Info

This note, that was found here, as a part of a collection
is written (completely with human hands) by Rupadarshi Ray,
was created on February 13, 2025 5:13:53 PM,
was last modified on September 1, 2026 10:38:29 PM, and
was exported on September 7, 2026 3:10:02 PM.

Algebraic number fields

Question

Is *algebraic number theory* study of *algebraic numbers* or subfield of number theory that uses *algebraic* tools?

algebraic numbers and integers

Definition. Algebraic numbers and integers

A **number field** is a finite extension

$$K \geq \mathbb{Q}$$

whose elements are **algebraic numbers** in K.
An **algebraic integer** in K is a root $\alpha \in p^{-1}(0) \subset K$ of a monic polynomial $p \in \mathbb{Z}[X] \subset \mathbb{Q}[X] \subset K[X]$ which constitute the **ring of integers**

$$\mathscr{O}_K \{\alpha \in K | p(\alpha) = 0, p \in \mathbb{Z}[X]\}$$

[1]

> **Proposition:** The minimal polynomial m_α of an algebraic number α has integer coefficients $\iff$ it is an algebraic number, that is,
>
> $$m_\alpha(X) \in \mathbb{Z}[X] \iff \alpha \in \mathscr{O}_K$$

- $\implies$ is easy. So we assume α is an algebraic integer, so there is a monic polynomial $f \in \mathbb{Z}[X]$ such that

  $$f(\alpha) = 0$$

  and we know

  $$\frac{f}{m_\alpha}(X) = g(X) \in \mathbb{Q}[X]$$

  - Assume $g(X) \notin \mathbb{Z}[X]$ then there is a coefficient which in reduced form has a denominator $\neq 1 \implies$ there is a prime p which divides it.
  - Let $u > 0$ be the largest integer such that $p^u g$ does not have any denominators divisible by p. And say $v > 0$ be the smallest integer such that $p^v h$ has no denominator divisible by p. We have

    $$p^u g p^v h = p^{u+h} f$$

  - Going modulo p we have

    $$(p^u g \bmod p)(p^v h \bmod p) = 0 \in \mathbb{Z}_p[X]$$

    where the left side is a product of non-zero polynomials $p^u g \bmod p$ and $p^v h \bmod p$ (non-zero as they do not have any denominators divisible by p), but it's product is zero, which contradicts $\mathbb{Z}_p$ being a field.

> **Corollary:**
>
> $$\mathscr{O}_\mathbb{Q} = \mathbb{Z}$$

- The minimal polynomial of $\frac{a}{b}$ is $X - \frac{a}{b}$ which has integer coefficients $\iff$ $\frac{a}{b} \in \mathbb{Q}$.

> Let K be a number field and $\alpha \in K$. Then α is an algebraic integer $\iff$ the Abelian group
>
> $$\mathbb{Z}[\alpha]$$
>
> is finitely generated.

> **Corollary:** Let K be a number field then $\mathscr{O}_K$ is a ring and
>
> $$\mathbb{Q}\mathscr{O}_K = K$$

Example

$$\mathbb{Z}\left[\frac{1}{2}\right]$$

is **not** finitely generated as $\frac{1}{2}$is not an algebraic integer in $\mathbb{Q}$.

norms and traces

Definition. Norm and trace for a finite extension of number fields

Let $L \geq K$ be a finite extension of number field K. Then we have an embedding

$$K \hookrightarrow \mathrm{EndVec}_K(L)$$

as scalars. We call

$$N_{L/K}(\alpha) := \det(\alpha) \in K$$

as the **norm** of α and

$$\mathrm{tr}_{L/K}(\alpha) := \mathrm{tr}(\alpha)$$

as the **trace**.

