Algebraic Number Theory

Lecture 10, 10th December 2021

Last lecture

K: number field

$$j: K \longrightarrow K_{\mathbb{C}} := \prod_{\tau: K \to \mathbb{C}} \mathbb{C}$$

$$a \longmapsto (\tau(a) = (a_\tau))$$

$F: z \mapsto \bar{z}$

Action of $G(\mathbb{C}/\mathbb{R}) = \langle F \rangle$ on $\mathrm{Hom}_{\mathbb{Q}}(K:\mathbb{C})$: $F(\tau) = \bar{\tau}$

$K_{\mathbb{C}}$: $(F(z))_\tau = \overline{z_{\bar{\tau}}}$.

$\langle x, y \rangle = \sum_\tau x_\tau \bar{y}_\tau$, $\langle F(x), F(y) \rangle = F\langle x, y \rangle$.

$$K_{\mathbb{R}} = \{ z \in K_{\mathbb{C}} \mid z_{\bar{\tau}} = \overline{z_\tau} \}.$$

$$\| $$

$[K_{\mathbb{C}}]^+$ F-invariant subspace $(z_\tau) \in K_{\mathbb{C}} \mid z_\tau \in \mathbb{R},\ z_{\tau} = \overline{z_{\tau}} \}$

$(K_{\mathbb{R}}, \langle , \rangle)$ euclidean vector space

(new numbering)

Theorem 6.4 Let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}_K$, and let $c_\tau > 0$ be real numbers for such $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ such that $c_\tau = c_{\bar{\tau}}$ and

$$(*) \quad \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, [\mathcal{O}_K : \mathfrak{a}].$$

Then there exists $a \in \mathfrak{a}$, $a \neq 0$ with

$$|\tau(a)| < c_\tau$$

for all $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

In addition to the additive $j: K \to K_{\mathbb{C}}$ we will also consider the:

"Multiplicative" Minkowski theory

Define
$$j: K^\times \longrightarrow K_{\mathbb{C}}^\times = \prod_\tau \mathbb{C}^\times$$

and
$$N: K_{\mathbb{C}}^\times \longrightarrow \mathbb{C}^\times$$
$$(z_\tau) \longmapsto \prod_\tau z_\tau$$

Then the norm is given by their composition,
$$N_{K/\mathbb{Q}}(a) = N(j(a)). \quad \text{(Prop. 3.6)}$$

Now consider
$$\ell: \mathbb{C}^\times \longrightarrow \mathbb{R}$$
$$z \longmapsto \log|z|,$$
which induces a surjective homomorphism
$$\ell: K_{\mathbb{C}}^\times \longrightarrow \prod_\tau \mathbb{R}$$
$$(z_\tau) \longmapsto (\ell(z_\tau))$$

and we get the commutative diagram

$$\begin{tikzcd}
K^\times \arrow[r, "j"] \arrow[d, "N_{K/L}"'] & K_{\mathbb{C}}^\times \arrow[r, "\ell"] \arrow[d, "N"'] & \prod_\tau \mathbb{R} \arrow[d, "\mathrm{Tr}"] \\
\mathbb{Q}^\times \arrow[r] & \mathbb{C}^\times \arrow[r] & \mathbb{R}
\end{tikzcd}$$

$G(\mathbb{C}/\mathbb{R}) = \langle F \rangle$ acts on all these groups:

- on $K^\times$ trivially
- on $K_{\mathbb{C}}^\times$ as before
- on $(x_\tau) \in \prod_\tau \mathbb{R}$ by $F(x)_\tau = x_{\bar{\tau}}$.

Considering the fixed modules under this action (notation $[\cdot]^+$) one can check that we get:

$$\begin{tikzcd}
K^\times \arrow[r, "j"] \arrow[d, "N_{K/L}"'] & K_{\mathbb{R}}^\times \arrow[r, "\ell"] \arrow[d, "N"'] & \left[\prod_\tau \mathbb{R}\right]^+ \arrow[d, "\mathrm{Tr}"] \\
\mathbb{Q}^\times \arrow[r] & \mathbb{R}^\times \arrow[r] & \mathbb{R}
\end{tikzcd}$$

Explicitly we have

$$\left[\prod_{\tau} \mathbb{R}\right]^{+} = \prod_{\substack{\rho \\ \text{real emb.}}} \mathbb{R} \times \prod_{\substack{\sigma \\ \text{compl. emb.}}} \left[\mathbb{R}\times\mathbb{R}\right]^{+} .$$

elements (x,x)

$[\mathbb{R}\times\mathbb{R}]^{+}$ consists of the elements (x,x) and we identify it with $\mathbb{R}$ by the map $(x,x) \to 2x$.

