol}(\Gamma) = |D(\mathfrak{a})|^{1/2} = N_{K/\mathbb{Q}}(\mathfrak{a}) \cdot |D_K|^{1/2}$.

Bounding the Volume of Φ_Γ

Proposition

Let Γ be a lattice in $K_{\mathbb{R}}$. Let $c_1,\dots,c_{r_1},C_1,\dots,C_{r_2}\in\mathbb{R}_{>0}$ satisfy

$$c_1\cdots c_{r_1}(C_1\cdots C_{r_2})^2>\left(\frac{2}{\pi}\right)^{r_2}\mathrm{vol}(\Gamma).$$

Then there exists a non-zero $v=(x_1,\dots,x_{r_1},z_1,\dots,z_{r_2})\in\Gamma$, such that $|x_j|<c_j$, for all $j=1,\dots,r_1$, and $|z_k|<C_k$, for all $k=1,\dots,r_2$.

- Let X denote the set of all elements

$$(x_1,\dots,x_{r_1},u_1+iv_1,\dots,u_{r_2}+iv_{r_2})$$

in $K_{\mathbb{R}}=\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$, such that:

  - $|x_j|<c_j$, for $j=1,\dots,r_1$;
  - $|u_k+iv_k|^2=u_k^2+v_k^2<C_k^2$, for $k=1,\dots,r_2$.

Then X is centrally symmetric and convex.

Bounding the Volume of Φ_Γ (Cont'd)

- Note, also, that X is the Cartesian product of r_1 intervals $-c_j < x_j < c_j$ and r_2 circles $u_k^2 + v_k^2 < C_k^2$.

  So

$$\begin{aligned} \mathrm{vol}_{\mathbb{R}}(X) &= (2c_1)\cdots(2c_{r_1})(\pi C_1^2)\cdots(\pi C_{r_2}^2) \\ &= 2^{r_1}\pi^{r_2} c_1 \cdots c_{r_1}(C_1^2 \cdots C_{r_2}^2). \end{aligned}$$

  Under the hypothesis of the statement, we see that

$$\begin{aligned} \mathrm{vol}(X) &= 2^{r_2}\mathrm{vol}_{\mathbb{R}}(X) \\ &> 2^{r_1+r_2}\pi^{r_2}\left(\frac{2}{\pi}\right)^{r_2}\mathrm{vol}(\Gamma) \\ &\overset{r_1+2r_2=n}{=} 2^n \mathrm{vol}(\Gamma). \end{aligned}$$

  The result now follows from Minkowski's Theorem.

Bounding the Norm

- We will be particularly interested in the special case where $\Gamma = i(\mathfrak{a})$ is the lattice associated to an ideal.

Proposition

Let $\mathfrak{a}$ be a non-zero integral ideal of $\mathbb{Z}_K$. Then there exists a nonzero $\alpha \in \mathfrak{a}$, such that

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^{r_2} N_{K/\mathbb{Q}}(\mathfrak{a})|D_K|^{1/2}.$$

- By a previous proposition, $\mathrm{vol}(\mathfrak{a}) = N_{K/\mathbb{Q}}(\mathfrak{a})|D_K|^{1/2}$. Choose

$$M > \left(\frac{2}{\pi}\right)^{r_2} N_{K/\mathbb{Q}}(\mathfrak{a})|D_K|^{1/2} = \left(\frac{2}{\pi}\right)^{r_2} \mathrm{vol}(\mathfrak{a}).$$

Then choose $c_1, \ldots, c_{r_1}, C_1, \ldots, C_{r_2} \in \mathbb{R}_{>0}$, satisfying

$$c_1 \cdots c_{r_1} (C_1 \cdots C_{r_2})^2 = M.$$

Bounding the Norm (Cont'd)

- By the preceding proposition, there is a non-zero element $\alpha \in \mathfrak{a}$, such that:
  - $|\rho_1(\alpha)| < c_1, \ldots, |\rho_{r_1}(\alpha)| < c_{r_1}$;
  - $|\sigma_1(\alpha)| < C_1, \ldots, |\sigma_{r_2}(\alpha)| < C_{r_2}$.

