Algebraic Number Theory

Lecture 14, 28th January

Lecture 13

From now we consider again the more general case:

$$\begin{array}{ccccccc} & & \mathrm{Frac}(A) & & \text{fin. extension} & & \\ \text{Ex} & \mathbb{Q} & \subset & \overset{\shortparallel}{K} & \subset & L & \quad (\text{Ex: } K \text{ number field}) \\ & \cup & & \cup & & \cup & \\ & \mathbb{Z} & \subset & \mathcal{O}_K = A & \subset & \mathcal{O} & \quad (\mathrm{char}(K) = 0 \text{ or } |K| < \infty) \end{array}$$

Dedekind domain

integral closure of A in L

Proposition 10.1 $\mathcal{O}$ is a Dedekind domain

Let $\mathfrak{p} \neq (0)$ be a prime ideal in A.
In $\mathcal{O}$ we have the unique factorization

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \qquad (\star)$$

where $\mathfrak{P}_i$ are pairwise different prime ideals in $\mathcal{O}$ and $e_1, \dots, e_r \geq 1$.

$\mathfrak{P}_i$ = prime ideals "above $\mathfrak{p}$".

These are exactly those prime ideals $\mathfrak{P}$ in $\mathcal{O}$ with $A \cap \mathfrak{P} = \mathfrak{p}$.

Definition 10.3

i) The exponent e_i in $(\star)$ is called the <u>ramification index</u> of $\mathfrak{P}_i$ over $\mathfrak{p}$.

ii) The degree of the field extension
$$f_i = [\mathcal{O}/\mathfrak{P}_i : A/\mathfrak{p}]$$
is called the <u>inertia degree</u> of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Theorem 10.4 (Fundamental identity)

Let $\mathrm{char}(K)=0$ or $|K|<\infty$, $n=[L:K]$ and $\mathfrak{p}\subset A$ prime.

If $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r}$ then

$$\sum_{i=1}^{r} e_i f_i = n.$$

Example 10.5

$n=2$

$A=\mathbb{Z}$, $K=\mathbb{Q}$, $L=\mathbb{Q}(i)$, $\mathcal{O}=\mathcal{O}_L=\mathbb{Z}[i]$.

$p=2$: $(2)=(1+i)^2$, $r=1$, $e_1=2$

$(2=-i\cdot(1+i)^2)$ $f_1=\left[\mathbb{Z}[i]/(1+i) : \mathbb{Z}/2\mathbb{Z}\right]=1$

$e_1\cdot f_1=2$

$p\equiv 1 \bmod 4$: $(p)=(a+bi)(a-bi)$, $r=2$, $e_1=e_2=1$

$(p=a^2+b^2)$

$f_{1,2}=\left[\mathbb{Z}[i]/(a\pm bi) : \mathbb{Z}/p\mathbb{Z}\right]=1$

$e_1f_1+e_2f_2=2.$

$p\equiv 3 \bmod 4$: $(p)=(p)$, $r=1$, $e_1=1$, $f_1=\left[\mathbb{Z}[i]/p\mathbb{Z} : \mathbb{Z}/p\mathbb{Z}\right]=2$

$$e_1 f_1 = 1 \cdot 2 = 2$$

<u>Proof</u>: • By the chinese remainder theorem (Thm 10.4) (Thm. 1.30) we have

$$\mathcal{O}/p\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}.$$

All these spaces are $K = A/p$ vector spaces.

Want to show: 1) $\dim_K \mathcal{O}/p\mathcal{O} = n$,

2) $\dim_K \mathcal{O}/\mathfrak{P}_i^{e_i} = e_i f_i$.

(Sketch)

1) Let $\overline{\omega}_1, \dots, \overline{\omega}_m$ be a basis of $\mathcal{O}/p\mathcal{O}$ and write $\omega_1, \dots, \omega_m \in \mathcal{O}$ for representatives.

One can then show: $\omega_1, \dots, \omega_m$ are a basis of L/K, i.e $m = n = [L:K]$.

