Prime Ideal Theorem on Number Fields

Hikmet Burak Özcan

İzmir Institute of Technology

İzmir Mathematics Days 2, Dokuz Eylül University

13 September 2019

Overview

1. Definitions and Preliminaries
2. Motivation
3. Prime Ideal Theorem
4. References

Definitions and Preliminaries

- A **number field** K is a finite degree extension of the field of rational numbers $\mathbb{Q}$, i.e., a field which is a finite dimensional vector space over the field $\mathbb{Q}$.

  Examples:

⋆ $\mathbb{Q}$ itself is a number field of degree 1.

⋆

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

is a quadratic number field, namely, a number field of degree 2.

Basic Definitions in Algebraic Number Theory

- An **algebraic number** is a complex number $\alpha \in \mathbb{C}$ which is a root of a non-zero polynomial $f(x) \in \mathbb{Q}[x]$.
- An **algebraic integer** is a complex number $\alpha \in \mathbb{C}$ which is a root of a monic polynomial with coefficients in $\mathbb{Z}$
- $i \in \mathbb{Q}(i)$ is an algebraic integer while $\frac{1}{2}$ is not an algebraic integer.
- The set of algebraic integers of a number field K is called the **ring of integers** of K denoted by $\mathcal{O}_K$.
- The set of algebraic integers of $\mathbb{Q}$ is $\mathbb{Z}$, i.e., $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
- The **minimal polynomial** f of an algebraic number α is the (non-zero) monic polynomial in $\mathbb{Q}[X]$ of smallest degree such that $f(\alpha) = 0$.

Properties of $\mathcal{O}_K$

For a number field K of degree n, the ring of integers $\mathcal{O}_K$ has the following properties:

- $\mathcal{O}_K$ is a ring.
- $\mathcal{O}_K$ is a free abelian group of finite rank n.
- $\mathcal{O}_K$ is a Dedekind domain, i.e,. every non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ can be written in a unique way (up to permutation of the factors) as a product of prime ideals.

Ideals in Number Fields

Definition

Let K be a number and let $\mathfrak{a} \subseteq \mathcal{O}_K$ be a non-zero ideal. The norm of $\mathfrak{a}$, denoted by $N(\mathfrak{a})$, is defined as the index $|\mathcal{O}_K : \mathfrak{a}|$.

- The norm $N(\mathfrak{a})$ is finite for every non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$.
- Norm is a multiplicative function on ideals which means that

$$N(\mathfrak{a}_1\mathfrak{a}_2) = N(\mathfrak{a}_1)N(\mathfrak{a}_2)$$

for every non-zero ideal $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq \mathcal{O}_K$.

Dedekind's recipe for factorization of ideals into primes

For a given prime number p, we may consider the principal ideal $p\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{p_1}^{e_1}\mathfrak{p_2}^{e_2}\cdots\mathfrak{p_r}^{e_r},$$

where $\mathfrak{p_i}$'s are distinct prime ideals.

Dedekind's Recipe

- Suppose that $\mathcal{O}_K = \mathbb{Z}[\theta]$, where $\theta \in \mathcal{O}_K$.
- Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of θ.
- $f(x) \equiv f_1^{\alpha_1}(x).\, f_2^{\alpha_2}(x).\cdots.\, f_r^{\alpha_r}(x)\ (mod\ p)$, where $f_i(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial.
- $\mathfrak{p}_i = (p, f_i(\theta)) \subseteq \mathcal{O}_K$ is a prime ideal with $N(\mathfrak{p_i}) = p^{deg(f_i)}$.
- Then, we have that

$$p\mathcal{O}_K = \mathfrak{p_1}^{\alpha_1}\mathfrak{p_2}^{\alpha_2}\cdots\mathfrak{p_r}^{\alpha_r},$$

where $\mathfrak{p_i}$'s are distinct prime ideals.

Example

- Consider the ring of Gaussian integers $\mathcal{O}_K = \mathbb{Z}[i]$.
- $x^2 + 1$ is the minimal polynomial of i.
- $x^2 + 1 \equiv (x+2)(x+3)$ $(mod\ 5)$.
- $\mathfrak{p}_1 = (5, i+2) = (2+i)$ and $\mathfrak{p}_2 = (5, i+3) = (2-i)$ are prime ideals.
- $5\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$, where $N(\mathfrak{p}_i) = 5$ for $i = 1, 2$

Example

- $x^2 + 1 \equiv x^2 + 1$ $(mod\ 7)$.
- $\mathfrak{p}_1 = (7, i^2 + 1) = (7)$ is a prime ideal.
- $7\mathbb{Z}[i] = \mathfrak{p}_1$, where $N(\mathfrak{p}_1) = 7^2$

Motivation

Let $\mathbb{P} \subset \mathbb{N}$ be the set of prime numbers and

$$\pi(x) = |\{p \in \mathbb{P} \mid p \leq x\}|$$

be the prime counting function. For example, $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$.