- Norm is multiplicative and trace is additive as $\det, \mathrm{tr}$ are like that resp.
- For $a \in K$ we have

$$N_{L/K}(a\alpha) = a^{\deg L/K} N_{L/K}(\alpha)$$

and

$$\mathrm{tr}_{L/K}(a\alpha) = \mathrm{tr} a_{L/K}(\alpha)$$

> **Proposition:** Let $K \leq L$ be an extension of number fields of degree n. Then there are n distinct embeddings
>
> $$L \hookrightarrow \bar{K}$$

Definition. Conjugates

Let $K \leq L$ be an extension of number fields of degree n. From

> **Proposition:** Let $K \leq L$ be an extension of number fields of degree n. Then there are n distinct embeddings
>
> $$L \hookrightarrow \bar{K}$$

we have

$$\sigma_1, \ldots, \sigma_n$$

are n embeddings $L \hookrightarrow \bar{K} < \mathbb{C}$. Then for $\alpha \in L$ we call

$$\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$$

conjugates of α.

> **Proposition:**
>
> **Definition.** Conjugates
>
> Let $K \leq L$ be an extension of number fields of degree n. From
>
> > **Proposition:** Let $K \leq L$ be an extension of number fields of degree n. Then there are n distinct embeddings
> >
> > $$L \hookrightarrow \bar{K}$$
>
> we have
>
> $$\sigma_1, \ldots, \sigma_n$$
>
> are n embeddings $L \hookrightarrow \bar{K} < \mathbb{C}$. Then for $\alpha \in L$ we call
>
> $$\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$$
>
> **conjugates** of α.
>
> Then for $\alpha \in L$ we have
>
> $$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$
> $$\mathrm{tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

> **Corollary from norm and trace:** Let K be a number field.
>
> - $\alpha \in \mathscr{O}_K \implies$ norm and trace of α belongs to $\mathbb{Z}$, so
>
> $$N, \mathrm{tr} : \mathscr{O}_K \to \mathbb{Z}$$
>
> - norm of α is ± 1 (unit in $\mathbb{Z}$) $\iff$ α is a unit in $\mathscr{O}_K$

> **Proposition:** Let K be a number field. Then
>
> $$\mathscr{O}_K$$
>
> is a free Abelian group of rank $[K, \mathbb{Q}]$.

> **Proposition:** Let K be a number field. Then $\mathscr{O}_K$ is **integrally closed**.

ideal numbers

Definition. Let $I \subseteq R$ be a non-zero ideal, then the **norm** of I is

$$N(I) := \left| \frac{R}{I} \right|$$

> **Proposition:** Let I be a non-zero ideal of $\mathscr{O}_K$ then $N(I)$ is finite and
>
> $$N(\alpha \mathscr{O}_K) = \left| N_{K/\mathbb{Q}}(\alpha) \right|$$

The set of all non-zero fractional ideals

$$I_K$$

of a number field K forms a group under multiplication.

discriminant

Definition. Signature of number fields

Let K be a number field of degree n with r_1 number of real embeddings and r_2 number of complex embeddings from

> **Proposition:** Let $K \leq L$ be an extension of number fields of degree n. Then there are n distinct embeddings
>
> $$L \hookrightarrow \bar{K}$$

Then

$$\text{sig}(K) := (r_1, r_2)$$

where $n = r_1 + 2r_2$.

Given n embeddings

$$\sigma_k : K \to \mathbb{C}$$

we have the product

$$\begin{aligned} \sigma : K &\to \mathbb{C}^n \\ x &\mapsto (\sigma_1(x), \dots, \sigma_n(x)) \end{aligned}$$

And given a $\mathbb{Z}$-basis $\{\alpha_1, \dots, \alpha_n\}$ of $\mathscr{O}_K$ we have $n \times n$ matrix

$$[\sigma]_{\{\alpha_1,\dots,\alpha_n\}} = (\sigma_i(\alpha_j))_{i,j}$$

The determinant

$$\det(\sigma_i(\alpha_j))$$

computes "volume" of $K/\mathscr{O}_K$, which serves as a is a measure of *density* of $\mathscr{O}_K$ in K.

To get a real number we rather consider

$$\det([\sigma]^2_{\{\sigma_1,\dots,\sigma_n\}}) = \det \text{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j) \in \mathbb{Z}$$

Definition. Discriminant

Let $\alpha_1, \dots, \alpha_n \in K$. Then

$$\text{disc}(\alpha_1, \dots, \alpha_n) := \det \text{tr}_{K/\mathbb{Q}}[\alpha_i\alpha_j]_{i,j} \in \mathbb{Z}$$

In particular, if $\alpha_1, \dots, \alpha_n$ is a $\mathbb{Z}$-basis of $\mathscr{O}_K$ then its disc is called the **discriminant Δ_K of K**.

