Algebraic Number Theory & Arithmetic Geometry

Mathematics Graduate Colloquium
Syracuse University

Caleb McWhorter

April 21, 2018

$\approx$ Definition (Algebraic Number Theory)

The study of number fields, i.e. finite extensions $K/\mathbf{Q}$.

$\approx$ Definition (Algebraic Number Theory)

The study of number fields, i.e. finite extensions $K/\mathbf{Q}$.

$\approx$ Definition (Arithmetic Geometry)

The study of Algebraic Number Theory problems using geometric techniques (meaning schemes).

Ultimately, the goal for both fields is the same…

Ultimately, the goal for both fields is the same…

We want to solve Diophantine equations.

Problem

Find the integer solutions to $y^2 = x^3 - 2$.

$$y^2 = x^3 - 2 \iff x^3 = y^2 + 2$$

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2})$$

We use the fact that $\mathbf{Z}[\sqrt{-2}]$ is a UFD.

Factor $x = u\pi_1^{e_1} \cdots \pi_r^{e_r}$ with $u_i \in \mathbf{Z}[\sqrt{-2}]^\times = \{\pm 1\}$ and $\pi_i \in \mathbf{Z}[\sqrt{-2}]$ distinct irreducibles.

Claim: $y+\sqrt{-2}$, $y-\sqrt{-2}$ are relatively prime in $\mathbf{Z}[\sqrt{-2}]$.

Proof. If an irreducible π divides both, then

$$\pi \mid \left[(y+\sqrt{-2})-(y-\sqrt{-2})\right] = -(\sqrt{-2})^3$$

But $\sqrt{-2}$ is irreducible so that we may assume $\pi=\sqrt{-2}$. Now $\pi \mid y+\sqrt{-2}$ implies

$$y+\sqrt{-2} = \pi(a+b\sqrt{-2}) = \sqrt{-2}(a+b\sqrt{-2})$$

Expanding and relating parts, $y=-2b$ so that

$$x^3 = y^2+2 \equiv 4b^2+2 \equiv 2 \mod 4$$

a contradiction. □

We had $x = u\pi_1^{e_1} \cdots \pi_r^{e_r}$. Because $x^3 = (y - \sqrt{2})(y + \sqrt{2})$, for each π_i dividing x, we know π^{3e_i} divides $y + \sqrt{-2}$ or $y - \sqrt{-2}$. Therefore,

$$y + \sqrt{-2} = u \prod_{i \in I} \pi_i^{3e_i}$$

But then $y + \sqrt{-2}$ is a cube in $\mathbf{Z}[\sqrt{-2}]$. Hence,

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3$$

Expanding

$$y + \sqrt{-2} = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}$$

This gives a system of equations (using also $y^2 = x^3 - 2$):

$$\begin{aligned} y &= a^3 - 6ab^2 \\ 1 &= b(3a^2 - 2b^2) \\ y^2 &= x^3 - 2 \end{aligned}$$

But then $b = \pm 1$ so that $y = \pm 5$ and then $x = 3$. The only solutions are then $(3, \pm 5)$.

Idea of the Proof:

We factored $y^2 + 2$ in the larger ring $\mathbf{Z}[\sqrt{-2}] \supseteq \mathbf{Z}$.

Trying this with $y^2 = x^3 - 61$, one finds there are no solutions. But $(5, \pm 8)$ are clearly solutions…

What went wrong?

Trying this with $y^2 = x^3 - 61$, one finds there are no solutions. But $(5, \pm 8)$ are clearly solutions…

What went wrong?

$$\mathbf{Z}[\sqrt{-61}] \text{ is } \textit{not} \text{ a UFD.}$$

So we are looking for an object with…

- Is an object with ‘interesting’ and ‘nice’ factoring.
- Should generalize ordinary factoring $\mathbf{Z} \subseteq \mathbf{Q}$.
- Have ‘close’ relationship with a number field $K/\mathbf{Q}$.

So we are looking for an object with…

- Is an object with ‘interesting’ and ‘nice’ factoring.
- Should generalize ordinary factoring $\mathbf{Z} \subseteq \mathbf{Q}$.
- Have ‘close’ relationship with a number field $K/\mathbf{Q}$.

This will be the ring of integers of K, denoted $\mathcal{O}_K$.

