Recall from last week:

Chinese Remainder Theorem (CRT):

R a ring, $I_i \subset R$ ideals, s.t.

$\forall i \neq j \quad I_i + I_j = R$ (I_i, I_j are coprime)

Then $R / \prod_{i=1}^{n} I_i \simeq \prod_{i=1}^{n} R/I_i$

Apply this to the case $R = \mathcal{O}_K$,

$I_i = \mathfrak{p}_i^{n_i}$, where $\mathfrak{p}_i$ – distinct non-zero prime ideals. Let $\mathfrak{a} = \prod_{i=1}^{k} I_i = \prod_{i=1}^{k} \mathfrak{p}_i^{n_i}$

Exercise 5.1:

$$\mathcal{O}_K / \mathfrak{a} \simeq \prod_{i=1}^{k} \mathcal{O}_K / \mathfrak{p}_i^{n_i}$$

Corollary 9.4 $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ prime, then $\forall n \geq 0$ $\mathfrak{p}^n / \mathfrak{p}^{n+1} \simeq \mathcal{O}_K / \mathfrak{p}$ as $\mathcal{O}_K$-modules

Proof We have $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$ (because $\mathfrak{p} \neq (1)$) $\Rightarrow \exists x \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$.

Consider the map $\alpha: \mathcal{O}_K \longrightarrow \mathfrak{p}^n / \mathfrak{p}^{n+1}$

$$y \longmapsto xy$$

Claim 1: $\ker \alpha = \mathfrak{p}$

$y \in \ker \alpha \Leftrightarrow xy \in \mathfrak{p}^{n+1}$

Clearly if $y \in \mathfrak{p}$ then $xy \in \mathfrak{p}^{n+1}$, so $\mathfrak{p} \subset \ker \alpha$

Assume $y \in \ker \alpha$, but $y \notin \mathfrak{p}$

then $(y) + \mathfrak{p} \supsetneq \mathfrak{p}$, but $\mathfrak{p}$ is maximal

$\Rightarrow (y) + \mathfrak{p} = \mathcal{O}_K \Rightarrow \exists z \in \mathcal{O}_K,\ w \in \mathfrak{p}$, s.t. $y \cdot z + w = 1$; multiply by x:

$x = \underbrace{xyz}_{\in\, \mathfrak{p}^{n+1}} + \underbrace{xw}_{\in\, \mathfrak{p}^{n+1}} \in \mathfrak{p}^{n+1}$ — contradicts the choice of x.

$\mathfrak{p}^{n+1}$ because $y \in \ker \alpha$

$\Rightarrow \mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathfrak{p}^n/\mathfrak{p}^{n+1}$

Claim 2 α is surjective

Note: $(x) \subset \mathfrak{p}^n \Rightarrow (x)/\mathfrak{p}^n = \mathfrak{a} \subset \mathcal{O}_K$ ideal

Rewrite this:

$$(x) = \mathfrak{p}^n \cdot \mathfrak{a};$$

we have $\mathfrak{a} \simeq \prod_{i=1}^{k} \mathfrak{p}_i^{n_i}$, and

$\mathfrak{p}_i \neq \mathfrak{p}$ (otherwise $x \in \mathfrak{p}^{n+1}$)

$\Rightarrow$ $\mathfrak{p}^n$ and $\mathfrak{a}$ are coprime (see Exercise 5.1 and the proof of CRT)

Consider the ideal $(x)\cdot\mathfrak{p} = \mathfrak{p}^{n+1}\cdot\mathfrak{a}$

By CRT:

$$(*) \quad \mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/(x)\cdot\mathfrak{p} \simeq \mathcal{O}_K/\mathfrak{p}^{n+1} \times \mathcal{O}_K/\mathfrak{a}$$

