ZAHLENTHEORIE NOTE 11

- <u>IDEAL CLASS GROUP</u>

Let A be a Dedekind domain. If we have two nonzero ideals I, J, we can multiply them to get a nonzero ideal IJ. Moreover we have a "neutral" element, given by the trivial ideal A: $I \cdot A = I$.

In a Dedekind domain, there is a way to extend these operations into group operations.

<u>def</u>: FRACTIONAL IDEAL Let $F = \mathrm{Frac}\, A$.
A fractional ideal is a finitely generated A-submodule $M \subseteq F$, $M \neq (0)$.

<u>Rmk</u>: Let $M \subseteq F$ be an A-submodule. Then
M is f.g. $\iff \exists\, d \in A$ s.t. $dM \subseteq A$
Hence $I = dM$ is an ideal in A and $M = \frac{1}{d} I$ which justifies the name "fractional ideal".

<u>proof</u>: $(\Rightarrow)$ $M = \langle \frac{a_1}{d_1}, \dots, \frac{a_n}{d_n} \rangle$, $d = d_1 \cdots d_n$
$(\Leftarrow)$ A is noetherian hence dM is finitely generated: $dM = \langle a_1, \dots, a_n \rangle$. Then
$M = \langle \frac{a_1}{d}, \dots, \frac{a_n}{d} \rangle$. $\square$

If $I, J \subseteq F$ are two fractional ideal then we can define their product as for usual ideals

$$IJ = \langle a_i b_i \mid a_i \in I, b_i \in J \rangle$$

and this is again a fractional ideal.

<u>Example</u>: Let A be a DVR with maximal ideal $m = (t)$ and $F = \mathrm{Frac}\, A$. Then we claim that every fractional ideal is of the form

$$I = (t^k), \quad k \in \mathbb{Z} \qquad \left(\begin{array}{c} A\text{-submodule} \\ \text{of } F \text{ generated} \\ \text{by } t^k \end{array}\right)$$

and these are all distinct, with

$$(t^k) \subseteq (t^h) \iff k \geq h$$

<u>proof</u>: Let $I \subseteq F$ be a fractional ideal. Then we have seen that there is $d \in A$ s.t. $dI \subseteq A$.

We can write $d = u \cdot t^a$ for $u \in A^*$, $a \geq 0$ and $dI = (t^b)$. Hence $I = \frac{1}{d}(dI) = u^{-1}(t^{b-a}) = (t^{b-a})$. Now

$$\begin{aligned}
(t^k) \subseteq (t^h) &\iff t^k \in (t^h) \\
&\iff t^k = a \cdot t^h \text{ for } a \in A \\
&\iff t^k = u \cdot t^{h+e} \text{ for } u \in A^*, e \geq 0 \\
&\iff \exists\, e \geq 0 \text{ s.t. } t^{k-h-e} = u \in A^* \\
&\iff \exists\, e \geq 0 \text{ s.t. } k-h-e = 0 \iff k \geq h. \quad \square
\end{aligned}$$

<u>Remark</u>: Fractional ideals behave well w.r.t. localization. Indeed, let A = Dedekind domain, $\mathfrak{p} \subseteq A$ maximal prime

$I \subseteq F$ fractional ideal. Then $I_{\mathfrak{p}} = \{ \frac{a}{s} \mid a \in I, s \in A \setminus \mathfrak{p} \}$ is a fractional ideal of $A_{\mathfrak{p}}$ and if J is another fractional ideal, then $(I \cdot J)_{\mathfrak{p}} = I_{\mathfrak{p}} J_{\mathfrak{p}}$.

<u>Lemma</u>: Let $I \subseteq A$ be a nonzero ideal and let

$$I^* = \{ a \in F \mid aI \subseteq A \}$$

Then I^* is a fractional ideal and $II^* = A$.

<u>proof</u>: Let $d \in I$, $d \neq 0$. Then $dI^* \subseteq A$ so that I^* is a fractional ideal.

