ZAHLENTHEORIE SS 2019 - NOTE 9

Today we look at the behaviour of prime ideals under extensions of Dedekind domains.
Our setting will be always the following

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

Let $\mathfrak{p} \subseteq A$ be a nonzero prime, and let $\mathfrak{p}R$ be the ideal generated by $\mathfrak{p}$ in R. Then, let

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

be the unique factorization of $\mathfrak{p}R$ in R.

In this case, we say that $\mathfrak{P}_i$ LIES ABOVE $\mathfrak{p}$ or $\mathfrak{p}$ LIES BELOW $\mathfrak{P}_i$. This is justified by the following picture

$$\begin{tikzcd}
\mathfrak{P}_1^{e_1} \\ \mathfrak{P}_r^{e_r} & R \arrow[r, dash] \arrow[d, dash] & K \arrow[d, dash] \\
\mathfrak{p} & A \arrow[r, dash] & F
\end{tikzcd}$$

We make a couple of remarks

Rmk: (1) If $\mathfrak{p}_i$ lies above $\mathfrak{p}$, then

$$\mathfrak{p}_i \cap A = \mathfrak{p}$$

proof: we know that $\mathfrak{p}_i \supseteq \mathfrak{p}$ so that $\mathfrak{p}_i \cap A \supseteq \mathfrak{p}$. Moreover, we know that $\mathfrak{p}_i \cap A$ is a prime ideal, and since $\mathfrak{p}$ is maximal it must be $\mathfrak{p}_i \cap A = \mathfrak{p}$. $\square$

(2) If $\mathfrak{p}_i$ lies above $\mathfrak{p}$, then

$R/\mathfrak{p}_i$ is an extension of $A/\mathfrak{p}$

proof: the ring extension $A \hookrightarrow R$ induces an extension $A/\mathfrak{p} \hookrightarrow R/\mathfrak{p}_i$, since $\mathfrak{p} \subseteq \mathfrak{p}_i$. $\square$

def: RAMIFICATION INDEX and INERTIA DEGREE

Let $\mathfrak{p}R = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Then we define the

RAMIFICATION INDEX : $e_{\mathfrak{p}_i}(\mathfrak{p}) = e_i$

INERTIA DEGREE : $f_{\mathfrak{p}_i}(\mathfrak{p}) = f_i = [R/\mathfrak{p}_i : A/\mathfrak{p}]$

def: PRIMES that RAMIFY

We say that a prime $\mathfrak{p} \subseteq A$ RAMIFIES in R if $\mathfrak{p}R = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and one of the e_i is ≥ 2.

__Prop__: In the situation

A = Dedekind domain

F = Frac A

K = finite field extension of F

R = integral closure of A in R

Let $\mathfrak{p} \subseteq A$ be a nonzero prime and

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

its unique factorization in R. Then

$$\sum_{i=1}^{r} e_i f_i = \sum_{i=1}^{r} e_{\mathfrak{p}_i}(\mathfrak{p}) f_{\mathfrak{p}_i}(\mathfrak{p}) = [K:F]$$

In particular, it is independent of $\mathfrak{p}$.

proof: First we observe that the inclusion $A \hookrightarrow R$ induces an extension of rings $A/\mathfrak{p} \to R/\mathfrak{p}R$. Since $A/\mathfrak{p}$ is a field this means that $R/\mathfrak{p}R$ is a $A/\mathfrak{p}$-vector space, of finite dimension, since we know that R is finitely generated as an A-module.

Then we claim that

$$\sum_{i=1}^{r} e_i f_i = \dim_{A/\mathfrak{p}}\left(R/\mathfrak{p}R\right) = [K:F]$$

We prove both equalities:

$\dim_{A/\mathfrak{p}}(R/\mathfrak{p}R) = [K:F]$ [Only when]

• $\underline{\dim_{A/p}(R/pR) = [K:F]}$ $[A = \mathbb{Z}]$

Let $n = [K:F]$. Then we know that $R \cong A^{\oplus n}$ as an A-module. Then we get that

$$R/pR \cong A^{\oplus n}/p(A^{\oplus n}) \cong A^{\oplus n}/(pA)^{\oplus n}$$

$$\cong (A/pA)^{\oplus n}, \text{ hence}$$

(because $A = \mathbb{Z}$)

$\dim_{A/p}(R/pR) = n$.