Definition (Algebraic Integer)

Given a number field $K/\mathbf{Q}$, let $\alpha \in K$ and define $p_\alpha(x)$ to be the minimal polynomial for α. We say α is an algebraic integer if $p_\alpha(x) \in \mathbf{Z}[x]$.

Example

- $\sqrt{2}$ is an algebraic integer, $p_{\sqrt{2}}(x) = x^2 - 2$.
- i is an algebraic integer, $p_i(x) = x^2 + 1$.
- $\frac{1}{\sqrt{2}}$ is *not* an algebraic integer, $p_{1/\sqrt{2}}(x) = 2x^2 - 1$.

Proposition

Let $K/\mathbf{Q}$ be a number field and let $\alpha \in K$. The following are equivalent:

(a) $p_\alpha(x) \in \mathbf{Z}[x]$

(b) $f(\alpha) = 0$ *for some monic* $f(x) \in \mathbf{Z}[x]$

(c) $\mathbf{Z}[\alpha]$ *is a finitely generated* $\mathbf{Z}$*-module*

(d) *there is a nonzero finitely generated subgroup* $M \subseteq K$ *such that* $\alpha M \subseteq M$.

Definition (Ring of Integers)

The ring of integers of a number field K is the set of algebraic integers in K, denoted $\mathcal{O}_K$ or $\mathbf{Z}_K$.

Properties of O_K:

- $\mathbf{Z} \subseteq \mathcal{O}_K$.

Properties of O_K:

- $\mathbf{Z} \subseteq \mathcal{O}_K$.
- $\mathcal{O}_K$ is a ring.

Proposition

Let $K/\mathbf{Q}$ be a number field and let $\alpha \in K$. The following are equivalent:

(a) $p_\alpha(x) \in \mathbf{Z}[x]$

(b) $f(\alpha) = 0$ *for some monic* $f(x) \in \mathbf{Z}[x]$

(c) $\mathbf{Z}[\alpha]$ *is a finitely generated* $\mathbf{Z}$*-module*

(d) *there is a nonzero finitely generated subgroup* $M \subseteq K$ *such that* $\alpha M \subseteq M$.

Properties of O_K:

- $\mathbf{Z} \subseteq \mathcal{O}_K$.
- $\mathcal{O}_K$ is a ring.
- $\mathcal{O}_K$ is an integral domain.
- For any $\alpha \in K$, there is an integer $d \geq 1$ such that $m\alpha \in \mathcal{O}_K$.

Lemma

For any $\alpha \in K$, there is an integer $d \geq 1$ such that $m\alpha \in \mathcal{O}_K$.

Proof. Let $\alpha \in K$ and take any polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbf{Q}[x]$ with $f(\alpha) = 0$. Multiply by d^n for any integer $d \geq 1$, we find

$$d^n f(x) = (dx)^n + a_{n-1}d(dx)^{n-1} + \cdots + a_0 d^n$$

Lemma

For any $\alpha \in K$, there is an integer $d \geq 1$ such that $m\alpha \in \mathcal{O}_K$.

Proof. Let $\alpha \in K$ and take any polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbf{Q}[x]$ with $f(\alpha) = 0$. Multiply by d^n for any integer $d \geq 1$, we find

$$d^n f(x) = (dx)^n + a_{n-1}d(dx)^{n-1} + \cdots + a_0 d^n$$

Choosing d to be the lcm of the denominators of $\{a_0, \ldots, a_{n-1}\}$. Then $d\alpha$ is a root of $d^n f(x) \in \mathbf{Z}[x]$ so that $d\alpha \in \mathcal{O}_K$. $\square$

Properties of O_K:

- $\mathbf{Z} \subseteq \mathcal{O}_K$.
- $\mathcal{O}_K$ is a ring.
- $\mathcal{O}_K$ is an integral domain.
- For any $\alpha \in K$, there is an integer $d \geq 1$ such that $d\alpha \in \mathcal{O}_K$.
- $K = \mathrm{Frac}(\mathcal{O}_K)$

Proposition

$K = \mathrm{Frac}(\mathcal{O}_K)$

Proof. Let $F = \mathrm{Frac}(\mathcal{O}_K)$. We know $F \subseteq K$. If $[K : F] > 1$, there is an $\alpha \in K \setminus F$ which is algebraic over $\mathbf{Q}$. There exists $d \in \mathbf{Z}$ such that $d\alpha \in \mathcal{O}_K \subseteq F$. But $d\alpha \notin F$, a contradiction. □

