

Lecture 1 (03-01-2022)

03 January 2022 17:27

Did chapter 1 of Number Fields. Characterised Pythagorean triples and talked about regular primes.

Lecture 2 (06-01-2022)

06 January 2022 17:30

Recall: Algebraic integers.

- $K \subseteq \mathbb{C}$ is a **number field** if $\dim_{\mathbb{Q}} K < \infty$.

In this case, $K = \mathbb{Q}[\alpha]$ for some $\alpha \in K$. α here will be algebraic over \mathbb{Q} .

$f = \min_{\mathbb{Q}}(\alpha) \in \mathbb{Q}[x]$ denotes the monic irreducible polynomial satisfied by α over \mathbb{Q} .

If $f \in \mathbb{Z}[x]$, then α is called an **algebraic integer**.

Equivalent definition: α satisfies some monic polynomial in $\mathbb{Z}[x]$
(Need to verify that equivalent!)

- Theorem. Let $\alpha \in \mathbb{C}$. TFAE:

- α is an algebraic integer.
- $\mathbb{Z}[x]$ is f.g. as a group.
- \exists a subring $A \subset \mathbb{C}$ s.t. $\alpha \in A$ and A is f.g. as a group.
- \exists a f.g. subgroup $A \subset \mathbb{C}$ with $A \neq 0$ s.t. $\alpha A \subseteq A$.

- Corollary. $A := \{\alpha \in \mathbb{C} : \alpha \text{ is an alg. int.}\}$ is a subring of \mathbb{C}

- let $K \subseteq \mathbb{C}$ be a number field. Then,

$\mathcal{O}_K := A \cap K$ is called the **number ring** of K .

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Let $m \in \mathbb{Z}$ be square-free. Then,

$$\mathcal{O}_{\sqrt{m}} = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2, 3 \pmod{4} \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{if } m \equiv 1 \pmod{4} \end{cases}$$

$$\Theta_{\mathbb{Q}(\sqrt{m})} = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{if } m \equiv 1 \pmod{4} \end{cases}$$

↳ Exercise, can show with machinery so far.

- $\omega = e^{\frac{2\pi i}{m}}$. Then, $\Theta_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega]$. \rightarrow will show later!

- Theorem: $\Theta [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$.

② $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois.

③ $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$.

④ Recall: $m = p_1^{r_1} \cdots p_t^{r_t}$, then

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1} \times \cdots \times \mathbb{Z}/p_t^{r_t},$$

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{r_1})^* \times \cdots \times (\mathbb{Z}/p_t^{r_t})^*.$$

• p : prime > 2 , then $(\mathbb{Z}/p^r)^*$ is cyclic.

$$(\mathbb{Z}/2)^* = \langle 1 \rangle,$$

$$(\mathbb{Z}/2^2)^* \cong \mathbb{C}_2,$$

$$(\mathbb{Z}/2^n)^* \cong \mathbb{C}_2 \times \mathbb{C}_{2^{n-2}} \quad \text{for } n \geq 3.$$

• $(\mathbb{Z}/p)^* \cong \mathbb{C}_{p-1} \quad \forall p \text{ prime.}$

⑤ Let $p > 2$ be a prime. ($\omega := e^{\frac{2\pi i}{p}}$)

Then, $G = \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ has order $p-1$ and is cyclic.

$$\therefore \exists ! H \leq G \text{ s.t. } |H| = \frac{p-1}{2}.$$

$(\mathbb{Q}(\omega))^H$ is the unique quadratic

$$H \left(\begin{array}{c} \mathbb{Q}(\omega) \\ | \end{array} \right)$$

$\mathbb{Q}[\omega]^H$ is the unique quadratic ext^H of \mathbb{Q} contained in $\mathbb{Q}[\omega]$.

$$\mathbb{Q}[\omega]^H \quad | \quad \deg = 2$$

As we shall see,

Q

$$\mathbb{Q}[\omega]^H = \mathbb{Q}[\sqrt{\pm p}], \quad + \text{ if } p \equiv 1 \pmod{4}, \\ - \text{ if } p \equiv 3 \pmod{4}.$$

6 Roots of unity in $\mathbb{Q}[\omega]$.

Theorem. Let $m \geq 3$. $\omega := e^{2\pi i/m}$. Let $\eta \in \mathbb{Q}[\omega]$ be a root of unity.

Then, $\eta^m = 1$ if m even,
 $\eta^{2m} = 1$ if m odd.

Proof.

Suffices to prove when m even.
 $(m \text{ odd} \Rightarrow (-\omega) \text{ primitive } 2m^{\text{th}} \text{ root of 1})$

Let n be s.t. $\eta^n = 1$.

Suffices to show $n \mid m$.

By elementary group theory, $\mathbb{Q}[\omega]^x$ contains an ℓ^{th} primitive root of 1, with $\ell = \text{lcm}(m, n)$.

Thus, $\mathbb{Q}[\omega] \subset \mathbb{Q}[e^{2\pi i/\ell}] \subset \mathbb{Q}[\omega]$.

$$\Rightarrow \varphi(m) = \varphi(\ell). \quad \therefore m \mid \ell.$$

$$\Rightarrow m = \ell.$$

QED

Corollary. The fields $\{\mathbb{Q}[e^{2\pi i/m}]\}_{m \geq 2}$ are pairwise non-isomorphic.

Lecture 3 (10-01-2022)

10 January 2022 17:27

Defn.

Let $K \subseteq C$ be a degree n "ext" of \mathbb{Q} .

Let $\sigma_1, \dots, \sigma_n$ be the n embeddings of K/\mathbb{Q} in C .

Recall the functions trace and norm:

$$\text{Tr}_{K/\mathbb{Q}} : K \rightarrow \mathbb{Q} \quad \text{and}$$

$$N_{K/\mathbb{Q}} : K \rightarrow \mathbb{Q}$$

defined as

$$\text{Tr}_{K/\mathbb{Q}}(\beta) = \sum_{i=1}^n \sigma_i(\beta),$$

$$N_{K/\mathbb{Q}}(\beta) = \prod_{i=1}^n \sigma_i(\beta).$$

A priori, not clear why $\text{Tr}_{K/\mathbb{Q}}$ and $N_{K/\mathbb{Q}}$ are \mathbb{Q} -valued.

This is a fact from Galois theory.

- We may drop the subscript if no confusion.

From definition, it is clear that $\text{Tr}_{K/\mathbb{Q}}$ is additive and $N_{K/\mathbb{Q}}$ is multiplicative. Thus, both are homomorphisms interpreted with correct domain and operation.

- Properties:

$$\text{Tr}(1) = [K : \mathbb{Q}], \quad N(1) = 1.$$

More generally:

$$\text{Tr}(r) = nr, \quad N(r) = r^n \quad \text{for } r \in \mathbb{Q}.$$

If $r \in \mathbb{Q}$, $\beta \in K$, then $\text{Tr}(r\beta) = r \cdot \text{Tr}(\beta)$,
 $N(r\beta) = r^n \cdot N(\beta)$.

In particular, Tr is \mathbb{Q} -linear.

- Write $K = \mathbb{Q}[\alpha]$. Let $f = \min_{\mathbb{Q}} \alpha \in \mathbb{Q}[x]$.

Then,

$$f = (x - \sigma_1 \alpha)(x - \sigma_2 \alpha) \cdots (x - \sigma_n \alpha).$$

II) $\text{Tr}_{K/\mathbb{Q}}(\alpha) = -\text{coeff. of } x^{n-1} \in \mathbb{Q}.$

$$\text{N}_{K/\mathbb{Q}}(\alpha) = (-1)^n f(0) \in \mathbb{Q}$$

Now, consider a general element $\beta \in K$.

Let m and l be the degrees as shown:
 $n = ml$.

$$\begin{array}{c} K \\ |^m \\ \mathbb{Q}[\beta] \\ |^l \\ \mathbb{Q} \end{array}$$

Let $\theta_1, \dots, \theta_l$ be embeddings of $\mathbb{Q}[\beta]/\mathbb{Q}$.

Extend each θ_i to an embedding K/\mathbb{Q} .

This will give us all the $\{\sigma_i\}_{i=1}^n$.

Thus, $\text{Tr}_{K/\mathbb{Q}}(\beta) = m \cdot \text{Tr}_{\mathbb{Q}[\beta]/\mathbb{Q}}(\beta) \in \mathbb{Q}$ and

$$\text{N}_{K/\mathbb{Q}}(\beta) = (\text{N}_{\mathbb{Q}[\beta]/\mathbb{Q}}(\beta))^m \in \mathbb{Q}.$$

now β plays the role of α .

Corollary. If $\beta \in \mathcal{O}_K$, then $\text{Tr}_{K/\mathbb{Q}}(\beta), \text{N}_{K/\mathbb{Q}}(\beta) \in \mathbb{Z}$.

Prop. Let K be a number field.

Let $\alpha \in \mathcal{O}_K$.

$$\alpha \text{ is a unit in } \mathcal{O}_K \iff N(\alpha) = \pm 1.$$

Proof. $(\Rightarrow) \alpha \beta = 1 \Rightarrow N(\alpha) N(\beta) = 1 \Rightarrow N(\alpha) = \pm 1$ since $N(\alpha), N(\beta) \in \mathbb{Z}$.

(\Leftarrow) Clearly, $\alpha \neq 0$.

Thus, $\frac{1}{\alpha} \in K$

Since $N(\alpha) = \pm 1$, we have $\frac{1}{\alpha} = \pm \alpha_2 \alpha_3 \cdots \alpha_n$,

where $\alpha_2, \dots, \alpha_n$ are the other conjugates of α .

They satisfy same polynomial.

$$\therefore \alpha_2, \dots, \alpha_n \in A.$$

$$\therefore \frac{1}{\alpha} = \pm \alpha_2 \cdots \alpha_n \in A \cap K.$$

?

Acknowledgment:

$$\min_Q \alpha = x^n + a_{n-1}x^{n-1} + \dots + a_1x + 1.$$

$$\min_Q \gamma_\alpha = x^n + (a_n x^{n-1} + \dots + a_1 x + 1).$$

Thus, we have $U(\mathcal{O}_K) = \{\alpha \in \mathcal{O}_K : N(\alpha) = \pm 1\}$.

Check: $U(\mathcal{O}_{\mathbb{Q}(\zeta_m)})$ is finite when $m < 0$.

Moreover, $U(\mathcal{O}_{\mathbb{Q}(\zeta_m)}) = \{\pm 1\}$ if $m < -3$.

Remark: If $N(\alpha)$ is prime ($\alpha \in \mathcal{O}_K$), then α is irreducible in \mathcal{O}_K .

Exercise: Use norm and trace to show $\sqrt{3} \notin \mathbb{Q}[\sqrt[4]{2}]$.

Transitivity: We can define $\text{Tr}_{L/K} : L \rightarrow K$ for number fields $K \subseteq L$.

Suppose we have extensions $K \subseteq L \subseteq M$. Then, we have

$$\text{Tr}_{M/K} = \text{Tr}_{M/L} \circ \text{Tr}_{L/K} \quad \text{and} \quad N_{M/K} = N_{M/L} \circ N_{L/K}.$$

Def'n.: $K/\mathbb{Q} \rightarrow \text{deg } n$.

$\sigma_1, \dots, \sigma_n \rightarrow$ embeddings of K/\mathbb{Q} in \mathbb{C} .

Let $\alpha_1, \dots, \alpha_n \in K$ be arbitrary.

Define $A = (a_{ij})_{nm}$ by $a_{ij} = \sigma_i(\alpha_j)$.

We define the **discriminant** of $\alpha_1, \dots, \alpha_n$ by

$$\text{disc}_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = \det(A)^2 = \det([\sigma_i(\alpha_j)])^2.$$

Remark: The above is well-defined since we are squaring (and thus, order does not matter).

Theorem: $\text{disc}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)) \in \mathbb{Q}$.

Proof.: $(\sigma_i \alpha_j)^T (\sigma_i \alpha_j) = \begin{pmatrix} \sigma_1 \alpha_1 & \dots & \sigma_n \alpha_1 \\ \vdots & \ddots & \vdots \\ \sigma_1 \alpha_n & \dots & \sigma_n \alpha_n \end{pmatrix} \begin{pmatrix} \sigma_1 \alpha_1 & \dots & \sigma_1 \alpha_n \\ \vdots & \ddots & \vdots \\ \sigma_n \alpha_1 & \dots & \sigma_n \alpha_n \end{pmatrix}$

$$\begin{aligned}
 & \left(\begin{array}{cccc|c} \cdot & \cdots & \cdot & \cdots & \sigma_{1dn} & \cdots & \sigma_{ndn} \\ \sigma_{1dn} & \cdots & \sigma_{ndn} & & \sigma_{1dn} & \cdots & \sigma_{ndn} \end{array} \right) \\
 &= \begin{pmatrix} \sum (\sigma_i \alpha_i)^2 & \cdots & \sum (\sigma_i \alpha_i)(\sigma_j \alpha_j) \\ \vdots & \ddots & \vdots \end{pmatrix} \\
 &= \begin{pmatrix} \text{Tr}(\alpha_1^2) & \cdots & \text{Tr}(\alpha_1 \alpha_n) \\ \vdots & \ddots & \vdots \end{pmatrix}
 \end{aligned}$$

Take det.

b)

Theorem: $K/\mathbb{Q} \rightarrow \deg n$.

Let $\alpha_1, \dots, \alpha_n \in K$.

$\alpha_1, \dots, \alpha_n$ are lin. dep over $\mathbb{Q} \Leftrightarrow \text{disc}(\alpha_1, \dots, \alpha_n) = 0$.

Proof. (\Rightarrow) clear. The rows in def' of the matrix satisfy some dependency.

(\Leftarrow) Assume $\alpha_1, \dots, \alpha_n$ are lin. indep over \mathbb{Q} . Thus, they form a basis for K/\mathbb{Q} . Moreover, given any $\alpha \in K^\times$, $\{\alpha \alpha_1, \dots, \alpha \alpha_n\}$ is a \mathbb{Q} -basis for K .

Suppose $\text{disc} = 0$. Then, $\det \begin{pmatrix} \text{Tr}(\alpha_1 \alpha_1) & \cdots & \text{Tr}(\alpha_1 \alpha_n) \\ \vdots & \ddots & \vdots \\ \text{Tr}(\alpha_n \alpha_1) & \cdots & \text{Tr}(\alpha_n \alpha_n) \end{pmatrix} = 0$.

$\therefore \exists r_1, \dots, r_n \in \mathbb{Q}$ not all 0 s.t

$$r_1 \begin{pmatrix} \text{Tr}(\alpha_1 \alpha_1) \\ \vdots \\ \text{Tr}(\alpha_n \alpha_1) \end{pmatrix} + \cdots + r_n \begin{pmatrix} \text{Tr}(\alpha_1 \alpha_n) \\ \vdots \\ \text{Tr}(\alpha_n \alpha_n) \end{pmatrix} = 0.$$

Let $\alpha := r_1 \alpha_1 + \cdots + r_n \alpha_n \neq 0$.

we have

$$\text{Tr}(\alpha_1 \alpha) = \text{Tr}(\alpha_2 \alpha) = \dots = \text{Tr}(\alpha_n \alpha) = 0.$$

$\therefore \text{Tr} = 0$ on a basis of K over \mathbb{Q} .

$\because \text{Tr}$ is \mathbb{Q} -linear, this gives $\text{Tr} = 0$.
but $\text{Tr}(1) = n \neq 0 \rightarrow \square$

Lecture 4 (13-01-2022)

13 January 2022 17:27

Remark: The last theorem also shows that if $\alpha_1, \dots, \alpha_n \in \mathbb{D}_K$, then $\text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.

Theorem: Let $K = \mathbb{Q}[\alpha]$ be a deg n ext^h of \mathbb{Q} .

Let $f = \min_{\mathbb{Q}} \alpha \in \mathbb{Q}[\alpha]$.

Let $\alpha_1, \dots, \alpha_n$ be the n conjugates of α in \mathbb{C} .
Then,

$$\begin{aligned} \text{disc}(1, \alpha, \dots, \alpha^{n-1}) &= \prod_{r < s} (\alpha_r - \alpha_s)^2 \\ &= \pm N_{K/\mathbb{Q}}(f'(\alpha)). \end{aligned}$$

+ iff $n(n-1)/2 \in 2\mathbb{Z}$ iff $n \equiv 0, 1 \pmod{4}$.

Proof: Let $\sigma_1, \sigma_2, \dots, \sigma_n$ be the n -embeddings of K/\mathbb{Q} in \mathbb{C} .

$$\begin{aligned} \text{disc}(1, \alpha, \dots, \alpha^{n-1}) &= \det(\sigma_i(\alpha^{j-1}))^2 \\ &= \det(\sigma_i(\alpha^{j-1}))^2 \end{aligned}$$

$$\begin{aligned} &= \det \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{n-1} \end{pmatrix} \\ &= \prod_{i < j} (\alpha_i - \alpha_j)^2. \quad \text{--- (1)} \end{aligned}$$

Vandermonde

$$f(x) = \prod_{i=1}^n (x - \alpha_i)$$

$$\Rightarrow f'(x) = \sum_{i=1}^n (x - \alpha_1) \dots \widehat{(x - \alpha_i)} \dots (x - \alpha_n)$$

$$\Rightarrow f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j). \quad \text{--- (2)}$$

$$\begin{aligned}
 N_{K/\mathbb{Q}}(f'(\alpha)) &= \prod_{i=1}^n \sigma_i(f'(\alpha)) \\
 &= \prod_{i=1}^n f'(\sigma_i(\alpha)) \\
 &= \prod_{i=1}^n f'(\alpha_i).
 \end{aligned}$$

$f' \in \mathbb{Q}[x]$

By (1) and (2), we are now done.

Corollary

$$K = \mathbb{Q}[\omega], \quad \omega = e^{2\pi i/p}, \quad p > 2 \text{ prime.}$$

$$\text{disc}(1, \omega, \dots, \omega^{p-1}) = \pm N(f'(\omega)) = \pm p^{p-2}.$$

Proof. $f = \frac{x^p - 1}{x - 1} = x^{p-1} + \dots + 1.$

$$\begin{aligned}
 (x-1)f &= x^{p-1} \Rightarrow f + (x-1)f = p x^{p-1} \\
 \Rightarrow f'(\omega) &= \frac{p\omega^{p-1}}{\omega-1} = \frac{p}{\omega(\omega-1)} \\
 \Rightarrow N(f'(\omega)) &= \frac{p^{p-1}}{1 \cdot p} = p^{p-2}.
 \end{aligned}$$

$$\therefore \text{disc}(1, \omega, \dots, \omega^{p-1}) = \pm p^{p-2}.$$

+ iff $p \equiv 1, 2 \pmod{4}$.
↑ (not possible)

Also note that $\mathbb{Q}[\omega]/\mathbb{Q}$ is a Galois extn. Thus, $\sigma_i \omega \in \mathbb{Q}[\omega]$

Vi. $\therefore \det(\sigma_i \omega^{j-1}) \in \mathbb{Q}[\omega].$

$$\begin{aligned}
 \Rightarrow \sqrt{\pm p^{p-2}} &\in \mathbb{Q}[\omega]
 \end{aligned}$$

$$\Rightarrow \boxed{\sqrt{\pm p} \in \mathbb{Q}[\omega]}$$

+ iff $p \equiv 1 \pmod{4}$.