  Note that this also implies that $|\overline{\sigma}_k(\alpha)| < C_k$.

  Now $N_{K/\mathbb{Q}}(\alpha)$ is formed from the product over all embeddings (including the complex conjugates).

  It follows that

$$N_{K/\mathbb{Q}}(\alpha) < c_1 \cdots c_{r_1} (C_1 \cdots C_{r_2})^2 = M.$$

  We can do this for any M bigger than the given bound.

  We conclude that there exists a non-zero $\alpha \in \mathfrak{a}$ as in the statement.

Subsection 3

Finiteness of the Class Number

The Class Group Revisited

- Recall that the **class group** is the group of all fractional ideals of $\mathbb{Z}_K$, modulo the principal fractional ideals.
- We showed the finiteness of the class number in the case of imaginary quadratic fields.
- We write $C(K)$ for the class group.
- The order h_K of $C(K)$ is the **class number**.

Finiteness of the Class Group

Theorem

The class group $C(K)$ is finite.

Claim: Every ideal class $[\mathfrak{a}]$ contains an integral ideal $\mathfrak{c}$ of norm at most

$$M = \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2}.$$

We first take any representative $\mathfrak{b}$ of the class $[\mathfrak{a}^{-1}]$.

We assume that $\mathfrak{b}$ is contained in $\mathbb{Z}_K$.

If not, we can multiply through by a suitable element in $\mathbb{Z}_K$.

By the preceding proposition, there exists $\beta \in \mathfrak{b}$, with $\beta \neq 0$, such that

$$|N_{K/\mathbb{Q}}(\beta)| \leq \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2} N_{K/\mathbb{Q}}(\mathfrak{b}).$$

Finiteness of the Class Group (Cont'd)

- Define
$$\mathfrak{c} = \langle \beta \rangle \mathfrak{b}^{-1} \in [\mathfrak{a}].$$

Since $\beta \in \mathfrak{b}$, every element of $\mathfrak{c}$ is integral. So $\mathfrak{c} \subseteq \mathbb{Z}_K$.

Finally,

$$N_{K/\mathbb{Q}}(\mathfrak{c}) = |N_{K/\mathbb{Q}}(\beta)| N_{K/\mathbb{Q}}(\mathfrak{b})^{-1} \leq \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2} = M.$$

But there are only finitely many integral ideals whose norm is at most any given bound M.

To see this, consider the factorization of an integral ideal into primes.

Use the multiplicativity of the norm.

There can only be finitely many primes whose norm is bounded.

Thus, there can only be finitely many ideal classes.

Constructing the Class Group

- Given a number field K, compute D_K and the constant M.

  We know that:
  - Every ideal of $\mathbb{Z}_K$ is equivalent to an ideal with norm at most M;
  - Ideals factor uniquely into prime ideals;
  - The norm is multiplicative.

  We list all prime ideals whose norm is bounded by M.

  Then we list all products of those whose norm is at most M.

  Every integral ideal will be equivalent to at least one ideal on this list.

  So the class number is bounded by the number of these ideals.
- In fact, the claim that every ideal class contains an ideal of norm at most $M = \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2}$ is far from being best possible.
- When it comes to finding the class group explicitly, it is helpful to have a much better bound.

Finding Better Bounds

- The main problem is that the convex shape X is a "hypercube".
- Something more spherical gives better bounds.

  Example: In $\mathbb{R}^2$, consider the open square of area 4 given by

$$\{(x,y) : |x| < 1, |y| < 1\}.$$

  It has no lattice point other than $(0,0)$.

  Note that the bound for circles is much better.

  There is no circle of area more than π containing no lattice point other than $(0,0)$.

  Better still is a square with sides which are diagonal, parallel to $y = \pm x$.

  Every such square of area more than 2 contains a lattice point other than $(0,0)$.

X_t and its Volume

- Suppose, for $t > 0$, we consider the subset of $K_{\mathbb{R}}$ defined by

$$X_t = \{(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) : |x_1| + \cdots + |x_{r_1}| + 2|z_1| + \cdots + 2|z_{r_2}| < t\}.$$

- Now we get a region of a different shape.
- It is clearly bounded and centrally symmetric.