Properties of O_K:

- $\mathbf{Z} \subseteq \mathcal{O}_K$.
- $\mathcal{O}_K$ is a ring.
- $\mathcal{O}_K$ is an integral domain.
- For any $\alpha \in K$, there is an integer $d \geq 1$ such that $d\alpha \in \mathcal{O}_K$.
- $K = \mathrm{Frac}(\mathcal{O}_K)$
- If $L/K/\mathbf{Q}$ are number fields, then $\mathcal{O}_L \cap K = \mathcal{O}_K$. In particular, $\mathcal{O}_L \cap \mathbf{Q} = \mathbf{Z}$.

Properties of O_K:

- $\mathbf{Z} \subseteq \mathcal{O}_K$.
- $\mathcal{O}_K$ is a ring.
- $\mathcal{O}_K$ is an integral domain.
- For any $\alpha \in K$, there is an integer $d \geq 1$ such that $d\alpha \in \mathcal{O}_K$.
- $K = \mathrm{Frac}(\mathcal{O}_K)$
- If $L/K/\mathbf{Q}$ are number fields, then $\mathcal{O}_L \cap K = \mathcal{O}_K$. In particular, $\mathcal{O}_L \cap \mathbf{Q} = \mathbf{Z}$.
- $\mathcal{O}_K \cong \mathbf{Z}x_1 \oplus \cdots \oplus \mathbf{Z}x_n \cong \mathbf{Z}^n$, where $n = [K\colon \mathbf{Q}]$

Properties of O_K:

- $\mathbf{Z} \subseteq \mathcal{O}_K$.
- $\mathcal{O}_K$ is a ring.
- $\mathcal{O}_K$ is an integral domain.
- For any $\alpha \in K$, there is an integer $d \geq 1$ such that $d\alpha \in \mathcal{O}_K$.
- $K = \mathrm{Frac}(\mathcal{O}_K)$
- If $L/K/\mathbf{Q}$ are number fields, then $\mathcal{O}_L \cap K = \mathcal{O}_K$. In particular, $\mathcal{O}_L \cap \mathbf{Q} = \mathbf{Z}$.
- $\mathcal{O}_K \cong \mathbf{Z}x_1 \oplus \cdots \oplus \mathbf{Z}x_n \cong \mathbf{Z}^n$, where $n = [K\colon \mathbf{Q}]$
- $K = \mathbf{Q}(x_1, \ldots, x_n)$.
- Prime ideals in $\mathcal{O}_K$ are maximal.

Properties of O_K:

- $\mathbf{Z} \subseteq \mathcal{O}_K$.
- $\mathcal{O}_K$ is a ring.
- $\mathcal{O}_K$ is an integral domain.
- For any $\alpha \in K$, there is an integer $d \geq 1$ such that $d\alpha \in \mathcal{O}_K$.
- $K = \mathrm{Frac}(\mathcal{O}_K)$
- If $L/K/\mathbf{Q}$ are number fields, then $\mathcal{O}_L \cap K = \mathcal{O}_K$. In particular, $\mathcal{O}_L \cap \mathbf{Q} = \mathbf{Z}$.
- $\mathcal{O}_K \cong \mathbf{Z}x_1 \oplus \cdots \oplus \mathbf{Z}x_n \cong \mathbf{Z}^n$, where $n = [K\colon \mathbf{Q}]$
- $K = \mathbf{Q}(x_1, \ldots, x_n)$.
- Prime ideals in $\mathcal{O}_K$ are maximal.
- Ideals in $\mathcal{O}_K$ factor into products of prime ideals in $\mathcal{O}_K$.

Even more properties to come…

Suppose $K/\mathbf{Q}$ has degree n. For $\alpha \in K$, define $\mu_\alpha : K \to K$ via $x \mapsto \alpha x$. This is a $\mathbf{Q}$-linear map, so fixing a basis, we can represent μ_α by an $n \times n$ matrix.