2) Consider the descending chain of K-vector spaces

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i^2/\mathfrak{P}_i^{e_i} \supseteq \dots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq (0)$$

The successive quotients are $\mathfrak{p}_i^v / \mathfrak{p}_i^{v+1}$, which are all isomorphic to $\mathcal{O}/\mathfrak{p}_i$:

Let $\alpha \in \mathfrak{p}_i^v \setminus \mathfrak{p}_i^{v+1}$ and consider

$$\varphi : \mathcal{O} \longrightarrow \mathfrak{p}_i^v / \mathfrak{p}_i^{v+1}$$
$$a \longmapsto a\alpha \mod \mathfrak{p}_i^{v+1}.$$

We have $\ker(\varphi) = \mathfrak{p}_i$ and φ is surjective since $\mathfrak{p}_i^v = \gcd(\mathfrak{p}_i^{v+1}, (\alpha))$.

$$\mathfrak{p}_i^{v+1} + (\alpha) = \alpha\mathcal{O} + \mathfrak{p}_i^{v+1}$$

This shows

$$\dim_k \mathfrak{p}_i^v / \mathfrak{p}^{v+1} = \dim_k \mathcal{O}/\mathfrak{p}_i =: f_i$$

and $\dim \mathcal{O}/\mathfrak{p}_i^{e_i} = e_i \cdot f_i$ $\square$

Recall: By Prop 3.2 there exists a primitive element $\theta \in L$ with $L = k(\theta)$.

By Prop 3.12 we can write $\theta = \frac{\tilde{\theta}}{a}$

with $\tilde{\theta} \in \mathcal{O}$ and $a \in A^{c_k}$, i.e. we can assume that $\theta \in \mathcal{O}$.

Let $p(x) \in A[x]$ be the minimal polynomial of θ. We will use $p(x)$ to understand the decomposition of prime ideals $\mathfrak{p} \subset A$ in $\mathcal{O}$.

For all but fin. many $\mathfrak{p}$ we will obtain an explicit result. The exceptional cases are those ideals which are not coprime to the "conductor" of the ring $A[\theta]$:

<u>Definition 10.6</u> The ideal

($\mathcal{F}$ for Führer) $$\mathcal{F} = \{\alpha \in \mathcal{O} \mid \alpha\mathcal{O} \subseteq A[\theta]\} \subset \mathcal{O}$$

is called the <u>conductor</u> of the ring $A[\theta]$.

$\mathcal{F}$ is the biggest ideal in $\mathcal{O}$ contained in $A[\theta]$.

We have $\mathcal{F} \neq (0)$ since by Lemma 3.13 we have $\underset{\neq 0}{d(1, \theta, \dots, \theta^{n-1})} \in \mathcal{F}$.

$$\begin{array}{c} \mathcal{O} \\ \cup \\ A[\theta] \\ \cup \\ \mathcal{F} \neq (0) \end{array}$$

Proposition 10.7 Let $\mathfrak{p} \subset A$ be a prime ideal which is coprime to the conductor $\mathcal{F}$ of $A[\theta]$ (i.e. $\mathfrak{p}\mathcal{O} + \mathcal{F} = \mathcal{O}$)

Let
$$\bar{p}(X) = \bar{p}_1(X)^{e_1} \cdots \bar{p}_r(X)^{e_r}$$
be the factorization of $\bar{p}(X) = p(X) \bmod \mathfrak{p}$ into irreducibles $\bar{p}_i(X) = p_i(X) \bmod \mathfrak{p}$ over $A/\mathfrak{p}$.

min. pol. of θ in $A[X]$

$p_i(X) \in A[X]$

Then
$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O} \qquad i = 1, \dots, r$$
are the different prime ideals of $\mathcal{O}$ above $\mathfrak{p}$.

The inertia degree is $f_i = \deg p_i$ and we have
$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}.$$

Example 10.8 $K = \mathbb{Q}(i)$, $\theta = i$, $p(x) = x^2+1$, $A = \mathbb{Z}$

$$F = A(i) = \mathbb{Z}[i] = \mathcal{O}_K = \mathcal{O}$$

$p=2$: $\quad x^2+1 \equiv (x+1)^2 \mod 2$

$p = 4n+1$: $\quad x^2+1 = (x-(2n)!)(x+(2n)!) \mod p$

(We proved $(2n!)^2 \equiv -1 \mod p$ in Theorem 1.3)

$p = 4n+3$: $\quad x^2+1$ can not be factored mod p

<u>Proof sketch</u> (Prop 10.7): Set $\mathcal{O}' = A[\theta] \subset \mathcal{O}$

$$\bar{A} = A/p.$$

One then shows

$$\mathcal{O}/p\mathcal{O} \cong \mathcal{O}'/p\mathcal{O}' \cong \bar{A}[x]/(\bar{p}(x)).$$

consider $A[x] \to \bar{A}(x)/(\bar{p}(x))$

$\mathcal{O}' = A[x]/p(x)$

$$p\mathcal{O} + \underset{\mathcal{O}'}{\underset{\cap}{F}} = \mathcal{O} \Rightarrow p\mathcal{O} + \mathcal{O}' = \mathcal{O}$$

$\Rightarrow \mathcal{O}' \to \mathcal{O}/p\mathcal{O}$ surjective with kernel $p\mathcal{O}'$.