• $\underline{\sum_{i=1}^{r} e_i f_i = \dim_{A/p}(R/pR)}$

We see that

$$R/pR = R/p_1^{e_1} \cdots p_r^{e_r} \overset{CRT}{\cong} R/p_1^{e_1} \times \cdots \times R/p_r^{e_r}$$

Moreover, we observe that we have a ring extension $A/p \hookrightarrow R/p_i^{e_i}$, since $p \subseteq p_i^{e_i}$ so that each $R/p_i^{e_i}$ is an A/p-vector space, and the above isomorphism is an isomorphism of A/p-vector spaces. Hence

$$\dim_{A/p}(R/pR) = \sum_{i=1}^{r} \dim_{A/p}(R/p_i^{e_i})$$

So it is enough to prove that $\dim_{A/p}(R/p_i^{e_i}) = e_i f_i$

To do so, observe that we have a chain of subspaces

$\ldots 2 \quad \ldots \quad \supset p_i^{e_i} \quad \supset$

$$R/\mathfrak{p}_i^{e_i} \supseteq \mathfrak{p}_i/\mathfrak{p}_i^{e_i} \supseteq \mathfrak{p}_i^2/\mathfrak{p}_i^{e_i} \supseteq \dots \supseteq \mathfrak{p}_i^{e_i}/\mathfrak{p}_i^{e_i} = 0$$

This chain has length e_i, and we see that

$$\left(\mathfrak{p}_i^{j}/\mathfrak{p}_i^{e_i}\right) \Big/ \left(\mathfrak{p}_i^{j+1}/\mathfrak{p}_i^{e_i}\right) \cong \mathfrak{p}_i^{j}/\mathfrak{p}_i^{j+1}$$

so it is enough to prove that $\dim_{A/\mathfrak{p}}\left(\mathfrak{p}_i^{j}/\mathfrak{p}_i^{j+1}\right) = f_i$
and by definition of f_i, it is enough to show that

$$\dim_{R/\mathfrak{p}_i}\left(\mathfrak{p}_i^{j}/\mathfrak{p}_i^{j+1}\right) = 1$$

Observe that the $(R/\mathfrak{p}_i)$-subspaces of $\mathfrak{p}_i^{j}/\mathfrak{p}_i^{j+1}$ correspond to the ideals in $\mathfrak{p}_i^{j}$ which contain $\mathfrak{p}_i^{j+1}$. There are only two of these ideals: $\mathfrak{p}_i^{j}$ and $\mathfrak{p}_i^{j+1}$, hence there are only two subspaces, which means

$$\dim_{R/\mathfrak{p}_i}\left(\mathfrak{p}_i^{j}/\mathfrak{p}_i^{j+1}\right) = 1. \qquad \square$$

So this puts some restrictions on the possible values of e_i, f_i. If the field extension is Galois, we have even more restrictions:

Now, suppose that we are in the following situation:

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

we assume that K/F is GALOIS, with Galois group $G = \mathrm{Gal}(K/F)$.

Let $\mathfrak{p} \subseteq A$ be a prime ideal, and let

$$\mathfrak{p}R = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

be its unique factorization.

Observe that $G = \mathrm{Gal}(K/F)$ acts on the set of prime ideals of R by setting

$$\sigma \cdot \mathfrak{q} = \sigma(\mathfrak{q})$$

<u>Prop</u>: In the above situation G acts transitively on the set of primes lying over $\mathfrak{p}$.
In particular, the ramification index and the inertia degree are the same for each $\mathfrak{p}_i$.

<u>proof</u>: First we show that G acts on the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Since $\mathfrak{p} \subseteq R \subseteq F$, $\forall \sigma \in G$ we have

$$\mathfrak{p}R = \sigma(\mathfrak{p}R) = \sigma(\mathfrak{p}_1)^{e_1} \cdots \sigma(\mathfrak{p}_i)^{e_i}$$

$$\mathfrak{p}R = \sigma(\mathfrak{p}R) = \sigma(\mathfrak{p}_1)^{e_1} \cdots \sigma(\mathfrak{p}_i)^{e_i}$$

and by the uniqueness of the factorization we must have that $\sigma(\mathfrak{p}_i)$ is one of the $\mathfrak{p}_1, \dots, \mathfrak{p}_r$.

Now we show that the action is transitive.

Suppose that $\mathfrak{p}_1, \mathfrak{p}_2$ are two distinct primes lying over $\mathfrak{p}$. We need to show that there is $\sigma \in G$ s.t. $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$.

Suppose that $\sigma(\mathfrak{p}_1) \neq \mathfrak{p}_2$ for each $\sigma \in G$.

Then by the CRT there exists $\alpha \in \mathfrak{p}_2$ $\alpha \notin \sigma(\mathfrak{p}_1)$, for each $\sigma \in \mathfrak{p}_i$. Then consider

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

We have $N_{K/F}(\alpha) \in R \cap \mathfrak{p}_2 = \mathfrak{p}$ so $N_{K/F}(\alpha) \in \mathfrak{p}_1$ as well. Since $\mathfrak{p}_1$ is prime, this means that $\sigma(\alpha) \in \mathfrak{p}_1$ for some σ, hence $\alpha \in \sigma^{-1}(\mathfrak{p}_1)$, contradiction.

