ZAHLENTHEORIE SS 2019 - NOTE 8

We saw last time the following Proposition

Prop: A noetherian domain, not a field.
A is a Dedekind domain $\Longleftrightarrow$ $A_{\mathfrak{p}}$ is a DVR for every nonzero prime $\mathfrak{p}$.

We proved ($\Rightarrow$) and the other direction ($\Leftarrow$) is in the exercises. The important direction is ($\Rightarrow$) in any case.

Another result that we are going to need from the exercises is:

Thm: [CHINESE REMAINDER THEOREM]
A ring. Two ideals $I, J \subseteq A$ are coprime if $I+J=A$.
Let $I_1, I_2, \dots, I_n$ be ideals, pairwise coprime. Then
(1) $I_1 \cap \dots \cap I_n = I_1 \cdot I_2 \cdot \dots \cdot I_n$
(2) The natural map
$$A/I_1 \cdot \dots \cdot I_n \to A/I_1 \times \dots \times A/I_n$$
is an isomorphism.

proof: we prove it in the case of two ideals, the general proof is in the exercises. Since $I_1 + I_2 = A$, there are $x_1 \in I_1$, $x_2 \in I_2$ s.t. $x_1 + x_2 = 1$.
Now we prove the two points:

(1) $I_1 \cdot I_2 \subseteq I_1 \cap I_2$ is always true.

For the converse, let $z \in I_1 \cap I_2$. Then

$$z = z \cdot 1 = z(x_1 + x_2) = \underset{\underset{I_1 I_2}{\Uparrow}}{zx_1} + \underset{\underset{I_1 I_2}{\Uparrow}}{zx_2} \in I_1 I_2$$

(2) Consider the natural map of rings

$$A \longrightarrow A/_{I_1} \times A/_{I_2}$$
$$a \longmapsto (a + I_1, a + I_2)$$

- We prove it is surjective: it is enough to prove that $(1,0)$, $(0,1)$ are in the image.

For $(1,0)$ consider x_2:

$$x_2 \in I_2 \Rightarrow x_2 + I_2 = 0 + I_2$$
$$x_2 + x_1 = 1 \Rightarrow x_2 + I_1 = 1 + I_1$$

Symmetric for $(0,1)$.

- The kernel of the map is $I_1 \cap I_2 = I_1 \cdot I_2$ by definition

hence we get $A/_{I_1 I_2} \xrightarrow{\sim} A/_{I_1} \times A/_{I_2}$ □

Thm: UNIQUE FACTORIZATION of IDEALS in DEDEKIND DOMAIN

A Dedekind domain, $I \subseteq A$ nonzero ideal.

Then

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

for certain distinct primes $\mathfrak{p}_i \subseteq A$ and $n_i > 0$.

Moreover, this factorization is unique.

proof: EXISTENCE of FACTORIZATION

: since A is noetherian, I contains a product of nonzero prime ideals: $I \supseteq q_1^{m_1}\cdots q_r^{m_r}$.

Hence I corresponds to an ideal in $A/q_1^{m_1}\cdots q^{m_r}$.

We observe that the ideals $q_1^{m_1},\dots,q_r^{m_r}$ are coprime: indeed, since A is a Dedekind domain, the ideals $q_1,\dots,q_s$ are maximal, and if q_i, q_j are distinct, q_i+q_j is an ideal that is strictly bigger than q_i, q_j. Since these are maximal, it follows that $q_i+q_j = A$.

Exercise: show that this implies $q_i^{m_i}+q_j^{m_j} = A$ as well.

Then, the CRT tells us that

$$A/q_1^{m_1}\cdots q_r^{m_r} \cong A/q_1^{m_1}\times\dots\times A/q_r^{m_r}$$

Hence $I/q_1^{m_1}\cdots q_r^{m_r}$ corresponds to an ideal in $A/q_1^{m_1}\times\dots\times A/q_r^{m_r}$

Exercise: every ideal in a finite product of rings $A_1\times\dots\times A_r$, is a product of ideals $I_1\times\dots\times I_r$.

So we consider ideals in $A/q_1^{m_1}$:

Lemma: The ideals in $A/\ {}^{m_1}$ ... all of the

Lemma: the ideals in $A/q_i^{m_i}$ are all of the form $q_i^{n_i}/q_i^{m_i}$ for $0 \leq n_i \leq m_i$.