$a \mapsto \bar{a}$

Since $\bar{p}(x) = \prod_{i=1}^{r} \bar{p}_i(x)^{e_i}$ the chinese remainder thm. gives

$$\underbrace{\bar{A}[x] / (\bar{p}(x))}_{R} \cong \bigoplus_{i=1}^{r} \bar{A}[x] / (p_i(x))^{e_i} .$$

Then argue

- $[R/\mathfrak{p}_i : \bar{A}] = \deg p_i$
- In R we have $(0) = (\bar{p}) = \bigcap_{i=1}^{r} (\bar{p}_i)^{e_i}$

and use the isomorphism

$$R = \bar{A}[x] / (\bar{p}(x)) \longrightarrow \mathcal{O}/p\mathcal{O}$$

$$\bar{f}(x) \bmod \bar{p} \longmapsto \bar{f}(\theta) \bmod p\mathcal{O}$$

to deduce $p\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ and $f_i = \deg p_i$.

"$\square$"

Definition 10.9 Let $\mathfrak{p} \subset A$ be prime and

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

i) $\mathfrak{p}$ is said to <u>split completely</u> (or <u>totally split</u>) in L, if $r = n = [L:K]$, i.e $e_i = f_i = 1$ for all $i = 1, \dots, r$.

ii) $\mathfrak{p}$ is called <u>nonsplit</u> (or <u>indecomposed</u>) if $r = 1$, i.e. there is just one prime ideal over $\mathfrak{p}$.

iii) $\mathfrak{P}_i$ is called <u>unramified</u> over A (or over K) if $e_i = 1$ and if $[\mathcal{O}/\mathfrak{P}_i : A/\mathfrak{p}]$ is separabel.

(all minimal pols. have simple zeros. always the case if K is a number field)

Otherwise $\mathfrak{P}_i$ is called <u>ramified</u>

If $e_i > 1$ and $f_i = 1$ then $\mathfrak{P}_i$ is called <u>totally ramified</u>.

iv) $\mathfrak{p}$ is called <u>unramified</u> if all $\mathfrak{P}_i$ over $\mathfrak{p}$ are unramified. Otherwise, $\mathfrak{p}$ is called <u>ramified</u>.

In particular: split completely $\Rightarrow$ unramified.

v) The extension L/K is called unramified if all prime ideals $\mathfrak{p} \subset A$ are unramified.

<u>Example 10.10</u> $K = \mathbb{Q}(i)$

- $(2) = (1+i)^2$ is ramified
- $\underset{\substack{\| \\ a^2+b^2}}{p} \equiv 1 \bmod 4$: $(p) = (a+bi)(a-bi)$ split completely
- $p \equiv 3 \bmod 4$: $(p) = (p)$ (p) is <u>inert</u>

$\Big\}$ unramified

<u>Proposition 10.11</u> There are just finitely many prime ideals of K (meaning A) which are ramified over L.

<u>Proof:</u> Let θ be a primitive element ($L = K(\theta)$) with minimal polynomial $p(x) \in A[X]$

and $d := d(1, \theta_1, \dots, \theta^{n-1}) = \prod_{i<j} \underbrace{(\theta_i - \theta_j)^2}_{\in A} \neq 0$
(discriminant).

Then every ideal $\mathfrak{p}$ which is coprime to (d) and the conductor $\mathcal{F}$ of $A(\theta)$ is unramified:

By Prop. 10.7 we see that $e_i = 1$ for all $i = 1, \dots, r$, since $\bar{p}(X) = p(X) \bmod \mathfrak{p}$ has no multiple roots (since $d \not\equiv 0 \bmod \mathfrak{p}$). $\square$

Definition 10.12 The discriminant $d_{\mathcal{O}/A}$ of $\mathcal{O}/A$ is the ideal generated by the discriminants $d(\omega_1, \dots, \omega_n)$ of all bases $\omega_1, \dots, \omega_n$ of L/K contained in $\mathcal{O}$.

One can show:

$\mathfrak{p}$ is ramified in $L \iff \mathfrak{p}$ divides $d_{\mathcal{O}/A}$.

In example: $d_{\mathbb{Z}[i]/\mathbb{Z}} = (4)$

$\Rightarrow$ (2) only ramified ideal