Notation: Let $\alpha \in \mathbb{C}$ be algebraic of degree n .

Then, $1, \alpha, \dots, \alpha^{n-1}$ is a basis of $\mathbb{Q}(\alpha)/\mathbb{Q}$.

$$\text{disc}(\alpha) := \text{disc}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(1, \alpha, \dots, \alpha^{n-1}).$$

$$p > 2 \text{ prime : } \text{disc}(e^{2\pi i/p}) = \pm p^{p-2}.$$

Cor: Prime factors of $\text{disc}(\omega)$ involve p only we now show a similar result for non-primes.

Now, let $\omega^1 = e^{2\pi i/m}$, $m > 2$ is any integer.

Let $f(x) := \min_{\alpha} (\omega) \in \mathbb{Z}[x]$, $\deg(f) = \varphi(m)$.

$$x^m - 1 = f(x) \cdot g(x) \quad \text{in } \mathbb{Z}[x].$$

$$\begin{aligned} \text{disc}(\omega) &= \text{disc}(1, \omega, \dots, \omega^{\varphi(m)-1}) \\ &= \pm N_{\mathbb{Q}(\omega)/\mathbb{Q}}(f'(\omega)). \end{aligned}$$

$$\frac{d}{dx} \rightarrow m \cdot x^{m-1} = f'g + fg'$$

$$\stackrel{x=\omega}{\Rightarrow} m \cdot \omega^{m-1} = f'(\omega)g(\omega)$$

$$\stackrel{\text{take } N \text{ note } \omega \text{ is unit}}{\Rightarrow} m^{\varphi(m)} \cdot (\pm 1) = N(f'(\omega)) \cdot N(g(\omega))$$

$$\begin{aligned} &\mathbb{Z}[\omega] \\ &\because g(\omega) \in \mathbb{Q} \subset \mathbb{Z}[\omega] \\ &\therefore N(g(\omega)) \in \mathbb{Z} \end{aligned}$$

$$\begin{aligned} \therefore N(f'(\omega)) &\mid m^{\varphi(m)} \\ &\pm \text{disc}(\omega) \end{aligned}$$

$$\therefore \{\text{prime factors of } \text{disc}(\omega)\} \subseteq \{\text{prime factors of } m\}.$$

Recall:

Defn. Let G be a f.g. abelian group.

G is said to be free if $G \cong \mathbb{Z}^n$ for some $n \in \mathbb{N}_0$.

n is uniquely determined and is called the rank of G .

$$(G/\mathbb{Z}_G \cong (\mathbb{Z}/2\mathbb{Z})^n) \therefore n = \log_2 |G/\mathbb{Z}_G|$$

Facts: $G \cong \mathbb{Z}^n$

- Any subgroup of G is also free of rank $\leq n$.

$A \leq B \leq G$ with A of rank $n \Rightarrow B$ is free of rank n .

- K/\mathbb{Q} : deg n .

Pick a basis $\alpha_1, \dots, \alpha_n$ of K/\mathbb{Q} .

Upon multiplication with appropriate (nonzero) integers, we may assume $\alpha_i \in \mathcal{O}_K$.

$$\sum_{i=1}^n \mathbb{Z} \alpha_i \subseteq \mathcal{O}_K.$$

free of rank n ($\{\alpha_1, \dots, \alpha_n\}$ is a \mathbb{Z} -basis)

Theorem

$K/\mathbb{Q} \rightarrow \deg n$.

$\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ basis of K/\mathbb{Q} .

$d := \text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z} \setminus \{0\}$.

Every $\alpha \in \mathcal{O}_K$ can be written as

$$\frac{m_1 \alpha_1 + \dots + m_n \alpha_n}{d} \quad (3)$$

with $m_i \in \mathbb{Z}$ with $d \mid m_i^2$.

$$\text{Gr. 0} \quad \sum_{i=1}^n \mathbb{Z} \alpha_i \subseteq \mathcal{O}_K \subseteq \sum_{i=1}^n \mathbb{Z} \frac{\alpha_i}{d}. \quad (4)$$

In particular, \mathcal{O}_K is a free abelian group of rank n .

② If d is square-free, then $d \mid m_i^2 \Leftrightarrow d \mid m_i$.

By (3), $\mathcal{O}_K \subseteq \sum \mathbb{Z} \alpha_i$.

By (4), we get $\mathcal{O}_K = \sum \mathbb{Z} \alpha_i$.

Defⁿ: \mathcal{O}_K : free abelian group of rank n .

$\{\alpha_1, \dots, \alpha_n\}$ \rightarrow bases of $\mathcal{O}_K / \mathbb{Z}$.
 $\{\beta_1, \dots, \beta_n\}$ \rightarrow

Then, $\text{disc}(\alpha_1, \dots, \alpha_n) = \text{disc}(\beta_1, \dots, \beta_n)$

Thus, $\text{disc}(\mathcal{O}_K) := \text{disc}(\alpha_1, \dots, \alpha_n)$ is well-defined.

We can write $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = A \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$ for some $A \in GL_n(\mathbb{Z})$.

Then, $\begin{pmatrix} \sigma_1 \alpha_1 & \cdots & \sigma_n \alpha_1 \\ \vdots & \ddots & \vdots \\ \sigma_1 \alpha_n & \cdots & \sigma_n \alpha_n \end{pmatrix} = A \begin{pmatrix} \sigma_1 \beta_1 & \cdots & \sigma_n \beta_1 \\ \vdots & \ddots & \vdots \\ \sigma_1 \beta_n & \cdots & \sigma_n \beta_n \end{pmatrix}$.

Since $\det(A^T) = 1$, we are done. □

Lecture 5 (17-01-2022)

17 January 2022 17:32

Theorem

$$K/\mathbb{Q} \rightarrow \deg n.$$

$\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$: basis of K/\mathbb{Q} .

$$d := \text{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z} \setminus \{0\}.$$

Every element of \mathcal{O}_K can be written as

$$\frac{m_1 \alpha_1 + \dots + m_n \alpha_n}{d}; \quad m_i \in \mathbb{Z}, \quad d \mid m_i^2.$$

Proof.

Let $\alpha \in \mathcal{O}_K$.

$$\alpha = x_1 \alpha_1 + \dots + x_n \alpha_n; \quad x_i \in \mathbb{Q}.$$

$\sigma_1, \dots, \sigma_n \rightarrow$ embeddings.

$$\sigma_i(\alpha) = x_1 \sigma_i(\alpha_1) + \dots + x_n \sigma_i(\alpha_n). \quad (i=1, \dots, n)$$

$$\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

\uparrow
 $GL_n(\mathbb{C})$

By Cramer's rule,

$$x_j = \frac{y_j}{\delta},$$

$$y_j = \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) & \dots \\ \vdots & \ddots & \vdots & \ddots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) & \dots \end{pmatrix}$$

$$\delta^2 = d, \quad y_j \rightarrow \text{alg. integer}.$$

$$\therefore d x_j = \delta y_j.$$

\uparrow
 \mathbb{Q}

\downarrow
 \mathbb{A}

$$\therefore \delta y_j \in \mathbb{Z}.$$

$$\text{Write } m_j := \delta y_j \in \mathbb{Z}.$$

$$\text{Then } d \mid m_j^2 - x_j \cdot d.$$

Then, $d \mid m_j^2$, as desired. □

Defn. Any basis $\alpha_1, \dots, \alpha_n$ of \mathcal{O}_K/\mathbb{Z} is called an integral basis of \mathcal{O}_K .

Had seen: any two integral bases have the same discriminant.

EXAMPLES: $K = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ squarefree.

$$\begin{aligned} \bullet m = 2, 3 \text{ (4). } & \{1, \sqrt{m}\} \rightarrow \text{integral basis.} \\ \text{disc}(K) = & \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = (-2\sqrt{m})^2 = 4m. \end{aligned}$$

$$m = 1 \quad (4).$$

$$\text{disc}(K) = \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = m.$$

Theorem: $m = p^r$, p prime. $\omega := e^{2\pi i/m}$.

Then,

$$\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega].$$

$$(K := \mathbb{Q}[\omega])$$

Proof. (i) $\mathbb{Z}[\omega] = \mathbb{Z}[1-\omega]$.

(ii) $\text{disc}(\omega) = \prod_{i < j} (\alpha_i - \alpha_j)^2$

$(\alpha_i \rightarrow \text{conjugates of } \omega)$

$\{1, 1-\omega, (1-\omega)^2, \dots, (1-\omega)^{\varphi(m)-1}\}$ is a basis of K/\mathbb{Q} .

$$\text{disc}(1-\omega) = \prod_{i < j} \left((1-\alpha_i) - (1-\alpha_j) \right)^2$$

$$= \prod_{i < j} (\alpha_i - \alpha_j)^2$$

(iii) Assume $\mathbb{Z}[\omega] \subsetneq \mathcal{O}_{\mathbb{Q}(\omega)}$.

Let $n := \varphi(m)$.

by the theorem, every element of \mathcal{O}_K can be written as

$$\frac{m_1 \cdot 1 + m_2 \cdot (1-\omega) + \dots + m_{n-1} \cdot (1-\omega)^{n-1}}{d},$$

$$d := \text{disc}(\omega), \quad m_i \in \mathbb{Z}, \quad d \mid m_i^2.$$

By hypothesis, $\exists \alpha \in \mathcal{O} \setminus \mathbb{Z}[\omega]$.

(ii) We saw that $\text{disc}(\omega) \mid m^{q(m)}$
 $\therefore \text{disc}(\omega) = \pm p^s$.

Can choose $\alpha \in \mathcal{O}_K$ s.t.

$$\alpha = \frac{m_1}{p} + \frac{m_2}{p} (1-\omega) + \dots + \frac{m_{n-1}}{p} (1-\omega)^{n-1},$$

with $m_j \in \mathbb{Z}$ and $i \in [n-1]$ s.t.

- $p \nmid m_i$,
- $p \mid m_j$ for $j < i$.

Then, after subtracting an element of $\mathbb{Z}[\omega]$, we get

$$\beta \in \frac{m_i (1-\omega)^i + \dots + m_{n-1} (1-\omega)^{n-1}}{p} \in \mathcal{O}_K \setminus \mathbb{Z}[\omega].$$

$$\begin{aligned} (\text{v}) \quad N_{\mathcal{O}(\omega)/\mathbb{Q}}(1-\omega) &= \prod_{k=1}^p (1-\omega^k) && \leftarrow n \text{ factors} \\ &\quad p \nmid k \\ &= (1-\omega)^n \cdot f(\omega), && f(\omega) \in \mathbb{Z}[\omega]. \end{aligned}$$

OTOH, $N(1-\omega) = p$. (See end.)

$$\text{Thus, } (1-\omega)^n f(\omega) = p.$$

$\rightarrow 0$

$\vdash \text{all } i < n$.

$$\text{Thus, } (1-\omega)^p f(\omega) = p. \\ \rightarrow \frac{p}{(1-\omega)^j} \in \mathbb{Z}[\omega] \quad \text{for all } j \leq n.$$

$$\text{Now, } p \cdot \frac{p}{(1-\omega)^{i+1}} = \frac{m_{i-1}}{1-\omega} + \underbrace{m_i + m_{i+1}(1-\omega) + \dots +}_{\in \mathbb{Z}[\omega]}.$$

\uparrow
 Θ_k

$$\therefore \frac{m_{i-1}}{1-\omega} \in \Theta_k \setminus \mathbb{Z}[\omega]. \quad p \nmid m_{i-1}.$$

$$N\left(\frac{m_{i-1}}{1-\omega}\right) = \frac{m_{i-1}^n}{p} \notin \mathbb{Z}. \quad \rightarrow \leftarrow$$

Now, we check that $N(1-\omega) = p$.

$$f(x) = \min_{\omega} (x).$$

$$x^{p^r} - 1 = f(x) \cdot (x^{p^{r-1}} - 1).$$

$$\begin{aligned} \therefore f(x) &= \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} \\ &= \underline{y^{p-1}} \end{aligned}$$

$y = x^{p^{r-1}}$

$$\begin{aligned} &= y^{p-1} + \dots + 1. \\ &= (x^r)^{p-1} + \dots + 1. \end{aligned}$$

$$f(1) = \prod_{\substack{i=1 \\ p \nmid i}}^{p^r} (1 - \omega^i) = N(1-\omega).$$

!!

☞

Next class: $\mathbb{Q}[\omega] = \mathbb{Z}[\omega]$ for any root ω of 1.

Lecture 6 (20-01-2022)

20 January 2022 17:29

- $K/\mathbb{Q} \rightarrow \deg n.$
- $\mathcal{O}_K \rightarrow \text{free abelian of rank } n.$
- $\text{disc}(K) := \text{disc}(\mathcal{O}_K) := \text{discriminant of any } \mathbb{Z}\text{-basis of } \mathcal{O}_K.$

Exercise 2.27. $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K : \text{lin. indep } / \mathbb{Q}$

$\{\alpha_1, \dots, \alpha_n\}$ is an integral basis of \mathcal{O}_K
 $\Leftrightarrow \text{disc}(\alpha_1, \dots, \alpha_n) = \text{disc}(K).$

Soln. (\Rightarrow) by defn.

(\Leftarrow) Let $H = \langle \alpha_1, \dots, \alpha_n \rangle.$

Then, H is free of rank n .

By earlier exercise, $\text{disc}(H) = |G/H|^2 \cdot \text{disc}(G).$

By hypothesis, we get $|G/H|^2 = 1. \therefore G = H. \blacksquare$

Notation: $\omega_m := e^{2\pi i/m}$ for $m \in \mathbb{Z} \setminus \{0\}.$

Saw: $\mathcal{O}_{\mathbb{Q}[\omega]} = \mathbb{Z}[\omega]$ for $\omega = \omega_p.$

- $K, L : \text{number fields}$

$KL \rightarrow \text{the compositum is also a number field.}$

$$\mathcal{O}_K \cdot \mathcal{O}_L \subseteq \mathcal{O}_{KL}.$$

Equality may not hold.

Example. $K = \mathbb{Q}[\sqrt{3}], L = \mathbb{Q}[\sqrt{7}]$.

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{3}], \mathcal{O}_L = \mathbb{Z}[\sqrt{7}].$$

$$\mathcal{O}_K \cdot \mathcal{O}_L = \mathbb{Z}[\sqrt{3}, \sqrt{7}].$$

$(3 \cdot 7 = 1 \quad (4))$

However, $\frac{\sqrt{3} + \sqrt{7}}{2} \in \mathcal{O}_{KL} = \mathcal{O}_{\mathbb{Q}(\sqrt{3}, \sqrt{7})}$.

$$\begin{aligned} \text{Let } \alpha := \frac{\sqrt{3} + \sqrt{7}}{2}. \quad \text{Then, } \alpha^2 &= \frac{3+7+2\sqrt{21}}{4} \\ \Rightarrow \alpha^2 &= \frac{5+\sqrt{21}}{2} \\ \Rightarrow \left(\alpha^2 - \frac{5}{2}\right)^2 &= \frac{21}{4} \\ \Rightarrow \alpha^4 - 5\alpha^2 + \frac{25}{4} - \frac{21}{4} &= 0 \\ \Rightarrow \alpha^4 - 5\alpha^2 + 1 &= 0. \end{aligned}$$

$$\therefore \alpha \in \mathcal{O}_{KL} \setminus \mathcal{O}_K \cdot \mathcal{O}_L.$$

Theorem: Let K, L be number fields such that

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}].$$

$$\text{let } d := \gcd(\text{disc}(K), \text{disc}(L)).$$

$$\text{Then, } \mathcal{O}_{KL} \subseteq \frac{1}{d} \cdot \mathcal{O}_K \cdot \mathcal{O}_L.$$

In particular, if $d = 1$, then $\mathcal{O}_{KL} = \mathcal{O}_K \cdot \mathcal{O}_L$.

Cor. $\mathcal{O}_{\mathbb{Q}[\omega]} = \mathbb{Z}[\omega]$ for any $\omega = \omega_m$.

Proof: We saw this for prime powers. Use induction on number of prime factors of m .

Let $\# \text{pf}(m) \geq 2$. Write $m = m_1 m_2$ with $\gcd(m_1, m_2) = 1$. m_i have fewer prime factors.

$$\omega := \omega_m, \quad \omega_1 := \omega_{m_1}, \quad \omega_2 := \omega_{m_2}.$$

By "ind",

$$\mathcal{O}_{\mathbb{Q}[\omega_1]} = \mathbb{Z}[\omega_1], \quad \mathcal{O}_{\mathbb{Q}[\omega_2]} = \mathbb{Z}[\omega_2].$$

Note: $\mathcal{O}_{\mathbb{Q}[\omega_1]} \cdot \mathcal{O}_{\mathbb{Q}[\omega_2]} = \mathcal{O}_{\mathbb{Q}[\omega]}$.

Proof (\subseteq) is clear.

(2) Let $rm_1 + sm_2 = 1$.

$$w_1^s \cdot w_2^r = w \in \mathbb{Q}[\omega_1] \cdot \mathbb{Q}[\omega_2].$$

⊗

$$\textcircled{2} \quad [\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\omega_1) : \mathbb{Q}] [\mathbb{Q}(\omega_2) : \mathbb{Q}].$$

$\downarrow \quad \downarrow$

: these two are coprime

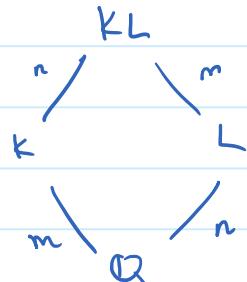
$$\text{Recall: } \varphi(m) = \varphi(m_1)\varphi(m_2) \quad \text{since } \gcd(m_1, m_2) = 1.$$

$$\textcircled{3} \quad \gcd(\text{disc}(\omega_1), \text{disc}(\omega_2)) = 1.$$

(we had seen that prime factors of $\text{disc}(\omega_m)$ are

Thus, by theorem, we get $\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega_1] \cdot \mathbb{Z}[\omega_2]$ same proof as earlier.
 $= \mathbb{Z}[\omega]$.
 $w \in \mathbb{Z}[\omega]$. ⊗

Proof of theorem



$$d := \gcd(\text{disc}(K), \text{disc}(L)).$$

$$\text{IS: } \mathcal{O}_{KL} \subseteq \frac{1}{d} \cdot \mathcal{O}_K \cdot \mathcal{O}_L.$$

Step 1. Let σ be an embedding of K in \mathbb{C} .
 $\dashv \dashv \dashv \dashv \dashv \dashv$

Then, \exists an embedding θ of KL s.t. $\theta|_K = \sigma$, $\theta|_L = \tau$.

If σ has n distinct extensions $\sigma_1, \dots, \sigma_n: K \rightarrow \mathbb{C}$.

Then, $\sigma_i|_L$ are all distinct.

Indeed $\sigma_i|_L = \sigma_j|_L \Rightarrow \sigma_i|_{KL} = \sigma_j|_{KL}$ ($\because \sigma_i|_K = \sigma = \sigma_j|_K$)

↓

i.e.:

$$\downarrow \\ i = j.$$

Thus, $\{\sigma_i|_L\}_{i=1}^n$ are n distinct embeddings of L in \mathcal{C} .
 But there are exactly n in total since $[L:\mathbb{Q}] = n$.
 $\therefore \sigma_i|_L = \tau$ for some $i \in [n]$. \square

Step 2. Let $\{\alpha_1, \dots, \alpha_m\}$ be an integral basis of \mathcal{O}_K .