Let $y \in \mathfrak{p}^n$. By $(*)$ $\exists\, z \in \mathcal{O}_K$

s.t. $z \equiv y \pmod{\mathfrak{p}^{n+1}}$, $z \equiv 0 \pmod{\mathfrak{a}}$

$\Updownarrow$ $\qquad\qquad$ $\Updownarrow$

$z - y \in \mathfrak{p}^{n+1} \Rightarrow z \in \mathfrak{p}^n$ $\qquad$ $z \in \mathfrak{a}$

$\Rightarrow z \in \mathfrak{a} \cap \mathfrak{p}^n = \mathfrak{p}^n\cdot\mathfrak{a} = (x)$

because $\mathfrak{a}$ and $\mathfrak{p}^n$ are coprime (see the proof of CRT)

$\Rightarrow \exists\, w \in \mathcal{O}_K: \quad z = x\cdot w$

$$\alpha(w) = x\cdot w \pmod{\mathfrak{p}^{n+1}} = z \pmod{\mathfrak{p}^{n+1}}$$
$$\equiv y \pmod{\mathfrak{p}^{n+1}}$$

$\Rightarrow$ α is surj. $\square$

10. Ideal class group of a number field

Recall: K - number field $\Rightarrow \mathcal{O}_K$ is a Dedekind domain. A fract. ideal in K is a fin. gen. $\mathcal{O}_K$-submodule in K.

$\mathcal{J}(\mathcal{O}_K) = \mathcal{J}(K) =$ multiplicative group of non-zero fract. ideals in K

$\forall\, I \in \mathcal{J}(K)$ can be written as

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{n_i}, \quad \mathfrak{p}_i \text{ - distinct}$$

non-zero prime ideals in $\mathcal{O}_K$; $n_i \in \mathbb{Z}$

This means

$$\mathcal{J}(K) \simeq \bigoplus_{\substack{\text{non-zero} \\ \text{prime ideals} \\ \text{in } \mathcal{O}_K}} \mathbb{Z}$$

Rem $\mathcal{J}(K)$ is the group of Weil divisors on $\operatorname{Spec} \mathcal{O}_K$, sometimes denoted $\operatorname{Div}(\mathcal{O}_K)$

Inside $\mathcal{J}(K)$ we have a subgroup of principal ideals:

let $x \in K^\times$, then $\underbrace{(x)}_{x \cdot \mathcal{O}_K} \in \mathcal{J}(K)$

$y \in K^\times$ then $(xy) = (x)\cdot(y)$ in $\mathcal{J}(K)$

$\Rightarrow$ we get a group homomorphism

$$\varphi : K^\times \longrightarrow \mathcal{J}(K)$$
$$x \longmapsto (x)$$

$$\operatorname{Ker}\varphi = \{x \in K^\times \mid \underbrace{(x) = \mathcal{O}_K}_{\Downarrow\ x \in \mathcal{O}_K,\ \text{and } \exists y \in \mathcal{O}_K :\ xy = 1}\} = \mathcal{O}_K^\times$$

$\operatorname{Coker}\varphi$ – ?

<u>Def</u> $\operatorname{Coker}\varphi = \mathcal{J}(K)/\varphi(K^\times) = Cl(K)$

is called <u>ideal class group</u> of K

<u>Rem</u> $Cl(K)$ "measures" how many non-principal ideals exist in $\mathcal{O}_K$.

If $\mathcal{O}_K$ is PID $\Rightarrow \forall \mathfrak{a} \subset \mathcal{O}_K$

$\mathfrak{a} = (x)$ for some $x \in \mathcal{O}_K$

$\Rightarrow \forall I \in \mathcal{J}(K)$ $\quad I = \mathfrak{a}_1/\mathfrak{a}_2 = (x_1)/(x_2)$

$= (x_1/x_2) \Rightarrow I$ is also principal

$\Rightarrow \varphi$ is surj., and $Cl(K) = 1$

The converse also true: $Cl(K)=1 \Leftrightarrow \mathcal{O}_K$ is PID

Goal: prove that $Cl(K)$ is finite.