Euclid offered a proof of the infinitude of primes for the first time in his work *"Elements"* c. 300 BC. So, we have that

$$\lim_{x \to \infty} \pi(x) = \infty.$$

In 1896, **Jacques Hadamard** and **Charles Jean de la Vallée Poussin** proved independently **Prime Number Theorem** which gives an asymptotic formula for the prime counting function $\pi(x)$:

$$\pi(x) \sim \frac{x}{logx}.$$

Now, one could think about

- $K = \mathbb{Q}$
- $\mathcal{O}_K = \mathbb{Z}$
- $p\mathcal{O}_K = p\mathbb{Z}$
- $N(p\mathbb{Z}) = |\mathbb{Z} : p\mathbb{Z}| = p$ for every prime number p
- $\pi(x) = |\{p\mathbb{Z} \subset \mathbb{Z} \mid N(p\mathbb{Z}) \leq x\}|$.

Thus, the prime counting function $\pi(x)$ can be considered as a function which counts prime ideals whose norm is not greater than x.

Question

If K is a number field, $\mathcal{O}_K$ its ring of integers and $\mathbb{P}_K$ the set of prime ideals in $\mathcal{O}_K$, then what can we say asymptotically about the function defined as

$$\pi_K(x) = |\{\mathfrak{p} \in \mathbb{P}_K \mid N(\mathfrak{p}) \leq x\}|?$$

Landau's Prime Ideal Theorem

Theorem

Let K be a number field, $\mathcal{O}_K$ its ring of integers and $\mathbb{P}_K$ the set of prime ideals in $\mathcal{O}_K$ and

$$\pi_K(x) = |\{\mathfrak{p} \in \mathbb{P}_K \mid N(\mathfrak{p}) \leq x\}|$$

be the prime ideal counting function. Then, there is an asymptotic formula for $\pi_K(x)$:

$$\pi_K(x) \sim x/\log(x).$$

Dedekind Zeta Function and Analytic Properties

Definition

The **Dedekind zeta function** of a number field K is defined for complex numbers s with $Re(s) > 1$ by the Dirichlet series

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subseteq \mathcal{O}_K} \left(\frac{1}{N(\mathfrak{a})} \right)^s .$$

- If $K = \mathbb{Q}$, then

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

is the Riemann zeta function.

Some Analytic Properties of Dedekind Zeta Function

- The Dedekind zeta function $\zeta_K(s)$ is absolutely convergent when $\Re(s) > 1$.
- The Dedekind zeta function $\zeta_K(s)$ has an Euler product which is a product over all the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$

$$\zeta_K(s) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

- **Erich Hecke** first proved that the Dedekind zeta function $\zeta_K(s)$ has an analytic continuation to the complex plane as a meromorphic function, having a simple pole only at $s = 1$.

Prime Ideal Theorem for Gaussian Integers

$p = 4k + 3$

- Let $p = 4k + 3$ be a prime number and $p \leq \sqrt{x}$.
- $\mathfrak{p} = (p) \subset \mathbb{Z}[i]$ is a prime ideal.
- $N(\mathfrak{p}) = p^2$.

$p = 4k + 1$

- Let $p = 4k + 1$ be a prime number and $p \leq x$.
- $p = a^2 + b^2$ for some integer a, b.
- $p = (a + bi)(a - bi) \in \mathbb{Z}[i]$.
- $\mathfrak{p}_1 = (a + bi)$ and $\mathfrak{p}_2 = (a - bi)$ are prime ideals.
- $N(\mathfrak{p}_{1,2}) = p$.

Therefore,

$$\pi_{\mathbb{Q}(i)}(x) \sim \frac{\pi(\sqrt{x})}{2} + \frac{2\pi(x)}{2} \sim \frac{x}{log(x)}.$$

References

F. Oggier, Lecture Notes on Introduction to Algebraic Number Theory

F. Jarvis, Algebraic Number Theory, Springer, 2014

R. Murty, Problems in Analytic Number Theory, Springer, 2008

THANK $\sim$ YOU