They are also a \mathbb{Q} -basis of K .

$\{\beta_1, \dots, \beta_n\} \rightarrow \mathbb{Z}$ -basis of \mathcal{O}_L (\mathbb{Q} -basis of L).

$$\Rightarrow \{\alpha_i \beta_j : i \in [m], j \in [n]\} \subseteq \mathcal{O}_{KL}$$

is a basis of KL over \mathbb{Q} .

Given $\alpha \in \mathcal{O}_{KL}$, we can write

$$\alpha = \sum r_{ij} \alpha_i \beta_j, \quad r_{ij} \in \mathbb{Q}.$$

Clear denominators to write

$$\alpha = \frac{1}{r} \sum_{ij} m_{ij} \alpha_i \beta_j, \quad m_{ij} \in \mathbb{Z}, \quad r \in \mathbb{Z} \setminus \{0\}.$$

We may assume $\gcd(\{r\} \cup \{m_{ij}\}_{i,j}) = 1$.

$$\text{Aim: } \mathcal{O}_{KL} \subseteq \frac{1}{r} \cdot \mathcal{O}_K \cdot \mathcal{O}_L.$$

Suffices to prove that $r \mid d$. ($\because \alpha_i \in \mathcal{O}_K, \beta_j \in \mathcal{O}_L$)
 $\gcd(d \text{disc}(k), \text{disc}(l))$

Enough to show $r \mid \text{disc}(k)$.

$$\alpha = \sum_{ij} m_{ij} \alpha_i \beta_j / r.$$

Let $\sigma_1, \dots, \sigma_m$: embeddings of KL/L in C .

(Note that $\sigma_1|_K, \dots, \sigma_m|_K$ are the m embeddings of K in C)

$$\sigma_i \alpha = \frac{1}{r} \sum_{ij} m_{ij} \cdot (\sigma_i \alpha_i) \cdot \beta_j.$$

$$\text{Define } x_i := \sum_j m_{ij} \beta_j / r \quad \text{for } i \in [m].$$

$$\text{Then, } \sigma_i(x_i) = x_i \quad \forall j \in [m].$$

$$\alpha = \sum_i \alpha_i x_i.$$

$$\begin{pmatrix} \sigma_1 \alpha \\ \vdots \\ \sigma_m \alpha \end{pmatrix} = \begin{pmatrix} \sigma_1 \alpha_1 & \dots & \sigma_1 \alpha_m \\ \vdots & \ddots & \vdots \\ \sigma_m \alpha_1 & \dots & \sigma_m \alpha_m \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

By Cramer's rule, $x_i = \frac{\gamma_i}{\delta}$ in the usual way.

In particular, $\delta^2 = \text{disc}(K)$.

$$\text{Also, } \gamma_i, \delta \in A. \quad \therefore x_i \delta^2 = \gamma_i \delta.$$

$\begin{smallmatrix} \cap \\ L \end{smallmatrix} \qquad \begin{smallmatrix} \cap \\ A \end{smallmatrix}$

$$x_i \delta^2 = \sum_j \frac{m_{ij}}{r} \delta^2 \beta_j. \quad \in L \cap A = O_L.$$

$\therefore \{\beta_1, \dots, \beta_m\}$ is a basis of O_L/\mathbb{Z} , we get

$$\frac{m_{ij} \cdot \delta^2}{r} \in \mathbb{Z} \quad \forall i, j.$$

$$\Rightarrow r \mid m_{ij} \cdot \text{disc}(K) \quad \begin{cases} \forall i, j. \\ \text{by } \text{gcd} = 1 \text{ hypothesis} \end{cases}$$

$$\Rightarrow r \mid \text{disc}(K).$$

Remark. In general, $O_K = \mathbb{Z}[\alpha]$ for some $\alpha \in O_K$ is NOT necessary.

Exercise 2.30.: Let $K = \mathbb{Q}[\sqrt[3]{7}, \sqrt[3]{10}]$.

Then, $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K$.

FACT: Let $K = \mathbb{Q}[\alpha]$, for some $\alpha \in \mathcal{O}_K$ with
 $1, \alpha, \dots, \alpha^n : \mathbb{Q}$ -basis for K .

Then, \exists an integral basis $\left\{ 1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}} \right\}$ of \mathcal{O}_K .

Here $d_i \in \mathbb{N}$ with $d_1 | d_2 | \dots | d_{n-1}$, $f_i(x) \in \mathbb{Z}[x]$: monic,
 $\deg(f_i) = i$.

Further, the d_i are uniquely determined.

(f_i are easy to change.)

Exercise 2.41.: Let m be a cubefree integer. Let $\alpha = \sqrt[3]{m}$.
 $K = \mathbb{Q}[\sqrt[3]{m}]$.

Then:

- If m is squarefree, then \mathcal{O}_K has an integral basis:

$$\begin{cases} 1, \alpha, \alpha^2 & m \not\equiv \pm 1 \pmod{9}, \\ 1, \alpha, \frac{\alpha^2 + \alpha + 1}{3} & m \equiv \pm 1 \pmod{9} \end{cases}$$

- If m is not squarefree, then write $m = h k^2$,
with $\gcd(h, k) = 1$, $h \& k$ squarefree.

An integral basis of \mathcal{O}_K is

$$\begin{cases} 1, \alpha, \frac{\alpha^2}{k} & \text{if } m \not\equiv \pm 1 \pmod{9}, \\ 1, \alpha, \frac{\alpha^2 + k^2 \alpha + k^2}{3k} & \text{if } m \equiv \pm 1 \pmod{9}. \end{cases}$$

EXAMPLES: ① $K = \mathbb{Q}[\sqrt[3]{2}]$. $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\} \rightarrow$ Basis.

② $K = \mathbb{Q}[\sqrt[3]{4}]$. $\{1, \sqrt[3]{4}, \frac{\sqrt[3]{4^2}}{2}\}$

③ $K = \mathbb{Q}[\sqrt[3]{10}]$. $\{1, \sqrt[3]{10}, \sqrt[3]{10^2} + \sqrt[3]{10} + 1\}$.

$$③ \quad K = \mathbb{Q}[\sqrt[3]{10}]. \quad \left\{ 1, \sqrt[3]{10}, \frac{\sqrt[3]{10^2} + \sqrt[3]{10} + 1}{3} \right\}.$$

Lecture 7 (24-01-2022)

24 January 2022 17:25

Thm

K/\mathbb{Q} : deg n . Pick $\alpha \in \mathbb{O}_K$ s.t. $K = \mathbb{Q}[\alpha]$.
 Then, $\exists f_1(x), \dots, f_{n-1}(x) \in \mathbb{Z}[x]$ monic with $\deg(f_i) = i$ and
 integers $d_1, \dots, d_{n-1} \in \mathbb{Z}_{>0}$ with $d_1 \mid d_2 \mid \dots \mid d_{n-1} \neq 0$ such that

$$\left\{ 1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}} \right\} \text{ is a } \mathbb{Z}\text{-basis for } \mathbb{O}_K.$$

Moreover, the d_i are unique.

Proof

$\{1, \alpha, \dots, \alpha^{n-1}\}$: basis of K/\mathbb{Q} .

$$d = \text{disc}(\alpha), \text{ then } \mathbb{O}_K \subseteq \sum_{i=1}^n \mathbb{Z} \frac{\alpha^{i-1}}{d}.$$

(Had seen that any $\beta \in \mathbb{O}_K$ can be written as $\frac{1}{d} \sum_{i=1}^n m_i \alpha^{i-1}$ with $d \mid m_i^2, m_i \in \mathbb{Z}$.)

$$\text{Define } F_k := \mathbb{Z} \frac{1}{d} \oplus \dots \oplus \mathbb{Z} \frac{\alpha^{k-1}}{d} \cong \mathbb{Z}^k.$$

$$R_k := F_k \cap \mathbb{O}_K \quad \text{for } k = 1, \dots, n.$$

$$\text{Note } R_n = F_n \cap \mathbb{O}_K = \mathbb{O}_K.$$

$$R_1 = \mathbb{Z} \frac{1}{d} \cap \mathbb{O}_K = \mathbb{Z}.$$

$k=1$: $\{1\}$ is a basis for R_1 . Let $K \geq 1$.

As induction hypothesis, assume we have gotten a basis for R_k as $\left\{ 1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{k-1}(\alpha)}{d_{k-1}} \right\}$ with

the desired properties.

Aim: Extend the basis of R_k to R_{k+1} .

$$R_{k+1} = \sum_{i=1}^{k+1} \mathbb{Z} \frac{\alpha^{i-1}}{d} \rightarrow \mathbb{Z} \frac{\alpha^k}{d}$$

$$\text{Define } \pi: F_{k+1} = \sum_{i=1}^{R+1} \mathbb{Z} \frac{\alpha^{i-1}}{d} \rightarrow \mathbb{Z} \frac{\alpha^k}{d}$$

to be the projection map.

Restrict π to the subgroup R_{k+1} .

$$\pi: R_{k+1} \rightarrow \mathbb{Z} \frac{\alpha^{k+1}}{d} \cong \mathbb{Z}.$$

Claim: $\pi(R_{k+1}) \neq 0$

Proof. $\alpha^k \in R_{k+1}$ and $\pi(\alpha^k) = \alpha^k \neq 0$. \square

Thus, $\pi(R_{k+1})$ is a nonzero subgroup of \mathbb{Z} .

Write $\pi(R_{k+1}) = \mathbb{Z} \cdot \pi(\beta)$ for some $\beta \in R_{k+1}$.

$$\frac{f_{k-1}(\alpha)}{d_{k-1}} \in R_k. \quad \text{Then,} \quad \frac{\alpha \frac{f_{k-1}(\alpha)}{d_{k-1}}}{d_{k-1}} \in R_{k+1}.$$

↳ alg. int.

$$\Downarrow \quad \pi\left(\frac{\alpha \cdot \frac{f_{k-1}(\alpha)}{d_{k-1}}}{d_{k-1}}\right) = m \cdot \pi(\beta) \quad \text{for some } m \in \mathbb{Z}.$$

$$\Rightarrow \pi\left(\underbrace{\frac{\alpha \cdot \frac{f_{k-1}(\alpha)}{d_{k-1}} - m\beta}{d_{k-1}}}_{\in R_k}\right) = 0.$$

$$\Omega_k \cap F_k = R_k.$$

$$\text{Let } \gamma := \frac{\alpha \frac{f_{k-1}(\alpha)}{d_{k-1}} - m\beta}{d_{k-1}} \in R_k.$$

By induction hyp., $\{1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{k-1}(\alpha)}{d_{k-1}}\}$ is a \mathbb{Z} -basis for R_k .

Thus, we can write γ as a \mathbb{Z} -linear combination of above. Using that, we get

$$\beta = \frac{1}{m} \left[\frac{\alpha \frac{f_{k-1}(\alpha)}{d_{k-1}}}{d_{k-1}} - \sum_{i=1}^k m_i \frac{f_{i-1}(\alpha)}{d_{i-1}} \right]$$

(all of these into d)

$$\begin{aligned}
 &= \frac{1}{m d_{k-1}} \left(\alpha f_{k-1}(\alpha) - \sum_{i=1}^{k-1} m_i' f_{i-1}(\alpha) \right) \\
 &\quad \text{monic } \mathbb{Z}\text{-poly in } \alpha \text{ of deg } = k \\
 &= \frac{f_k(\alpha)}{d_k}. \quad (d_k := m \cdot d_{k-1})
 \end{aligned}$$

all of these
div. divide d_{k-1}

Now, one checks that $\left\{ 1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_k(\alpha)}{d_k} \right\}$ is a basis for R_k using the fact that

(if $d_k < 0$,
replace with $\frac{f_k}{d_k}$)

$$0 \rightarrow R_k \hookrightarrow R_{k+1} \rightarrow \mathbb{Z} \cdot \pi(\beta) \rightarrow 0$$

is exact.

(Check that d_k is uniquely determined from d_{k-1} .)

EXAMPLE: Let $K = \mathbb{Q}(\alpha)$ be a deg 5 ext, with $\alpha \in O_K$.

$\left\{ 1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_4(\alpha)}{d_4} \right\}$: basis of O_K .

$$\begin{aligned}
 (a) \text{disc}(\alpha) &= \text{disc}(1, \alpha, \dots, \alpha^4) \\
 &= \text{disc}(1, \alpha, \alpha^2, \alpha^3, f_4(\alpha)) \quad \text{f}_4 \text{ is monic} \\
 &= \text{disc}(1, \dots, f_3(\alpha), f_4(\alpha)) \quad \text{use the other rows/columns} \\
 &\vdots \\
 &= \text{disc}(1, f_1(\alpha), f_2(\alpha), f_3(\alpha), f_4(\alpha)).
 \end{aligned}$$

$$\begin{aligned}
 \text{disc}(O_K) &= \text{disc}\left(1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_4(\alpha)}{d_4}\right) \\
 &= \frac{1}{(d_1 \cdots d_4)^2} \text{disc}(1, \dots, f_4(\alpha)) \\
 &= \frac{\text{disc}(\alpha)}{(d_1 \cdots d_4)^2}.
 \end{aligned}$$

$$(d_1 \cdots d_4)^2$$

Moreover, $\left| \mathcal{O}_K \left(\sum_{i=1}^5 \mathbb{Z}_{\alpha^{i-1}} \right) \right| = d_1 \cdots d_4.$

$$As \quad d_1 \mid d_2 \mid \cdots \mid d_4, \quad d_1 \mid d_2, \quad d_1 \mid d_3, \quad d_1 \mid d_4.$$

$$\begin{array}{c} \therefore d_1^4 \mid \text{disc}(\alpha). \\ \parallel^4 \quad d_2^3 \mid \text{disc}(\alpha), \quad d_3^2 \mid \text{disc}(\alpha). \end{array}$$

Chapter 3: Prime Decomposition in Number Rings.

Def. let A be an integral domain. A is a Dedekind domain if

- (i) A is Noetherian, i.e., every ideal of A is finitely generated.
- (ii) All nonzero prime ideals of A are maximal.
- (iii) A is integrally closed, i.e., if $\alpha \in \text{Frac}(A)$ satisfies a monic polynomial $\in A[x]$, then $\alpha \in A$.

Examples. ① Fields are Dedekind domains.

② All PIDs are Dedekind domains.

Only (iii) is nontrivial. Use that PID \Rightarrow UFD.

Thm. A is Noetherian \Leftrightarrow All increasing chains of ideals stabilise, i.e., if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ are ideals of A , then $\exists n \in \mathbb{N}$ s.t. $I_n = I_{n+1} = \cdots$ \Leftrightarrow Any nonempty collection of ideals of A has a maximal element.

Thm. Let K be a number field. Then, \mathcal{O}_K is a Dedekind domain.

Proof.

(i) Noetherian.

$\mathcal{O}_K \cong \mathbb{Z}^n$ as groups. Any ideal of \mathcal{O}_K is a subgroup, hence free of rank $\leq n$. Thus, f.g. as a \mathbb{Z} -module.
 \therefore f.g. as an ideal.

(ii) To show : $p \neq 0$ prime $\Rightarrow p$ maximal

Let $0 \neq I \subset \mathcal{O}_K$ be an ideal. Pick $0 \neq \alpha \in I$.

$$N_{K/\mathbb{Q}}(\alpha) = m \neq 0.$$

$m = \alpha \cdot \beta$, β = product of other conjugates of α .

Note that $\beta = \frac{m}{\alpha} \in K$.

Moreover, β is a product of alg. integers. $\therefore \beta \in A$.

$$\therefore \beta \in \mathcal{O}_K.$$

$$\therefore m = \beta \alpha \in I.$$

$$\Rightarrow (m) \subseteq \langle \alpha \rangle.$$

$$\mathcal{O}_K / \langle m \rangle \cong \mathbb{Z}^n / m \mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n.$$

\downarrow
finite ring.

Thus, \mathcal{O}_K / I is also finite.

Since finite integral domains are fields we are done.

(iii) Note that K is a field containing \mathcal{O}_K .

Also, given any $\beta \in K$, $\exists m \in \mathbb{Z} \setminus \{0\}$ s.t. $m\beta \in \mathcal{O}_K$.

$$\therefore \text{Frac}(\mathcal{O}_K) = K.$$

If $\beta \in K$ is integral over \mathcal{O}_K , then β is integral over \mathbb{Z} . $\therefore \beta \in \mathcal{O}_K$. (Transitivity of integral closures.) \square

Thm.

(will prove later)

Let R be a Dedekind domain.

Let $I \neq 0$ be an ideal. Then, $\exists J \neq 0$ ideal s.t.

IJ is a principal ideal.

($R \rightarrow$ Dedekind)

Corollary: Define the equiv rel" on $\{\text{nonzero ideals of } R\}$ by

$I \sim I'$ if $\exists 0 \neq J \trianglelefteq R$ s.t. IJ and $I'J$ are principal.

Let $\text{Cl}(R) = R/\sim$. Then, multiplication of ideals in $\text{Cl}(R)$ is well-defined. Moreover, the set of ^{nonzero} principal ideals is an equivalence class and is the identity.

The above theorem tells us that $\text{Cl}(R)$ is a group.

Lecture 8 (27-01-2022)

27 January 2022 15:36

Thm.

R : Dedekind domain.

I : nonzero ideal of R .

Then, $\exists J \neq 0$ ideal of R s.t. IJ is principal.

Proof. Step 1: Every nonzero ideal of R contains a finite product of nonzero prime ideals. (Only need R Noetherian)

Proof. Let $\Sigma = \{\text{ideals } \neq 0 \text{ that do not contain ...}\}$.

If $\Sigma \neq \emptyset$, then $\exists \mathfrak{a} \in \Sigma$ maximal ($\because R$ Noetherian).

\mathfrak{a} not prime. $\exists a, b \notin R \setminus \mathfrak{a}$ s.t. $ab \in \mathfrak{a}$.
 $\therefore \langle \mathfrak{a}, a \rangle, \langle \mathfrak{a}, b \rangle \notin \Sigma$.

Thus, both contain a product ...

But $\langle \mathfrak{a}, a \rangle \langle \mathfrak{a}, b \rangle \subseteq \mathfrak{a}$. $\Rightarrow \leftarrow$

Step 2. Let $0 \subsetneq \mathfrak{a} \subsetneq R$.

Then, $\exists y \in \text{frac}(R) \setminus R$ s.t. $y\mathfrak{a} \subseteq R$.

Proof. Pick $0 \neq a \in \mathfrak{a}$.

By 1, $\langle a \rangle$ contains a finite product of maximal ideals.
(Dedekind: prime + nonzero \Rightarrow maximal.)

$$\mathfrak{a} \supseteq \langle a \rangle \supseteq \prod_{i=1}^r \mathfrak{p}_i : \text{minimal.}$$

$$\langle a \rangle \not\supseteq \mathfrak{p}_1 \dots \hat{\mathfrak{p}}_i \dots \mathfrak{p}_r.$$

Pick a prime $\mathfrak{p} \supseteq \mathfrak{a}$.

