Algebraic Number Theory

Lecture 3, 22th October 2021

1.2 Ideals

Motivation: We already saw that the ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, since

$$6 = \underbrace{2}_{a}\cdot\underbrace{3}_{b} = \underbrace{(1+\sqrt{-5})}_{c}\underbrace{(1-\sqrt{-5})}_{d}. \quad (\star)$$

Kummer proposed the idea of "ideal numbers" a, b, c, d which break $(\star)$ into smaller pieces in such a way that the factorization becomes unique.

Whatever these "ideal numbers" are, if p is an ideal number and $p \mid a$ and $p \mid b$ then we should have $p \mid a \pm b$. Also if $p \mid a$ then $p \mid a \cdot x$ for any $x \in R$.

To deal with these type of objects Dedekind suggested to represent an "ideal number" by the set of all numbers which are divisible by it. This leads to the notion of ideals.

Definition 1.19 Let R be a commutative unitary ring. A non-empty subset $I \subset R$ is called an <u>ideal</u> of R, if

i) $a, b \in I \Rightarrow a+b \in I$

ii) $a \in I,\ x \in R \Rightarrow a \cdot x \in I$

Example: $n\mathbb{Z} = \{n \cdot a \mid a \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$ for any n.

Remarks 1.20

i) $(I, +, \cdot)$ is a subring of R.

ii) $R, \{0\}$ are ideals for any R.

iii) If $\varphi: R \to S$ is a ring hom. then

$$\operatorname{Ker} \varphi = \{x \in R \mid \varphi(x) = 0\} \text{ is an ideal.}$$

iv) For an ideal I we can consider the quotient ring $R/I = \{\bar{a} \mid a \in R\}$ given by the set of all equivalence classes of $a \in R$

$$\bar{a} = \{b \mid \underbrace{a-b \in I}_{a \equiv b \bmod I}\}.$$

This is a ring by $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a} \cdot \bar{b} = \overline{ab}$

For $\bar{a}$ we also write $a \bmod I$.

We have the canonical projection

$$p : R \to R/I$$
$$a \mapsto \bar{a},$$

which is a surjective ring homomorphism with $\mathrm{Ker}(p) = I$. ($\Rightarrow$ Every ideal is the kernel of some ring hom)

v) We have the isomorphism theorem:

Any ring hom $\varphi : R \to S$ induces an isomorphism

$$\bar{\varphi} : R/\mathrm{Ker}(\varphi) \xrightarrow{\sim} \mathrm{im}(\varphi).$$

$$\left(\begin{tikzcd} \varphi : R \arrow[r, "p"] \arrow[dr] & R/\mathrm{Ker}\varphi \arrow[d, "\tilde{\varphi}"] \\ & R' \end{tikzcd} \right)$$

If not stated otherwise then R (and all rings) is always a commutative unitary ring in the following.

Definition 1.21

i) For $a \in R$ we define

$$(a) = Ra = \{ca \mid c \in R\}.$$

This is an ideal in R. It is called the <u>principal ideal</u> generated by a.

$(0) = R$
$(0) = \{0\}$

ii) Let R be a domain.
If every ideal in R is a principal ideal then R is called a principal ideal domain (PID).

Not every ring is a PID, but we have the

Proposition 1.22 Every Euclidean ring is a PID.

Proof: Check yourself. (Consider $a \in I$ where $N(a) = \min_{x \in I} \{N(x)\}$.
Then show $I = (a)$)

Lemma 1.23 Let R be a commutative & unitary ring

i) $a \mid b \iff (b) \subseteq (a)$ for $a, b \in R$.

$a \sim b \iff (a) = (b)$

ii) If $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals of R, then $\mathfrak{a}_1 \cap \mathfrak{a}_2$ and $\mathfrak{a}_1 + \mathfrak{a}_2 = \{a_1 + a_2 \mid a_i \in \mathfrak{a}_i\}$ are ideals.

iii) $v \in R$ is a multiple of a and $b \iff (v) \subseteq (a) \cap (b)$

iv) $d \in R$ is a divisor of a and $b \iff (a) + (b) \subseteq (d)$.

