Number Fields, Prime Ideal Decomposition, Orders

Osmanbey Uzunkol

TÜBİTAK BİLGEM
Mathematical and Computational Sciences Labs

ECC 2016 Computational Algebraic Number Theory School
1. September 2016

References:

1. Marcus: Number Fields,
2. Neukirch: Algebraische Zahlentheorie
3. Stevenhagen: Number Rings, http://websites.math.leidenuniv.nl/algebra/ant.pdf

Neukirch, Preface, Algebraische Zahlentheorie, 1992

Die Zahlentheorie nimmt unter den mathematischen Disziplinen eine ähnlich idealisierte Stellung ein wie die Mathematik selbst unter den Naturwissenschaften. Frei von der Pflicht, von außen kommenden Gegebenheiten dienlich sein zu müssen.

Starting with 1+1=2

Primes as sum of Squares (Neukirch):
$2 = 1 + 1,\ 5 = 1 + 4,\ 13 = 4 + 9,\ 17 = 1 + 16,\ 29 = 4 + 25, \cdots.$

Gaussian integers $\mathbb{Z}[i]$: For all $p \in \mathbb{P} \setminus \{2\}$ we have
$p = a^2 + b^2,\ a, b \in \mathbb{Z}$ iff $p \equiv 1 \bmod 4$.

Starting with 1+1=2

Primes as sum of Squares (Neukirch):
$2 = 1 + 1,\ 5 = 1 + 4,\ 13 = 4 + 9,\ 17 = 1 + 16,\ 29 = 4 + 25, \cdots$.

Gaussian integers $\mathbb{Z}[i]$: For all $p \in \mathbb{P} \setminus \{2\}$ we have
$p = a^2 + b^2,\ a, b \in \mathbb{Z}$ iff $p \equiv 1 \bmod 4$.

Another example

Finding integral solutions (Stevenhagen): Find all integral solution to $x^2 + 1 = y^3$.
Find all integral solution to $x^2 + 19 = y^3$.

$$18^2 + 19 = 7^3.$$

Local Rings

Let R be an integral domain, $S \subseteq R$ be multiplicatively closed containing 1.

Definition

Localized ring can be defined

$$S^{-1}R = \{\frac{r}{s} : r \in R, s \in S\}.$$

We have $R \subseteq S^{-1}R \subseteq Q(R) = K$.

Localization at prime ideals

Let $\mathfrak{p}$ be a prime ideal of R. Then setting $S = R \setminus \mathfrak{p}$ one obtains

$$S^{-1}R := R_{\mathfrak{p}} = \{\frac{r}{s} : r \in R, s \notin \mathfrak{p}\}.$$

This is a local ring with the unit group

$$R_{\mathfrak{p}}^* = \{\frac{r}{s} : r, s \notin \mathfrak{p}\}.$$

Hence the unique maximal ideal $R_{\mathfrak{p}} \setminus R_{\mathfrak{p}}^*$ is of course

$$\mathfrak{p}R_{\mathfrak{p}} = \{\frac{r}{s} : r \in \mathfrak{p}, s \notin \mathfrak{p}\}.$$

Localization at prime ideals

Theorem

Let I be an ideal R. Then

$$S^{-1}I = \{\frac{r}{s} : r \in I, s \in S\} \subseteq S^{-1}R$$

is an ideal. Moreover, all ideals of $S^{-1}R$ are of this form and $I \cap S =$ iff $S^{-1}I \neq S^{-1}R$.
If I is a fractional $R-$ideal then

$$S^{-1}I = \{\frac{r}{s} : r \in I, s \in S\} \subseteq K$$

is a fractional $S^{-1}R-$ideal.

We denote an $R_{\mathfrak{p}}-$ideal by $I_{\mathfrak{p}}$.

Invertibality condition

Lemma

Let I be a fractional $R-$ideal. Then

$$I = \cap_{\mathfrak{m}} I_{\mathfrak{m}}.$$

Theorem

A fractional $R-$ideal I is invertible iff the following conditions hold:

1. *I is finitely generated*
2. *$I_{\mathfrak{m}}$ is a principal fractional $R_{\mathfrak{m}}-$ideal for all maximal ideals $\mathfrak{m}$.*

Local number rings

Theorem

Let $R_{\mathfrak{p}}$ be a local number ring. Then every non-zero ideal of $R_{\mathfrak{p}}$ contains some power of its maximal ideal.

Theorem

Let $\mathfrak{p}$ be a prime ideal of a number ring R. TFAE

1. *$\mathfrak{p}$ is an invertible ideal*
2. *$R_{\mathfrak{p}}$ is a principal ideal domain and every $R_{\mathfrak{p}}-$ideal is a power of $pR_{\mathfrak{p}}$*
3. *There exists a $\pi \in R_{\mathfrak{p}}$ such that every $\alpha \in K^*$ can uniquely be written as $x = u \cdot \pi k$ with $u \in R_{\mathfrak{p}}^*$ and $k \in \mathbb{Z}$*

A local ring satisfying 2. and 3. is called a discrete valuation ring (DVR).

Definition

A number ring is called a Dedekind ring if for any prime ideal $\mathfrak{p}$ the localization at $\mathfrak{p}$, $R_{\mathfrak{p}}$ is a DVR.

Theorem

Let R be a number ring which is also a Dedekind ring. Then each ideal I can uniquely be factored

$$I = \prod_{1=1}^{s} \mathfrak{p}_i,$$

where $\mathfrak{p}_i'$s are pairwise coprime.

Number Fields, Prime Ideal Decomposition, Orders

TEŞEKKÜR EDERİM!

osmanbey.uzunkol@tubitak.gov.tr