Algebraic Number Theory

[all rings are commutative unless specified otherwise]

Joydip Ghosh

Personal note

January 21, 2024

Algebraic number, algebraic integer and number field

Algebraic Number

- Definition: Root of a polynomial over $\mathbb{Z}$.
- Example: $\frac{3+\sqrt{-5}}{7}$
- Non-example: π

Algebraic Integer [set forms a ring denoted by $\mathbb{A}$]

- Definition: Root of a monic polynomial over $\mathbb{Z}$.
- Example: $2 + \sqrt{3}$
- Non-example: π, $\frac{3+\sqrt{-5}}{7}$

Number Field [set forms a field denoted by $\mathbb{K}$]

- Definition-1: Subfield of $\mathbb{C}$ and a finite extension over $\mathbb{Q}$.
- Definition-2: $\mathbb{Q}[\alpha]$ for some algebraic number $\alpha \in \mathbb{C}$ [See primitive element theorem on slide 11].

Sets of number fields and number rings in $\mathbb{C}$

- Corresponding to every number field there is a number ring: $\mathbb{K} \mapsto \mathbb{K} \cap \mathbb{A}$.

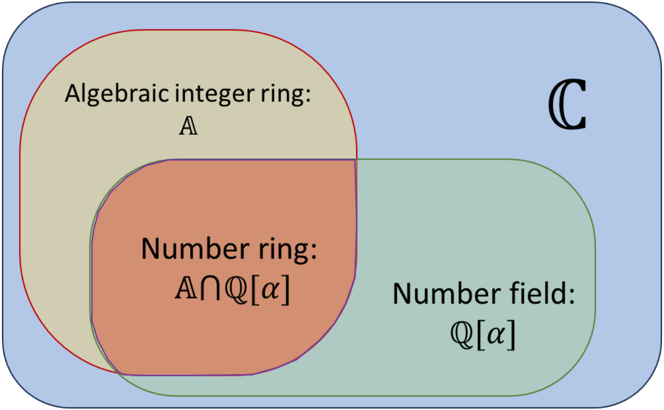


Figure 1: Venn diagram for number rings and number fields.

Some number fields and corresponding number rings

- $\mathbb{Q}[\omega]$ is called a *Cyclotomic* field for $\omega = e^{\frac{2\pi i}{m}}$, a primitive m^{th} root of unity.
- $\mathbb{Q}[\sqrt{m}]$ is called a *Quadratic* field for $m \in \mathbb{Z}$, a square-free integer.
- The following table shows some number fields and their corresponding rings, where $m, a, b \in \mathbb{Z}$:

$\mathbb{K}$	$\mathbb{K} \cap \mathbb{A}$
$\mathbb{C}$	$\mathbb{A}$
$\mathbb{Q}[\omega]$: $\omega = e^{\frac{2\pi i}{m}}$	$\mathbb{Z}[\omega]$
$\mathbb{Q}[\sqrt{m}]$	$a + b\sqrt{m} : m \not\equiv 1 \bmod 4$ $\frac{a+b\sqrt{m}}{2} : a \equiv b \bmod 2, m \equiv 1 \bmod 4$
$\mathbb{Q}$	$\mathbb{Z}$

Table 1: Number fields and their corresponding number rings.

Basics of Ideals: Definitions

Ideal:

R is a commutative ring. $I \subseteq R$ is an *ideal* of R, if

i. I is an additive subgroup of R

ii. $rI \subseteq I$, $\forall r \in R$. [Equivalently, $ri \in I$, $\forall r \in R, \forall i \in I$]

Maximal Ideal:

I is a maximal ideal of R, if there is no *proper* ideal in between R and I.

Prime Ideal:

I is a prime ideal of R, if $ab \in I \Rightarrow a \in I$ or $b \in I$ $\forall a, b \in R$.

Fact:

In a commutative ring, a maximal ideal is always prime.

Dedekind domain: Definition

Dedekind domain:

An integral domain, where all non-zero ideals factor uniquely into prime ideals.