Definition 1.24 Let $a_1, \dots, a_n \in R$.

We define a <u>greatest common divisor</u> (gcd) (resp. a <u>least common multiple</u> (lcm)) of $a_1, \dots, a_n$ by the following two properties

i) $\gcd(a_1, \dots, a_n) \mid a_i$ (resp. $a_i \mid \operatorname{lcm}(a_1, \dots, a_n)$) for all $i = 1, \dots, n$

ii) from $t \mid a_i$ (resp. $a_i \mid t$) for all $i = 1, \dots, n$ we obtain $t \mid \gcd(a_1, \dots, a_n)$ (resp. $\operatorname{lcm}(a_1, \dots, a_n) \mid t$) $t \in R$.

Note: gcd and lcm do not need to exist. But if they do they are unique up to units.

Example 1.25 In $R = \mathbb{Z}[\sqrt{-3}]$

$$a_1 = 4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$$

$$a_2 = 2 \cdot (1+\sqrt{-3})$$

have no gcd.

Proposition 1.26 Let R be a PID.

i) For any $a, b \in R$ the gcd and lcm exist and

$$(\gcd(a,b)) = (a) + (b)$$

$$(\operatorname{lcm}(a,b)) = (a) \cap (b)$$

ii) For $a_1, \dots, a_n \in R$ there exist $x_1, \dots, x_n \in R$ with

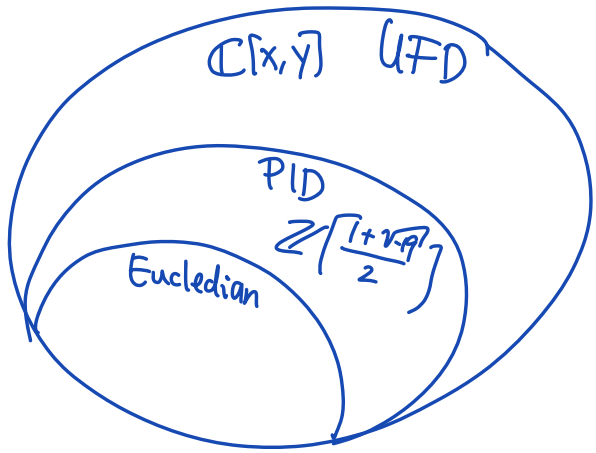
$$\gcd(a_1, \dots, a_n) = x_1 a_1 + \dots + x_n a_n .$$

Proof: Can be obtained from Lemma 1.23.

Proposition 1.27 PID are factorial.

Proof: Algebra course

So we have the following



Definition 1.28 Let $\mathfrak{a}, \mathfrak{b}$ ideals in R

i) $\mathfrak{a}$ and $\mathfrak{b}$ are called <u>coprime</u> if $\mathfrak{a}+\mathfrak{b}=R$.

ii) We define the product of $\mathfrak{a}, \mathfrak{b}$ by

$$\mathfrak{a}\cdot\mathfrak{b} = \left\{ \sum_{i=1}^{r} a_i b_i \;\middle|\; r\geq 0,\ a_i\in\mathfrak{a}, b_i\in\mathfrak{b} \right\}$$

This is again an ideal of R and

$$\mathfrak{a}\cdot\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}.$$

<u>Ex:</u> $(3), (5)$ are coprime ideals in $\mathbb{Z}$.

$$2\cdot 3 - 5 = 1 \implies n = 2n\cdot 3 - n\cdot 5 \in (3)+(5) = (1) = \mathbb{Z}$$

$$(3)\cdot(5) = (15) = (3)\cap(5) = (\mathrm{lcm}(3,5))$$

$$(2)\cdot(4) = (8) \subset (2)\cap(4) = (4)$$

Lemma 1.29

i) If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime ideals then

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}.$$

ii) If $\mathfrak{b}$ is coprime to $\mathfrak{a}_1, \dots, \mathfrak{a}_n$, then $\mathfrak{b}$ is coprime to $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$.