Suppose that the Lemma is true: then we see that

$$I/q_1^{m_1} \cdots q_r^{m_r} \cong q_1^{n_1}/q_1^{m_1} \times \cdots \times q_r^{n_r}/q_r^{m_r}$$
$$\cong$$
$$q_1^{n_1} \cdot q_2^{n_2} \cdots q_r^{n_r} / q_1^{m_1} \cdots q_r^{m_r}$$

Hence

$$I = q_1^{n_1} \cdots q_r^{n_r}$$

and we can leave out the q_i s.t. $n_i = 0$, because then $q_i^{n_i} = A$.

Now we prove the Lemma:

<u>proof of Lemma</u>: in general, let A be a Dedekind domain and $q \subseteq A$ a nonzero prime. Then A/q^m is a local ring with unique maximal ideal q/q^m. Then

$$A/q^m \underset{\substack{\uparrow \\ \text{localization} \\ \text{at a maximal} \\ \text{ideal in a local} \\ \text{ring is an iso}}}{\cong} \left(A/q^m\right)_{q/q^m} \underset{\substack{\uparrow \\ \text{properties of localization} \\ (A/I)_p \cong A_p/I_p}}{\cong} A_q/(q_q)^m$$

But A_q is a DVR, because A is Dedekind, hence all the ideals are of the form q_q^n, and $q_q^n \supseteq q_q^m$ iff $0 \leq n \leq m$. $\square$

UNIQUENESS of FACTORIZATION: now we prove that factorization is unique. So, suppose that $I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}, n_i > 0$.
Now, let $q \subseteq A$ be any nonzero prime. We look at the localization I_q in A_q. We have

$$I_q = (\mathfrak{p}_{1q})^{n_1} \cdots (\mathfrak{p}_{s_q})^{n_s}$$

Moreover, we know that

$$\mathfrak{p}_{i_q} \neq A_q \Leftrightarrow \mathfrak{p}_i \subseteq q \Leftrightarrow \mathfrak{p}_i = q$$

Hence, we see that

$$I_q = A_q \quad \text{if } q \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$$

$$I_{\mathfrak{p}_i} = \mathfrak{p}_{i\mathfrak{p}_i}^{n_i}$$

Hence, the primes appearing in the decomposition of I are

$$\{\mathfrak{p}_1, \dots, \mathfrak{p}_s\} = \{q \mid I_q \neq A_q\}$$

so they are uniquely determined by I.
Moreover, the exponents are also uniquely determined by I, because they are determined by $I_{\mathfrak{p}_i}$. □

<u>Remark</u>: let $I \subseteq A$ be a nonzero ideal. Then, for every nonzero prime $\mathfrak{p} \subseteq A$ the ideal $I_\mathfrak{p}$ is of the form $I_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^{e_\mathfrak{p}(I)}$, for an uniquely determined exponent $e_\mathfrak{p}(I)$.
Then, we can write the unique factorization as

$$I = \prod_{\mathfrak{p} \subseteq A} \mathfrak{p}^{e_\mathfrak{p}(I)}$$

$\mathfrak{p}\neq(0)$

where $e_{\mathfrak{p}}(I)=0$ for all $\mathfrak{p}$ but finitely many.

Now, we prove that the rings of integers of a number field are Dedekind domains.

Lemma: Let $A\subseteq B$ be rings and $\mathfrak{p}\subseteq B$ a prime ideal. Then $\mathfrak{p}\cap A$ is a prime ideal in A.

proof: easy exercise □

Lemma: Let K be a number field and $\mathcal{O}_K$ the ring of integers. If $\mathfrak{p}\subseteq\mathcal{O}_K$ is a nonzero prime then $\mathbb{Z}\cap\mathfrak{p}$ is a nonzero prime.

proof: Let $\alpha\in\mathfrak{p}$, $\alpha\neq0$ and let $m_\alpha(x)$ be the minimal polynomial of α over $\mathbb{Q}$.

$$\alpha^n+a_{n-1}\alpha^{n-1}+\dots+a_1\alpha+a_0=0$$

Then we know that the $a_i\in\mathbb{Z}$, because α is integral over $\mathbb{Z}$. Moreover, $a_0\neq0$, because

$$a_0=(-1)^n N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)\neq0.$$

Hence, we see that

$$\mathbb{Z}\ni a_0=\underbrace{-\alpha^n-a_{n-1}\alpha^{n-1}-\dots-a_1\alpha}_{\in\mathfrak{p}}$$

Hence $a_0\in\mathbb{Z}\cap\mathfrak{p}$ and $a_0\neq0$. □

Rmk: The same proof shows the following: A = integrally closed domain, $F = \mathrm{Frac}\, A$, K/F finite extension, R = integral closure of A in K. If $\mathfrak{p} \subseteq R$ is a nonzero prime, then $\mathfrak{p} \cap A$ is a nonzero prime.