<u>Example</u> $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

$\mathfrak{p} = (2, 1+\sqrt{-5})$, $\mathfrak{q} = (3, 1+\sqrt{-5})$

prime ideals but not principal

(Exercise 3.3.(1))

<u>Notation:</u> $I \in \mathcal{J}(K) \Rightarrow [I] \in Cl(K)$

the image of I in $Cl(K)$

$[\mathfrak{p}] \neq 1$, $[\mathfrak{q}] \neq 1$ in $Cl(K)$

$[\mathfrak{p}]^2 = [\mathfrak{p}^2]$

$$\mathfrak{p}^2 = (4, 2+2\sqrt{-5}, (1+\sqrt{-5})^2) = (4, 2+2\sqrt{-5}, -4+2\sqrt{-5})$$

$2\sqrt{-5} = 4 - 4 + 2\sqrt{-5} \in \mathfrak{p}$; $2 + 2\sqrt{-5} - 2\sqrt{-5} = \underset{\mathfrak{p}}{\underset{\cap}{2}}$

$\Rightarrow \mathfrak{p}^2 = (2)$ principal

$\Rightarrow [\mathfrak{p}]^2 = 1$

$[\mathfrak{p}] \cdot [\mathfrak{q}] = [\mathfrak{p} \cdot \mathfrak{q}] = 1$, because

$\mathfrak{p} \cdot \mathfrak{q} = (1+\sqrt{-5})$ – Exercise 3.3 (2)

$\Rightarrow [\mathfrak{q}] = [\mathfrak{p}]^2 \cdot [\mathfrak{q}] = [\mathfrak{p}]$

In fact, $Cl(K) \simeq \mathbb{Z}/2\mathbb{Z}$ in this case.

<u>Recall from Lecture 5</u>

$$\underset{\text{as } \mathbb{Z}\text{-module}}{\mathbb{Z}^n \simeq} \mathcal{O}_K \subset \underset{\text{as } \mathbb{Q}\text{-vector space}}{K \simeq} \mathbb{Q}^n \hookrightarrow \mathbb{R}^n \simeq K \otimes_{\mathbb{Q}} \mathbb{R}$$

$\mathcal{O}_K$ is a lattice in $\mathbb{R}^n$, i.e.
$\exists$ a basis in $\mathbb{R}^n$ $e_1, \dots, e_n \in \mathcal{O}_K$, s.t.
$\mathcal{O}_K = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_n$;
$\mathfrak{a} \subset \mathcal{O}_K$ an ideal $\Rightarrow$ $\mathfrak{a}$ is a sublattice in $\mathcal{O}_K$; $\mathfrak{a} = \mathbb{Z}\cdot e_1' \oplus \dots \oplus \mathbb{Z}e_n'$
$e_i' \in \mathfrak{a}$

If $x \in K^\times$, then $x \cdot \mathfrak{a} =$
$= \mathbb{Z}\cdot(xe_1') \oplus \dots \oplus \mathbb{Z}(xe_n')$
also a lattice
$\forall$ $I \in \mathcal{J}(K)$ is of the form
$x \cdot \mathfrak{a}$ for some $x \in K^\times$, $\mathfrak{a} \subset \mathcal{O}_K$
$\Rightarrow$ I is a lattice in $\mathbb{R}^n$

The norm of a fractional ideal

Assume that $\Lambda_1, \Lambda_2 \subset K \simeq \mathbb{Q}^n \hookrightarrow \mathbb{R}^n$ are two lattices.

Let $A \in \mathrm{End}_{\mathbb{Q}}(K)$ be such that

$A(\Lambda_1) = \Lambda_2$,

e.g. choose bases $\Lambda_1 = \langle e_1 \dots e_n \rangle$

$\Lambda_2 = \langle e_1' \dots e_n' \rangle$

let $Ae_i = e_i'$

<u>Def</u> The index $[\Lambda_1 : \Lambda_2] = |\det A| \in \mathbb{Q}_{>0}$

<u>Lemma</u> $[\Lambda_1 : \Lambda_2]$ is well-defined, i.e. does not depend of the choice of A

<u>Proof</u> Let $A' \in \mathrm{End}_{\mathbb{Q}}(K)$ s.t.