Then, $\mathfrak{p} \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_r$.

$\Rightarrow \mathfrak{p} \supseteq \mathfrak{p}_i$ for some i .

But nonzero primes are maximal. Thus, $p = p_i$.
Wlog $p = p_i$.

By minimality, $\langle \alpha \rangle \not\subseteq p_2, \dots, p_r$.
pick $b \in p_2 \dots p_r \setminus \langle \alpha \rangle$.

Then, $b | p_i \subseteq p_1 p_2 \dots p_r \subset \langle \alpha \rangle$.

Then, $y = \frac{b}{\alpha} \in \text{Frac}(R) \setminus R$ does the job.

Step 3. $I \neq 0$: proper ideal (if $I = R$, take $J = R$)

Claim: $\exists J \neq 0$ ideal s.t. IJ : principal ideal.

Proof. Pick $0 \neq \alpha \in I$.

$$\begin{aligned} J &:= \{ f \in R : \beta I \subset \langle \alpha \rangle \} \\ &= (\alpha : I). \end{aligned}$$

Then, $J \neq 0$ is an ideal. ($\alpha \in J$.)

Also, $IJ \subseteq \langle \alpha \rangle$.

We show that $IJ = \langle \alpha \rangle$.

Define $\hat{\alpha} := \frac{1}{\alpha} IJ$: ideal of R .

Clearly, $0 \neq \hat{\alpha}$.

We show $\hat{\alpha} = R$.

Assume $\hat{\alpha} \neq R$.

By step 2., let $y \in \text{Frac}(R) \setminus R$ be s.t. $y \hat{\alpha} \subseteq R$.

Idea: Show that y is integral over R . (Since R is Dedekind, this is \Leftrightarrow .)

$$\cdot \alpha \in I \Rightarrow y \cdot \frac{1}{\alpha} IJ \subseteq R$$

$$\Rightarrow y \cdot \frac{1}{\alpha} \alpha J \subseteq R$$

$$\Rightarrow yJ \subseteq R.$$

$$yJI = y\alpha a = \alpha(ya) \subseteq \alpha R = \langle \alpha \rangle.$$

$$\therefore (yJ) I \subseteq \langle \alpha \rangle$$

$$\Rightarrow yJ \subseteq R$$

$$\Rightarrow yJ \subseteq J$$

From this it follows that y is integral over R . \rightarrow
 (J) is f.g.)

$$\text{Thus, } J = R \quad \text{or} \quad \frac{1}{\alpha} IJ = R.$$

$$\therefore IJ = \langle \times \rangle.$$

□

Großartig! Let R : Dedekind Domain.

$\text{Cl}(R) := \{ \text{nonzero ideals of } R \} / \sim$
 $\hookrightarrow \text{class group of } R$

$$I \sim J \text{ if } \alpha I = \beta J \text{ for some } \alpha, \beta \neq 0 \text{ in } R.$$

Then, $\text{Cl}(R)$ is a group.

↳ Facts to check: ① $[I][J] = [IJ]$ well defined.

② The set of principal ideals ($\neq 0$) form a class.

③ $[R]$ is the identity element.

EXAMPLE. $R = (R[x, y]) / \langle x^2 + y^2 - 1 \rangle$ is a Dedekind domain.

$\text{Cl}(R)$ is then infinite. This does NOT happen for number rings, as we shall see later.

Corollary 2.

Defn: If $I, J, K \trianglelefteq R$ are ideals s.t. $I = JK$, then we say J divides I or $J \mid I$.

For a Ded. domain: $J \mid I$ iff $I \subset J$.

Proof. (\Rightarrow) true in any ring.

(\Leftarrow) Assume $I \subseteq J \neq 0$.

Let $J' \neq 0$ be s.t. $JJ' = \langle \alpha \rangle \neq 0$.

Then, $IJ' \subseteq \langle \alpha \rangle$.

$$\Rightarrow \alpha := \frac{1}{\lambda} IJ' \quad : \text{ideal of } R.$$

Check $I = Ja$. □

Corollary 3. (Cancellation law) $R: DD, I, J, K \trianglelefteq R$ non-zero.

$$IJ = IK \Rightarrow J = K.$$

Proof Let $I' \neq 0$ be s.t. $I'I' = \langle \alpha \rangle$.

$$\Rightarrow I'IJ = I'IK$$

$$\Rightarrow \alpha J = \alpha K \quad (\alpha \neq 0)$$

$$\Rightarrow J = K. \quad \square$$

Theorem. $R: DD$.

Every nonzero ideal can be written as a product of (nonzero) prime ideals (i.e., maximal ideals).

Proof. EXISTENCE of factorisation:

If not, pick I maximal s.t.

$R \rightarrow$ empty product. $\therefore I \neq R$.

Also, I not prime.

Pick $P \supsetneq I$ prime. Then, $I = P\bar{J}$ for some $\bar{J} \trianglelefteq R$.

$I = PJ \nsubseteq J$. Thus, J = product of primes.
 $\Rightarrow I = PJ = \underline{\underline{n}}$. \rightarrow

Uniqueness: $I = P_1 \dots P_r$
 $= Q_1 \dots Q_s$.

$$\Rightarrow Q_1 \dots Q_s \subseteq P_1. \quad \text{wlog } Q_1 \leq P_1.$$

$P_1 = Q_1$ by maximality. ... \blacksquare

Lecture 9 (31-01-2022)

31 January 2022 17:36

Thm. R : DD.

Any nonzero ideal I can be written uniquely as a product of prime ideals.

Defn. Let R be a DD and $I, J \subseteq R$ be nonzero ideals.

We define

$$\begin{aligned} \gcd(I, J) &:= I + J, && (\text{smallest ideal containing } I, J) \\ \operatorname{lcm}(I, J) &:= I \cap J. && (\text{largest ideal contained in } I, J) \end{aligned}$$

Remark. Write $I = \prod_{i=1}^r P_i^{n_i}$, $J = \prod_{i=1}^r P_i^{m_i}$, where P_i are distinct prime ideals, $n_i, m_i \geq 0$.

$$\text{Then, we have } \gcd(I, J) = \prod_{i=1}^r P_i^{\min(n_i, m_i)},$$

$$\operatorname{lcm}(I, J) = \prod_{i=1}^r P_i^{\max(n_i, m_i)}.$$

Thm. Let R be a DD. Let $I \neq 0$ be an ideal.

Let $\alpha \in I \setminus \{0\}$ be arbitrary. Then, $\exists \beta \in I$ s.t. $I = \langle \alpha, \beta \rangle$.

Remark DD need not be UFD. In particular, it need not be a PID.

Proof. To show $\exists \beta$ s.t. $I = \langle \alpha, \beta \rangle = \langle \alpha \rangle + \langle \beta \rangle$
 $= \gcd(\langle \alpha \rangle, \langle \beta \rangle)$.

As $\langle \alpha \rangle \subseteq I$, we have $|I| < |\langle \alpha \rangle|$ since R is a DD.

$\Rightarrow \langle \alpha \rangle = IJ$ for some $J \neq 0$ ideal.

In the usual way, decompose in primes as:
 $I = \prod_{i=1}^r P_i^{n_i}$, $\langle \alpha \rangle = \prod_{i=1}^r P_i^{m_i} \cdot \prod_{j=1}^s Q_j^{t_j}$.
 $(m_i \geq n_i \geq 1)$

Choose $\beta_i \in P_i^{n_i} \setminus P_i^{n_i+1}$ for $i = 1, \dots, r$.

Note $\{P_i^{n_i+1}\} \cup \{Q_j\}$, are pairwise comaximal. \hookrightarrow nonempty by unique factorisation

By CRT

$$R / \frac{n_i+1}{nP_i \cap Q_j} \cong \prod R / P_i^{n_i+1} \times \prod R / Q_j.$$

$$\exists \beta \in R \text{ s.t. } \begin{aligned} \beta &\equiv \beta_i \pmod{P_i^{n_i+1}} & \forall i \in \{1, \dots, r\}, \\ &\equiv 1 \pmod{Q_j} & \forall j \in \{1, \dots, s\}. \end{aligned}$$

$\therefore \beta \in P_i^{n_i} \setminus P_i^{n_i+1} \quad \forall i \quad \text{and} \quad \beta \in R \setminus Q_j \quad \forall j.$

$$\therefore \beta \in \left(\bigcap_{i=1}^r (P_i^{n_i} \setminus P_i^{n_i+1}) \right) \cap \left(\bigcap_{j=1}^s (R \setminus Q_j) \right)$$

$$\Rightarrow \beta \in \prod_{i=1}^r P_i^{n_i} \quad \text{but} \quad \beta \notin P_i^{n_i+1} \quad \forall i.$$

$$\Rightarrow \langle \beta \rangle = \prod_{i=1}^r P_i^{n_i} \cdot \prod T_j^{l_j}$$

T_j is not equal to any P_k or Q_ℓ !

$$\therefore \gcd(\langle \alpha \rangle, \langle \beta \rangle) = \prod_{i=1}^r P_i^{n_i} = I.$$

□

Remark. PID $\not\Rightarrow$ UFD.

Theorem. Let R be a DD. R is a UFD $\Leftrightarrow R$ is a PID.

Proof. Only need to show UFD \Rightarrow PID.

Let R be a DD which is not a PID. We show it is not a UFD.

As $R \neq \text{PID}$, \exists some ideal of R , not principal.

$\therefore \exists$ prime ideal P which is not principal. (\because every nonzero ideal is a product of primes)

Let $\Sigma := \{ I \trianglelefteq R : I \neq 0, IP \text{ is principal} \}$.

$\Sigma \neq \emptyset$. By Noetherian-ness, pick $M \in \Sigma$ maximal.

$MP = \langle \alpha \rangle$. Note that $M \not\subseteq R$ since $RP = P$ is not principal.

Claim: α is irreducible but not prime.

Thus, R is not a UFD since prime \equiv irreducible in a UFD.

Proof. ① α is irreducible.

Suppose not. Then, $\alpha = \beta\gamma$ where β, γ non-unit.

Then, $MP = \langle \beta \rangle \langle \gamma \rangle$.

By uniqueness of prime decomposition, we may assume $P \nmid \langle \beta \rangle$.

Write $\langle \beta \rangle = P\tilde{P}$. Note: $\tilde{P} \in \Sigma$.

Thus, $\alpha = M \cdot P = P \cdot \tilde{P} \cdot \langle \gamma \rangle$.

By cancellation, $M = \tilde{P} \langle \gamma \rangle$, $\langle \gamma \rangle \neq R$.

Thus, $\tilde{P} \subsetneq M$. This contradicts maximality of M . \rightarrow

② α is not prime.

As before, we have $MP = \langle \alpha \rangle$.

Also, $M \not\subseteq \langle \alpha \rangle$, $P \not\subseteq \langle \alpha \rangle$.

Choose $a \in M \setminus \langle \alpha \rangle$, $b \in P \setminus \langle \alpha \rangle$.

Then, $\alpha \nmid a$, $\alpha \nmid b$ but $\alpha \mid ab$. \square

We are now done. \square

EXAMPLES. ① $\mathbb{Z} \subseteq \mathbb{Z}[i] = \bigoplus_{\mathbb{Q}(i)}$.

• $2\mathbb{Z}[i] = \langle 1+i \rangle \langle 1-i \rangle = \langle 1+i \rangle^2$ prime decomposition.

• $p \in \mathbb{Z}$ integer prime.

$$p \equiv 3 \pmod{4} \Rightarrow p \nmid \mathbb{Z}[i] = p.$$

$$\left(\frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]} \right) \cong \frac{\mathbb{Z}[x]}{\langle p, x^2+1 \rangle} \cong \frac{(\mathbb{Z}/p)[x]}{(x^2+1)} \leftarrow \begin{array}{l} \text{field since} \\ x^2+1 \text{ is irreducible in } \mathbb{Z}/p \\ \text{as } p \equiv 3 \pmod{4}. \end{array}$$

$p \equiv 1 \pmod{4} \Rightarrow P = \pi \bar{\pi}$ for some Gaussian prime $\pi \in \mathbb{Z}[\alpha]$.

Write $P = a^2 + b^2$ in \mathbb{Z} with $a, b \not\equiv 0 \pmod{p}$.

Then, $a^2 + b^2 \equiv 0 \pmod{P}$.

$$\Rightarrow \left(\frac{a}{b}\right)^2 \equiv -1.$$

$$\therefore P \in \mathbb{Z}[\alpha] = \langle P, a + ib \rangle \langle P, a - ib \rangle.$$

$$\text{Thus, } 2 = P^2, \quad \langle P \rangle = P, \quad \langle P \rangle = P_1 P_2.$$

\downarrow \downarrow

$P \equiv 3 \pmod{4}$ $P \equiv 1 \pmod{4}$

(D) $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{-5}] = \bigoplus_{\alpha \in \mathbb{Z}[\sqrt{-5}]} \langle \alpha \rangle$

$$\langle 2 \rangle = \langle 2, 1 - \sqrt{-5} \rangle^2,$$

$$\langle 3 \rangle = \langle 3, \sqrt{-5} - 1 \rangle \langle 3, \sqrt{-5} + 1 \rangle$$

$$\langle 5 \rangle = \langle \sqrt{-5} \rangle^2,$$

$$\langle 7 \rangle = \langle 7, \sqrt{-5} + 2 \rangle \langle 7, \sqrt{-5} - 2 \rangle.$$

(look at $\mathbb{Z}[\sqrt{-5}]$)

Defn. Let L/K be number fields.

Let $R = \mathcal{O}_K$ and $S = \mathcal{O}_L$.

By "a prime in R ", we shall mean a nonzero prime ideal of R .

Let P : prime in R , \mathfrak{Q} : prime in S

TPAE:

- (i) $\mathfrak{Q} \mid PS$,
- (ii) $\mathfrak{Q} \supseteq PS$,
- (iii) $\mathfrak{Q} \supsetneq P$,
- (iv) $\mathfrak{Q} \cap R = P$,
- (v) $\mathfrak{Q} \cap K = P$.

Proof. (i) \Rightarrow (ii) is simple.

(ii) \Rightarrow (iii) — — —

(iv) \Rightarrow (ii) obvious

(iii) \Rightarrow (iv): $\mathfrak{Q} \cap R$ is prime.

Check $\mathfrak{Q} \cap R \neq 0$: pick $\alpha \notin K \cap R$. Then, $N_{L/K}(\alpha) \in \mathfrak{Q} \cap R$.

As nonzero primes are maximal, we are done. H.

(iv) \Leftrightarrow (v): Suffice to prove $Q \cap K = Q \cap R$.
 Only (\subseteq). $\alpha \in Q \cap K$
 $\Rightarrow \alpha \in S \cap K \Rightarrow \alpha$ is alg. and in K
 $\Rightarrow \alpha \in O_K = R$ □

Defn. If any of the above conditions are met, we say that Q lies over P or P lies under Q .

Example: ① $\mathbb{Q}[\sqrt{-1}] \supseteq \mathbb{Z}[\sqrt{-1}]$

1	1	$ $	$(1+i)$	(3)	\backslash	$(2+i)$	$(2-i)$
\mathbb{Q}	\mathbb{Z}		$\langle 2 \rangle$	$\langle 3 \rangle$		$\langle 5 \rangle$	

② $\mathbb{Q}[\sqrt{-5}] \supseteq \mathbb{Z}[\sqrt{-5}]$

1	1	$ $	$\langle 2, 1+\sqrt{-5} \rangle$	$\langle 3, 1+\sqrt{-5} \rangle$	\backslash	$\langle 3, 1-\sqrt{-5} \rangle$	
\mathbb{Q}	\mathbb{Z}		$\langle 2 \rangle$	$\langle 3 \rangle$			

- Thm.
- ① Every prime Q of S lies over a unique prime P of R .
 - ② Given a prime P in R , \exists a prime Q in S lying over P .

Proof. ① Clear since P is recovered as $Q \cap R$.

② If $P \subsetneq S$, pick any prime factor of PS (These are precisely all the 0's)

Just need to check that $PS \neq S$.

As $P \subsetneq R$, $\exists \gamma \in K \setminus R$ s.t. $\gamma P \subseteq R$.

If $PS = S$, then $\gamma PS \subseteq S$

$\Rightarrow \gamma S \subseteq S$

$\Rightarrow \gamma \in S$.

$\therefore \gamma \in S \cap K \subseteq R$. □

Defn.

S	L	
$ $	$ $	
P	R	K

$$\begin{array}{ccc} | & | \\ P & R & K \end{array}$$

$$PS = \prod_{i=1}^r Q_i^{e_i}, \quad Q_i : \text{distinct primes of } S \text{ lying over } P.$$

Then, $e(Q_i | P) := e_i$
 $= \text{ramification index of } Q_i/P.$

Note: If Q is a prime in S , and P as before, we define

$$e(Q | P) = \begin{cases} e_i & ; \text{ if } Q = Q_i, \\ 0 & ; \text{ if } Q \neq Q_i. \end{cases}$$

Example. ① $\mathbb{Q}[i]$ $\mathbb{Z}[i]$ $\langle 1+i \rangle$ $\langle 3 \rangle$ $\langle 1+2i \rangle$ $\langle 1-2i \rangle$

		$ _{e=2}$	$ _{e=1}$	$\cancel{1}/1$
\mathbb{Q}	\mathbb{Z}	2	3	5

Any prime of $\mathbb{Z}[i]$ lying over p has ramification index 1
except when $p = 2$.

$$\begin{aligned} \text{disc}(\mathbb{Q}[i]) &= \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 \\ &= 4 = 2^2. \end{aligned}$$

Note: 2 is the only prime with ramification index $\neq 1$.

Suppose we have:

\mathbb{Q}	S	L
P	R	K
p	\mathbb{Z}	\mathbb{Q}

We have an inclusion $R/p \hookrightarrow S/\mathbb{Q}$.

Moreover, we had seen that both the above are finite fields in a result earlier to show that num. fields are Dv.

Moreover, we had seen that both the above are finite fields in a proof earlier to show that num. fields are D.

→ There is a ring map $\varphi : R \rightarrow S/\mathfrak{Q}$ given by $r \mapsto s \mapsto s/\mathfrak{Q}$.
 $\ker(\varphi) = R \cap \mathfrak{Q} = P$.

Defn. $f(\mathfrak{Q}/P) = [S/\mathfrak{Q} : R/P]$.
= inertial degree of \mathfrak{Q} over P

Lecture 10 (03-02-2022)

03 February 2022 17:29

Defn.

$$\begin{array}{c} Q_1 \cdots Q_r \\ \backslash \quad / \\ P \end{array} \quad \begin{array}{c} S \\ | \\ R \end{array} \quad \begin{array}{c} L \\ | \\ K \end{array}$$

$$PS = \prod_{i=1}^r Q_i^{e_i}.$$

- $e(Q_i | P) = e_i$
= ramification index of $Q_i | P$.

- $f(Q_i | P) = [S/Q_i : R/P]$
↓ finite fields ↓
= inertial degree of $Q_i | P$.