> **Proposition:** The symmetric bilinear form
>
> $$\begin{aligned} K \times K &\to \mathbb{Q} \\ (x, y) &\mapsto \text{tr}_{K/\mathbb{Q}}(xy) \end{aligned}$$
>
> is non-degenerate. Thus $\Delta_K \neq 0$.

Hence, $\Delta_K \neq 0$.

prime decomposition and ramification

> **Proposition:** Let $\mathfrak{p} \subset \mathscr{O}_K$ be prime ideal. Then
>
> - $N(\mathfrak{p}) \in \mathfrak{p} \cap \mathbb{Z}$
> - $\mathfrak{p} \cap \mathbb{Z}$ is a **prime ideal** of $\mathbb{Z}$
> - Hence,
>
> $$\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$$
>
> for some prime $p \in \mathbb{Z}$.

Definition. Prime ideals above primes

When

> **Proposition:** Let $\mathfrak{p} \subset \mathscr{O}_K$ be prime ideal. Then
>
> - $N(\mathfrak{p}) \in \mathfrak{p} \cap \mathbb{Z}$
> - $\mathfrak{p} \cap \mathbb{Z}$ is a **prime ideal** of $\mathbb{Z}$
> - Hence,
>
> $$\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$$
>
> for some prime $p \in \mathbb{Z}$.

we say $\mathfrak{p}$ **is above** p

$$\begin{array}{ccc} \mathfrak{p} & \subset & \mathscr{O}_K & \subset & K \\ & & | & & \\ p\mathbb{Z} & \subset & \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

We have the morphisms

$$\mathbb{Z} \overset{\iota}{\hookrightarrow} \mathscr{O}_K \to \mathscr{O}_K/\mathfrak{p}$$

whose kernel is

$$\{a \in \mathbb{Z} \mid a \in \mathfrak{p}\} = \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$$

so by quotienting

$$\mathbb{Z}_p \hookrightarrow \mathscr{O}_K/\mathfrak{p}$$

which is a finite field extension of $\mathbb{Z}_p$.

Definition. The **inertial degree** of $\mathfrak{p} \subset \mathscr{O}_K$ *above* $p \in \mathbb{Z}$ is

$$f(\mathfrak{p}) := \dim_{\mathbb{Z}_p}(\mathscr{O}_K/\mathfrak{p})$$

$$N(\mathfrak{p}) = |\mathscr{O}_K/\mathfrak{p}| = p^{f(\mathfrak{p})}$$

Definition. Ramification index of $\mathscr{O}_K$

Let $\mathfrak{p} \subset \mathscr{O}_K$ be a prime ideal *above* $p \in \mathbb{Z}$. We call **ramification index** of $\mathfrak{p}$, $e(\mathfrak{p})$, the power of $\mathfrak{p}$ that divides $p\mathscr{O}_K$.
Hence,

$$p\mathscr{O}_K = \mathfrak{p}_1^{e(\mathfrak{p}_1)} \dots \mathfrak{p}_g^{e(\mathfrak{p}_g)}$$

We say p is **ramified** if $e(\mathfrak{p}_i) > 1$ for some i, otherwise p is non-ramified (that is, when $p\mathscr{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_g$).

Proposition: In

Definition. Ramification index of $\mathscr{O}_K$

Let $\mathfrak{p} \subset \mathscr{O}_K$ be a prime ideal *above* $p \in \mathbb{Z}$. We call **ramification index** of $\mathfrak{p}$, $e(\mathfrak{p})$, the power of $\mathfrak{p}$ that divides $p\mathscr{O}_K$.
Hence,

$$p\mathscr{O}_K = \mathfrak{p}_1^{e(\mathfrak{p}_1)} \dots \mathfrak{p}_g^{e(\mathfrak{p}_g)}$$

We say p is **ramified** if $e(\mathfrak{p}_i) > 1$ for some i, otherwise p is non-ramified (that is, when $p\mathscr{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_g$).