Lemma

The volume of the region X_t is

$$\mathrm{vol}(X_t) = 2^{r_1} \pi^{r_2} \frac{t^n}{n!}.$$

- We use $i_{\mathbb{R}}$ to write X_t as a subset of $\mathbb{R}^n$.

  We set $z_j = u_j + iv_j$, for $j = 1, \dots, r_2$.

X_t and its Volume (Cont'd)

- Then $i_{\mathbb{R}}(X_t)$ is the set of points

$$\{(x_1,\dots,x_{r_1},u_1,v_1,\dots,u_{r_2},v_{r_2})\},$$

satisfying

$$|x_1|+\cdots+|x_{r_1}|+2\sqrt{u_1^2+v_1^2}+\cdots+2\sqrt{u_{r_2}^2+v_{r_2}^2}<t.$$

We compute $\mathrm{vol}(X)=2^{r_2}\mathrm{vol}_{\mathbb{R}}(X)$.
Make a change of variable to put

$$(u_j,v_j)=\left(\frac{R_j}{2}\cos\theta_j,\frac{R_j}{2}\sin\theta_j\right).$$

The usual formula for change of variables to polar co-ordinates gives

$$4du_jdv_j=R_jdR_jd\theta_j.$$

X_t and its Volume (Cont'd)

- Then

$$\begin{aligned}
\mathrm{vol}_{\mathbb{R}}(X_t) &= \int_{X_t} 1 dx_1 \cdots dx_{r_1} du_1 dv_1 \cdots du_{r_2} dv_{r_2} \\
&= 2^{r_1} \int_{X_t, x_i \geq 0} 1 dx_1 \cdots dx_{r_1} du_1 dv_1 \cdots du_{r_2} dv_{r_2} \\
&= 2^{r_1} 4^{-r_2} \int_{X_t, x_i \geq 0} R_1 \cdots R_{r_2} dx_1 \cdots dx_{r_1} dR_1 d\theta_1 \cdots dR_{r_2} d\theta_{r_2} \\
&= 2^{r_1} 4^{-r_2} (2\pi)^{r_2} \int_{Y_t} R_1 \cdots R_{r_2} dx_1 \cdots dx_{r_1} dR_1 \cdots dR_{r_2},
\end{aligned}$$

where

$$Y_t = \{(x_1, \ldots, x_{r_1}, R_1, \ldots, R_{r_2}) : x_j, R_k \geq 0, \\ x_1 + \cdots + x_{r_1} + R_1 + \cdots + R_{r_2} < t\}.$$

X_t and its Volume (Cont'd)

- Write $I_{r_1,r_2}(t) = \int_{Y_t} R_1 \cdots R_{r_2}\, dx_1 \cdots dx_{r_1}\, dR_1 \cdots dR_{r_2}$.

  Then simple changes of variables show that

$$I_{r,s}(t) = t^{r+2s} I_{r,s}(1), \quad I_{r,s}(1) = \frac{I_{r-1,s}(1)}{r+2s}, \quad I_{0,s}(1) = \frac{I_{0,s-1}(1)}{2s(2s-1)}.$$

  Using the second repeatedly gives $I_{r,s}(1) = \frac{(2s)!}{(r+2s)!} I_{0,s}(1)$.

  Then the third, using $I_{0,0}(1) = 1$, gives $I_{0,s}(1) = \frac{1}{(2s)!}$.

  Then we get

$$I_{r_1,r_2}(t) = t^n I_{r_1,r_2}(1) = t^n \frac{(2r_2)!}{n!} I_{0,r_2}(1) = \frac{1}{n!} t^n.$$

  Combining these shows that

$$\mathrm{vol}(X_t) = 2^{r_2} \mathrm{vol}_{\mathbb{R}}(X_t) = 2^{r_2} 2^{r_1} 4^{-r_2} (2\pi)^{r_2} I_{r_1,r_2}(t) = 2^{r_1} \pi^{r_2} \frac{t^n}{n!}.$$

The Minkowski Bound

Proposition

Every ideal class of K contains an integral ideal $\mathfrak{c}$ of norm at most

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|D_K|^{1/2}.$$

- The set X_t has a more natural interpretation when we consider those elements $\alpha \in K$ such that $i(\alpha) \in X_t$.