Prop" (Multiplicative property of e and f).

$$\begin{array}{c} T \\ | \\ Q \\ | \\ P \end{array} \quad \begin{array}{c} S_1 \\ | \\ S_2 \\ | \\ R \end{array} \quad \begin{array}{c} L_1 \\ | \\ L_2 \\ | \\ K \end{array}$$

- $e(T | P) = e(T | Q) \cdot e(Q | P)$.
- $f(T | P) = f(T | Q) \cdot f(T | P)$.

Proof. e : extend P to S_2 and then S_1 .

f : usual field theory. \square

EXAMPLE

$$\begin{array}{c} P \\ | \\ \mathbb{P} \end{array} \quad \begin{array}{c} R \\ | \\ \mathbb{Z} \end{array} \quad \begin{array}{c} K \\ | \\ \mathbb{Q} \end{array}$$

$$[K:\mathbb{Q}] = m.$$

$$f := f(P \mid_p \mathbb{Z}).$$

Claim : $f \leq m$.

$$\underline{\text{Proof.}} \quad f(P \mid_p \mathbb{Z}) = [R/P : \mathbb{Z}/p].$$

$$R \cong \mathbb{Z}^m \quad (\text{as groups})$$

$$R/P \leftarrow (\mathbb{Z}/p\mathbb{Z})^m$$

↓

$$\text{Cardinality } p^f. \quad \therefore f \leq m.$$

◻

Defn

$$\begin{array}{ll} R & K \\ I & |^n \\ \mathbb{Z} & \mathbb{Q} \end{array}$$

Let $I \neq 0$ be an ideal of R .

$$\|I\| := |R/I| < \infty.$$

Lemma 1. I, J : nonzero ideals in R , then

$$\|IJ\| = \|I\|\cdot\|J\|.$$

Proof. Case 1. $I + J = R$.

$$\text{By CRT : } \frac{R}{IJ} \cong \frac{R}{I} \times \frac{R}{J}.$$

$$\text{Thus, } \|IJ\| = \left| \frac{R}{IJ} \right| = |R/I| \cdot |R/J| = \|I\|\cdot\|J\|.$$

General Case. Write $I = \prod_{i=1}^r P_i^{n_i}$

$$J = \prod_{i=1}^r P_i^{m_i}, \quad n_i, m_i \geq 0.$$

$$\begin{aligned} \text{By case 1, we get } \|I\| &= \prod \|P_i^{n_i}\|, \\ \|J\| &= \prod \|P_i^{m_i}\|, \\ \|IJ\| &= \prod \|P_i^{m_i+n_i}\|. \end{aligned}$$

Enough to show $\|P^n\| = \|P\|^n$ for $0 \neq P$ prime.

Claim. $\|P^n\| = \|P\|^n$ for $0 \neq P$ prime and $n \geq 1$.

Proof. For $n=1$, it is true.

Let $n \geq 2$. We have

$$0 \rightarrow \frac{P^{n-1}}{P^n} \rightarrow \frac{R}{P^n} \rightarrow \frac{R/P^{n-1}}{P^n} \rightarrow 0.$$

Thus, $|R/P^n| = |R/P^{n-1}| \cdot |P^{n-1}/P^n|$.

$$(R/P \cong P^{n-1}/P^n)$$

Inductively, we are done. \square

This finishes the proof. \square

Thm 1: Let $P S = \prod_{i=1}^r Q_i^{e_i}$

$$\begin{array}{ccc} Q & S & L \\ | & | & | \\ P & R & K \end{array}$$

Let $f_i := f(Q_i; P)$.

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

Cor. $e_i \leq n, f_i \leq n \quad \forall i$.

Thm 2: $I \neq 0$ ideal of R .

Then,

$$\|IS\| = \|I\|^n.$$

$$\begin{array}{cc} S & L \\ | & | \\ R & K \end{array}$$

Proof ① $K = \mathbb{Q}$:

$$PS = \prod_{i=1}^r Q_i^{e_i}$$

$$\begin{array}{ccc} Q_1 \dots Q_r & S & L \\ \diagdown & | & | \\ P & \mathbb{Z} & \mathbb{Q} \end{array}$$

$$\Rightarrow \|PS\| = \prod_{i=1}^r \|Q_i\|^{e_i}$$

$$P^n = \prod_{i=1}^r (P^{f_i})^{e_i}$$

$$\Rightarrow P^n = P^{\sum f_i e_i} \Rightarrow n = \sum f_i e_i.$$

We only proved this for $K = \mathbb{Q}$ yet!

② Sufficient to prove for I prime by factoring I into primes.
Let $0 \neq P$ be a prime

S/Q_i is a \mathbb{Z}/P
vec. space of dim f_i

② Sufficient to prove for I prime by factoring I into primes.

Let $0 \neq P$ be a prime

$$\text{IS} : \|PS\| = \|P\|^n.$$

"

"

$$|S/PS| \quad |R/P|^n$$

S/PS is a vector space over R/P .

Thus claim is equivalent to : $\dim_{R/P}(S/PS) = n$.

Step 1. $\dim_{R/P}(S/PS) \leq n$.

Proof. Let $\bar{\alpha}_1, \dots, \bar{\alpha}_{n+1} \in S/PS$, we wish to show that

-they are linearly dependent over R/P .

$\alpha_1, \dots, \alpha_{n+1} \in S \subseteq L$ are linearly dependent over K .

Thus, $\exists a_1, \dots, a_{n+1} \in K$ not all zero s.t.

$$\sum_{i=1}^n a_i \alpha_i = 0.$$

Can assume $a_i \in R$. Now, need to show some

a_i is not in P .

FTSOC, assume that $a_i \in P \neq 0$.

Then, $I := \langle a_1, \dots, a_{n+1} \rangle \subseteq P$.

Can choose $0 \neq I \neq R$ s.t. $II = \langle 0 \rangle$.

Thus, $\exists \gamma \in K \setminus R$ s.t. $\gamma I \subseteq R$.

Claim : $\gamma I \not\subseteq P$.

Once we prove the claim, we can replace a_i with γa_i and be done.

End of Step 1.

Step 2. We have $\dim_{R/\mathfrak{p}}(S/\mathfrak{p}S) = n$.

$$\mathfrak{p}R = \prod_{i=1}^r R/\mathfrak{p}_i^{e_i}.$$

$$\dim_{R/\mathfrak{p}_i}(S/\mathfrak{p}_i S) =: n_i \leq n,$$

by Step 1.

$$\begin{array}{ccc} S & L \\ | & |_n \\ R & R & K \\ | & | & |_m \\ \mathfrak{p} & \mathbb{Z} & \mathbb{Q} \end{array}$$

$$\|\mathfrak{p}S\| = \mathfrak{p}^m$$

||

$$\left(\because S/\mathfrak{p}S \cong \mathbb{Z}^m / \mathfrak{p}\mathbb{Z}^m \text{ (as groups)} \right)$$

$$\prod_{i=1}^r \|\mathfrak{p}_i S\|^{e_i}$$

$$\prod_{i=1}^r \|\mathfrak{p}_i\|^{n_i e_i}$$

$$\prod_{i=1}^r \mathfrak{p}^{\text{fin. } e_i}$$

$S/\mathfrak{p}_i S$ is a vec space over R/\mathfrak{p}_i of dim n_i

$$f_i := f(\mathfrak{p}_i \cap \mathbb{Z}), e_i = e(\mathfrak{p}_i \cap \mathbb{Z}).$$

$$\text{Thus, } \sum f_i n_i e_i = mn. \quad \text{--- (*)}$$

By Thm 1 (for $K = \mathbb{Q}$), we have

$$\sum e_i f_i = m.$$

Since each n_i is $\leq n$, equality (*) can hold only if each $n_i = n$.

End of Step 2.

Now, we prove Thm (1) in the general case!

$$(1) \quad PS = \prod_{i=1}^r Q_i^{e_i}.$$

$$f_i = c(R \cdot 1D)$$

$$\begin{array}{ccc} S & L \\ | & |_n \\ R & R & K \\ | & | & |_m \\ \mathfrak{p} & \mathbb{Z} & \mathbb{Q} \end{array}$$

$$f_i := f(Q_i | P).$$

$$\begin{matrix} I & I_n \\ P & R & K \end{matrix}$$

$$\text{TS: } n = \sum f_i e_i.$$

$$\frac{\|P\|^n}{\|P\|^r} = \prod_{i=1}^r \|Q_i\|^{e_i}$$

v. space blah blah...

$$\therefore n = \sum f_i e_i.$$

Prop. Let $0 \neq \alpha \in R$.

Then,

$$\|\alpha R\| = |N_{K/Q}(\alpha)|.$$

$$\begin{matrix} R & K \\ I & I_n \\ \mathbb{Z} & \mathbb{Q} \end{matrix}$$

Proof. Pick a Galois closure $M \supseteq K \supseteq \mathbb{Q}$.

Let $\sigma_1, \dots, \sigma_n : K \rightarrow M$ be distinct embeddings and extend them

$$t: M \rightarrow M.$$

$$N_{K/Q}(\alpha) = \prod \sigma_i(\alpha).$$

$$\text{Note } \sigma_i(t) \subseteq t.$$

$$\begin{matrix} T = \Theta & M \\ I & I_n \\ R & K \\ \mathbb{Z} & \mathbb{Q} \end{matrix}$$

$$\text{Enough to show } \|\alpha T\| = |N_{M/Q}(\alpha)|.$$

$$\left(\because \|\alpha T\| = \|\alpha R\|^n \text{ and } |N_{M/Q}(\alpha)| = |N_{K/Q}(\alpha)|^n \right)$$

Note: $\langle \alpha \rangle = \langle \sigma_i \alpha \rangle$ in the ring T .

$$\|\alpha T\| = \|\langle \sigma_i \alpha \rangle T\|$$

Lecture 11 (07-02-2022)

07 February 2022 17:32

Recall:

$$\begin{array}{cc} S & L \\ | & |_n \\ R & K \\ | & | \\ \mathbb{Z} & \mathbb{Q} \end{array}$$

① $I \neq 0$ ideal of R .

$$\|I\| := \|R/I\|.$$

$$\|IJ\| = \|I\| \cdot \|J\|.$$

$$② \|IS\| = \|I\|_R^n.$$

③ $0 \neq \alpha \in R$,

$$\|\langle \alpha \rangle\|_R = |\text{N}_{K/R}(\alpha)|.$$

④ $\wp \neq p$: prime of R .

$$PS = \prod_{i=1}^r Q_i^{e_i}, \quad f_i := f(\alpha; \wp).$$

$$\text{Then, } \sum_i e_i f_i = n.$$

Corollary $0 \neq \alpha \in R$. Suppose $|\text{N}_{K/R}(\alpha)| = p \in \mathbb{Z}$ prime.

Then, $\|\langle \alpha \rangle\|_R$ is prime.

Thus, $|R/\alpha R|$ is prime.

$\therefore R/\alpha R$ is a field and hence, α is prime (in R). \square

EXAMPLES. ① $K = \mathbb{Q}[\omega]$, $\omega = e^{\frac{2\pi i}{m}}$.

$$m = p^r.$$

$N_{K/\mathbb{Q}}(1-\omega) = \pm p \therefore \langle 1-\omega \rangle$ is a prime ideal.

Proof.

$$\begin{aligned} \text{Let } f(x) &= \min_{\mathbb{Q}}(\omega) \\ &= \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} \\ &= x^{p-1} + \cdots + 1 \quad \text{for } y=x^{p^{r-1}} \end{aligned}$$

Then, min poly of $1-\omega$ is $\pm f(1-x)$.

$$\text{Thus, } \pm N_{K/\mathbb{Q}}(1-\omega) = f(1-0) = +1.$$

$$\therefore \pm N_{K/\mathbb{Q}}(1-\omega) = f(1) = 1+1+\cdots+1 = p. \quad \square$$

Another proof of $1-\omega$ being prime:

$$\text{We can write } p = (1-\omega)^n \cdot u \quad \text{for some unit } u \in \mathcal{U}(\mathbb{Z}[\omega]).$$

$$\text{Suppose } \langle 1-\omega \rangle = \prod_i Q_i^{e_i} \quad \text{for primes } Q_i \subseteq \mathbb{Z}[\omega].$$

$$\text{Then, } p \in \mathbb{Z}[\omega] = \left(\prod_i Q_i^{e_i} \right)^n.$$

$$\text{But also, } \sum e_i f_i = n.$$

$$\Rightarrow r=1, e_1 = f_1 = 1. \quad \therefore \langle 1-\omega \rangle = Q, \text{ esp.}$$

Def.

$$\begin{array}{ccc} P & R & K \\ | & | & | \\ p & \mathbb{Z} & \mathbb{Q} \end{array}$$

If $e(P|p) = n$, the p is said to split completely.

$$② \alpha = 2^{\frac{1}{3}}$$

$$\text{Let } P = \langle \alpha \rangle.$$

$$2\mathbb{Z}[\alpha] = P^3.$$

$$e(P|p) = 3. \quad \therefore f(P|p) = 1.$$

$$\begin{array}{ccc} P & \mathbb{Z}[\alpha] & \mathbb{Q}[\alpha] \\ | & | & | \\ p = 2 & \mathbb{Z} & \mathbb{Q} \end{array}$$

$$5\mathbb{Z}(\alpha) = \mathbb{Q}_1 \mathbb{Q}_2.$$

$$\mathbb{Q}_1 = \langle 5, \alpha + 2 \rangle,$$

$$\mathbb{Q}_2 = \langle 5, \alpha^2 + 3\alpha - 1 \rangle.$$

$$\frac{\mathbb{Z}(x)}{\langle 5, x^3 - 2 \rangle} = \frac{\mathbb{F}_5[x]}{\langle x^3 - 2 \rangle}$$

$$= \frac{\mathbb{F}_5(x)}{\langle x+2 \rangle \langle x^2 + 3x - 1 \rangle}.$$

$$\textcircled{3} \quad \alpha^3 = \alpha + 1.$$

$$\begin{array}{c} R = \mathbb{Z}[x] \\ | \\ \mathbb{Z} \end{array} \quad \begin{array}{c} \mathbb{Q}[\alpha] \\ | \\ \mathbb{Q} \end{array}$$

$$\text{disc}(1, \alpha, \alpha^2) \rightarrow \text{square free}. \quad \therefore \Theta_{\mathbb{Q}(\alpha)} = \mathbb{Z}(\alpha).$$

$$23R = P\mathbb{A}^2$$

as

$$\frac{\mathbb{Z}(x)}{\langle 23 \rangle} = \frac{\mathbb{F}_{23}(x)}{\langle x^3 - 8 - 1 \rangle}$$

$$P = \langle 23, \alpha - 3 \rangle,$$

$$Q = \langle 23, \alpha - 10 \rangle.$$

$$= \frac{\mathbb{F}_{23}(x)}{\langle (x-3)(x-10)^2 \rangle}.$$

$$\therefore e(P|23) = 1, \quad e(Q|23) = 2.$$

$$1 \cdot f(P|23) + 2 \cdot f(Q|23) = 3.$$

Note: Different ramification indices!

Theorem: Assume L/K is Galois.

$$\text{Let } G = \text{Gal}(L/K),$$

$$\Sigma = \{ \text{primes in } L \text{ lying over } P \}.$$



$$\text{primes in } L \equiv \text{primes in } \mathbb{Q}$$

$$\begin{array}{ccc} S & L \\ | & |_n \\ P & R & K \\ | & & | \\ & & \mathbb{Q} \end{array}$$

Then, G acts on Σ and does so transitively.

Proof. Let $Q \in \Sigma$.

To show: $\sigma(Q) \in \Sigma$.

Note that $\sigma|_S$ is an automorphism.

Thus, $\sigma(Q)$ is prime in S .

But $\sigma(P) = P$. $\therefore \sigma(Q) \cap R \supseteq P \neq 0$.

$\therefore P$ is max'l, $\sigma(Q) \cap R = P$
or $\sigma(Q) \in \Sigma$. ✓

Now, assume that the action is not transitive.

Then, $\exists Q' \in \Sigma, Q \in \Sigma$ s.t. $\sigma Q \neq Q' \quad \forall \sigma \in G$.

Choose $x \in S$ s.t.

$$\begin{aligned} x &\equiv 1 \mod \sigma Q \quad \forall \sigma \in G. \\ &\equiv 0 \mod Q'. \end{aligned}$$

$$\begin{aligned} N_{LK}(x) &= \prod_{\sigma \in G} \sigma(x) \\ \cap_R &= \begin{cases} 1 & \mod Q \\ 0 & \mod Q' \end{cases} \end{aligned} \quad \left(\begin{array}{l} x \equiv 1 \mod \sigma Q \text{ for } \text{II} \\ \sigma(x) \equiv 1 \mod \sigma Q \text{ for } \text{I} \end{array} \right)$$

$$\therefore N_{LK}(x) \in Q' \cap R = P.$$

But then $N_{LK}(x) \in Q$. \rightarrow

Corollary If LK is Galois, then $e(Q|P)$ is constant for all Q over P . Similarly, $f(Q|P)$ is the same.

In this case, $n = \sum e_i f_i = \text{ref.}$

Proof. $Q_1 \dots Q_r \in L$

$\forall i$	$ $	$ _n$	P	R	$ _k$
-------------	-----	-------	-----	-----	-------

$PS = \prod_{i=1}^r Q_i^{e_i}$

Fix σ s.t. $\sigma(Q_1) = Q_2$.

$PS = \prod \sigma(Q_i)^{e_i}$

$= Q_2^{e_1} \cdot \sigma(Q_2)^{e_2} \cdots \sigma(Q_r)^{e_r}$

$\therefore e_1 = e_2$. Similarly ...

$$\begin{array}{ccc} S & \xrightarrow{\sigma} & S \\ | & & | \\ Q_1 & \longrightarrow & Q_2 \end{array} \quad \begin{array}{c} \therefore S/Q_1 \cong S/Q_2 \\ \Rightarrow f_1 = f_2. \end{array}$$

Recall that $P \in \text{Spec}(R)$ is said to be ramified in S (or L) if $e(Q|P) > 1$ for some prime Q over P . Else, it is said to be unramified (if $e(Q|P) = 1$ for all primes Q over P).

EXAMPLES. ① $\omega = \exp\left(\frac{2\pi i}{p^r}\right)$.

Then, $\langle p \rangle \mathbb{Z}$ is ramified (for $p \geq 3$).
 $p \geq [\omega] = \langle 1 - \omega \rangle^{\varphi(p^r)}$.

② $\langle 23 \rangle = P\mathbb{Z}^2$.

23 is ramified in $\mathbb{Q}(\alpha)$.

① $|\text{disc}(R)| = p$. P was ramified.

② $|\text{disc}(R)| = 23$. 23 was ramified.

Theorem: Suppose p is ramified in R .

Then, $p \mid \text{disc}(R)$.

$$\begin{array}{ccc} R & K \\ | & | \\ p \mathbb{Z} & \mathbb{Q} \end{array}$$

(We will prove the converse later. We will also prove that if $n > 2$, then $\text{disc}(R) \neq \pm 1$. \therefore Some prime is ramified.)

Proof. Let P : prime in R s.t. $e(P|p) > 1$.

$$pR = P \cdot I \quad \text{s.t.} \quad P \nmid I.$$

$\hookrightarrow I$ is a product of all primes P_i over p .

Let $\{\alpha_1, \dots, \alpha_n\}$ be an integral basis of R .