$A'(\Lambda_1) = \Lambda_2$

$B = (A')^{-1} \cdot A \quad \Rightarrow \quad B(\Lambda_1) = \Lambda_1$

$\Downarrow$

the matrix of B in the basis $e_1 \dots e_n$ consists of integers, because $|\det B| = 1$

$\Rightarrow \det A \cdot (\det A')^{-1} = 1 \quad \square$

<u>Rem</u> The index is multiplicative:

$\Lambda_1, \Lambda_2, \Lambda_3 \subset K$ lattices

$$[\Lambda_1 : \Lambda_2] = [\Lambda_1 : \Lambda_3] \cdot [\Lambda_3 : \Lambda_2]$$

(exercise)

<u>Def</u> Let $I \in \mathcal{J}(K)$. The norm of I is

$$\mathrm{Norm}(I) = [\mathcal{O}_K : I] \in \mathbb{Q}_{>0}$$

<u>Proposition 10.1</u> Properties of the norm:

1) $\forall \mathfrak{a} \subset \mathcal{O}_K$ ideal $\mathrm{Norm}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ (i.e. the usual index of $\mathfrak{a}$ in $\mathcal{O}_K$)

2) $\forall I \in \mathcal{J}(K)$, $x \in K^\times$, then

$$\mathrm{Norm}(x \cdot I) = |N_{K/\mathbb{Q}}(x)| \cdot \mathrm{Norm}(I)$$

3) $I_1, I_2 \in \mathcal{J}(K)$, then

$$\mathrm{Norm}(I_1 \cdot I_2) = \mathrm{Norm}(I_1) \cdot \mathrm{Norm}(I_2),$$ i.e.

$$\mathrm{Norm}: \mathcal{J}(K) \longrightarrow \mathbb{Q}_{>0}$$ is a multiplicative group homomorphism.

<u>Proof</u> 1) $\mathrm{Norm}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$ in the sense defined above.

Let $\underset{\mathfrak{a}}{\underset{\parallel}{\Lambda_2}} \subset \underset{\mathcal{O}_K}{\underset{\parallel}{\Lambda_1}} \subset K$

We can find a basis $\Lambda_1 = \langle e_1 \dots e_n \rangle$,
s.t. $\Lambda_2 = \langle d_1 e_1, \dots, d_n e_n \rangle$ for some $d_i \in \mathbb{Z}$

Then $A = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$ $\quad A(\Lambda_1) = \Lambda_2$

$$[\Lambda_1 : \Lambda_2] = \det A = \prod_{i=1}^{n} d_i = \left| \prod_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z} \right|$$

$$= |\Lambda_1 / \Lambda_2|$$

2) $\mathrm{Norm}(x \cdot I) = [\mathcal{O}_K : xI] \overset{\text{Remark above}}{=}$

$$= [\mathcal{O}_K : I] \cdot [I : xI] = \mathrm{Norm}(I) [I : xI]$$

$[I : xI] = |\det A|$, where
$A =$ multiplication by x
$\det A$ is by definition $N_{K/\mathbb{Q}}(x)$

3) $I_1 = x \cdot \mathfrak{a}_1$, $I_2 = y \cdot \mathfrak{a}_2$ for some $x, y \in K^\times$, $\mathfrak{a}_1, \mathfrak{a}_2 \subset \mathcal{O}_K$ ideals

$$\mathrm{Norm}(I_1 I_2) = \mathrm{Norm}(xy \cdot \mathfrak{a}_1 \mathfrak{a}_2)$$

$$\overset{2)}{=} |N_{K/\mathbb{Q}}(x)| \cdot |N_{K/\mathbb{Q}}(y)| \cdot \mathrm{Norm}(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$$