  Suppose $\alpha \in K$.

  Let

  $$i(\alpha) = (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}).$$

  Then $x_j = \rho_j(\alpha)$, and $z_k = \sigma_k(\alpha)$. Now $2|z_k| = |z_k| + |\overline{z}_k|$.

  So the expression $|x_1| + \cdots + |x_{r_1}| + 2|z_1| + \cdots + 2|z_{r_2}|$ can be viewed as $\sum_\tau |\tau(\alpha)|$, where τ runs over all embeddings of K into $\mathbb{C}$.

The Minkowski Bound (Cont'd)

- Let $[\mathfrak{a}]$ be any ideal class.

  Take any integral representative $\mathfrak{b}$ of $[\mathfrak{a}^{-1}]$.

  In order to apply Minkowski's Theorem, we choose a value of t for which the volume of X_t is at least $2^n N_{K/\mathbb{Q}}(\mathfrak{b})|D_K|^{1/2}$.

  This simply requires choosing t so that

$$2^{r_1}\pi^{r_2}\frac{t^n}{n!} > 2^n \mathrm{vol}(\mathfrak{b}) = 2^n N_{K/\mathbb{Q}}(\mathfrak{b})|D_K|^{1/2}.$$

  Equivalently, since $n = r_1 + 2r_2$,

$$t^n > n!\left(\frac{4}{\pi}\right)^{r_2} N_{K/\mathbb{Q}}(\mathfrak{b})|D_K|^{1/2}.$$

  By Minkowski's Theorem, there exists a non-zero element $\beta \in \mathfrak{b}$ with $i(\beta)$ in X_t. This is valid for any t satisfying this inequality.

The Minkowski Bound (Cont'd)

- We deduce that there is a non-zero element $\beta \in \mathfrak{b}$ in X_t, where

$$t^n = n!\left(\frac{4}{\pi}\right)^{r_2} N_{K/\mathbb{Q}}(\mathfrak{b})|D_K|^{1/2}.$$

The arithmetic mean - geometric mean inequality implies that

$$\left(\prod_{\tau}|\tau(\beta)|\right)^{1/n} \leq \frac{1}{n}\sum_{\tau}|\tau(\beta)|.$$

The left-hand side is just $N_{K/\mathbb{Q}}(\beta)$.
The right-hand side is at most $\frac{1}{n}t$, by definition of X_t.
Thus, $|N_{K/\mathbb{Q}}(\beta)|^{1/n} \leq \frac{t}{n}$. I.e., $|N_{K/\mathbb{Q}}(\beta)| < (\frac{t}{n})^n$.
By picking t^n as above, we conclude that there exists $\beta \in i^{-1}(X_t) \cap \mathfrak{b}$, such that

$$|N_{K/\mathbb{Q}}(\beta)| < \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} N_{K/\mathbb{Q}}(\mathfrak{b})|D_K|^{1/2}.$$

So, if $\mathfrak{c} = \langle\beta\rangle\mathfrak{b}^{-1} \in [\mathfrak{a}]$, then $N_{K/\mathbb{Q}}(\mathfrak{c}) = |N_{K/\mathbb{Q}}(\beta)|N_{K/\mathbb{Q}}(\mathfrak{b})^{-1}$.

Example

- Suppose $K = \mathbb{Q}(\sqrt{5})$.

  Then $d = 5 \equiv 1 \mod 4$.

  Hence $D = d = 5$.

  Moreover, $r_2 = 0$.

  The Minkowski bound is

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|D_K|^{1/2} = \frac{2}{2^2}\left(\frac{4}{\pi}\right)^{0}|5|^{1/2} = \frac{\sqrt{5}}{2} = 1.118\ldots.$$

  So every ideal is equivalent to one with norm 1.

  But the only ideal of norm 1 is the full ring of integers, which is principal.

  Thus the class number is 1.

Example

- Consider $K = \mathbb{Q}(\sqrt[3]{2})$.

  The discriminant is 108.

  Moreover, $r_2 = 1$.