Let $\alpha \in I \setminus pR$. $(\alpha \in P_i \wedge P_i \text{ over } p)$

$$\alpha = \sum m_i \alpha_i \notin pR.$$

$\therefore p \nmid m_i$ for some i . WLOG, $p \nmid m_1$.

$$\begin{aligned} \text{disc}(\alpha, \alpha_2, \dots, \alpha_n) &= \text{disc}(\sum m_i \alpha_i, \alpha_2, \dots, \alpha_n) \\ &= \text{disc}(m_1 \alpha_1, \alpha_2, \dots, \alpha_n) \\ &= m_1^2 \text{disc}(\alpha_1, \dots, \alpha_n) \end{aligned}$$

$$= m_1^2 \operatorname{disc}(R).$$

Note: $p \nmid m_1$. To show that $p \mid \operatorname{disc}(R)$, it suffices to show that $p \mid \operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n)$.

Let L be a Galois closure of K/\mathbb{Q} .

Let $\sigma_1, \dots, \sigma_n \in \operatorname{Gal}(L/\mathbb{Q})$ be the distinct embeddings of K in \mathbb{C} .

$$\begin{array}{c} S \\ | \\ R \\ | \\ \mathbb{Z} \\ | \\ \mathbb{Q} \end{array}$$

$\operatorname{Gal}(L/\mathbb{Q})$ acts transitively on the set of primes of S lying over $p \in \mathbb{Z}$.

$$\begin{matrix} T_{1,1} & \cdots & T_{1,m_1} & \cdots & T_{r,1} & \cdots & T_{r,m_r} \\ \searrow & / & & & \swarrow & & \\ p = p_1 & \cdots & p_r & & & & \\ & \searrow & / & & & & \\ & & p & & & & \end{matrix}$$

$$\alpha \in P_i \quad \forall i.$$

$$\therefore \alpha \in T_{i,j} \quad \forall i, j.$$

Now, let $\sigma \in \operatorname{Gal}(L/K)$.

Fix $T = T_{i,j}$.

Then, $\sigma^{-1}(T)$ is prime in S over p .

$$\therefore \alpha \in \sigma^{-1}(T) \text{ or } \sigma(\alpha) \in T.$$

\therefore Each $\sigma(\alpha)$ belongs to each T .

Thus, $\det \begin{pmatrix} \sigma_1(\alpha) & \sigma_1(\alpha_2) & \cdots \\ \vdots & \vdots & \ddots \\ \sigma_n(\alpha) & \sigma_n(\alpha_2) & \cdots \end{pmatrix}^L \in T_{i,j} \cap \mathbb{Z} \neq T_{i,j}.$

$$\therefore p \mid \operatorname{disc}.$$

□

Corollary. ① $\alpha \in R$.

$f \in \mathbb{Z}[x]$ monic with $f(\alpha) = 0$.

If p is a prime such that

$p \nmid N(f'(\alpha))$, then p is unramified.

$$\begin{array}{c} R \\ | \\ \mathbb{Z} \\ | \\ \mathbb{Q}[\alpha] \\ | \\ n \end{array}$$

② Only finitely many primes of \mathbb{Z} are ramified in R .

$$\begin{array}{c} p \\ | \\ \mathbb{Z} \\ | \\ \mathbb{Q} \\ | \\ n \end{array}$$

③ $\begin{array}{c} L \\ \downarrow \\ K \\ \downarrow \\ \mathbb{Q} \end{array}$ Only finitely many primes of K are ramified in L .

Lecture 12 (10-02-2022)

10 February 2022 17:32

(Splitting of primes in a quadratic extension)

Theorem 1. $K = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ squarefree.

$$R = \mathcal{O}_K.$$

Let $p \geq 2$ be a prime integer.

Note: Since $[K:\mathbb{Q}] = 2$, pR is one of P^2 or P_1P_2 or P .

- $p \mid m$.

$$\text{Then, } pR = \langle p, \sqrt{m} \rangle^2.$$

- $p \nmid m$.

- $p = 2$, m odd.

$$2R = \begin{cases} (2, 1 + \sqrt{m})^2, & m \equiv 3 \pmod{4} \\ \left\langle 2, \frac{1 + \sqrt{m}}{2} \right\rangle \left\langle 2, \frac{1 - \sqrt{m}}{2} \right\rangle, & m \equiv 1 \pmod{4} \\ 2R, & m \equiv 5 \pmod{8} \end{cases}$$

- $p > 2$, m arbitrary

$$pR = \begin{cases} \langle p, n + \sqrt{m} \rangle \langle p, n - \sqrt{m} \rangle & p \equiv n^2 \pmod{m} \\ pR & p \text{ is sq. free mod } m \end{cases}$$

Proof. Just compute. Use $R = \frac{\mathbb{Z}[x]}{(x^2 - m)}$ or $\frac{\mathbb{Z}[x]}{(x^2 - x - \frac{m-1}{4})}$

and then quotient.

Theorem 2. (Splitting of primes in a cyclotomic extension)

Let $m \geq 3$. $\omega = e^{2\pi i/m}$, $K = \mathbb{Q}[\omega]$, $R := \mathcal{O}_K = \mathbb{Z}[\omega]$.

Let $p \geq 2$ be an integer prime.

Let $p \geq 2$ be an integer prime.

While $m = p^r n$ with $p \nmid n$.

Let $\alpha := \omega^n = \exp\left(\frac{2\pi i}{p^r}\right)$, $\beta := \omega^{p^r} = \exp\left(\frac{2\pi i}{n}\right)$.

$$p\mathbb{Z}[\alpha] = \langle (1-\alpha)^{\frac{\varphi(p^r)}{p^r}} \mathbb{Z}[\alpha] \rangle_{\text{prime}}$$

$$\text{disc}(\mathbb{Z}[\beta]) = \text{disc}(\beta) | n^{\frac{\varphi(r)}{r}}$$

$$(p, n) = 1 \Rightarrow p \nmid \text{disc}(\mathbb{Z}[\beta]).$$

Thus, p is unramified in $\mathbb{Z}[\beta]$.

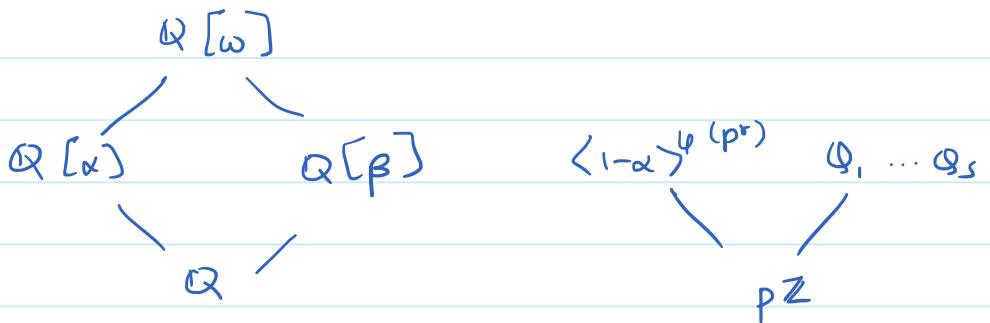
$$p\mathbb{Z}[\beta] = Q_1 \dots Q_s \quad \text{for distinct primes of } \mathbb{Z}[\beta].$$

$$\begin{array}{c} \mathbb{Q}(\beta) \\ \downarrow \\ \mathbb{Q} \end{array}$$

Galois.

Thus, $f(Q_i|p) = f$ is constant.

$$S = \frac{\varphi(n)}{\text{ord}_n(p)}$$



For each i , fix a prime P_i over Q_i .

$P_i \cap \mathbb{Z}[\alpha]$: prime to $\mathbb{Z}[\alpha]$
lying over $p\mathbb{Z}$.

$$\begin{array}{cccc} P_1 & \dots & P_r & \mathbb{Z}[\omega] \\ | & & | & | \\ Q_1 & \dots & Q_r & \mathbb{Z}[\beta] \end{array}$$

$$\text{Thus, } P_i \cap \mathbb{Z}[\alpha] = (1-\alpha)\mathbb{Z}[\alpha] \quad \forall i.$$

$$\begin{array}{ccc} & & | \\ & & \mathbb{Z} \\ \swarrow & & \searrow \\ P\mathbb{Z} & & \mathbb{Z} \end{array}$$

$$e(P_i | p\mathbb{Z}) = e(P_i | \langle 1-\alpha \rangle) \cdot e(\langle 1-\alpha \rangle | p\mathbb{Z})$$

" $\varphi(p^r)$

$$\Rightarrow e(P_i | p) \geq \varphi(p^r).$$

$$f(P_i | p) = f(P_i | Q_i) \cdot f(Q_i | p)$$

$$\Rightarrow f(P_i | p) \geq f = \text{ord}_n(p).$$

$$p\mathbb{Z}[\alpha] = \langle 1-\alpha \rangle^{\varphi(p^r)}$$

$$p\mathbb{Z}[\beta] = Q_1 \cdots Q_s$$

Also, $P_1 \cdots P_s$ divides $p\mathbb{Z}[\omega]$.

$$\varphi(m) \geq \sum_{\substack{\text{||} \\ \varphi(p^r)}} \varphi(p^r) \cdot f$$

$$\Rightarrow \varphi(n) \geq \sum f = fs = \varphi(n).$$

$$\varphi(p^r) \varphi(n)$$

Thus, equality everywhere.

$$p\mathbb{Z}[\omega] = P_1 \cdots P_s^{\varphi(p^r)}.$$

Q.E.D.

Cor. $\omega = \exp\left(\frac{2\pi i}{m}\right), \quad p \nmid m.$

Then, $p\mathbb{Z}[\omega] = \prod_{i=1}^s P_i, \quad \text{where } s = \frac{\varphi(n)}{\text{ord}_n(p)}.$

Q.E.D.

Theorem. $L = K[\alpha]$ for some $\alpha \in S$.

$$R[\alpha] \subseteq S.$$

$\downarrow \quad \downarrow$

free abelian groups of m^n

S	L
$ $	$ ^n$
R	K
$ $	$ _m$

Thus, the group $S_{/\text{ord}_n}$ is finite (and abelian).

Q.E.D.

Thus, the group $S/R[\alpha]$ is finite (and abelian). \mathbb{Z} \mathbb{Q}

Let $p \in \mathbb{Z}$ and take $P \in \text{Spec}(R)$ over p .

Assume $P \times |S/R[\alpha]|$. Let $g(\alpha) = \min_k(\alpha) \in R[\alpha]$.

We have the natural projection $R[x] \rightarrow R/p[x]$, $n \mapsto \bar{n}$.

$$R[\alpha] \cong R[x]/\langle g(x) \rangle$$

In $(R/P)[x]$, factor $\bar{g} = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}$.

$$f_i := \deg(\bar{g}_i) \geq 1.$$

(Can pick lifts g_i having same degree.)

Define $Q_i = \langle P, g_i(\alpha) \rangle S$.

Then,

$$PS = \prod Q_i^{e_i}$$

$$\text{Also, } f(Q_i|_P) = f_i.$$

Proof (sketch). Claims:

① Either $Q_i = S$ or $Q_i \in \text{Spec}(S)$ and $|S/Q_i| = |R/p|^{\deg(\bar{g}_i)}$.

② $Q_i + Q_j = S$ for $i \neq j$. $\exists i, \bar{g}_i + \bar{g}_j = 1$
 ↓ lift to $R[x]$. Put $x = \alpha$. \square

Exercise

$$\hookrightarrow ③ PS \mid Q_1^{e_1} \cdots Q_s^{e_s}$$

Assume the claims.

Wlog assume that Q_1, \dots, Q_s are proper and $Q_{s+1} = \dots = Q_r = S$

Then, $f(Q_i|_P) = f_i = \deg \bar{g}_i$ for $i \in [s]$.

$$\text{Also, } PS \mid Q_1^{e_1} \cdots Q_s^{e_s}$$

$$\therefore PS = Q_1^{d_1} \cdots Q_s^{d_s} \quad \text{for some } 0 \leq d_i \leq e_i.$$

$$\text{But } n = \sum_1^s d_i \cdot f_i \leq \sum_{i=1}^s e_i \cdot f_i \leq \sum_{i=1}^r e_i \cdot f_i = n.$$

\therefore All are equalities and $s=r$.

Lecture 13 (14-02-2022)

14 February 2022

17:25

Theorem. $K = \mathbb{Q}[\omega]$, $\omega = e^{\frac{2\pi i}{n}}$, $p \in \mathbb{Z}$ prime.

Suppose $p \nmid n$. (p : unramified)

$$p\mathbb{Z}[\omega] = P_1 \cdots P_r$$

$$f(P_i | p) = f = \text{ord}_n(p). \quad (f(P_i | p) \text{ is constant since Galois ext.})$$

Proof. Let $P \subseteq \mathbb{Z}[\omega]$ be a prime over p .

$$f = [\mathbb{Z}[\omega]/P : \mathbb{Z}/p\mathbb{Z}]$$

$\mathbb{Z}[\omega]/P$ is a Galois ext. of degree f over \mathbb{F}_p .

In fact, $\text{Gal}(\mathbb{Z}[\omega]/P, \mathbb{F}_p) = \langle \tau \rangle$ is cyclic of order f , where τ is the Frobenius map $x \mapsto x^p$.

$$\text{Also, } \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong (\mathbb{Z}/n)^*$$

$$(\omega \mapsto \omega^\alpha) \longleftrightarrow \bar{\alpha}.$$

$$(\text{Here, } (\alpha, n) = 1.)$$

As $(p, n) = 1$, we have the automorphism $\sigma \in \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ given by $\sigma(\omega) = \omega^p$.

Then, $\sigma(\sigma) = \text{ord}_n(p)$, in view of the above isomorphism.

To show: $f = \text{ord}_n(p)$

Enough to show: $\sigma^\alpha = \text{id} \Leftrightarrow \tau^\alpha = \text{id}$.

$$\text{Note: } \sigma^\alpha = \text{id} \Leftrightarrow \sigma^\alpha(\omega) = \omega \Leftrightarrow \omega^{p^\alpha} = \omega \Leftrightarrow \omega^{p^\alpha - 1} = 1 \Leftrightarrow p^\alpha \equiv 1 \pmod{n}$$

$$\therefore \tau^\alpha = \text{id} \Leftrightarrow \tau^\alpha(\bar{\omega}) = \bar{\omega} \Leftrightarrow \bar{\omega}^{p^\alpha} = \bar{\omega} \Leftrightarrow \omega^{p^\alpha} = \omega \pmod{P}$$

$$\begin{array}{c} \xrightarrow{\text{define } \bar{\omega} \text{ by}} \\ \frac{\mathbb{Z}[\omega]}{P} = \mathbb{F}_p[\bar{\omega}] \end{array}$$

$$\text{Let } b = (p^\alpha \pmod{n}).$$

Clearly $b \neq 0$, & $(p, n) = 1$.

Claim. If $\omega^b = \omega \pmod{P}$, then $b = 1$.

Proof. If $b > 1$, note

$$n = (1-\omega)(1-\omega^2)\cdots(1-\omega^{n-1})$$

$$\text{if } b > 1, \text{ then } 1 - \omega^{b-1} \in P \text{ as } \omega(1 - \omega^{b-1}) \in P.$$

Thus, $n \in P$. Also, $p \in P$. As $(n, p) = 1$, we have $1 \in P$. \square

Thus, $\omega^{b^a} = \omega \pmod{p} \Leftrightarrow \omega^b = \omega \pmod{p} \Leftrightarrow b = 1$. \square

Def'n - Let K/\mathbb{Q} be Galois.

$$G = \text{Gal}(K/\mathbb{Q})$$

$$P \mathcal{O}_K = (P_1 \cdots P_r)^e, \quad f := t(P_i/p)$$

$$n = \text{ref.}$$

Let P lie over p , i.e., $P = P_i$ for some $i \in [r]$

$D_P = \text{decomposition group of } P$ (we had shown that
 $= \{\sigma \in G : \sigma P = P\}$ G acts transitively on $\{P_1, \dots, P_r\}$)
 stabiliser of P .

$$\text{orbit of } P = [G : D_P]$$

$$\parallel \qquad \parallel$$

$$r$$

$$\frac{\text{ref}}{|D_P|}$$

Prop ^

$$\text{Thus, } |D_P| = \text{ref.}$$

Hence,

$$[K^{D_P} : \mathbb{Q}] = r. \quad \square$$

$$k(P) = \mathcal{O}_K/P \quad : \text{residue field of } P$$

(nonzero primes are max'l)

\mathcal{O}_K/P is a Galois ext' of $\mathbb{Z}/p = \mathbb{F}_p$.

$\text{Gal}(k(P)/\mathbb{F}_p) = \langle \tau \rangle$, where τ is the Frobenius automorphism.

Let $\sigma \in D_P$.

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{\sigma} & \mathcal{O}_K \\ \downarrow & & \downarrow \end{array}$$

$$\begin{array}{ccc} \mathcal{O}_K/P & \xrightarrow{\bar{\sigma}} & \mathcal{O}_K/P \\ \bar{x} & \mapsto & \bar{\sigma(x)} \end{array}$$

(well defined since $\sigma(P) = P$.)

This is an isomorphism.

Then, we get a natural map

$$D_p \xrightarrow{\varphi} \text{Gal}(K(p)/\mathbb{F}_p)$$

$$\sigma \mapsto \bar{\sigma}.$$

Moreover, φ is a homomorphism.

We now wish to show that φ is surjective. First, some lemmas

Lemma 1. (Notations as above)

$$D_{\sigma p} = \sigma D_p \sigma^{-1}.$$

□

Lemma 2. $D_p \subset G = \text{Gal}(K/\mathbb{Q})$. Let $D := D_p$.

K

K/K^D is Galois with Galois group $D = D_p$.

|
K^D

As usual, $K^D = \{x \in K : \sigma x = x \ \forall \sigma \in D\}$.

|
Q

Then, K^D is the smallest subfield of K/\mathbb{Q} s.t. P is the only prime of \mathcal{O}_K lying over $P \cap K^D$.

Proof. $\text{Gal}(K/K^D) = D$.

P K
| |

D acts transitively on the set of primes of \mathcal{O}_K lying over $P \cap K^D$.

P ∩ K^D K^D
| |

D fixes D.

P Q
| |

$\Rightarrow P$ is the only prime of \mathcal{O}_K lying over $P \cap K^D$.

K

Conversely, suppose F is s.t. P is the only prime of \mathcal{O}_K lying over $P \cap \mathcal{O}_F$.

|
F
|

Then, $\text{Gal}(K/F) \leq G$ fixes P.

Q

$\Rightarrow \text{Gal}(K/F) \subseteq D$

↙ Fund. Galois Thm.

$\Rightarrow K^D \subseteq F$.

□

Lemma 3. Let $\mathfrak{P} = P \cap \mathcal{O}_{K^D}$.

K
|
ef

As e, f, n are multiplicative, so $R = \underline{n}$.

Lemma 3. Let $P = P \cap K^D$.

As e, f, n are multiplicative, so $r = r = \frac{n}{ef}$.
 # of primes lying over \mathfrak{p}

P	K
1	1/ef
\mathfrak{p}	K^D
1	1/r

As $r(K/\mathfrak{p}) = 1$, we get $r(K^D/\mathfrak{p}) = r$.