we have

$$[K : \mathbb{Q}] = \sum_{i=1}^{g} e(\mathfrak{p}_i) f(\mathfrak{p}_i)$$

As

$$p\mathscr{O}_K = \mathfrak{p}_1^{e(\mathfrak{p}_1)} \dots \mathfrak{p}_g^{e(\mathfrak{p}_g)}$$
$$p^{[K:\mathbb{Q}]} = N(p\mathscr{O}_K) = N(\mathfrak{p}_1^{e(\mathfrak{p}_1)} \dots \mathfrak{p}_g^{e(\mathfrak{p}_g)})$$

and since norm is multiplicative and

$$N(\mathfrak{p}) = |\mathscr{O}_K/\mathfrak{p}| = p^{f(\mathfrak{p})}$$

we have

$$N(\mathfrak{p}_1^{e(\mathfrak{p}_1)} \dots) = \prod_i p^{f(\mathfrak{p}_i)e(\mathfrak{p}_i)}$$

Proposition: Let K be a number field, $\exists \theta$ such that

$$\mathscr{O}_K = \mathbb{Z}[\theta]$$

and $p \in \mathbb{Z}$ prime. Let

$$m_\theta(X) \bmod p = \prod_i \phi_i(X)^{e_i} \text{ in } \mathbb{Z}_p[X]$$

with ϕ_i coprime and irreducible. Then setting

$$\mathfrak{p}_i := (p, \tilde{\phi}_i(\theta)) = p\mathscr{O}_K + \tilde{\phi}_i(\theta)\mathscr{O}_K$$

where $\tilde{\phi}_i$ is any lift of ϕ_i to $\mathbb{Z}[X]$, gives us the factorization of $p\mathscr{O}_K = \mathscr{O}_K$

$$p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}^{e_g}$$

Definition. Inert, totally ramified primes

	e	f	g	
inert	1	n	1	
totally ramified	n	1	n	

Let K is a number field. Then p is **ramified** $\iff p \mid \Delta_K$.

[2]

Corollary of

Let K is a number field. Then p is **ramified** $\iff p \mid \Delta_K$.

There are only a finite number of ramified primes for a number field K.

[3]

ideal class group

glossary

K	algebraic integers	elements	norm	trace	number of embeddings into $\mathbb{C}$	Δ_K
$\mathbb{Q}$	$\mathbb{Z}$					
$\mathbb{Q}(\sqrt{2})$	$\mathbb{Z}[\sqrt{2}]$?	$a + b\sqrt{2}$	$a^2 - 2b^2$	$2a$	2; $\sqrt{2} \mapsto \sqrt{2}, -$	
$\mathbb{Q}(i)$ that is $\mathbb{Q}(\sqrt{-1})$	$\mathbb{Z}$?					
$\mathbb{Q}(\sqrt{5})$	$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$				2; $\sqrt{5} \mapsto \sqrt{5}, -$	5
$\mathbb{Q}(\sqrt{m})$	?					

number fields vs elliptic curves

number fields	**elliptic curves**
K	$E := V(y^2 - f(x))$ **where $f(X)$ is a smooth cubic**
ring of integers $\mathcal{O}_K$ whose elements are roots of monic polynomials	rational points on the elliptic curves $E(\mathbb{Q}) := E \cap \mathbb{Q}P^2$
Proposition: Let K be a number field. Then $\mathcal{O}_K$ is a free Abelian group of rank $[K, \mathbb{Q}]$.	**(Mordell-Weil theorem)** F be a number field (finite extension of $\mathbb{Q}$) and $E(F)$ be an elliptic curve curve ($y^2 = f(x)$) with a F-rational point $O \in E(F)$ then $(E(F), +, O)$ is a finitely generated Ab group. $\implies E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{\text{rank}(E/\mathbb{Q})}$
$\mathcal{O}_K^\times$ is a finitely generated Abelian group with rank $r_1 + r_2 - 1$, $\implies \mathcal{O}_K^\times = \underbrace{\mu(K)}_{\text{torsion}} \oplus \mathbb{Z}^{r_1+r_2-1}$	
Class group $\text{Cl}(K)$	$Ш(E/\mathbb{Q})$ *Shafarevich-Tate group*
Dedekind zeta function $\zeta_K(s) := \sum_{I \subseteq \mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(I)^s}$ $= \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^s}$	• Hasway-Weil L-function $L(E, s)$ is a meromorphic function on $\mathbb{C}$ where $L(E, s) = \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_{\text{primes } p} \left(1 - \frac{a_p}{p^s} + \epsilon($ where $\epsilon(p) = \begin{cases} 0 \\ 1 \end{cases}$ • a_n is recovered via a_p for p primes • $a_p = \begin{cases} p + 1 - \lvert\{E(\mathbb{F}_p)\}\rvert & \text{good rec} \\ \pm 1 & \text{mult rec} \\ 0 & \text{not good} \end{cases}$
(Analytic class number formula ~1839) $\lim_{s \to 0} \frac{\zeta_K(s)}{s^{r_1+r_2-1}} = -\frac{R_K h_K}{\lvert\mu(K)\rvert}$	⚠ **Birch and Swinnerton-Dyer conjecture** Let $E(F)$ where F be a number field. Then analytic rank(E) = order at $s = 1$ of $L(E, s)$ = algebraic rank$(E) = r$. (implicit in this conjecture is $L(E, s)$ is holomorphic at $s = 1$) Finer version using other refined invariants of E