This gives an isomorphism

$$\left[\prod_{\tau} \mathbb{R}\right]^{+} \cong \mathbb{R}^{r+s} .$$

Under this identification the map ℓ is given by

$$\ell : K_{\mathbb{R}}^{*} \longrightarrow \mathbb{R}^{r+s}$$

$$x \longmapsto \left(\log|x_{\rho_1}|, \dots, \log|x_{\rho_r}|, \log(|x_{\sigma_1}|^2), \dots, \log(|x_{\sigma_s}|)^2\right).$$

We will use this again later when proving Dirichlets unit theorem.

§7 The class number

Definition 7.1 Let $\mathfrak{a} \neq (0)$ be an ideal in $\mathcal{O}_K$. Then

$$n(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = |\mathcal{O}_K/\mathfrak{a}|$$

is called the <u>absolute norm</u> of $\mathfrak{a}$.

Remark 7.2 i) By Prop. 3.19 the absolute norm is always finite.

ii) If $\mathfrak{a} = (a) \neq (0)$, then

$$n(\mathfrak{a}) = |N_{K/\mathbb{Q}}(a)|.$$

If $\omega_1, \dots, \omega_n$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$ the $a\omega_1, \dots, a\omega_n$ is a $\mathbb{Z}$-basis of $a\mathcal{O}$. If $A = (a_{ij})$ with $a\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$ then $|N_{K/\mathbb{Q}}(a)| \underset{\text{def}}{=} |\det(A)| \underset{\text{Prop 3.19}}{=} [\mathcal{O}_K : \mathfrak{a}] = n(a)$

Proposition 7.3 If $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ is the prime factorization of an ideal $\mathfrak{a} \neq (0)$, then

$$n(\mathfrak{a}) = n(\mathfrak{p}_1)^{\nu_1} \cdots n(\mathfrak{p}_r)^{\nu_r}.$$

Proof: • By the chinese remainder theorem (Thm 1.30) we have

$$\mathcal{O}_K/\mathfrak{a} \cong \bigoplus_{i=1}^{r} \mathcal{O}_K/\mathfrak{p}_i^{\nu_i},$$

i.e. it suffices to consider the case $\mathfrak{a} = \mathfrak{p}^\nu$ for some prime ideal $\mathfrak{p}$.

• In the chain $\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \dots \supseteq \mathfrak{p}^\nu$ we have $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ (due to uniquness of prime fact.).

Claim: $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ is an $\mathcal{O}_K/\mathfrak{p}$-vector space of dim 1.

If $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ then setting $\mathfrak{b} = (a) + \mathfrak{p}^{i+1}$ gives

$$\mathfrak{p}^i \supset \mathfrak{b} \supsetneq \mathfrak{p}^{i+1}.$$

Multiplying with $\mathfrak{p}^{-i}$ (in J_K) gives

$$\mathcal{O}_K = \mathfrak{p}^i \mathfrak{p}^{-i} \supseteq \mathfrak{b}\mathfrak{p}^{-i} \supsetneq \mathfrak{p}^{i+1}\mathfrak{p}^{-i} = \mathfrak{p}.$$

Since $\mathfrak{p}$ is maximal we get $\mathfrak{b}\mathfrak{p}^{-i} = \mathcal{O}_K$, i.e $\mathfrak{b} = \mathfrak{p}^i$. Therefore (the class of) a spans

$\mathfrak{p}^i/\mathfrak{p}^{i+1}$, i.e $\dim_{\mathcal{O}_K/\mathfrak{p}} \mathfrak{p}^i/\mathfrak{p}^{i+1} = 1$ and $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K/\mathfrak{p}$.

$$\Rightarrow \quad [\mathfrak{p}^i : \mathfrak{p}^{i+1}] = [\mathcal{O}_K : \mathfrak{p}] = \mathcal{N}(\mathfrak{p})$$

$$\Rightarrow \quad \mathcal{N}(\mathfrak{p}^v) = [\mathcal{O}_K : \mathfrak{p}^v]$$

$$= [\mathcal{O}_K : \mathfrak{p}] \cdot [\mathfrak{p} : \mathfrak{p}^2] \cdot \ldots \cdot [\mathfrak{p}^{v-1} : \mathfrak{p}^v]$$

$$= \mathcal{N}(\mathfrak{p})^v. \qquad \square$$

<u>Corollary 7.4</u> For ideals $\mathfrak{a}, \mathfrak{b}$ with $\mathfrak{a}, \mathfrak{b} \neq (0)$ we have

$$\mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}).$$

We extend the absolute norm to all fractional ideals, which gives a group homomorphism

$$\mathcal{N} : J_K \longrightarrow \mathbb{Q}^\times_{>0}$$

$$\frac{\mathfrak{a}}{\mathfrak{b}} \longmapsto \frac{\mathcal{N}(\mathfrak{a})}{\mathcal{N}(\mathfrak{b})}$$