We prove that $II^* = A$: by definition $II^* \subseteq A$ so II^* is an ideal in A and it is enough to show $(II^*)_{\mathfrak{p}} = A_{\mathfrak{p}}$ for every nonzero prime $\mathfrak{p} \subseteq A$.

We see that $(II^*)_{\mathfrak{p}} = I_{\mathfrak{p}} \cdot (I^*)_{\mathfrak{p}}$ and moreover it is easy to see (do it!) that

$$(I^*)_{\mathfrak{p}} = (I_{\mathfrak{p}})^* = \{ a \in F \mid a I_{\mathfrak{p}} \subseteq A_{\mathfrak{p}} \}$$

Now, since $A_{\mathfrak{p}}$ is a DVR, we know that $I_{\mathfrak{p}} = (t^k)$ where $\mathfrak{p}_{\mathfrak{p}} = (t)$ and $k \geq 0$. Then

$$(I_{\mathfrak{p}})^* = \left\{ ut^h \;\middle|\; \begin{matrix} u \in A_{\mathfrak{p}}^* \\ h \in \mathbb{Z} \end{matrix} \text{ s.t. } ut^h I_{\mathfrak{p}} \subseteq A_{\mathfrak{p}} \right\}$$

$$= \{ ut^h \mid ut^h t^k \in A_{\mathfrak{p}} \}$$

$$= \{ ut^h \mid ut^{h+k} \in A_{\mathfrak{p}} \}$$

$$= \{ ut^h \mid h+k \geq 0 \} = \{ ut^h \mid h \geq -k \}$$

$$= \{ ut^e t^{-k} \mid e \geq 0 \} = (t^{-k})$$

and $(t^k)(t^{-k}) = (1) = A$. $\square$

<u>Thm</u>: The set $\mathcal{D}(A)$ of fractional ideals is a group under the product of ideals. Moreover every fractional ideal can be written uniquely as

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

$\mathfrak{p}_i \subseteq A$ nonzero prime, $e_i \in \mathbb{Z}$. Hence

$$\mathcal{D}(A) \cong \bigoplus_{\mathfrak{p} \subseteq A} \mathbb{Z} \cdot \mathfrak{p}.$$

<u>proof</u>: we need to prove the existence of inverses. Let $J \subseteq F$ be a fractional ideal. Then $J = \frac{1}{d} I$ for a nonzero ideal $I \subseteq A$. Then

$$J(dI^{-1}) = \frac{1}{d} I \cdot d I^{-1} = \frac{1}{d} d \cdot I I^{-1} = 1 \cdot A = A.$$

For the second part, we can write

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$
$$(d) = \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_s^{b_s}$$

So

$$J = \frac{1}{d} I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \mathfrak{q}_1^{-b_1} \cdots \mathfrak{q}_s^{-b_s}.$$

every fractional ideal is of the desired form. The uniqueness follows from the uniqueness of the factorization in A.

A distinguished subgroup of $\mathcal{J}(A)$ is the one

formed by PRINCIPAL FRACTIONAL IDEALS

$$\mathcal{P}(A) = \{ (x) \mid x \in F, x \neq 0 \}$$

<u>def</u>: IDEAL CLASS GROUP

The ideal class group of A is defined as

$$Cl(A) \overset{def}{=} \mathcal{D}(A) / \mathcal{P}(A).$$

The ideal class group is a central object of algebraic number theory. For example we have

<u>Rmk</u>: The following are equivalent

(1) A is an UFD

(2) A is a PID

(3) $Cl(A) = 0$.

<u>proof</u>: (1) $\Leftrightarrow$ (2) is in the exercises.

(2) $\Leftrightarrow$ (3) is by definition of $Cl(A)$.