  The Minkowski bound is

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|D_K|^{1/2} = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)^{1}|108|^{1/2} = \frac{6}{27}\left(\frac{4}{\pi}\right)\sqrt{108} = 2.940\ldots.$$

  So every ideal is equivalent to one whose norm is at most 2.

  The only ideal of norm 1 is the full ring of integers, which is principal.

  The ideal $\langle 2\rangle = \mathfrak{p}_2^3$, where $\mathfrak{p}_2 = \langle\sqrt[3]{2}\rangle$ is also principal.

  Thus every ideal is equivalent to a principal ideal.

  So the class group is trivial.

Example

- Consider $K = \mathbb{Q}(\sqrt{-5})$.

  Here, $d = -5 \equiv 3 \mod 4$.

  So the discriminant is $D = 4d = -20$.

  Moreover, $r_2 = 1$.

  The Minkowski bound is

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|D_K|^{1/2} = \frac{2}{2^2}\left(\frac{4}{\pi}\right)^{1}|-20|^{1/2} = \frac{1}{2}\frac{4}{\pi}\sqrt{20} = 2.84\ldots.$$

  So every ideal is equivalent to an integral ideal of norm at most 2.

  The full ring of integers is the only ideal of norm 1.

  An ideal of norm 2 must divide the prime 2.

  We have $\langle 2\rangle = \mathfrak{p}_2^2$, where $\mathfrak{p}_2 = \langle 2, 1+\sqrt{-5}\rangle$.

  So there is a unique prime ideal of norm 2, and it is not principal.

  Thus the class number is 2.

Solutions to a Diophantine Equation

Corollary

There are no integer solutions to $x^3 = y^2 + 5$.

- Suppose x is even.
  Then y is odd.
  So $y^2 + 5 \equiv 2 \pmod 4$.
  This is impossible, as $8 \mid x^3$.
  So x must be odd.
  Suppose $p \mid (x, y)$.
  Then $p \mid x^3 - y^2$.
  So $p \mid 5$.
  The only possible common factor is 5.
  Now if $5 \mid x$ and $5 \mid y$, then $5^3 \mid x^3$.
  However, $5^2 \nmid y^2 + 5$.
  So x and y are coprime.

Solutions to a Diophantine Equation (Cont'd)

- Suppose that $x^3 = y^2 + 5$.

  Then $x^3 = (y + \sqrt{-5})(y - \sqrt{-5})$.

  Suppose $y + \sqrt{-5}$ and $y - \sqrt{-5}$ both lie in some prime ideal $\mathfrak{p}$ (i.e., they are not coprime).

  Notice that this implies that $x^3 \in \mathfrak{p}$.

  As $\mathfrak{p}$ is prime, $x \in \mathfrak{p}$.

  Now $2y$ is in $\mathfrak{p}$.

  As x is odd, 2 is not in $\mathfrak{p}$.

  But $\mathfrak{p}$ is prime.

  So this implies that $y \in \mathfrak{p}$.

  This contradicts the coprimality of x and y.

Solutions to a Diophantine Equation (Cont'd)

- Now we have
$$\langle y+\sqrt{-5}\rangle = \mathfrak{a}^3, \quad \langle y-\sqrt{-5}\rangle = \mathfrak{b}^3.$$

The class number of $\mathbb{Q}(\sqrt{-5})$ is 2.

Moreover, $\mathfrak{a}$ is an ideal whose cube is principal.

We conclude that $\mathfrak{a}$ is principal.

Similarly, $\mathfrak{b}$ is also principal.

So $y+\sqrt{-5} = u\alpha^3$, for some unit u.

But the units in $\mathbb{Q}(\sqrt{-5})$ are just ± 1, which are both cubes.

So $y+\sqrt{-5} = \alpha^3$, for some $\alpha = a+b\sqrt{-5}$.

Then $y+\sqrt{-5} = (a+b\sqrt{-5})^3$.

By considering the coefficients of $\sqrt{-5}$, $1 = b(3a^2-5b^2)$.

Then $b = \pm 1$. So $3a^2-5 = \pm 1$.

However, the latter has no integral solutions for a.

Degree and Discriminant of a Number Field

Corollary

If K is a number field with $[K:\mathbb{Q}] > 1$, then $|D_K| > 1$.

