# ZAHLENTHEORIE NOTE 10

We want to prove the following result which tells us exactly which primes ramify in an extension:

<u>Thm</u>: Let $K$ be a number field and $p \in \mathbb{Z}$ a prime.
$p$ ramifies in $\mathcal{O}_K \iff p \mid \Delta_K$.

We make some remarks about this. Recall that $p$ ramifies if and only if $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and one of the $e_i$ is $e_i \geq 2$. On the other hand, we have the following interpretation of the discriminant $\Delta_K$: Let $\alpha_1, \dots, \alpha_n$ be a basis of $\mathcal{O}_K$ over $\mathbb{Z}$ and consider the trace map

$$\widetilde{Tr}_{K/\mathbb{Q}} : K \longrightarrow \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q})$$
$$\alpha \longmapsto Tr_{K/\mathbb{Q}}(\alpha \cdot)$$

If $T$ is the matrix representing this map w.r.t. the bases $\alpha_1, \dots, \alpha_n$ in $K$
$\alpha_1^\vee, \dots, \alpha_n^\vee$ dual basis in $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q})$

then

$$\Delta_K = \det \widetilde{T}$$

We want to tie together this description of the discriminant with the ramification of $p$.

The key observation is the following: recall that we

have an extension of rings $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subseteq \mathcal{O}_K/p\mathcal{O}_K$ and we can consider $\mathcal{O}_K/p\mathcal{O}_K$ as a $\mathbb{F}_p$-vector space.

Then, we can define the TRACE of an element $\bar{\alpha} \in \mathcal{O}_K/p\mathcal{O}_K$ as the trace of the multiplication-by-$\alpha$ map

$$\mathrm{Tr}_{\mathcal{O}_K/p\mathcal{O}_K}(\bar{\alpha}) = \mathrm{trace}\left(\mathcal{O}_K/p\mathcal{O}_K \xrightarrow{\cdot\bar{\alpha}} \mathcal{O}_K/p\mathcal{O}_K\right)$$

This is related to the previous trace as follows.

<u>Lemma</u>: Let $\alpha \in \mathcal{O}_K$ and let $\bar{\alpha}$ be its class in $\mathcal{O}_K/p\mathcal{O}_K$. Then

$$\mathrm{Tr}_{\mathcal{O}_K/p\mathcal{O}_K}(\bar{\alpha}) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \quad (\text{in } \mathbb{F}_p)$$

<u>proof</u>: Let $\alpha_1, \dots, \alpha_n$ be a basis of $\mathcal{O}_K$ as $\mathbb{Z}$-module and let $a_{ij} \in \mathbb{Z}$ be such that

$$\begin{aligned} \alpha \cdot \alpha_1 &= a_{11}\alpha_1 + \dots + a_{1n}\alpha_n \\ \alpha \alpha_2 &= a_{21}\alpha_1 + \dots + a_{2n}\alpha_n \\ &\vdots \\ \alpha \alpha_n &= a_{n1}\alpha_1 + \dots + a_{nn}\alpha_n \end{aligned}$$

(observe that $a_{ij} \in \mathbb{Z}$ because $\alpha \cdot \alpha_i \in \mathcal{O}_K$)

so that the matrix representing $K \xrightarrow{\cdot\alpha} K$ is

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & & a_{nn} \end{pmatrix}$$

$$(a_{n1}\ a_{n2} \dots a_{nn})$$

Now, let $\overline{\alpha}_1, \dots, \overline{\alpha}_n$ be the classes of $\alpha_1, \dots, \alpha_n$ in $\mathcal{O}_K/p\mathcal{O}_K$: these are a basis of $\mathcal{O}_K/p\mathcal{O}_K$ as a $\mathbb{F}_p$-module and

$$\overline{\alpha}\,\overline{\alpha}_1 = \overline{a}_{11}\overline{\alpha}_1 + \dots + \overline{a}_{1n}\overline{\alpha}_n$$
$$\vdots$$
$$\overline{\alpha}\cdot\overline{\alpha}_n = \overline{a}_{n1}\overline{\alpha}_1 + \dots + \overline{a}_{nn}\overline{\alpha}_n$$

so that the matrix representing $\mathcal{O}_K/p\mathcal{O}_K \xrightarrow{\cdot\alpha} \mathcal{O}_K/p\mathcal{O}_K$ is

$$\overline{A} = \begin{pmatrix} \overline{a}_{11} & \overline{a}_{12} & \cdots \\ \overline{a}_{21} & \overline{a}_{22} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} = A \quad (\text{in } \mathbb{F}_p)$$

Hence

$$\operatorname{trace}(\overline{A}) \equiv \operatorname{trace}(A) \quad (\text{in } \mathbb{F}_p) \qquad \square$$

In the same way as before, we get the map

$$\widetilde{\operatorname{Tr}}_{\mathcal{O}_K/p\mathcal{O}_K} : \mathcal{O}_K/p\mathcal{O}_K \to \operatorname{Hom}_{\mathbb{F}_p}(\mathcal{O}_K/p\mathcal{O}_K, \mathbb{F}_p)$$

Moreover, if $\overline{T}$ is the matrix representing this linear map w.r.t. the bases: $\overline{\alpha}_1, \dots, \overline{\alpha}_n$
$\overline{\alpha}_1^\vee, \dots, \overline{\alpha}_n$

then

$$\overline{T} = \left(\operatorname{Tr}_{\mathcal{O}_K/p\mathcal{O}_K}(\overline{\alpha}_i\overline{\alpha}_j)\right) = \left(\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right) = T \quad (\text{in } \mathbb{F}_p)$$