Lemma 7.5 In every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$ there exists an $a \in \mathfrak{a}$, $a \neq 0$, with

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, N(\mathfrak{a}).$$

Proof: For fixed $\varepsilon > 0$ we can choose real $c_\tau > 0$ for $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K;\mathbb{C})$, with $c_\tau = c_{\bar{\tau}}$ and

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, N(\mathfrak{a}) + \varepsilon .$$

By Thm 6.4 we then get an $a_\varepsilon \in \mathfrak{a}$, $a_\varepsilon \neq 0$, with $|\tau(a_\varepsilon)| < c_\tau$. Thus

$$|N_{K/\mathbb{Q}}(a_\varepsilon)| = \prod_\tau |\tau(a_\varepsilon)| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, N(\mathfrak{a}) + \varepsilon .$$

Since the norm is an integer we find an $a \in \mathfrak{a}$, $a \neq 0$ with

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, N(\mathfrak{a}).$$

$\square$

Theorem 7.6 The ideal class group $Cl_K = J_K / P_K$ is finite. Its order

$$h_K = |Cl_K|$$

is called the <u>class number</u> of K.

proof: i) Let $\mathfrak{p} \neq (0)$ be a prime ideal of $\mathcal{O}$ and $\mathfrak{p} \cap \mathbb{Z} = (p) \neq (0)$ for a rational prime $p \in \mathbb{Z}$.

See Proof of Prop. 4.3

$\mathcal{O}/\mathfrak{p}$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$.

Suppose that $[\mathcal{O}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = k$, then

$$N(\mathfrak{p}) = |\mathcal{O}/\mathfrak{p}| = (\# \mathbb{Z}/p\mathbb{Z})^k = p^k .$$

ii) For a fixed prime $p \in \mathbb{Z}$ there are just finitely many prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ with $\mathfrak{p} \cap \mathbb{Z} = (p)$, since $p\mathcal{O}_K \subseteq \mathfrak{p}$ implies

$$\mathfrak{p} \mid p\mathcal{O} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_r^{r_r}$$

(The prime decomp. of $p\mathcal{O}$)

i) and ii) together imply that for a given $M \in \mathbb{R}$ there are just finitely many prime ideals $\mathfrak{p}$ with $\mathcal{N}(\mathfrak{p}) \leq M$. Therefor by Prop. 7.3 there are also just finitely many ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $\mathcal{N}(\mathfrak{a}) \leq M$.

- Let $M := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. We now want to show that any class $[\mathfrak{a}] \in Cl_K$ contains an ideal $\mathfrak{a}_1 \subset \mathcal{O}_K$ with $\mathcal{N}(\mathfrak{a}_1) \leq M$. This then implies $|Cl_K| < \infty$.

  class of $\mathfrak{a}$, $\mathfrak{a} \in J_K$

  By Prop 3.12 (i) there exists a $\gamma \in \mathcal{O}_K \setminus \{0\}$ with
  $$\mathfrak{b} := \gamma \mathfrak{a}^{-1} \subseteq \mathcal{O}_K.$$

  By Lemma 7.5 there exists a $\alpha \in \mathfrak{b}, \alpha \neq 0$ with
  $$|N_{K/\mathbb{Q}}(\alpha)| \leq M\, \mathcal{N}(\mathfrak{b}).$$

$$\Rightarrow M \geq |N_{K/\mathbb{Q}}(\alpha)|\, \mathcal{N}(\mathfrak{b})^{-1} = \mathcal{N}((\alpha)\mathfrak{b}^{-1}) = \mathcal{N}(\alpha \mathfrak{b}^{-1}).$$

Now set $\mathfrak{a}_1 = \alpha \mathfrak{b}^{-1} = \alpha \gamma^{-1} \mathfrak{a} \in [\mathfrak{a}]$

$\uparrow$

$\alpha \gamma^{-1} \in K^{\times}$.

Since $\alpha \in \mathfrak{b}$ we have $(\alpha) \subseteq \mathfrak{b}$, i.e

$$(\alpha)\mathfrak{b}^{-1} \subseteq \mathfrak{b}\mathfrak{b}^{-1} \subseteq \mathcal{O}_K$$

$\Rightarrow \quad \mathfrak{a}_1 = \alpha \mathfrak{b}^{-1} \subset \mathcal{O}_K$ with $N(\mathfrak{a}_1) \leq M$. $\square$