- By choosing any ideal $\mathfrak{a}$ in $\mathbb{Z}_K$ (whose norm is at least 1), the Minkowski bound shows that

$$1 \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|D_K|^{1/2}.$$

So

$$|D_K|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}.$$

Let γ_n denote the constant on the right-hand side of this inequality. Then $\gamma_2 = \frac{\pi}{2} > 1$. Moreover, for $n \geq 2$,

$$\frac{\gamma_{n+1}}{\gamma_n} = \left(\frac{\pi}{4}\right)^{1/2}\left(1+\frac{1}{n}\right)^n > 1.$$

So the γ_n are increasing. Thus $|D_K| > 1$.

Degree of a Number Field and Ramification

Corollary

If K is a number field with $[K:\mathbb{Q}] > 1$, then some prime p ramifies in K.

- The primes that ramify in K include all those dividing the discriminant. So the result follows from the preceding corollary.

Subsection 4

Dirichlet's Unit Theorem

Two Logarithmic Maps

- The group of units $\mathbb{Z}_K^\times$ for any number field K is multiplicative.
- Minkowski's Theorem refers to vector spaces, which are additive.
- To pass from a multiplicative to an additive setting, define a logarithm map by

$$\begin{array}{rcl} \ell : K_{\mathbb{R}}^\times & \to & \mathbb{R}^{r_1+r_2}; \\ (x_1,\ldots,x_{r_1},z_1,\ldots,z_{r_2}) & \mapsto & (\log|x_1|,\ldots,\log|x_{r_1}|,\log|z_1|^2,\ldots,\log|z_{r_2}|^2) \end{array}$$

- Define, also, another logarithm map (we will use the same letter, but this should cause no confusion):

$$\begin{array}{rcl} \ell : \mathbb{R}^\times & \to & \mathbb{R}; \\ x & \mapsto & \log|x|. \end{array}$$

Relation Between Logarithmic Maps

- Let tr denotes the map

$$\begin{aligned} \mathrm{tr} : \mathbb{R}^{r_1+r_2} &\to \mathbb{R} \\ (x_1, \ldots, x_{r_1+r_2}) &\mapsto x_1 + \cdots + x_{r_1+r_2}. \end{aligned}$$

- Then we have the commutative diagram

$$\begin{array}{ccccc} K^\times & \xrightarrow{i} & K_{\mathbb{R}}^\times & \xrightarrow{\ell} & \mathbb{R}^{r_1+r_2} \\ \Big\downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \Big\downarrow{\scriptstyle N} & & \Big\downarrow{\scriptstyle \mathrm{tr}} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{R}^\times & \xrightarrow[\ell]{} & \mathbb{R} \end{array}$$

Embedding Units in $\mathbb{Z}_K$ into $\mathbb{R}^{r_1+r_2}$

- Recall that
$$\mathbb{Z}_K^\times = \{\epsilon \in \mathbb{Z}_K : N_{K/\mathbb{Q}}(\epsilon) = \pm 1\}.$$
- Put
$$\begin{aligned} S &= \{y \in K_{\mathbb{R}}^\times : N(y) = \pm 1\}, \\ H &= \{x \in \mathbb{R}^{r_1+r_2} : \mathrm{tr}(x) = 0\}. \end{aligned}$$
- Notice that i maps $\mathbb{Z}_K^\times$ into S.
- Note, also, that ℓ maps $S \subseteq K_{\mathbb{R}}^\times$ into $H \subseteq \mathbb{R}^{r_1+r_2}$.
- The composite map takes the units $\mathbb{Z}_K^\times$ into the vector space H.
- Since $\mathbb{R}^{r_1+r_2}$ has dimension $r_1 + r_2$, and H is defined by the vanishing of a single linear function, H is a subspace of dimension $r = r_1 + r_2 - 1$.
- Let λ denote the composite map, taking $\mathbb{Z}_K^\times$ into H:
$$\lambda : \mathbb{Z}_K^\times \xrightarrow{i} S \xrightarrow{\ell} H.$$
- Let $\Gamma = \lambda(\mathbb{Z}_K^\times) \subseteq H$.

Structure of the Kernel of λ

Proposition

The kernel of λ is $\mu(K)$, the group of roots of unity in K.