So that

$$\det \overline{T} \equiv \Delta_K \quad (\text{in } \mathbb{F}_p)$$

With this, we can prove the theorem:

<u>proof of Theorem</u>: We have that

$$p \mid \Delta_K \iff \Delta_K = 0 \text{ in } \mathbb{F}_p$$
$$\iff \det \widetilde{T} = 0$$
$$\iff \widetilde{\mathrm{Tr}}_{\mathcal{O}_K/p\mathcal{O}_K} : \mathcal{O}_K/p\mathcal{O}_K \to \mathrm{Hom}_{\mathbb{F}_p}(\mathcal{O}_K/p\mathcal{O}_K, \mathbb{F}_p)$$
is not an isomorphism

Hence we need to prove that

$p$ ramifies $\iff \widetilde{\mathrm{Tr}}_{\mathcal{O}_K/p\mathcal{O}_K}$ is not an isomorphism

Now, suppose that $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Then

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

and it is easy to see (check explicitly) that the trace map $\widetilde{\mathrm{Tr}}_{\mathcal{O}_K/p\mathcal{O}_K}$ also splits as the direct sum

$$\widetilde{\mathrm{Tr}}_{\mathcal{O}_K/p\mathcal{O}_K} = \bigoplus_{i=1}^{r} \widetilde{\mathrm{Tr}}_{\mathcal{O}_K/\mathfrak{p}_i^{e_i}}$$

where $\widetilde{\mathrm{Tr}}_{\mathcal{O}_K/\mathfrak{p}_i^{e_i}} : \mathcal{O}_K/\mathfrak{p}_i^{e_i} \to \mathrm{Hom}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}_i^{e_i}, \mathbb{F}_p)$ is the analogous trace map defined on the ring extension $\mathbb{F}_p \subseteq \mathcal{O}_K/\mathfrak{p}_i^{e_i}$.

Now we prove our implications:

($\Rightarrow$) suppose that $p$ ramifies and w.l.o.g. $e_1 \geq 2$

Then we will prove that the map

$$\widetilde{\mathrm{Tr}}_{\mathcal{O}_K/\mathfrak{p}_1^{e_1}} : \mathcal{O}_K/\mathfrak{p}_1^{e_1} \to \mathrm{Hom}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}_1^{e_1}, \mathbb{F}_p)$$

is not an isomorphism. Indeed, let $\alpha \in \mathfrak{p}_1, \alpha \notin \mathfrak{p}_1^{e_1}$

Then $\overline{\alpha} \neq 0$ in $\mathcal{O}_K/\mathfrak{p}_1^{e_1}$ and we claim that

$$\widetilde{\mathrm{Tr}}_{\mathcal{O}_K/\mathfrak{p}_1^{e_1}}(\overline{\alpha}) = 0$$

or, equivalently, $\mathrm{Tr}_{\mathcal{O}_K/\mathfrak{p}_1^{e_1}}(\overline{\alpha\beta}) = 0$ for every $\beta \in \mathcal{O}_K$.

Observe that if $\beta \in \mathcal{O}_K$, then $\alpha\beta \in \mathfrak{p}_1$, hence $(\overline{\alpha\beta})^{e_1} = 0$

This means that the multiplication map

$$(\overline{\alpha\beta}) : \mathcal{O}_K/\mathfrak{p}_1^{e_1} \to \mathcal{O}_K/\mathfrak{p}_1^{e_1} \text{ is nilpotent}$$

hence, it has trace zero by linear algebra.

($\Leftarrow$) Suppose that $p$ does not ramify, then we want to prove that each map

$$\widetilde{\mathrm{Tr}}_{\mathcal{O}_K/\mathfrak{p}_i} \text{ is an isomorphism}$$

However, in this case $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field extension of $\mathbb{F}_p$, hence it is separable. Then we know that the trace of a separable field extension is always nondegenerate, meaning that $\widetilde{\mathrm{Tr}}_{\mathcal{O}_K/\mathfrak{p}}$ is an isomorphism $\square$

<u>Cor</u>: There are only finitely many primes which ramify in $K$.

<u>Example</u>: (1) QUADRATIC EXTENSIONS

Let $d \in \mathbb{Z}$ be safe

- $d \equiv 2, 3 \ (4)$: we know that

$$\Delta_{\mathbb{Q}(\sqrt{d})} = 4d$$

In particular, we see that 2 always ramifies. This is written explicitly in the previous notes.

- $d \equiv 1 \ (4)$: we know that

$$\Delta_{\mathbb{Q}(\sqrt{d})} = d$$

hence 2 never ramifies. We saw this explicitly in the previous notes

(2) CYCLOTOMIC EXTENSIONS

$p$ = odd prime. Then we know that

$$\Delta_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{(p-1)}{2}} p^{p-2}$$

hence the only prime that ramifies in $\zeta_p$ is $p$ itself.

In general, we know that

$$\Delta_{\mathbb{Q}(\zeta_n)} \mid n^{\varphi(n)}$$

hence, if $p$ ramifies in $\mathbb{Q}(\zeta_n)$, then $p \mid n$.

From the last exercise sheet, we already know that $p$ ramifies in $\mathbb{Q}(\zeta_n) \iff p \mid n$. $\square$

Ultima modifica: 28 mag 2019