ZAHLENTHEORIE SS 2019 - NOTE 6

Now we want to study in more detail the algebraic structure of the number rings $\mathcal{O}_K$, and in particular we want to compare them with $\mathbb{Z}$. So, let's look at $\mathbb{Z}$ a bit better: some properties of $\mathbb{Z}$ are

- $\mathbb{Z}$ is an <u>integrally closed domain</u>.
- $\mathbb{Z}$ is <u>noetherian</u>.
- $\mathbb{Z}$ is of <u>dimension one</u>: this means that every nonzero prime ideal is maximal.

We will see that every number ring $\mathcal{O}_K$ shares these properties. As a consequence we will generalize appropriately unique factorization in $\mathbb{Z}$ to unique factorization in $\mathcal{O}_K$:

<u>Thm</u>: Every ideal $I \subseteq \mathcal{O}_K$ factors uniquely as a product of prime ideals

$$I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}.$$

First, however, we need some commutative algebra

- <u>LOCALIZATION</u>

def: LOCAL RING

A ring is called LOCAL if it has an unique maximal ideal.

Rmk: Let A be a ring and $m \subseteq A$ an ideal. Then m is the unique maximal ideal of A iff $A \setminus m = A^*$

proof: ($\Rightarrow$) suppose m is the unique maximal, and let $u \in A \setminus m$. Then if u is not invertible, then $(u) \neq A$ so that (u) is contained in a maximal ideal. But then $(u) \subseteq m$, which is impossible.

($\Leftarrow$) if $I \subseteq A$ is an ideal and $I \not\subseteq m$, then there is a unit $u \in I$, hence $I = A$. $\square$

Example: THE RINGS $\mathbb{Z}_{(p)}$.

Let $p \in \mathbb{Z}$ be a prime and consider the ring

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; b \notin (p) \right\} = \left\{ \frac{a}{b} \;\middle|\; p \nmid b \right\}$$

Then this is a subring of $\mathbb{Q}$: indeed

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \quad \text{and if } \begin{matrix} p \nmid b_1 \\ p \nmid b_2 \end{matrix} \Rightarrow p \nmid b_1 b_2$$

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2} \quad \text{"} \quad \text{"}$$

Observe that $\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$ via $n \mapsto \frac{n}{1}$.

Moreover, in $\mathbb{Z}_{(p)}$ we have an ideal

$(p)_{(p)} = \left\{ \frac{a}{b} \mid a \in (p), b \notin (p) \right\} = \left\{ \frac{a}{b} \mid \begin{matrix} p \mid a \\ p \nmid b \end{matrix} \right\}$

and one sees easily that

$$\mathbb{Z}_{(p)} \setminus (p)_{(p)} = \mathbb{Z}_{(p)}^{*}$$

hence $\mathbb{Z}_{(p)}$ is local, and $(p)_{(p)}$ is the unique maximal ideal.

<u>In a way</u>, the only prime that matters in $\mathbb{Z}_{(p)}$ is p. All other primes q don't matter anymore. We have "localized" $\mathbb{Z}$ at p.

This process is more general, and works as follows:

<u>def</u>: MULTIPLICATIVELY CLOSED SUBSET

A = ring. A set $S \subseteq A$ is multiplicatively closed if

- $1 \in S$, $0 \notin S$.
- $a \in S, b \in S \Rightarrow ab \in S$.

<u>Example</u>: If $\mathfrak{p} \subseteq A$ is prime, then $S = A \setminus \mathfrak{p}$ is multiplicatively closed.

<u>def</u>: LOCALIZATION w.r.t. S

A = ring, $S \subseteq A$ mult. closed subset.

We define a ring

$$S^{-1}A = \left\{ \frac{a}{s} \;\middle|\; a \in A, s \in S \right\}$$ where we write

$$\frac{a}{s} = \frac{b}{t} \overset{\text{def}}{\iff} \exists\, u \in S \text{ s.t. } uat = ubs.$$

This is a ring with the operations

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

we have

$$0 = \frac{0}{1}, \quad 1 = \frac{1}{1}.$$

<u>Example</u>: (1) $\mathbb{Z}$, $S = \mathbb{Z} \setminus \{0\}$ (0 is prime)

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, b \neq 0 \right\} = \mathbb{Q}.$$

(2) A domain, $S = A \setminus \{0\}$

$$S^{-1}A = \operatorname{Frac} A$$

(3) $\mathbb{Z}$, $S = \mathbb{Z} \setminus (p)$, p prime

$$S^{-1}\mathbb{Z} = \mathbb{Z}_{(p)}$$

(4) A = ring, $\mathfrak{p} \subseteq A$ prime. We write

$$A_{\mathfrak{p}} := S^{-1}A, \quad S = A \setminus \mathfrak{p}$$

We collect here some properties of localization:

<u>Properties</u>: (1) There is a canonical ring homomorphism

$$A \to S^{-1}A, \quad a \mapsto \frac{a}{1}$$

(2) $(S^{-1}A)^{\times} \supseteq \left\{ \frac{s}{t} \,\middle|\, s, t \in S \right\}$

(3) If $I \subseteq A$ is an ideal, then

$$S^{-1}I = \left\{ \frac{a}{s} \,\middle|\, a \in I \right\} \subseteq S^{-1}A$$

is an ideal. Every ideal in $S^{-1}A$ has this form.

Moreover $S^{-1}I = A \iff I \cap S \neq \emptyset$.