Thus, $[K^D : \mathbb{Q}] = r(K^D/\mathfrak{p})$. Hence, $e(\mathfrak{p}/\mathfrak{p}) = f(\mathfrak{p}/\mathfrak{p}) = 1$.

In turn,

$$e(P/\mathfrak{p}) = e(\mathfrak{p}/\mathfrak{p}), \quad f(P/\mathfrak{p}) = f(\mathfrak{p}/\mathfrak{p}). \quad \text{B}$$

Back to the homomorphism $\varphi : D_p \rightarrow \text{Gal}(k(P)/\mathbb{F}_p)$.

$$\begin{aligned} &|| \\ &\langle \tau \rangle : \text{order } f = f(P/\mathfrak{p}) \end{aligned}$$

τ : Frobenius

Theorem. φ is surjective.

Pf. $k(P) = \mathbb{F}_p[\bar{a}]$, for some $\bar{a} \in k(P) = \mathbb{Q}_p/\mathfrak{p}$.

Choose a lift $a \in \mathbb{Q}_p$ of \bar{a} .

Define

$$f(x) = \prod_{\sigma \in D_p} (x - \sigma a).$$

If $\theta \in D_p$, we get $f^\theta(x) = f(x)$.

Thus, $f(x) \in K^D[x]$.

Moreover, $f(x) \in \mathbb{Q}_{K^D}[x]$.

Note that we saw $f(\mathfrak{p}/\mathfrak{p}) = 1$ Thus, $\mathbb{Q}_{K^D}/\mathfrak{p} \cong \mathbb{F}_p$.

P	K
\mathfrak{p}	1/ef
\mathfrak{p}	K^D
1/r	1/r
\mathfrak{p}	\mathbb{Q}

Going modulo \mathfrak{p} : $f(x) = \prod_{\sigma \in D_p} (x - \tilde{\sigma} a) \in \mathbb{F}_p[x]$.

0

1

 $\sigma \in D_p$

$$\mathbb{Z} \subseteq \Theta_{K^p} \subseteq \Theta_K.$$

$$\mathbb{Z}/p \cong \Theta_{K^p}/_p \subseteq \Theta_K/p.$$

Going modulo P : $\bar{f}(x) = \prod_{\sigma \in D_p} (x - \bar{\sigma}\bar{a}) \in \mathbb{F}_p[x]$

\bar{a} : root of $\bar{f}(x)$.

$$k(P) = \mathbb{F}_p[\bar{a}]$$

Thus, $\min_{\mathbb{F}_p}(\bar{a}) \mid \bar{f}(x)$ in $\mathbb{F}_p[x]$.

Also, $\bar{a}^\tau = \tau(\bar{a})$ is also a root of $\min_{\mathbb{F}_p}(\bar{a})$.
(as τ is an aut)

Thus, $\exists \sigma \in D_p$ s.t. $\bar{\sigma}\bar{a} = \tau(\bar{a})$.

As τ is determined by \bar{a} , we see that $\tau \in \text{Gal}(k(P))$.

As $\langle \tau \rangle = \text{Gal}(k(P)/\mathbb{F}_p)$, we are done. \square

We have the exact sequence

$$1 \rightarrow I_p \rightarrow D_p \xrightarrow{\varphi} \text{Gal}(k(P)/\mathbb{F}_p) \rightarrow 1,$$

where $I_p = \ker \varphi$

$$\begin{aligned} &= \text{inertial group of } p \\ &= \left\{ \sigma \in D_p \mid \bar{\sigma} = \text{id}_{k(P)} \right\} \\ &= \left\{ \mid \bar{\sigma}(\bar{x}) = \bar{x} \right\} \\ &= \left\{ \mid \sigma(x) = x \pmod{p} \right\}. \end{aligned}$$

$$\begin{aligned} \cdot |I_p| &= \frac{|D_p|}{|\text{Gal}(k(P)/\mathbb{F}_p)|} \\ &= \frac{ef}{f} = e. \end{aligned}$$

Corollary If $P \in \mathbb{Z}$ is unramified in K . Then $I_p = (1)$ and

Corollary. If $p \in \mathbb{Z}$ is unramified in K , then $I_p = (1)$ and φ is an isomorphism.

Now: Assume p is unramified.

$$D_p \xrightarrow[\cong]{\psi} \text{Gal}(k(p)/F_p) \\ \parallel \\ \langle \tau \rangle \\ \hookdownarrow \text{Frobenius.}$$

$\exists ! \text{ Frob}_p \in D_p$ called Frobenius element such that $\text{Frob}_p^p = \tau$.

Thus, Frob_p is the unique map s.t.

$$\text{Frob}_p(x) = x^p \pmod{p}, \\ \text{for all } x \in O_K.$$

Lemma. Let $\sigma \in G = \text{Gal}(K/\mathbb{Q})$.

Then, σp lies over p .

$$\text{Frob}_{\sigma p} = \sigma \text{Frob}_p \sigma^{-1}.$$

Proof. Let $x \in O_K$.

Then,

$$(\text{Frob}_p \sigma^{-1})(x) = (\sigma^{-1}(x))^p \pmod{p}.$$

That is,

$$\text{Frob}_p(\sigma^{-1}x) - \sigma^{-1}(x^p) \in p. \quad \forall x \in O_K.$$

Apply σ to get

$$\sigma \text{Frob}_p(\sigma^{-1}x) - x^p \in \sigma p \quad \forall x \in O_K.$$

By uniqueness, $\sigma \text{Frob}_p \sigma^{-1} = \text{Frob}_p$. □

Def. If K/\mathbb{Q} is Galois and $p \in \mathbb{Z}$ unramified, then

$\{\text{Frob}_{p_i} : i=1, \dots, r\}$ is a conjugacy class of $\text{Gal}(K/\mathbb{Q})$.

If K/\mathbb{Q} is abelian, the conjugacy class has a single elements denoted $\left(\frac{K/\mathbb{Q}}{p}\right)$.

↙ Artin symbol

$$\cdot \left(\frac{K/\mathbb{Q}}{-}\right) : \left\{ \begin{matrix} \text{unramified} \\ \text{primes} \end{matrix} \right\} \rightarrow G.$$

Extend this to a group homomorphism of a free abelian group

$$\oplus_{\substack{p \text{ unramified}}} \mathbb{Z}[p] \rightarrow G$$

Artin's Conjecture

$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$: profinite group, inverse limit of finite groups

Topology on $\overline{\mathbb{Q}}/\mathbb{Q}$:

Neighbourhoods of 1: $\left\{ \text{Gal}(\overline{\mathbb{Q}}/K) \mid K/\mathbb{Q} \text{ finite} \right\}$

$\text{GL}_n(\mathbb{C})$: give it the discrete topology.

Want: n -dimensional complex representation of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, i.e., a continuous homomorphism

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_n(\mathbb{C}).$$

That is, $K = \overline{\mathbb{Q}}^{K^p}$ should be a finite ext of \mathbb{Q} .

ρ factors as

$$\begin{array}{ccc} \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho} & \text{GL}_n(\mathbb{C}) \\ & \searrow \text{restriction} & \uparrow \rho' \\ & & \text{Gal}(K/\mathbb{Q}) \end{array}$$

As $\text{Gal}(K/\mathbb{Q})$ is finite, so is $\text{im}(\rho')$.

- ρ is a representation $\Rightarrow \text{im}(\rho)$ is finite.
 (\Leftarrow) not true, i.e., if $\rho: \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}(n, \mathbb{C})$ is a homom. with finite image, ρ need not be continuous.

(Ref: W. Stein: Computational ANT?)

Fix ρ . Suppose $p \in \mathbb{Z}$ is unramified in K .
let $\left(\frac{K \setminus \mathbb{Q}}{p} \right)$ denote the ^{obvious} conjugacy class.

Then, $\rho' \left(\left(\frac{K \setminus \mathbb{Q}}{p} \right) \right)$ lies in a conjugacy class of $\text{GL}(n, \mathbb{C})$.

Thus, it makes sense to talk about its characteristic polynomial, $F_p(x) \in \mathbb{C}[x]$.

$$F_p(x) = x^n + a_1 x^{n-1} + \dots + \det(\rho'(\text{Frob}_p)).$$

$$R_p(x) = x^n F_p\left(\frac{1}{x}\right) = 1 + a_1 x + \dots + \det(\rho'(\text{Frob}_p)) x^n.$$

Artin's L-function for ρ :

$$L(\rho, s) := \prod_{\substack{p \in \mathbb{Z} \\ \text{unramified}}} \frac{1}{R_p(p^{-s})}, \quad s \in \mathbb{C}.$$

Artin proves $L(\rho, -)$ is holomorphic on some right half plane.

Moreover, $L(\rho, -)$ extends to a meromorphic function on \mathbb{C} .

Conjecture: The extension is holomorphic on $\mathbb{C} \setminus \{s=0\}$.

Known: $n=1$.

$n=2$: Khare - Winterberger.

$n \geq 3$: Open (?)

Recall: Defn. Let $p > 2$ be prime.

If $(n, p) = 1$, we define

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & ; \text{ if } n \text{ is a square mod } p \\ -1 & ; \text{ else.} \end{cases}$$

Further, if $p \mid n$, then $\left(\frac{n}{p}\right) = 0$

We saw:

- $\left(\frac{-}{p}\right) : \mathbb{Z}_p \rightarrow \{1, -1\}$ is a group homomorphism.

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & ; \text{ if } p \equiv \pm 1 \pmod{8}, \\ -1 & ; \text{ if } p \equiv \pm 3 \pmod{8}. \end{cases}$

Thm 1 (Gauss Quadratic Reciprocity)

Let p, q be distinct odd primes.

Then, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} -1, & ; \text{ if } p, q \equiv 3 \pmod{4}, \\ 1, & ; \text{ else.} \end{cases}$

Recall that: $\left(\frac{q}{p}\right) = 1 \Leftrightarrow q$ is a square mod p

$\Leftrightarrow q$ is a product of two primes

in $\mathcal{O}_{\mathbb{Q}}[\sqrt{d(p)}]$,
 $d(p) = \begin{cases} 1 & ; p \equiv 1 \pmod{4}, \\ -1 & ; p \equiv -1 \pmod{4}. \end{cases}$

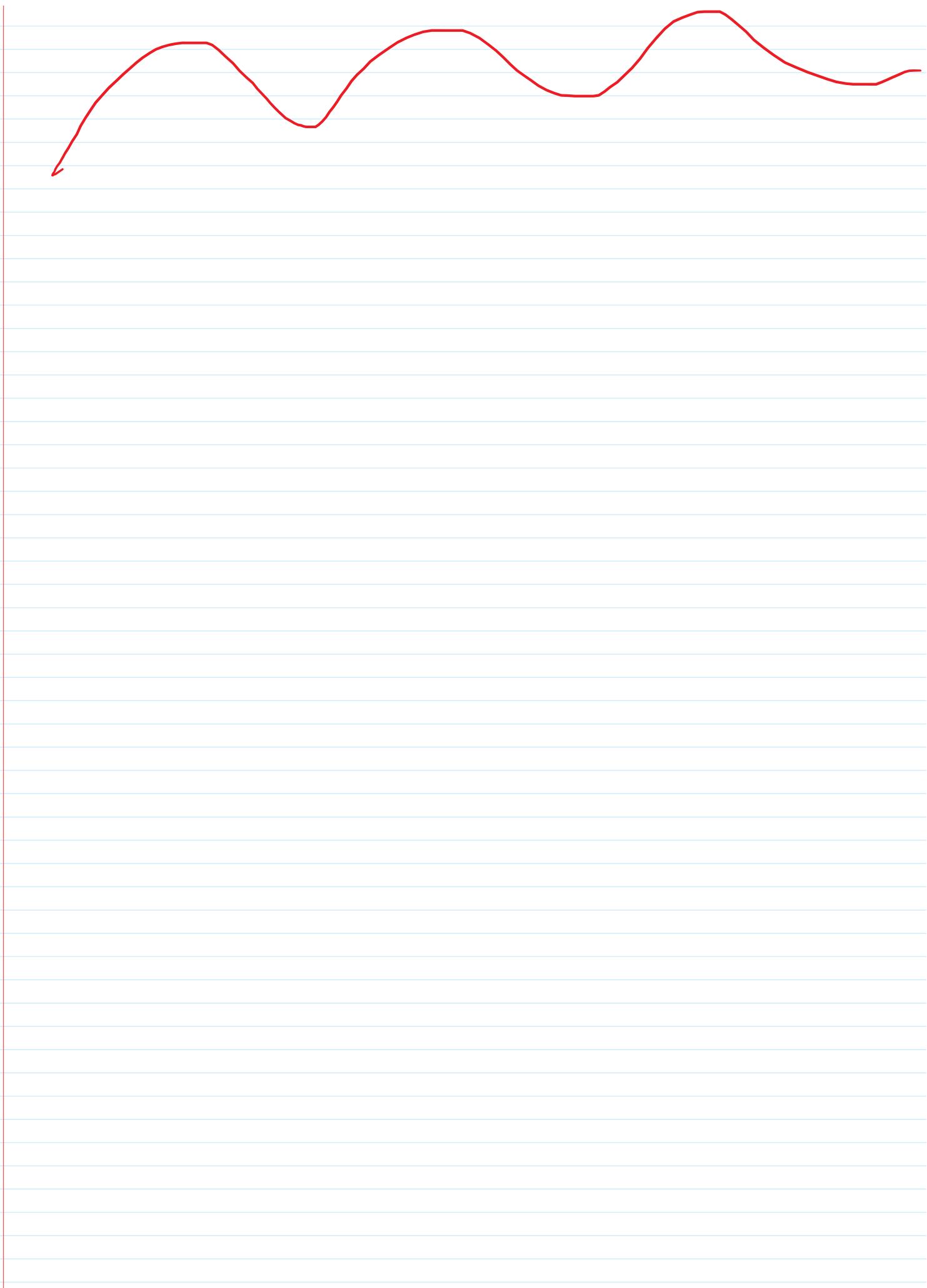
Lemma 2. Let a be a squarefree integer. $K = \mathbb{Q}[\sqrt{a}]$.

Let q be an odd prime.

q splits into two distinct primes in \mathcal{O}_K iff $q \nmid a$
and a is a square mod q .

Proof. Two options: $\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{a}] & \xrightarrow{\text{disc}} 4a \\ \mathbb{Z}\left[\frac{1+\sqrt{a}}{2}\right] & \xrightarrow{\text{disc}} a \end{cases}$

If $q \nmid a$, then $q \nmid \text{disc}(\mathcal{O}_K)$. Thus, q is unramified.



Lecture 16 (03-03-2022)

03 March 2022 17:30

Theorem.

$K/\mathbb{Q} : \{x_1, \dots, x_n\} \rightarrow \mathbb{Z}$ -basis of \mathcal{O}_K .

$\sigma_1, \dots, \sigma_n$: embeddings of K in \mathbb{C} .

Let

$$\lambda := \prod_i \left(\sum_j |\sigma_i x_j| \right).$$

Any ideal class contains an ideal I s.t. $\|I\| \leq \lambda$.

Let $\sigma_1, \dots, \sigma_r$ be the real embeddings, i.e., $\sigma_i(K) \subset \mathbb{R}$.

The remaining embeddings will come in conjugate pairs, say $\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}$. $\sigma_{r+s}(K) \not\subset \mathbb{R}$.

Note $r + 2s = n = [K : \mathbb{Q}]$.

Define $f : K \rightarrow \mathbb{R}^n$

$$\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Re} \sigma_{r+1}(\alpha), \operatorname{Im} \sigma_{r+1}(\alpha), \dots, \operatorname{Re} \sigma_{r+s}(\alpha), \operatorname{Im} \sigma_{r+s}(\alpha)).$$

Evidently, f is an injective homomorphism (of abelian groups).

Let $R = \mathcal{O}_K$. $f(R) \cong R \cong \mathbb{Z}^n$ as groups.

Claim: $f(R)$ is an n -dimensional lattice in \mathbb{R}^n , i.e., $f(R)$ has a \mathbb{Z} -basis which is \mathbb{R} -linearly independent.

Aside: $\langle 1, \sqrt{2} \rangle \cong \mathbb{Z}^2$ is not a lattice.

Proof of Claim: Let $\{x_1, \dots, x_n\}$ be any \mathbb{Z} -basis of $R = \mathcal{O}_K$.

Evidently, $\{f(x_1), \dots, f(x_n)\}$ is a \mathbb{Z} -basis for $f(R)$. We

show that it is linearly independent over \mathbb{R} .

$$\begin{vmatrix} f(x_1) \\ \vdots \end{vmatrix} = \begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_r(x_1) & \operatorname{Re}(\sigma_{r+1}(x_1)) & \dots \\ \vdots & \ddots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$\begin{pmatrix} f(x_1) \\ \vdots \\ f(x_n) \end{pmatrix} = \begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_r(x_1) & \operatorname{Re}(\sigma_{r+1}(x_1)) & \dots \\ \vdots & \ddots & \vdots & \vdots & \ddots \\ \sigma_1(x_n) & \dots & \sigma_r(x_n) & \operatorname{Re}(\sigma_{r+1}(x_n)) & \dots \end{pmatrix}$$

$\text{A} \quad //$

we show this has
 $\det \neq 0$

Note: $\begin{bmatrix} \operatorname{Re} z & \operatorname{Im} z \end{bmatrix} \xrightarrow{G_1 + iG_2} \begin{bmatrix} z & \operatorname{Im} z \end{bmatrix} \xrightarrow{\{ -2iG_2 \}} \begin{bmatrix} z & \bar{z} \end{bmatrix} \xleftarrow[G_2 + G_1]{-1/2i} \begin{bmatrix} z & -2i \operatorname{Im} z \end{bmatrix}$

Doing the above shows that

$$\det(A) = \frac{1}{(-2i)^s} \det \begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_r(x_1) & \sigma_{r+1}(x_1) & \overline{\sigma_{r+1}(x_1)} & \dots & \overline{\sigma_{r+s}(x_1)} & \overline{\sigma_{r+s}(x_1)} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \end{pmatrix}$$

Thus, $(\det(A))^2 = \frac{1}{(-2i)^{2s}} \operatorname{dis}(R) \neq 0$, as desired.

Defn. $\Lambda \subseteq \mathbb{R}^n$ is said to be a lattice of rank n if

Λ is a subgroup of \mathbb{R}^n set.

(i) $\Lambda \cong \mathbb{Z}^n$, and

(ii) \exists a \mathbb{Z} -basis $\{v_1, \dots, v_n\}$ of Λ which is lin. indep. over \mathbb{R} .

A fundamental parallelopiped:

$$\Sigma = \left\{ \sum_{i=1}^n \lambda_i v_i : 0 \leq \lambda_i < 1 \right\}.$$

The above naturally parameterises \mathbb{R}/Λ .

$$\operatorname{Vol}(\Lambda) := \left| \det \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right|.$$

The above is independent of choice of basis. ($GL(\mathbb{Z}) \dots$)

$$\text{Vol}(\mathbb{R}^n/\Lambda) := \text{Vol}(\Lambda).$$

Back to $R = \mathbb{Q}_k$. $x_1, \dots, x_m \mathbb{Z}$ -basis of \mathbb{Q}_k .
 $\Lambda_R := f(\Lambda)$. $f(x_1), \dots, f(x_m)$ basis of Λ_R over \mathbb{Z} .

$$\begin{aligned} \text{Vol}(\mathbb{R}^n/\Lambda_R) &= \left| \det \begin{pmatrix} f(x_1) \\ \vdots \\ f(x_m) \end{pmatrix} \right| \\ &= \frac{1}{2^n} \sqrt{\text{disc } R}. \end{aligned}$$

Corollary. $K = \sum_{i=1}^n \mathbb{Q} x_i$.

$$f(K) = \sum_{i=1}^n \mathbb{Q} f(x_i).$$

Since $\{f(x_1), \dots, f(x_n)\}$ forms an \mathbb{R} -basis of \mathbb{R}^n , we get $f(K)$ is dense in \mathbb{R}^n .