Lemma: Let $k \subseteq A$ be a finite extension of rings where k = field, A = domain. Then A is a field as well.

proof: Let $\alpha \in A$, $\alpha \neq 0$. Then the multiplication map $\cdot\alpha : \underset{a \mapsto \alpha x}{A \to A}$ is a k-linear map which is injective, since A is a domain. Since A is a finite-dimensional vector space, it is also surjective. Hence there is $x \in A$ s.t. $\alpha x = 1$. □

Prop: Let K be a number field and $\mathcal{O}_K$ a number ring. Then $\mathcal{O}_K$ is a Dedekind domain.

proof: We know already that $\mathcal{O}_K$ is noetherian and that it is integrally closed. We need to prove that it has dimaension one: this means two things

- every nonzero prime is maximal: Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a nonzero prime. Then $\mathfrak{p} \cap \mathbb{Z}$ is a nonzero prime

Consider the diagram

Consider the diagram

$$\begin{tikzcd} \mathcal{O}_K \arrow[r] & \mathcal{O}_K/\mathfrak{p} \\ \mathbb{Z} \arrow[u, hook] \arrow[r] & \mathbb{Z}/\mathfrak{p}\cap\mathbb{Z} \arrow[u, hook] \end{tikzcd}$$

Since $\mathcal{O}_K$ is finite over $\mathbb{Z}$, $\mathcal{O}_K/\mathfrak{p}$ is finite over $\mathbb{Z}/\mathfrak{p}\cap\mathbb{Z}$: if $x_1, \dots, x_n$ are generators of $\mathcal{O}_K$ over $\mathbb{Z}$ then $\bar{x}_1, \dots, \bar{x}_n$ are generators of $\mathcal{O}_K/\mathfrak{p}$ over $\mathbb{Z}/\mathfrak{p}\cap\mathbb{Z}$. Now we observe that $\mathfrak{p}\cap\mathbb{Z}$ is nonzero, hence maximal. So $\mathcal{O}_K/\mathfrak{p}$ is a finite extension of $\mathbb{Z}/\mathfrak{p}\cap\mathbb{Z}$, which is a field. Since $\mathcal{O}_K/\mathfrak{p}$ is a domain, it must be a field by the previous lemma. So, $\mathfrak{p}$ is maximal.

- <u>$\mathcal{O}_K$ is not a field</u> (so that there is a nonzero prime): If $\mathcal{O}_K$ is a field, then $\mathcal{O}_K \supseteq \mathbb{Q}$, because $\mathcal{O}_K \supseteq \mathbb{Z}$. But then every element of $\mathbb{Q}$ would be integral over $\mathbb{Z}$, which is absurd because $\mathbb{Z}$ is integrally closed. □

<u>Rmk</u>: With the same proof one shows the following:
A = Dedekind domain, $F = \mathrm{Frac}\, A$
K/F = finite extension, R = integral closure of A in K.
Then R is a Dedekind domain.

<u>Cor</u>: Let K be a number field. Then every nonzero ideal $I \subseteq \mathcal{O}_K$ factors uniquely as a product of nonzero prime ideals: $I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$.

<u>Example</u>: The ring of integers of $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}[\sqrt{-5}]$. Here we know that we have two different factorizations

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

However, if we look at the <u>ideal</u> generated by 6 in $\mathbb{Z}[\sqrt{-5})$ we see that we get

$$(6) = (2)(3)$$
$$(6) = (1+\sqrt{-5})(1-\sqrt{-5})$$

Let's look at the unique factorization of (6) into primes. We claim that this is

$$(2) = (2, 1+\sqrt{-5})^2$$
$$(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$
$$(1+\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$$
$$(1-\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$

First we check that those identities are true:

- $(2, 1+\sqrt{-5})^2 = (4, 2(1+\sqrt{-5}), 1+2\sqrt{-5}-5)$
$= (4, 2+2\sqrt{-5}, -4+2\sqrt{-5})$
$= (4, 2+2\sqrt{-5}, 2\sqrt{5})$
$= (4, 2, 2\sqrt{-5}) = (2)$

- $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (9, 3-3\sqrt{5}, 3+3\sqrt{-5}, 6)$

$$= (3)$$

because $\supseteq$ containment is always true as $3 = 9-6$.