Suppose $K/\mathbf{Q}$ has degree n. For $\alpha \in K$, define $\mu_\alpha : K \to K$ via $x \mapsto \alpha x$. This is a $\mathbf{Q}$-linear map, so fixing a basis, we can represent μ_α by an $n \times n$ matrix.

Definition (Norm)

$\mathrm{Nm}_{K/\mathbf{Q}} : K \to \mathbf{Q}$ via $\alpha \mapsto \det(\mu_\alpha)$.

Definition (Trace)

$\mathrm{Tr}_{K/\mathbf{Q}} : K \to \mathbf{Q}$ via $\alpha \mapsto \mathrm{trace}(\mu_\alpha)$.

Suppose $K/\mathbf{Q}$ has degree n. For $\alpha \in K$, define $\mu_\alpha : K \to K$ via $x \mapsto \alpha x$. This is a $\mathbf{Q}$-linear map, so fixing a basis, we can represent μ_α by an $n \times n$ matrix.

Definition (Norm)

$\mathrm{Nm}_{K/\mathbf{Q}} : K \to \mathbf{Q}$ via $\alpha \mapsto \det(\mu_\alpha)$.

Definition (Trace)

$\mathrm{Tr}_{K/\mathbf{Q}} : K \to \mathbf{Q}$ via $\alpha \mapsto \mathrm{trace}(\mu_\alpha)$.

$\mathrm{Nm}_{K/\mathbf{Q}}(\alpha\beta) = \mathrm{Nm}_{K/\mathbf{Q}}(\alpha)\mathrm{Nm}_{K/\mathbf{Q}}(\beta)$
$\mathrm{Nm}_{K/\mathbf{Q}}(c) = c^n$ for $c \in \mathbf{Q}$
$\mathrm{Nm}_{K/\mathbf{Q}} : K^\times \to \mathbf{Q}^\times$ is a homomorphism.
$\mathrm{Tr}_{K/\mathbf{Q}} : K \to \mathbf{Q}$ is $\mathbf{Q}$-linear

Proposition

For a number field $K/\mathbf{Q}$ of degree n,

$$Nm_{K/\mathbf{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$
$$Tr_{K/\mathbf{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

where $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbf{C}$ are the embeddings of K in $\mathbf{C}$.

Proposition

Let $K/\mathbf{Q}$ be a number field and $\alpha \in K$. Let $\mu_\alpha : K \to K$ denote multiplication by α. Then

$$\det(xI - \mu_\alpha) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)) = p_\alpha(x)^{[K:\mathbf{Q}(\alpha)]}$$

where $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbf{C}$ are the complex embeddings of K into $\mathbf{C}$.

In particular for $\alpha \in \mathcal{O}_K$, $\mathrm{Nm}_{K/\mathbf{Q}}(\alpha)$ and $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha)$ are integers.

Norm/Trace give a method of finding $\mathcal{O}_K$.

Example

Let $K = \mathbf{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer. Let $\alpha = a + b\sqrt{d} \in K$.

Example

Let $K = \mathbf{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer. Let $\alpha = a + b\sqrt{d} \in K$.

K has basis $\{1, \sqrt{d}\}$.

Example

Let $K = \mathbf{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer. Let $\alpha = a + b\sqrt{d} \in K$.

K has basis $\{1, \sqrt{d}\}$. Then with respect to this basis, we have

$$[\mu_\alpha] = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

Therefore, $\mathrm{Nm}_{K/\mathbf{Q}}(\alpha) = a^2 - db^2$ and $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = 2a$.

Example

Let $K = \mathbf{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer. Let $\alpha = a + b\sqrt{d} \in K$.

K has basis $\{1, \sqrt{d}\}$. Then with respect to this basis, we have

$$[\mu_\alpha] = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

Therefore, $\mathrm{Nm}_{K/\mathbf{Q}}(\alpha) = a^2 - db^2$ and $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = 2a$.

If $\alpha \in \mathcal{O}_K$, then $\mathrm{Nm}_{K/\mathbf{Q}}(\alpha), \mathrm{Tr}_{K/\mathbf{Q}}(\alpha) \in \mathbf{Z}$.

We know $a^2 - db^2, 2a \in \mathbf{Z}$. Multiplying $a^2 - db^2$ by 4, we obtain $(2a)^2 - d(2b)^2 \in \mathbf{Z}$.