For the last part, observe that if $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$ then

$$\mathfrak{p}R = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \mathfrak{p}_3^{e_3} \cdots \mathfrak{p}_r^{e_r}$$

$$\begin{aligned} \mathfrak{p}R &= \sigma(\mathfrak{p}R) \\ &= \sigma(\mathfrak{p}_1)^{e_1} \sigma(\mathfrak{p}_2)^{e_2} \cdots \sigma(\mathfrak{p}_r)^{e_r} \\ &= \mathfrak{p}_2^{e_1} \cdot \sigma(\mathfrak{p}_2)^{e_2} \cdots \sigma(\mathfrak{p}_r)^{e_r} \end{aligned}$$

and by uniqueness

$$e_1 = e_2$$

Furthermore, σ induces an isomorphism of $A/\mathfrak{p}$-modules

$$R/\mathfrak{P}_1 \cong R/\sigma(\mathfrak{P}_1) = R/\mathfrak{P}_2$$

hence $\quad f_1 = \dim_{A/\mathfrak{p}} R/\mathfrak{P}_1 = \dim_{A/\mathfrak{p}} R/\mathfrak{P}_2 = f_2$. $\square$

COMPUTING FACTORIZATIONS

We are in the usual situation

A = Dedekind domain

F = Frac A

K = finite field extension of F

R = integral closure of A in K

Example

$A = \mathbb{Z}$

$F = \mathbb{Q}$

K = number field

$R = \mathcal{O}_K$

In this situation we have the following

Prop: Suppose R is generated by a single element: $R = A[\alpha]$ and let $m_\alpha(X) \in A[X]$ be the minimal polynomial. Let $\mathfrak{p} \subseteq A$ be a nonzero prime ideal and let

$$\overline{m}_\alpha(X) = \overline{g}_1(X)^{e_1} \cdots \overline{g}_r(X)^{e_r}$$

be the unique factorization of $m_\alpha(X)$ in $A/\mathfrak{p}A[X]$ for certain $g_1(X), \dots, g_r(X) \in A[X]$. Then

(1) The $\mathfrak{P}_i = \mathfrak{p}R + (g_i(\alpha))$ are prime ideals in R.

(2) The prime factorization of $\mathfrak{p}R$ is

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

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

(3) the ramification indexes and the inertia degrees are

$$e_{\mathfrak{p}_i}(\mathfrak{p}) = e_i$$

$$f_{\mathfrak{p}_i}(\mathfrak{p}) = \text{degree } g_i(x).$$

<u>proof</u>: (1) We have $R \cong A[\alpha] \cong A[X]/(m_\alpha(X))$ hence

$$R/\mathfrak{p}_i \cong A[X]/(\mathfrak{p}, g_i(X), m_\alpha(X))$$

$$\cong (A/\mathfrak{p})[X]/(\bar{g}_i(X), \bar{m}_\alpha(X))$$

$$\cong (A/\mathfrak{p})[X]/(\bar{g}_i(X))$$

which is a field, since $A/\mathfrak{p}$ is a field and $\bar{g}_i(x)$ is irreducible

(2) We see that

$$R/\mathfrak{p}R \cong A[X]/(\mathfrak{p}, m_\alpha(X)) \cong (A/\mathfrak{p})[X]/(\bar{m}_\alpha(X))$$

$$\cong (A/\mathfrak{p})[X]/(\bar{g}_1(x)^{e_1} \cdots \bar{g}_r(x)^{e_r})$$

The prime ideals in this last ring are exactly those generated by $(\bar{g}_1(x)), \dots, (\bar{g}_r(X))$ hence the prime ideals in $R/\mathfrak{p}R$ are exactly those generated by $(g_1(\alpha)), \dots, (g_r(\alpha))$. So, the prime ideals in R which contain $\mathfrak{p}R$ are precisely the $\mathfrak{p}_i = (g_i(\alpha), \mathfrak{p})$. Hence

$$\mathfrak{p}R = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \text{ for certain } a_i > 0.$$

We also know that

$$R/\mathfrak{p}R \cong R/\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

and then we conclude thanks to the following Lemma

<u>Lemma</u>: R = Dedekind domain, $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ unique factorization of a nonzero ideal I, and suppose

$$R/I \cong R/\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

then $a_i = e_i$

<u>proof</u>: we look at the localization:

$$\begin{array}{ccccc} (R/I)_{\mathfrak{p}_i/I} & \cong & R_{\mathfrak{p}_i}/I_{\mathfrak{p}_i} & \cong & R_{\mathfrak{p}_i}/\mathfrak{p}_i^{a_i} \\ \wr\wr & & & & \\ (R/\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r})_{\mathfrak{p}_i/\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}} & \cong & R_{\mathfrak{p}_i}/\mathfrak{p}_i^{e_i} & & \end{array}$$