(4) There is a bijection

$$\left\{ \begin{array}{c} \text{prime ideals} \\ I \subseteq A \text{ s.t. } I \cap S = \emptyset \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{prime ideals} \\ \text{in } S^{-1}A \end{array} \right\}$$

$$I \longmapsto S^{-1}I$$

Which restricts to a bijection on maximal ideals

(5) $\mathfrak{p} \subseteq A$ prime. Then we have a bijection

$$\left\{ \begin{array}{c} \text{(prime) ideals in } A \\ \text{s.t. } I \subseteq \mathfrak{p} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{(prime) ideals in} \\ A_{\mathfrak{p}} \end{array} \right\}$$

$$I \longmapsto I_{\mathfrak{p}} := S^{-1}I$$

Moreover $A_{\mathfrak{p}}$ is local with maximal ideal $\mathfrak{p}_{\mathfrak{p}}$.

(6) A domain: $A \subseteq S^{-1}A \subseteq \operatorname{Frac} A$.

(7) $I \subseteq A$ ideal s.t. $I \cap S \neq \emptyset$. $S^{-1}(A/I) \simeq S^{-1}A / S^{-1}I$.

Let's look again at the example of $\mathbb{Z}_{(p)}$

<u>Example</u>: $p > 0$ prime number, $\mathfrak{p} = (p)$.

$$\mathbb{Z}_{(p)} = \left\{ \frac{n}{m} \,\middle|\, p \nmid m \right\}$$

Let's look at the ideals in $\mathbb{Z}_{(p)}$. Every ideal is of the form $I_{(p)}$, where $I \subseteq \mathbb{Z}$ is an ideal s.t. $I \subseteq (p)$. Hence, I must be of the form

$$I = (p^n f), \quad p, f \text{ coprime}, \ n \geq 1.$$
$$= (p^n) \cap (f)$$

Then we see that

$$\begin{aligned} I_{(p)} = S^{-1} I &= S^{-1}(p^n) \cap S^{-1}(f) \\ &= S^{-1}(p^n) \cap S^{-1} A \\ &= S^{-1}(p^n) \\ &= (p^n)_{(p)} = \left(\frac{p^n}{1}\right) \end{aligned}$$

Hence every ideal of $\mathbb{Z}_{(p)}$ is of the form

$$\left(\frac{p^n}{1}\right) = \left(\frac{p}{1}\right)^n$$

Moreover

$$\left(\frac{p^n}{1}\right) \subseteq \left(\frac{p^m}{1}\right) \Rightarrow \frac{p^n}{1} = \frac{a p^m}{b} \quad p \nmid b$$

$$\Rightarrow b \cdot p^n = a p^m \Rightarrow p^m \mid b p^n \Rightarrow p^m \mid p^n \Rightarrow m \leq n$$

and the converse is obvious, so

$$\left(\frac{p^n}{1}\right) \subseteq \left(\frac{p^m}{1}\right) \Leftrightarrow n \geq m$$

Hence, a complete list of ideals in $\mathbb{Z}_{(p)}$ is given by

$$\underset{\overset{\shortparallel}{0}}{(1)}, \underset{\overset{\shortparallel}{1}}{\left(\frac{p}{1}\right)}, \underset{\overset{\shortparallel}{2}}{\left(\frac{p^2}{1}\right)}, \underset{\overset{\shortparallel}{3}}{\left(\frac{p^3}{1}\right)}, \ldots, \underset{\overset{\shortparallel}{n}}{\left(\frac{p^n}{1}\right)}, \ldots, 0$$

$m^0, m^1, m^2, m^3, \dots, m^n,$

So we see that:
- <u>the maximal ideal is principal</u>
- <u>every ideal is a power of the maximal ideal.</u>
- <u>there are only two prime ideals: $(0), m$.</u>

In particular, given any ideal $J \subseteq \mathbb{Z}_{(p)}$ we can define

$$\mathrm{ord}(J) = \text{unique } e \geq 0 \text{ s.t. } J = m^e.$$

and this defines a map

$$\begin{aligned} \mathrm{ord}: \mathbb{Z}_{(p)} \setminus \{0\} &\longrightarrow \mathbb{Z} \\ \frac{a}{s} &\longmapsto \mathrm{ord}\left(\left(\frac{a}{s}\right)\right). \end{aligned}$$

How can we write this better: observe that if we write

$$\frac{a}{s} = p^e \cdot \frac{b}{s}, \quad p \nmid b, p \nmid s, \text{ then}$$

$$\mathrm{ord}\left(\frac{a}{s}\right) = e$$

This works also over $\mathbb{Q}$: we can define a <u>homomorphism of groups</u>

$$\begin{aligned} \mathrm{ord}_p: \mathbb{Q} \setminus \{0\} &\longrightarrow \mathbb{Z} \\ p^e \cdot \frac{a}{b} &\longmapsto e \\ p \nmid a, p \nmid b & \end{aligned}$$

Then

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \setminus \{0\} \mid \mathrm{ord}_p(x) \geq 0\} \cup \{0\}$$

$$(p)_{(p)} = \{x \in \mathbb{Q} \setminus \{0\} \mid \mathrm{ord}_p(x) \geq 1\} \cup \{0\}$$

$$(p^2)_{(p)} = \{x \in \mathbb{Q} \setminus \{0\} \mid \mathrm{ord}_p(x) \geq 2\} \cup \{0\}$$

Ultima modifica: 12:50