$\Rightarrow$ enough to prove $Norm(\mathfrak{a}_1 \cdot \mathfrak{a}_2) =$
$= Norm(\mathfrak{a}_1) \cdot Norm(\mathfrak{a}_2)$

Write: $\mathfrak{a}_1 = \prod_{i=1}^{k} \mathfrak{p}_i^{n_i}$; $\mathfrak{a}_2 = \prod_{i=1}^{k} \mathfrak{p}_i^{m_i}$

$n_i, m_i \geq 0$

$$Norm(\mathfrak{a}_1 \mathfrak{a}_2) \overset{1)}{=} \left| \mathcal{O}_K / \mathfrak{a}_1 \mathfrak{a}_2 \right|$$

By CRT:

$$\mathcal{O}_K / \mathfrak{a}_1 \mathfrak{a}_2 \simeq \prod_{i=1}^{k} \mathcal{O}_K / \mathfrak{p}_i^{n_i + m_i}$$

Remains to check: $\left| \mathcal{O}_K / \mathfrak{p}_i^{n_i + m_i} \right| = \left| \mathcal{O}_K / \mathfrak{p}_i^{n_i} \right| \cdot \left| \mathcal{O}_K / \mathfrak{p}_i^{m_i} \right|$

<u>Lemma</u> $\left| \mathcal{O}_K / \mathfrak{p}^n \right| = \left| \mathcal{O}_K / \mathfrak{p} \right|^n$ for any prime $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$, $n \geq 1$

<u>Proof</u> We have a subgroup

$$\mathfrak{p}^{n-1} / \mathfrak{p}^n \hookrightarrow \mathcal{O}_K / \mathfrak{p}^n$$

$\begin{matrix} \wr\| \\ \mathcal{O}_K / \mathfrak{p} \end{matrix} \longleftarrow$ Corollary 9.4.

$$\left(\mathcal{O}_K/p^n\right)\Big/\left(p^{n-1}/p^n\right) \cong \mathcal{O}_K/p^{n-1}$$

$$\Rightarrow \left|\mathcal{O}_K/p^n\right| = \left|\mathcal{O}_K/p^{n-1}\right| \cdot \left|p^{n-1}/p^n\right|$$

$$= \left|\mathcal{O}_K/p^{n-1}\right| \cdot \left|\mathcal{O}_K/p\right|$$

by induction on n get the claim $\square$

This completes the proof of Prop. 10.1.

<u>Proposition 10.2</u> $\forall d > 0$ $\exists$ only finitely many ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $\operatorname{Norm}(\mathfrak{a}) \leq d$

<u>Proof</u> $\operatorname{Norm}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$ index of the subgroup $\mathfrak{a} \subset \mathcal{O}_K$

$$\left|\mathcal{O}_K/\mathfrak{a}\right| \leq d \Rightarrow d\cdot\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$$

Then $\mathfrak{a}$ is the preimage of

$$\mathfrak{a}/d\mathcal{O}_K \subset \mathcal{O}_K/d\cdot\mathcal{O}_K$$

under the quotient map $\mathcal{O}_K \to \mathcal{O}_K/d\mathcal{O}_K$

$\Rightarrow \mathfrak{a}$ is uniquely determined by the choice of a subgroup in $\mathcal{O}_K / d \cdot \mathcal{O}_K$, but

$\mathcal{O}_K / d \cdot \mathcal{O}_K$ is a finite group

$\Rightarrow$ it contains only fin. many subgroups $\Rightarrow$ only fin. many possibilities for $\mathfrak{a}$. $\square$

<u>Rem</u> To prove that $Cl(K)$ is finite it is enough to show that $\exists d > 0$, s.t. $\forall$ element of $Cl(K)$ is represented by an ideal $\mathfrak{a}$ with $\mathrm{Norm}(\mathfrak{a}) \leq d$.