We know $a^2 - db^2, 2a \in \mathbf{Z}$. Multiplying $a^2 - db^2$ by 4, we obtain $(2a)^2 - d(2b)^2 \in \mathbf{Z}$.

Therefore, $2\mathcal{O}_K \subseteq \mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} \colon a, b \in \mathbf{Z}\}$.

$$\mathbf{Z}[\sqrt{d}] \subseteq \mathcal{O}_K \subseteq \frac{1}{2}\,\mathbf{Z}[\sqrt{d}]$$

We know $a^2 - db^2, 2a \in \mathbf{Z}$. Multiplying $a^2 - db^2$ by 4, we obtain $(2a)^2 - d(2b)^2 \in \mathbf{Z}$.

Therefore, $2\mathcal{O}_K \subseteq \mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} \colon a, b \in \mathbf{Z}\}$.

$$\mathbf{Z}[\sqrt{d}] \subseteq \mathcal{O}_K \subseteq \frac{1}{2}\,\mathbf{Z}[\sqrt{d}]$$

The quotient $\frac{1}{2}\mathbf{Z}[\sqrt{d}]/\mathbf{Z}[\sqrt{d}]$ is a group of order 4 with coset representatives: 0, $\frac{1}{2}$, $\frac{\sqrt{d}}{2}$, and $\frac{1+\sqrt{d}}{2}$.

In order to determine $\mathcal{O}_K$, we need to determine which of these representatives are algebraic integers. Clearly, $0 \in \mathcal{O}_K$ and $\frac{1}{2} \notin \mathcal{O}_K$. The minimal polynomial of $\frac{\sqrt{d}}{2}$ is $x^2 - \frac{d}{4}$, which is not in $\mathbf{Z}[x]$ as d is square free. Hence, $\frac{\sqrt{d}}{4} \notin \mathcal{O}_K$. Finally, the minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is

$$\left(x - \frac{1+\sqrt{d}}{2}\right)\left(x - \frac{1-\sqrt{d}}{2}\right) = x^2 - x + \frac{1-d}{4}.$$

Then $\frac{1+\sqrt{d}}{2}$ has minimal polynomial $p_\alpha(x) \in \mathbf{Z}[x]$. [That is, $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ if and only if $d \equiv 1 \mod 4$.] Therefore,

$$\mathcal{O} + K = \begin{cases} \mathbf{Z}[\sqrt{d}], & d \not\equiv 1 \mod 4 \\ \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \mod 4. \end{cases}$$

If $K = \mathbf{Q}(\sqrt{2})$, then $\mathcal{O}_K = \mathbf{Z}[\sqrt{2}]$.

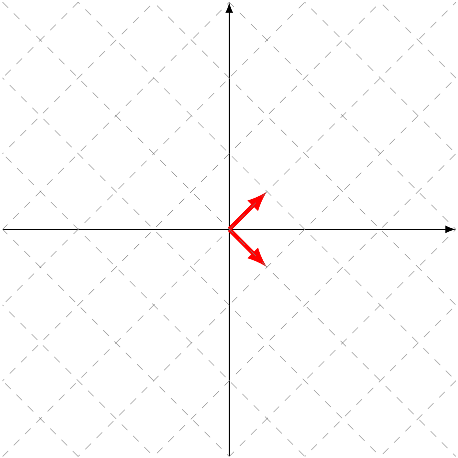

Figure: The lattice for $\mathbf{Z}[\sqrt{2}]$.

Definition (Norm)

For a nonzero ideal $I \subseteq \mathcal{O}_K$, $N(I) = \#(\mathcal{O}_K/I)$.

Definition (Norm)

For a nonzero ideal $I \subseteq \mathcal{O}_K$, $N(I) = \#(\mathcal{O}_K/I)$.

Proposition

Let $K = \mathbf{Q}(\alpha)$, where $\alpha \in \mathcal{O}_K$. For an integral prime p, $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_i$ is a prime ideal. Furthermore, if $\overline{p}_\alpha(x) = \overline{g}_1(x)^{e_1} \cdots \overline{g}_r^{e_r}$, then $\mathfrak{p}_i = (p, g_i(\alpha))$, where $\overline{g(x)} := g(x) \mod p$.

Example

Let $K = \mathbf{Q}(\alpha)$, where α is a root of $x^2 - 7$.