<u>Proof:</u> i) If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime then there exist $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ with $a+b=1$.

$\Rightarrow$ if $c \in \mathfrak{a} \cap \mathfrak{b}$ then $c = ca + cb \in \mathfrak{a}\mathfrak{b}$.

ii) $\exists\, b_i, a_i$: $1 = a_i + b_i$, $a_i \in \mathfrak{a}_i$, $b_i \in \mathfrak{b}$

$$1 = \prod_{i=1}^{n} (b_i + a_i) = \underbrace{b_1 \cdot \ldots \cdot b_n + \ldots}_{\in \mathfrak{b}} + a_1 \cdot \ldots \cdot a_n \in \mathfrak{b} + \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$$

$\Rightarrow$ $R = \mathfrak{b} + \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$. $\square$

Theorem 1.30 (Chinese remainder theorem)

Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be coprime ideals. Then the map

$$R/\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n \longrightarrow R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$$

$$x \bmod \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n \longmapsto (x \bmod \mathfrak{a}_1, \dots, x \bmod \mathfrak{a}_n)$$

is a ring isomorphism.

In particular: given $x_1, \dots, x_n \in R$ then there exist

Proof: Due to Lemma 1.29 ii) it suffices to show the $n=2$ case. $\left(R/\underset{\mathfrak{a}}{\mathfrak{a}_1} \cdot \underbrace{\mathfrak{a}_2 \cdots \mathfrak{a}_n}_{\mathfrak{b}} \xrightarrow{\sim} R/\mathfrak{a} \times R/\mathfrak{b} \right)$

We show that for coprime $\mathfrak{a}, \mathfrak{b}$ the ring homomorphism

$$\varphi : R \longrightarrow R/\mathfrak{a} \times R/\mathfrak{b}$$
$$x \longmapsto (x \bmod \mathfrak{a}, x \bmod \mathfrak{b})$$

is surjective.

Since $\mathfrak{a}$ and $\mathfrak{b}$ are coprime there are $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ with $a+b=1$.

For given $x_1, x_2 \in R$ set $x = x_2 a + x_1 b$.

Then $x = x_2 a + x_1(1-a) = x_1 \bmod \mathfrak{a}$

$x = x_2(1-b) + x_1 b = x_2 \bmod \mathfrak{b}$

and therefore $\varphi(x) = (x_1 \bmod \mathfrak{a}, x \bmod \mathfrak{b})$,

i.e. φ is surjective.

The kernel of φ is

$$\operatorname{Ker} \varphi = \mathfrak{a} \cap \mathfrak{b} \overset{\text{Lemma 1.29 i)}}{=} \mathfrak{a} \cdot \mathfrak{b}$$

and therefore we obtain an isomorphism

$$\bar{\varphi}: R/\mathfrak{a}\cdot\mathfrak{b} \to R/\mathfrak{a} \times R/\mathfrak{b}. \qquad \square$$

Classical case $R=\mathbb{Z}$.

m,n coprime $\Rightarrow$ $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$$x \equiv 1 \mod$$

$$x \equiv 2 \mod$$

Definition 1.31

i) An ideal $\mathfrak{p} \subset R$ is called <u>prime ideal</u> if $\mathfrak{p} \neq R$ and $x \cdot y \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

ii) An ideal $\mathfrak{m} \subsetneq R$ is called <u>maximal ideal</u> if for any ideal $\mathfrak{a}$ with $\mathfrak{m} \subseteq \mathfrak{a}$ we have $\mathfrak{m} = \mathfrak{a}$ or $\mathfrak{a} = R$.

Proposition 1.32

i) An ideal $\mathfrak{p}$ is prime iff $\mathfrak{p} \neq R$ and $R/\mathfrak{p}$ is a domain.

ii) An ideal m is maximal iff R/m is a field.

iii) Every maximal ideal is prime.
(converse false: (0) is prime in $\mathbb{Z}$ but not maximal)

iv) An element $p \in R \setminus \{0\}$ is prime iff (p) is prime.
$\neq (0)$