- <u>NORMS of IDEALS</u>

We are in our usual situation:

A = Dedekind domain	(e.g. $A = \mathbb{Z}$)
F = Frac A	(e.g. $F = \mathbb{Q}$)
K = finite field extension of F	(e.g. K = number field)
R = integral closure of A in K	(e.g. $R = \mathcal{O}_K$)

We want to define a homomorphism

$$\mathcal{N}_{K/F} : \mathcal{D}(R) \to \mathcal{D}(A)$$
$$I \longmapsto \mathcal{N}_{K/F}(I)$$

such that for every principal fractional ideal we have

$$\mathcal{N}_{K/F}((x)) = (N_{K/F}(x))$$

Since $\mathcal{D}(R)$ is freely generated by the prime ideals, it is enough to define this on the prime ideals:

<u>def</u>: IDEAL NORM

We define an homomorphism

$$\mathcal{N}_{K/F} : \mathcal{D}(R) \to \mathcal{D}(A)$$

by

$$\mathcal{N}_{K/F}(P) = (P \cap A)^{f_P(P \cap A)}$$

for every nonzero prime $P \subseteq R$.

Now we prove that this satisfies the required properties

<u>Prop</u>: (1) Suppose $F \subseteq K \subseteq L$ are finite field extensions and let $A \subseteq R \subseteq S$ be the integral closures of A in F, K, L respectively. Then

$$\mathcal{N}_{L/F}(I) = \mathcal{N}_{K/F}(\mathcal{N}_{L/K}(I))$$

for every $I \in \mathcal{D}(S)$.

(2) If $I \subseteq A$ is a nonzero ideal, then

$$\mathcal{N}_{K/F}(I \cdot R) = I^{[K:F]}$$

(3) Suppose K/F is Galois, let $I \subseteq R$ be a nonzero ideal. Then

$$\mathcal{N}_{K/F}(I) \cdot R = \prod_{\sigma \in Gal(K/F)} \sigma(I)$$

(4) Let $x \in K, x \neq 0$. Then

$$\mathcal{N}_{K/F}((x)) = (N_{K/F}(x))$$

<u>proof</u>: (1) It is enough to prove this when $Q \subseteq S$ is a nonzero prime; let $P = Q \cap R$, $\mathfrak{p} = Q \cap A = P \cap A$.

Then we know that the inertia degree is multiplicative from one exercise:

$$f_Q(\mathfrak{p}) = f_Q(P) \cdot f_P(\mathfrak{p})$$

So

$$\begin{aligned}
\mathcal{N}_{L/F}(Q) &= \mathfrak{p}^{f_Q(\mathfrak{p})} = \mathfrak{p}^{f_Q(P) \cdot f_P(\mathfrak{p})} \\
&= (\mathcal{N}_{K/F}(P))^{f_Q(P)} \\
&= \mathcal{N}_{K/F}(P^{f_Q(P)}) \\
&= \mathcal{N}_{K/F}(\mathcal{N}_{L/K}(Q)).
\end{aligned}$$

(2) It is enough to prove this when $I = \mathfrak{p} \subseteq A$

is a nonzero prime ideal: we have

$\mathfrak{p}R = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ with $f_i = f_{\mathfrak{P}_i}(\mathfrak{p})$

Then

$$N_{K/F}(\mathfrak{p}R) = \prod_{i=1}^{r} N_{K/F}(\mathfrak{P}_i)^{e_i} =$$

$$= \prod_{i=1}^{r} \mathfrak{p}^{f_i e_i} = \mathfrak{p}^{\sum f_i e_i} = \mathfrak{p}^{[K:F]}$$

It is enough to prove this when $\mathfrak{P} = \mathfrak{P}$ is prime

(3) Let $\mathfrak{P} \subseteq R$ be a nonzero prime and $\mathfrak{p} = \mathfrak{P} \cap A$.