$p = 7$: $\quad x^2 - 7 \equiv x^2 \mod 7$

EXAMPLE

Let $K = \mathbf{Q}(\alpha)$, where α is a root of $x^2 - 7$.

$p = 7$: $\quad x^2 - 7 \equiv x^2 \mod 7 \Rightarrow 7\mathcal{O}_K = (7)$: “7 is inert”

Example

Let $K = \mathbf{Q}(\alpha)$, where α is a root of $x^2 - 7$.

$p = 7$: $\quad x^2 - 7 \equiv x^2 \mod 7 \Rightarrow 7\mathcal{O}_K = (7)$: "7 is inert"

$p = 2$: $\quad x^2 - 7 \equiv x^2 + 1 \equiv (x+1)^2 \mod 2$

Example

Let $K = \mathbf{Q}(\alpha)$, where α is a root of $x^2 - 7$.

$p = 7$: $\quad x^2 - 7 \equiv x^2 \mod 7 \Rightarrow 7\mathcal{O}_K = (7)$: "7 is inert"

$p = 2$: $\quad x^2 - 7 \equiv x^2 + 1 \equiv (x+1)^2 \mod 2 \Rightarrow 2\mathcal{O}_K = (2, \sqrt{7}+1)^2$: "2 is ramified"

Example

Let $K = \mathbf{Q}(\alpha)$, where α is a root of $x^2 - 7$.

$p = 7$: $\quad x^2 - 7 \equiv x^2 \mod 7 \Rightarrow 7\mathcal{O}_K = (7)$: “7 is inert”

$p = 2$: $\quad x^2 - 7 \equiv x^2 + 1 \equiv (x+1)^2 \mod 2 \Rightarrow 2\mathcal{O}_K = (2, \sqrt{7}+1)^2$: “2 is ramified”

$p = 3$: $\quad x^2 - 7 \equiv x^2 - 1 = (x-1)(x+1)$
mod 3

Example

Let $K = \mathbf{Q}(\alpha)$, where α is a root of $x^2 - 7$.

$p = 7$: $\quad x^2 - 7 \equiv x^2 \mod 7 \Rightarrow 7\mathcal{O}_K = (7)$: "7 is inert"

$p = 2$: $\quad x^2 - 7 \equiv x^2 + 1 \equiv (x+1)^2 \mod 2 \Rightarrow 2\mathcal{O}_K = (2, \sqrt{7} + 1)^2$:
"2 is ramified"

$p = 3$: $\quad x^2 - 7 \equiv x^2 - 1 = (x-1)(x+1)$
$\mod 3 \Rightarrow 3\mathcal{O}_K = (3, \sqrt{7} - 1)(3, \sqrt{7} - 1)$: "3 splits"

Theorem (Dirichlet's Unit Theorem)

Let K be a number field of degree n with r real embeddings and s conjugate pairs of embeddings with $\sigma(K) \not\subseteq \mathbf{R}$. Then the abelian group $\mathcal{O}_K^\times$ is a finitely generated abelian group with rank $r+s-1$ and $\mathcal{O}_K^\times \cong \mu_K \times \mathbf{Z}^{r+s-1}$, where μ_K are the roots of unity in $\mathcal{O}_K$.

That is, there are $\mu_1, \ldots, \mu_{r+s-1} \in \mathcal{O}_K^\times$ such that every $\alpha \in \mathcal{O}_K^\times$ is of the form $\alpha = \zeta \cdot \mu_1^{n_1} \cdots \mu_{r+s-1}^{n_{r+s-1}}$.

Example

$K = \mathbf{Q}(\sqrt{d})$, where $d > 0$ is square free.

d	ϵ	$\mathrm{Nm}_{K/\mathbf{Q}}(\epsilon)$
2	$1+\sqrt{2}$	-1
10	$3+\sqrt{10}$	-1
93	$\dfrac{29+3\sqrt{93}}{2}$	-1
94	$2143295+221064\sqrt{94}$	-1

Definition (Pell's Equation)

$x^2 - dy^2 = 1$, where $(x, y) \in \mathbf{Z}^2$

Example

Find a positive pair of solutions to $x^2 - 1141y^2$.