Hence $R_{\mathfrak{p}_i}/(\mathfrak{p}_i)_{\mathfrak{p}_i}^{a_i} \cong R_{\mathfrak{p}_i}/(\mathfrak{p}_i)_{\mathfrak{p}_i}^{e_i}$. Now, since they are isomorphic, they have the same number of ideals and since $R_{\mathfrak{p}_i}$ is a DVR, the ideals on the left hand side are

$$R_{\mathfrak{p}_i}/(\mathfrak{p}_i)^{a_i} \supseteq \mathfrak{p}_{i\mathfrak{p}_i}/\mathfrak{p}_{\mathfrak{p}_i}^{a_i} \supseteq \cdots \supseteq \mathfrak{p}_{i\mathfrak{p}_i}^{a_i}/\mathfrak{p}_{i\mathfrak{p}_i}^{a_i}$$

so there are $a_i + 1$ of them. The same reasoning shows that on the right hand side there are $e_i + 1$

so $a_i = e_i$. $\square$

(3) Since $\mathfrak{p}R = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, it is clear that

$$e_{\mathfrak{P}_i}(\mathfrak{p}) = e_i$$

Moreover, we have

$$f_{\mathfrak{P}_i}(\mathfrak{p}) = f_i = \dim_{A/\mathfrak{p}} R/\mathfrak{P}_i =$$

$$= \dim_{A/\mathfrak{p}} (A/\mathfrak{p})[X]/(\bar{g}_i(x))$$

$$= \text{degree } g_i(X).$$

$\square$

<u>Example</u>: <u>Factorization of 2 in quadratic extensions</u>

We look at the factorization of (2) in ring of integers of the form $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, d sqfr.

- $d \equiv 2, 3 \ (4)$: $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cong \mathbb{Z}[\sqrt{d}]$

  Minimal polynomial $m(X) = X^2 - d$

  We look at the factorization in $\mathbb{Z}/2\mathbb{Z}[X] = \mathbb{F}_2[X]$:

  - $d \equiv 2 \ (4)$: $X^2 - d \equiv X^2$ in $\mathbb{F}_2[X]$, hence

    $$2\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = (2, \sqrt{d})^2$$

    $e_{(2,\sqrt{d})}(2) = 2$ So, 2 ramifies in

    $f_{(2,\sqrt{d})}(2) = 1$ $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$

  - $d \equiv 3 \ (4)$: $X^2 - d \equiv X^2 - 1 \equiv (X+1)^2$

$2\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = (2, \sqrt{d}+1)^2$

$e_{(2,\sqrt{d}+1)}(2) = 2$ 2 ramifies in
$f_{(2,\sqrt{d}+1)}(2) = 1$ $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$

- $d \equiv 1 \ (4)$: $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cong \mathbb{Z}[\alpha]$, $\alpha = \frac{1+\sqrt{d}}{2}$

minimal polynomial $m(X) = X^2 - X + \frac{1-d}{4}$
We look at the factorization in $\mathbb{F}_2[X]$
- $d \equiv 1 \ (8)$: $X^2 - X + \frac{1-d}{4} \equiv X^2 - X = (X-1)X$

$$2\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = (2, \alpha)\cdot(2, \alpha-1)$$

$e_{(2,\alpha)}(2) = 1$ $e_{(2,\alpha-1)}(2) = 1$
$f_{(2,\alpha)}(2) = 1$ $f_{(2,\alpha-1)}(2) = 1$

Moreover, we expect that the Galois group $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \langle 1, \sigma \rangle$ acts transitively on $\{(2,\alpha), (2,\alpha-1)\}$. Indeed, if $\sigma \in G$ is the element such that

$$\sigma(\sqrt{d}) = -\sqrt{d}$$

we get

$$\sigma(\alpha) = \sigma\left(\frac{1+\sqrt{d}}{2}\right) = \left(\frac{1-\sqrt{d}}{2}\right)$$
$$= 1-\alpha$$

Hence:

$$\sigma(2,\alpha) = (\sigma(2), \sigma(\alpha)) = (2, 1-\alpha)$$
$$= (2, \alpha-1).$$

- $d \equiv 5 \ (8)$: $x^2 - x + \frac{1-d}{4} \equiv x^2 + x + 1$ in $\mathbb{F}_2[x]$

and this is irreducible. Hence

$$(2) = (2, \alpha^2 + \alpha + 1)$$

so (2) is already prime, and

$$e_{(2)}(2) = 1.$$

$$f_{(2)}(2) = 2.$$