- Let $x \in \mu(K)$.
  For all embeddings τ of K into $\mathbb{C}$, one has $|\tau(x)| = 1$.
  So the image of x in $K_{\mathbb{R}}^{\times}$ is killed by ℓ.
  Thus, $\mu(K) \subseteq \ker(\lambda)$.

Structure of the Kernel of λ (Cont'd)

- Conversely, suppose $\epsilon \in \ker\lambda$.

  Then $|\tau(\epsilon)| = 1$, for all embeddings τ.

  Thus, $i(\epsilon)$ lies in a bounded region of $K_{\mathbb{R}}$.

  Also, $i(\epsilon) \in i(\mathbb{Z}_K)$, a lattice in $K_{\mathbb{R}}$.

  But lattices are discrete.

  Thus, there are finitely many possibilities for $i(\epsilon)$.

  Hence, $\ker(\lambda)$ is finite.

  $\ker(\lambda)$ is also closed under multiplication.

  So every element in $\ker(\lambda)$ is of finite order.

  Thus, it is a root of unity.

Algebraic Structure of Γ

Lemma

Γ is a subgroup of H.

- $\mathbb{Z}_K^\times$ is a group.

  Moreover, λ is a homomorphism.

  So

  $$\Gamma = \lambda(\mathbb{Z}_K^\times)$$

  is a group, contained in H.

Geometric Structure of Γ

Proposition

Γ is a lattice in H.

- We know $\Gamma = \lambda(\mathbb{Z}_K^\times)$ is a subgroup of H.
  We need to check that Γ is discrete.
  Let B denote a ball of radius $r \geq 0$ in H.
  We must show that $\Gamma \cap B$ is finite.
  We have

$$\ell^{-1}(\Gamma \cap B) = \ell^{-1}(\Gamma) \cap \ell^{-1}(B) = i(\mathbb{Z}_K^\times) \cap \ell^{-1}(B).$$

  By definition of ℓ, we see that $\ell^{-1}(B)$ is contained in a bounded region in $K_{\mathbb{R}}$. So $\ell^{-1}(B)$ is in a ball of some radius.
  Also, $i(\mathbb{Z}_K)$ is a lattice in $K_{\mathbb{R}}$. So it is discrete.
  Hence, $i(\mathbb{Z}_K^\times) \cap \ell^{-1}(B) \subseteq i(\mathbb{Z}_K) \cap \ell^{-1}(B)$ is finite.
  Applying ℓ again, we see that $\Gamma \cap B$ is finite.

A Decomposition of S

Proposition

There is a bounded region $B_S \subseteq S$ such that

$$S = \bigcup_{\epsilon \in \mathbb{Z}_K^\times} i(\epsilon) B_S.$$

- Let y denote an element of S. We want to write this as $i(\epsilon)x$ for some unit ϵ and some element x in a bounded region B_S of S.
  Consider the lattice $i(\mathbb{Z}_K) \subset K_{\mathbb{R}}$, of volume $|D_K|^{1/2}$.
  The lattice $yi(\mathbb{Z}_K)$ also has volume $|D_K|^{1/2}$, since multiplication by y has determinant $N(y) = \pm 1$ (recall that $y \in S$).
  Choose $c_1, \ldots, c_{r_1}$, $C_1, \ldots, C_{r_2} \in \mathbb{R}_{>0}$, with

$$M = c_1 \cdots c_{r_1} (C_1 \cdots C_{r_2})^2 > \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2}.$$

A Decomposition of S (Cont'd)

- Set
$$X = \{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in K_{\mathbb{R}} : |x_j| < c_j, |z_k| < C_k\}.$$
By a previous proposition, X contains a non-zero point $x \in yi(\mathbb{Z}_K)$.
We have $x = yi(\alpha)$, for some $\alpha \in \mathbb{Z}_K$.
This gives
$$N(x) = N(y)N(i(\alpha)) = \pm N_{K/\mathbb{Q}}(\alpha).$$
Consequently, $N_{K/\mathbb{Q}}(\alpha) < M$.
We know only finitely many ideals of $\mathbb{Z}_K$ have norm at most M.
Any element of norm at most M generates a principal ideal of norm at most M.
It follows that there are only finitely many non-associate numbers of norm at most M.