- $(2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, 6)$
$$= (6, 1+\sqrt{-5}) = (1+\sqrt{-5})$$

because
$$1+\sqrt{-5} = 3+3\sqrt{-5} - (2+2\sqrt{-5})).$$

- $(2, 1+\sqrt{-5})(3, 1-\sqrt{-5})$ is analogous.

Now we need to prove that
$$(2, 1+\sqrt{-5}), (3, 1+\sqrt{-5}), (3, 1-\sqrt{-5})$$
are primes in $\mathbb{Z}[\sqrt{-5}]$.

- $(2, 1+\sqrt{-5})$: we have $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[x]/(x^2+5)$

hence $\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) \cong \mathbb{Z}[x]/(x^2+5, 2, 1+x)$

$$\cong \mathbb{F}_2[x]/(x^2+5, x+1)$$

$$x^2+5 = \\ = x^2+1 = (x+1)^2$$

$$\cong \mathbb{F}_2[x]/(x+1) \cong \mathbb{F}_2$$

- $(3, 1+\sqrt{-5})$: $\mathbb{Z}[\sqrt{-5}]/(3, 1+\sqrt{-5}) \cong \mathbb{Z}[x]/(x^2+5, 3, 1+x)$

$$\cong \mathbb{F}_3[x]/(x^2+5, x+1)$$

We see that $(-1)^2+5 = 6 = 0$ in $\mathbb{F}_3$, hence $x+1$ divides x^2+5, so $(x^2+5, x+1) = (x+1)$

$$\mathbb{F}_3[x]/(x+1) \simeq \mathbb{F}_3$$

- analogous.

So the unique factorization of (6) into primes is:

$$(6) = (2, 1+\sqrt{-5})^2 (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

Some more remarks on unique factorization

Cor: $I, J \subseteq A$ nonzero ideals.

$I \subseteq J \iff I_{\mathfrak{p}} \subseteq J_{\mathfrak{p}}$ for all nonzero primes $\mathfrak{p} \subseteq A$

In particular

$I = J \iff I_{\mathfrak{p}} = J_{\mathfrak{p}}$ " " "

proof: $\boxed{\Rightarrow}$ is clear

$\boxed{\Leftarrow}$ Let $I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$ be the unique factorization of I. Let $J \supseteq I$ and suppose $\mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, then

$$A_{\mathfrak{q}} = I_{\mathfrak{q}} \subseteq J_{\mathfrak{q}}$$

hence $J_{\mathfrak{q}} = A_{\mathfrak{q}}$. So, the primes appearing in the unique factorization of J are amongst the $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$.

$$J = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_s^{m_s}$$

Now we have

$I \subseteq J \Rightarrow \mathfrak{p}_i^{n_i} \subseteq \mathfrak{p}_i^{m_i} \Rightarrow 0 \leq m_i \leq n_i$

$I_{\mathfrak{p}_i} = J_{\mathfrak{p}_i} \Rightarrow n_i = m_i \Rightarrow$ [illegible]
hence $J \supseteq I$. $\square$

Moreover, in a Dedekind domain every ideal can be generated by two elements

__Cor__: A = Dedekind domain, $I \subseteq J \subseteq A$ nonzero ideals. Then $J = I + (a)$ for a certain $a \in J$.

__proof__: it is enough to prove that every ideal in A/I is principal. Suppose $I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$. Then

$$A/I \cong A/\mathfrak{p}_1^{n_1} \times \cdots \times A/\mathfrak{p}_s^{n_s}$$

hence it is enough to prove that every ideal in $A/\mathfrak{p}_i^{n_i}$ is principal. However, we saw already that

$$A/\mathfrak{p}_i^{n_i} \cong A_{\mathfrak{p}_i} / \mathfrak{p}_i^{n_i}$$

and $A_{\mathfrak{p}_i}$ is a DVR, so every ideal is principal. $\square$

__Cor__ Let A be a Dedekind domain. Then every ideal is generated by at most two elements

__proof__: if $I \subseteq A$ is zero, clear.
if $I \neq 0$, then take $a \in I$, $a \neq 0$ and apply previous corollary. $\square$

Ultima modifica: 15:08