Definition (Pell's Equation)

$x^2 - dy^2 = 1$, where $(x, y) \in \mathbf{Z}^2$

Example

Find a positive pair of solutions to $x^2 - 1141y^2$. Dirichlet's Unit Theorem gives a method of finding the smallest solution (x_0, y_0):

$$x_0 = 1036782394157223963237125215$$
$$y_0 = 30693385322765657197397208$$

Definition (Fractional Ideal)

A fractional ideal of K is a nonzero finitely generated $\mathcal{O}_K$-submodule of K.

Definition (Fractional Ideal)

A fractional ideal of K is a nonzero finitely generated $\mathcal{O}_K$-submodule of K.

Lemma

Let I be a nonzero $\mathcal{O}_K$-submodule of K. The following are equivalent:

(i) *I is a fractional ideal*

(ii) $dI \subseteq \mathcal{O}_K$ *for some* $d \geq 1$

(iii) $dI \subseteq \mathcal{O}_K$ *for some* $0 \neq d \in \mathcal{O}_K$

(iv) $I = xJ$ *for some* $x \in K^\times$ *and nonzero ideal* $J \subseteq \mathcal{O}_K$

[For Commutative Algebra People: $(R : I) = \{x \in K \colon xI \subseteq R\}$.]

Example

(i) $\frac{5}{4}\mathbf{Z}$

(ii) $\langle 1, \frac{1}{2}(1+\sqrt{-5})\rangle \subseteq \mathbf{Z}[\sqrt{-5}]$

We denote by $\mathcal{I}_K$ the set of fractional ideals of K. This is an abelian group under multiplication with identity $\mathcal{O}_K$.

Definition (Principal Fractional Ideal)

Let $\mathcal{B}_K \subseteq \mathcal{J}_K$ be the group of principal fractional ideals, i.e. $x\mathcal{O}_K$ with $x \in K^\times$.

Definition (Principal Fractional Ideal)

Let $\mathcal{B}_K \subseteq \mathcal{J}_K$ be the group of principal fractional ideals, i.e. $x\mathcal{O}_K$ with $x \in K^\times$.

Definition (Ideal Class Group)

The ideal class group of K is

$$\mathrm{C}\ell_K := {}^{\mathcal{J}_K}\!/_{\mathcal{B}_K}$$

Theorem (Minkowski's Theorem)

Let Λ be a lattice in a Euclidean space V of dimension. Let X be a measurable subset of V that is symmetric and convex. Assume on of the following:

(i) $\operatorname{vol} X > 2^n \operatorname{covol} \Lambda$

(ii) $\operatorname{vol} X \geq 2^n \operatorname{covol} \Lambda$ *and X compact*

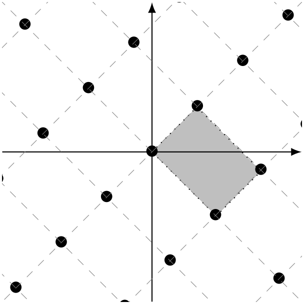

Figure: The fundamental domain for $\mathbf{Z}[\sqrt{2}]$.

Theorem

Let $K/\mathbf{Q}$ be a number field of degree n. Let r be the number of real embeddings $\rho : K \hookrightarrow \mathbf{C}$ and s be the number of complex conjugate embeddings $\sigma : K \hookrightarrow \mathbf{C}$, i.e. $\sigma(K) \nsubseteq \mathbf{R}$. Let I be a nonzero ideal of $\mathcal{O}_K$. Then I contains a nonzero element α with

$$|Nm_{K/\mathbf{Q}}(\alpha)| \leq \left(\frac{\pi}{4}\right)^s \frac{n!}{n} |\operatorname{disc} K|^{1/2} N(I)$$

Example

Let $K = \mathbf{Q}(i)$. For this field, we have $r = 0$ and $s = 1$ so

$$M_K = \left(\frac{\pi}{4}\right)^1 \frac{2!}{2} |-4|^{1/2} = \frac{4}{\pi} < 2.$$

Therefore, every element of $C\ell_K$ contains an ideal of norm 1. But then we have $C\ell_K = \{[\mathcal{O}_K]\} = 1$. Since $\mathcal{O}_K = \mathbf{Z}[i]$, this implies that $\mathbf{Z}[i]$ is a PID.

This is only the start of the overlap of Number Theory & Geometry.

Elliptic Curves