A Decomposition of S (Cont'd)

- Choose a set $\{\alpha_1, \ldots, \alpha_N\}$ consisting of a complete set of non-associate numbers of norm at most M.

  So $\alpha = \epsilon^{-1}\alpha_k$, for some k and some unit ϵ.

  But then

$$y = xi(\alpha)^{-1} = xi(\alpha_k)^{-1} i(\epsilon).$$

  Consider the set

$$B_S = \{s \in S : s \in i(\alpha_k)^{-1} \text{ for some } k\}.$$

  X is bounded.

  Moreover, B_S is the union of finitely many translates of X.

  We conclude that B_S is bounded.

  Every element $y \in S$ is of the form $xi(\epsilon)$, for some $x \in B_S$ and unit ϵ.

  So $S = \bigcup_{\epsilon \in \mathbb{Z}_K^\times} i(\epsilon) B_S$.

Structure of Γ

Corollary

Γ is a complete lattice in H.

- In $S \subseteq K_{\mathbb{R}}^{\times}$, there is a bounded region B_S, with $S = \bigcup_{\epsilon \in \mathbb{Z}_K^{\times}} i(\epsilon) B_S$.
  Then we will apply our logarithm maps, and take $B_H = \ell(B_S)$.
  Since ℓ is a logarithm map, we need to verify that B_H is bounded.
  B_S, as in the preceding proof, is a finite set of translates of X.
  But $\ell(X)$ is bounded, since $X \subset S$.
  So every element $x = (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in X$ has $N(x) = \pm 1$.
  Now $|x_j|$ and $|z_k|$ are bounded, so that $\prod_{j=1}^{r_1} |x_j| \cdot \prod_{k=1}^{r_2} |z_k|^2 = 1$
  So each $|x_j|$ and $|z_k|$ is bounded away from 0 (so there is a constant $c > 0$ such that each $|x_j| > c$ and each $|z_k| > c$).
  It follows easily that $\ell(X)$ is bounded in H.

Structure of Γ (Cont'd)

- A very similar argument applies to each translate $\ell(i(\alpha_k)^{-1}X)$.
  It follows that $B_H = \ell(B_S)$ is bounded.
  Applying ℓ to $S = \bigcup_{\epsilon\in\mathbb{Z}_K^\times} i(\epsilon)B_S$, the equality becomes

$$H = \bigcup_{\epsilon\in\mathbb{Z}_K^\times} (\lambda(\epsilon) + B_H).$$

  But $\Gamma = \lambda(\mathbb{Z}_K^\times)$. So this becomes

$$H = \bigcup_{\gamma\in\Gamma} (\gamma + B_H).$$

  The result follows from a previous proposition.

Dirichlet's Unit Theorem

Theorem (Dirichlet's Unit Theorem)

With $\mu(K)$ the group of roots of unity in K and $r = r_1 + r_2 - 1$,

$$\mathbb{Z}_K^\times \cong \mu(K) \times \mathbb{Z}^r.$$

Equivalently, there exist $\epsilon_1, \ldots, \epsilon_r$ such that all $\epsilon \in \mathbb{Z}_K^\times$ can be written uniquely in the form

$$\epsilon = \zeta \epsilon_1^{\nu_1} \cdots \epsilon_r^{\nu_r},$$

with $\zeta \in \mu(K)$ and $\nu_i \in \mathbb{Z}$.

- The map $\lambda : K^\times \to \mathbb{R}^{r_1+r_2}$ restricts to a map $\lambda : \mathbb{Z}_K^\times \to H$.
  Its kernel is $\mu(K)$ and its image is Γ.
  By the corollary, Γ is a complete lattice in an r-dimensional vector space.
  Therefore, $\Gamma \cong \mathbb{Z}^r$.

Fundamental Units

Definition

The ϵ_i are called **fundamental units**.

- For the imaginary quadratic fields $r_1 = 0$ and $r_2 = 1$.

  So $r = r_1 + r_2 - 1 = 0$.

  Therefore, we see again that imaginary quadratic fields have finitely many units.