ramification in number theory and algebraic geometry

> **Proposition:** Let D be any Dedekind domain with fraction field K, L/K a finite separable field extension and R the integral closure of D in L. Then R is again a Dedekind domain.

So

Definition. Ramified primes in Dedekind domains

From

> **Proposition:** Let D be any Dedekind domain with fraction field K, L/K a finite separable field extension and R the integral closure of D in L. Then R is again a Dedekind domain.

given any prime ideal $\mathfrak{p} \subset D$ of a Dedekind domain D, we have a primary decomposition

$$\mathfrak{p}R = \beta_1^{e_1} \dots \beta_r^{e_r}$$

where e_k is called the **ramification index** of the prime β_k. A prime $\mathfrak{p}$ is called **ramified** if some ramification index $e_k > 1$.

We say L/K is *unramified* if all prime ideals of R are *unramified* in L.

Definition. Ramification points of morphisms of curves

Let X, Y be two curves (complete, non-singular, 1 dimensional integral scheme over $k = \bar{k}$). Let

$$f : X \to Y$$

be a finite morphism, $P \in X$ and $Q = f(P)$. Then f is **unramified** at P if

- the induced map on stalks

  $$\mathcal{O}_{Y,Q} \to \mathcal{O}_{X,P}$$

  gives

$$\mathfrak{m}_Q \mathscr{O}_{X,P} = \mathfrak{m}_P$$

- and the extension of residue fields

$$k(Q) \to k(P)$$

  is separable

and otherwise it is **ramified** at P.

The map f is *unramified* if it is unramified at every point, and *ramified* if it is ramified at some point.

From

> **Proposition:** Let D be any Dedekind domain with fraction field K, L/K a finite separable field extension and R the integral closure of D in L. Then R is again a Dedekind domain.

let

$$\iota : D \hookrightarrow R$$

induce the morphism

$$\iota^* : \mathrm{Spec}(R) \to \mathrm{Spec}(D)$$

Then a point $\mathfrak{p}$ is a ramification point of the map $\iff$ the prime $\mathfrak{p}$ is a ramified prime.

Let $\mathfrak{p} \subset R$ be prime, that is $\mathfrak{p} \in \mathrm{Spec}(R)$. Then

$$\mathfrak{p} \mapsto \mathfrak{q} \iff f(\mathfrak{p}) = \mathfrak{p} \cap D = \mathfrak{q}$$

[4]

Current note has 0 direct children and 0 total descendants.

- stem
  - Objects stemming from spaces over $\mathbb{Q}$
    - Algebraic number fields

And it has 2 siblings.

- stem
  - Objects stemming from spaces over $\mathbb{Q}$
    - Elliptic curves over $\mathbb{Q}$
    - Algebraic number fields

---

1. https://feog.github.io/antchap1.pdf ↩
2. https://math.stackexchange.com/a/700951 ↩
3. https://feog.github.io/ANT10.pdf ↩
4. https://www.wstein.org/edu/2010/581b/projects/matthew_ward/581bfinalproject.pdf ↩