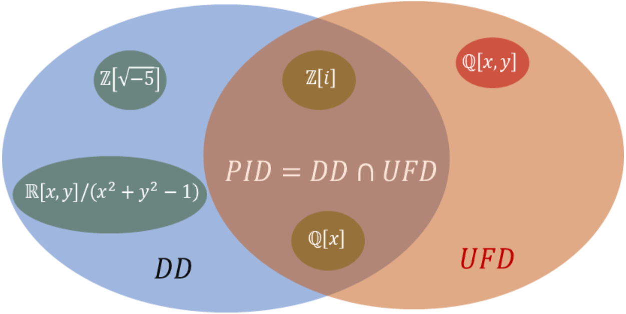


Figure 2: Venn diagram for Dedekind domain and UFD.

Dedekind domain: Properties

- For any set of ideals in a Dedekind domain, ‘lcm’ and ‘gcd’ are naturally defined.
- All non-zero prime ideals are maximal.
- Every number ring is a Dedekind domain.
- Every ideal in a Dedekind domain is generated by at most two elements (one of them is arbitrary).

Ideal Arithmetic

Arithmetic operations between two ideals can be defined as follows:

Operation	Definition	R=PID	R=DD
$I \cap J$	$(\{k : k \in I \cap J\})$	$(\mathrm{lcm}(i,j))$	$\mathrm{lcm}(I,J)$
IJ	$(\{ab : a \in I, b \in J\})$	(ij)	IJ
$I + J$ [1]	$(\{a + b : a \in I, b \in J\})$	$(\gcd(i,j))$	$\gcd(I,J)$
$I : J$	$\{a \in R : aJ \subset I\}$	$(\mathrm{lcm}(i,j)/j)$	–
$\sqrt[n]{I}$	$\{a \in R : a^n \in I\}$	–	–

Table 2: Arithmetic operations between two ideals.

[1] $I + J = I \cup J$

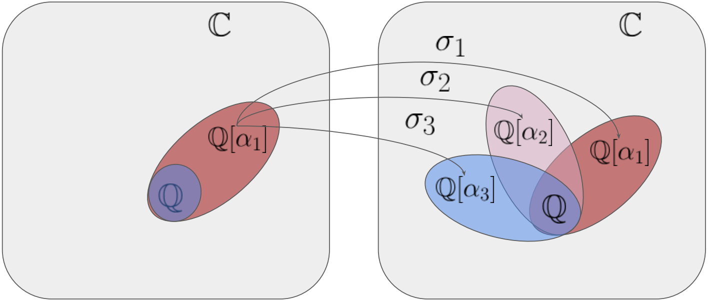
Appendix

Selected topics from (commutative) abstract algebra

Embedding extension lemma

- Lemma: $[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = n$ implies that there are exactly n embeddings of $\mathbb{Q}[\alpha_1]$ in $\mathbb{C}$.

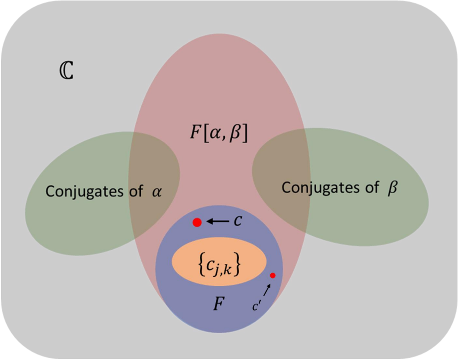
  - Visual proof: Each embedding σ_k maps $\mathbb{Q}[\alpha_1]$ into $\mathbb{Q}[\alpha_k]$, as shown in the figure below, where each α_k is conjugate to α_1. $[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = n$ implies that that there are exactly n conjugates of α_1.



Primitive element theorem

- Theorem: Basically, if α, β are algebraic over F, then $F[\alpha, \beta] = F[\alpha + c\beta]$ for some $c \in F$.

  - Visual proof: Define $c_{j,k} \equiv \frac{\alpha - \alpha_j}{\beta_k - \beta}$. So, $|\{c_{j,k}\}| < \infty$. Choose $c \in F - \{c_{j,k}\} \Rightarrow \alpha + c\beta \neq \alpha_j + c\beta_k, \forall j, k$. So, $F[\alpha + c\beta] \subseteq F[\alpha, \beta]$ has $[F[\alpha, \beta] : F]$ embeddings in $\mathbb{C}$.



Galois theory

- Theorem: $f(x) \in F[x]$ splitting over K is solvable iff $Gal(K/F)$ is solvable (i.e., it has a subnormal series with abelian factors).
  - Visualization: $f(x) = x^3 - 2$ with roots r_1, r_2 and r_3.