Then we know that $\mathfrak{p}R = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$

and the inertia degree is f for each $\mathfrak{P}_i$. Hence

$N_{K/F}(\mathfrak{P}) = \mathfrak{p}^f$ so that

$$N_{K/F}(\mathfrak{P}) \cdot R = \mathfrak{p}^f \cdot R = (\mathfrak{p}R)^f$$

$$= (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^{ef} = \prod_{\sigma \in Gal(K/F)} \sigma(\mathfrak{P})$$

where the last equality follows from the fact that $Gal(K/F)$ acts transitively on $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$

(4) First we observe that we have a homomorphism of rings

$$\mathcal{D}(A) \longrightarrow \mathcal{D}(R)$$

$$\mathfrak{p} \longmapsto \mathfrak{p}R$$

and you can check that this is injective, because if $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, then $\mathfrak{p} = \mathfrak{P}_i \cap A$.

Now we go back to our problem: it is enough to prove it for $\alpha \in R$.

- Suppose first that K/F is galois. It is enough to show that $N_{K/F}((\alpha))\cdot R = N_{K/F}(\alpha)\cdot R$.

However we know

$$N_{K/F}((\alpha))\cdot R = \prod_{\sigma\in Gal}(\sigma(\alpha))$$

$$N_{K/F}(\alpha) = \prod_{\sigma\in Gal(K/F)}\sigma(\alpha)$$

- In general, let $L \supseteq K \supseteq F$ be a finite extension with L/F Galois and let S be the integral closure of A in L. Then we know that

$$N_{L/F}(\alpha S) = N_{L/F}(\alpha)\cdot A$$

Moreover we also know that

$$\cdot\ N_{L/F}(\alpha S) = N_{K/F}(N_{L/K}(\alpha S))$$
$$= N_{K/F}((\alpha R)^{[L:K]})$$
$$= N_{K/F}(\alpha R)^{[L:K]}$$

$$\cdot\ N_{L/F}(\alpha) = N_{K/F}(N_{L/K}(\alpha)) = N_{K/F}(\alpha^{[L:K]})$$
$$= N_{K/F}(\alpha)^{[L:K]}$$

Hence we get

$$N_{K/F}(\alpha R)^{[L:K]} = (N_{K/F}(\alpha)\cdot A)^{[L:K]}$$

Since the group $\mathcal{D}(A)$ is torsion-free, it follows that $N_{K/F}(\alpha R) = N_{K/F}(\alpha)\cdot A$. $\square$

In the case of number fields, this norm can be computed as follows

def: NUMERICAL NORM

Let K be a number field and $I \subseteq \mathcal{O}_K$ a nonzero ideal. The numerical norm of I is defined as

$$\|I\| \overset{\text{def}}{:=} \left| \mathcal{O}_K / I \right|$$

Prop: The norm $\|I\|$ is well-defined, meaning that $\mathcal{O}_K/I$ is finite. Moreover

$$N_{K/\mathbb{Q}}(I) = (\|I\|)$$

In particular

$$\|I \cdot J\| = \|I\| \cdot \|J\|$$

proof: suppose $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Then

$$\mathcal{O}_K/I \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}$$

and

$$N_{K/\mathbb{Q}}(I) = \prod N_{K/\mathbb{Q}}(\mathfrak{p}_i^{e_i})$$

so it is enough to prove the statement when $I = \mathfrak{p}^e$ is the power of a nonzero prime. Let $(p) = \mathfrak{p} \cap \mathbb{Z}$. Then we have seen that $\mathcal{O}_K/\mathfrak{p}^e$ is a finite extension of $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, so that $\mathcal{O}_K/\mathfrak{p}^e$ is also finite. Moreover

$$N_{K/\mathbb{Q}}(\mathfrak{p}^e) = (p)^{e \cdot f} \text{ where } f = f_{\mathfrak{p}}(p)$$

and we proved last time that

$\dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^e) = ef$, hence

$$|\mathcal{O}_K/\mathfrak{p}^e| = p^{ef}. \qquad \square$$

Ultima modifica: 29 mag 2019