Def. Λ : lattice in $\mathbb{R}^n \rightarrow \text{rank } n$.

$M \subseteq \Lambda$: sublattice (of rank n) if ...

$$\text{Vol}(\mathbb{R}^n/M) = |\Lambda/M| \cdot \text{Vol}(\mathbb{R}^n/\Lambda).$$

• Suppose G : free abelian of rank n .

$H \leq G$: assume free ab. of rank n .

$|G/H|$: finite group.

- If Λ is a lattice, then any \mathbb{Z} -basis of Λ is \mathbb{R} -lin. indep.
 (Any two \mathbb{Z} -bases related by $GL(\mathbb{Z})$. One has det $\neq 0$. So does other.)
- Similarly, if $\Lambda' \leq \Lambda$ is a subgroup, Λ' is a free abelian group.
 Suppose $\text{rank}_{\mathbb{Z}}(\Lambda') = n$. Then, Λ' is also a lattice

(One way: can pick a \mathbb{Z} -basis $\{v_1, \dots, v_n\}$ for Λ and $d_1, \dots, d_n \in \mathbb{Z}$ s.t. $\{d_1v_1, \dots, d_nv_n\}$ is a \mathbb{Z} -basis for Λ' .)

- $\Lambda_R : n$ -dimensional lattice in \mathbb{R}^n .
"f(R)"

Let $I \neq 0$ be an ideal of R . Then, I is a free abelian group of rank n .

Then, $f(I) = \Lambda_I : \text{sublattice of } \Lambda_R$.

Moreover, $\text{Vol}(\Lambda_I) = \|I\| \cdot \text{Vol}(\Lambda_R)$.

(Λ_I is "sparser".)

- Define a norm function N on \mathbb{R}^n .

For $x = (x_1, \dots, x_n)$, define

$$N(x) = x_1 \cdots x_r (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{r+s-1}^2 + x_{r+s}^2).$$

If $\alpha \in K$, then

$$f(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Re}(\sigma_{r+1}(\alpha)), \operatorname{Im}(\sigma_{r+1}(\alpha)), \dots).$$

$$\begin{aligned} N_{K/R}(\alpha) &= \left(\prod_{i=1}^r \sigma_i(\alpha) \right) \left(\sigma_{r+1}(\alpha) \overline{\sigma_{r+1}}(\alpha) \right) \cdots \left(\sigma_{r+s}(\alpha) \overline{\sigma_{r+s}}(\alpha) \right) \\ &= N(f(\alpha)). \end{aligned}$$

Main Theorem: Let Λ be an n -dimensional lattice in \mathbb{R}^n .

Then, $\exists x \in \Lambda \setminus \{0\}$ s.t.

$$|N(x)| \leq \frac{n!}{n^n} \cdot \left(\frac{8}{\pi} \right)^s \cdot \text{Vol}(\mathbb{R}^n / \Lambda).$$

Proof in next class. First some applications.

Corollary: I : nonzero ideal in $R = \mathbb{O}_K$.

Then, $\exists \alpha \in I \setminus \{0\}$ s.t.

$$|N_{K/R}(\alpha)| \leq n! / 4^{s/2} \|I\|^s$$

Then, $\exists \alpha \in I \setminus \{0\}$ s.t.

$$|N_{k/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \frac{\|I\|}{\sqrt{|disc R|}}$$

Proof

Take $\Lambda = \Lambda_I$. Let $x = f(\alpha) \in \Lambda \setminus \{0\}$ be s.t.

$$\|N(f(x))\| = \|N(x)\| \leq \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^s \text{Vol}(\mathbb{R}^s / I)$$

$$|N_{k/\mathbb{Q}}(\alpha)| = \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^s \|I\| \cdot \frac{1}{2^s} \sqrt{|disc R|}$$

$$n = \frac{1}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|disc R|} \cdot \|I\|.$$

↳ Minkowski's Constant

Corollary. Every class C in \mathbb{O}_K contains an ideal I s.t.

$$\|I\| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \sqrt{|disc R|}.$$

Proof. Pick $J (\neq 0)$ in C^\perp . By previous thm, $\exists \alpha \in J$ s.t.

$$|N_{k/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \sqrt{|disc R|} \cdot \|J\|.$$

(*) $\subseteq J \Rightarrow \langle \alpha \rangle = JI$ for some I .

Necessarily, $I \in C$.

$$\therefore |N_{k/\mathbb{Q}}(\alpha)| = \|\langle \alpha \rangle\| = \|I\| \cdot \|J\|$$

∴

$$\frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \sqrt{|disc R|} \cdot \|J\|.$$

Cancelling $\|J\|$ gives $\|I\| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \sqrt{|disc R|}$.

□

Lecture 17 (07-03-2022)

07 March 2022 17:28

Q. K : number field.

Let $A \subseteq \mathbb{O}_K$ be a subring s.t. $\text{Frac}(A) = K$.

In particular if $A \neq \mathbb{O}_K$, then A is not integrally closed.

Thus, A cannot be a UFD or a PID.

Corollary. $\mathbb{Z}[\sqrt{17}]$ is not a PID. In general, $\mathbb{Z}[\sqrt{m}]$ is not a UFD for $m \equiv 1 \pmod{4}$ squarefree.

Minkowski's Theorem

Theorem. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank n .

Then, $\exists x \in \Lambda \setminus \{0\}$ s.t.

$$N(x) \leq \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^n \cdot \text{vol}\left(\frac{\mathbb{R}^n}{\Lambda}\right).$$

N was defined as follows (in terms of r, s):

$$N((x_1, \dots, x_n)) = x_1 \cdots x_r \cdot (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2),$$

where (r, s) satisfies $r + 2s = n$.

Lemma. $\Lambda \subseteq \mathbb{R}^n$: lattice of rank n .

let $E \subseteq \mathbb{R}^n$ be :

(i) convex, (ii) centrally symmetric, ($x \in E \Rightarrow -x \in E$)

(iii) lebesgue measurable with

$$\text{vol}(E) \geq 2^n \cdot \text{vol}(\mathbb{R}^n / \Lambda).$$

Then, $\exists x^* \in E \cap \Lambda$. Further, if E is compact, then one may relax above $>$ to \geq .

Prof. Let $\{v_1, \dots, v_n\}$ be a \mathbb{Z} -basis of Λ . (It is an \mathbb{R} -basis of \mathbb{R}^n)

$F = \left\{ \sum \lambda_i v_i : \lambda_i \in [0, 1] \right\}$ is the fundamental parallelotope.

Note $0 < \text{vol}(F) = \text{vol}(\mathbb{R}^n / \Lambda) < \frac{1}{2^n} \text{vol}(E) = \text{vol}\left(\frac{1}{2} E\right)$.

$$\frac{1}{2} E = \bigcup_{x \in \Lambda} (F + x) \cap \frac{1}{2} E.$$

Thus, $\text{vol}\left(\frac{1}{2} E\right) = \sum_{x \in \Lambda} \text{vol}\left((F + x) \cap \frac{1}{2} E\right)$

$$= \sum_{x \in \Lambda} \text{vol}\left(F \cap \left(\frac{1}{2} E - x\right)\right).$$

If $\{F \cap (\frac{1}{2} E - x)\}_{x \in \Lambda}$ are pairwise disjoint, then

$$\begin{aligned} \text{vol}\left(\frac{1}{2} E\right) &= \text{vol}\left(\bigcup_{x \in \Lambda} F \cap \left(\frac{1}{2} E - x\right)\right) \\ &\leq \text{vol}(F). \end{aligned}$$

$$\therefore \text{vol}(F) < \text{vol}(E). \quad \rightarrow \leftarrow$$

Then, $F \cap \left(\frac{E}{2} - x\right)$ and $F \cap \left(\frac{E}{2} - y\right)$ have nonempty intersection for some $x \neq y, x, y \in \Lambda$.

Thus, $\frac{1}{2} e - x = \frac{1}{2} e' - y \in F \quad \text{for some } e, e' \in E$.

In turn $\frac{1}{2} (e + (-e')) = x - y \in \Lambda \setminus \{0\}$.

$-e' \in E$ by sym., $\frac{1}{2}(e + -e') \in E$ by convexity.

This proves the first fact.

Now, if E is compact and $\text{vol}(E) = 2^n \cdot \text{vol}(\mathbb{R}^n / \Lambda)$, then

$$\text{vol}\left(\left(1 + \frac{1}{m}\right) E\right) = \left(1 + \frac{1}{m}\right)^n \text{vol}(E) > 2^n \text{vol}(\mathbb{R}^n / \Lambda).$$

also has (i) - (ii)

Thus, $\exists x_m \in \left(1 + \frac{1}{m}\right) E \setminus \{0\} \text{ s.t. } x_m \in \Lambda$.

Now, $\{x_m\}_m \subseteq 2E \cap \Lambda \leftarrow \text{finite set.}$

Thus, $\exists M$ s.t. $x_M = x_m$ for infinitely many m .

$$\therefore x_M \in \bigcap_{\text{inf many } m} (1 + \frac{1}{m})E = E.$$

Corollary

Let $A \subseteq \mathbb{R}^n$ be convex, centrally symmetric, and compact.

(compact \Rightarrow closed \Rightarrow measurable)

Assume $|N(a)| \leq 1 \forall a \in A$.

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank n .

Then, $\exists \mathbf{0} \neq x \in \Lambda$ s.t.

$$|N(x)| \leq \frac{2^n}{\text{vol}(A)} \cdot \text{vol}(\mathbb{R}^n/\Lambda).$$

Proof

Let $t > 0$ be s.t. $t^n = \dots$

Let $E = tA$. Then, E is ... $\text{vol}(E) = t^n \text{vol}(A) = 2^n \text{vol}(\mathbb{R}^n/\Lambda)$.

By previous result, $\exists x \in E \setminus \{\mathbf{0}\}$ s.t. write $x = ta$ for $a \in A \setminus \{\mathbf{0}\}$

Note $|N(x)| = t^n |N(a)| \leq t^n$. \square

Theorem

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank n .

Then, $\exists x \neq \mathbf{0} \in \Lambda$ s.t.

$$|N(x)| \leq \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^n \cdot \text{vol}(\mathbb{R}^n/\Lambda).$$

Proof

(i) (Weaker version)

Let $A = \{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_i| \leq 1, i \in \{1, \dots, n\},$

$$x_{r+1} + x_{r+2}^2 \leq 1, \dots, x_{n-1}^2 + x_n^2 \leq 1\}$$

compact, centrally symm., convex

$\forall a \in A : |N(a)| \leq 1$

$\therefore \exists x \neq \mathbf{0} \in \Lambda$ s.t.

$$|N(x)| \leq \frac{2^n}{\text{vol}(A)} \cdot \text{vol}(\mathbb{R}^n/\Lambda).$$

Note that $\text{vol}(A) = 2^n \cdot \pi^{\frac{n}{2}}$.

$$\therefore |N(x)| \leq \left(\frac{4}{\pi}\right)^n \cdot \text{vol}(\mathbb{R}^n/\Lambda).$$

(ii) We pick a better A.

$$A = \{x \in \mathbb{R}^n : |x_1| + \dots + |x_r| + 2 \left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \dots + \sqrt{x_{r+2s-1}^2 + x_{r+2s}^2} \right) \leq n\}$$

Again, same properties as before. Only Convexity needs to be checked. Use AM-GM...

Also check $|N(x)| \leq 1$.

Apply AM-GM to the following n-quantities:
 $|a_1|, \dots, |a_n|, \sqrt{|a_{r+1}| + |a_{r+2}|}, \sqrt{|a_{r+3}| + |a_{r+4}|}, \dots$
 ↪ repeat twice?

Finally, we are done once we show

$$\text{vol}(A) = \frac{n^n}{n!} \cdot 2^r \cdot \left(\frac{\pi}{2}\right)^s.$$

$$\text{Let } V_{r,s}(t) := \text{vol} \left(\left\{ x \in \mathbb{R}^{r+2s} : |x_1| + \dots + |x_r| + 2 \left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \dots + \sqrt{x_{r+2s-1}^2 + x_{r+2s}^2} \right) \leq t \right\} \right)$$

$$\cdot A = V_{r,s}(n) \text{ for } n = r+2s.$$

$$\cdot V_{r,s}(t) = t^{r+2s} \cdot V_{r,s}(1).$$

$$\underline{\text{Claim}} : V_{r,s}(1) = \frac{1}{(r+2s)!} \cdot 2^r \cdot \left(\frac{\pi}{2}\right)^s$$

$$\begin{aligned} V_{r,s}(1) &= 2 \int_0^1 V_{r-1,s}(1-x) dx && (\text{for } r \geq 1) \\ &= 2 \int_0^1 (1-x)^{r-1+2s} V_{r-1,s}(1) dx \\ &= 2 \cdot \frac{1}{r+2s} \cdot V_{r-1,s}(1). \end{aligned}$$

$$\begin{aligned} \text{By induction, } V_{r,s}(1) &= \frac{2^r}{(r+2s)(r-1+2s) \cdots (1+2s)} \cdot V_{0,s}(1) \\ &= \frac{2^r}{(2s)!} \cdot V_{0,s}(1). \end{aligned}$$

$$= \frac{(1+2s)(1+2s-1)\dots(1+2s-s)}{(r+2s)!} V_{0,s}(1).$$

$$\begin{aligned}
 V_{0,s}(1) &= \iint_{\text{circle}} V_{0,s-1}(1-2r) r dr d\theta \\
 &= (2\pi) \int_0^{\frac{1}{2}} (1-2r)^{2(s-1)} \cdot r \cdot V_{0,s-1}(1) dr \quad \begin{matrix} 1-2r = u \\ dr = -\frac{du}{2} \end{matrix} \\
 &= (2\pi) V_{0,s-1}(1) \int_0^{\frac{1}{2}} u^{2(s-1)} \left(\frac{1+u}{2}\right) \frac{du}{2} \\
 &= \frac{\pi}{2(2s)(2s-1)} V_{0,s-1}(1).
 \end{aligned}$$

Again, proceed inductively to finally get the desired result. \square

Lecture 18 (10-03-2022)

10 March 2022 17:22

Thm (Dirichlet's Unit Theorem)

Let K be a number field of $\deg n$.

Let $r = \#$ real embeddings and $s = \#$ non-real embeddings.

Then,

$$U(O_K) := O_K^\times$$

$$\cong W \times V$$

where $W = \{ \text{roots of } 1 \text{ in } O_K \} \rightarrow \text{cyclic finite}$,
 $V \cong \mathbb{Z}^{r+s-1}$

Defn. A basis of V is called a fundamental system of units in O_K .

Example. ① $K = \mathbb{Q}[\sqrt{m}]$, $m < 0$.

Then, $r=0$, $s=1$. Then, $r+s-1=0$, i.e., O_K^\times is finite.

② $K = \mathbb{Q}[\sqrt{m}]$, $m > 0$.

Then, $r=2$, $s=0$. $r+s-1=1$. Then, $O_K^\times \cong \{\pm 1\} \times \mathbb{Z}$.

③ $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

$r=4$, $s=0$. $r+s-1=3$. $O_K^\times = \{\pm 1\} \times \mathbb{Z}^3$.

$$N(1+\sqrt{2}) = N(2+\sqrt{3}) = 1. \quad N(\sqrt{2}+\sqrt{3}) = \pm 1.$$

Proof of the Theorem: Let $\sigma_1, \dots, \sigma_r, \sigma_{r+1}, \bar{\sigma}_{r+1}, \dots, \sigma_{r+s}, \bar{\sigma}_{r+s}$ be as usual.

We have the map

$$f: O_K \setminus \{0\} \longrightarrow \Lambda_{O_K} \setminus \{0\}$$

$$\alpha \mapsto (\sigma_1 \alpha, \dots, \sigma_r \alpha, \operatorname{Re}(\sigma_{r+1} \alpha), \operatorname{Im}(\sigma_{r+1} \alpha), \dots).$$

Define

$$\log: \Lambda_{O_K} \setminus \{0\} \longrightarrow \mathbb{R}^{r+s}$$

$$(x_1, \dots, x_n) \mapsto (\log|x_1|, \dots, \log|x_r|, \log(x_{r+1}^{\frac{1}{2}} + x_{r+2}^{\frac{1}{2}}), \dots)$$

By abuse, denote the composition $O_K \setminus \{0\} \xrightarrow{f} \Lambda \xrightarrow{\log} \mathbb{R}^{r+s}$ by \log .

Note $\log: O_K \setminus \{0\} \longrightarrow \mathbb{R}^{r+s}$ is well-defined and

$$\alpha \mapsto (\log(\sigma_1\alpha), \dots, \log(\sigma_r\alpha), \log|\sigma_{r+1}\alpha|^2, \dots, \log|\sigma_{r+s}\alpha|^2)$$

- $\log(\alpha\beta) = \log(\alpha) + \log(\beta)$, i.e., a monoid homomorphism.
 $(\log(1) = 0)$

$\log|_{\mathcal{U}(\mathbb{O}_k)}$ is a group homomorphism.

$\log(\mathcal{U}(\mathbb{O}_k)) \subseteq H = \{y \in \mathbb{R}^{r+s} : y_1 + \dots + y_{r+s} = 0\}$.

If $F \subseteq \mathbb{R}^{r+s}$ is bounded, then

$\log^{-1}(F)$ is a finite set.

(Bounded in lattice is finite. $\mathbb{O}_k \setminus \{0\} \xrightarrow{\sim} \Lambda_k \setminus \{0\}$ is an iso.)

$\log^{-1}((0, \dots, 0)) \subset \mathcal{U}(\mathbb{O}_k^*)$ is a finite subgroup.
 $\ker(\log)$

Thus, each element r has finite order.

$\therefore \ker(\log) \subseteq \text{roots of unity in } \mathbb{O}_k^*$

It is also clear since roots of unity go to roots of unity and have modulus 1.

$\therefore \ker(\log) = \{\text{roots of unity in } \mathbb{O}_k\}$ is a finite group.

$\log(\mathcal{U}(\mathbb{O}_k))$: subgroup of \mathbb{R}^{r+s} .

If S is Ldd, then $\log^{-1}(S)$ is finite.

Thus, S is finite (since $|\ker| < \infty$.)

Ex (5.31.): If $G \leq \mathbb{R}^n$ is a subgroup s.t. all bounded subsets of G are finite, then G is a lattice.

Thus, $\log(\mathcal{U}(\mathbb{O}_k))$ is a lattice in \mathbb{R}^{r+s} .

In particular, it is a free \mathbb{Z} -module. Thus, the s.e.s.

$$0 \rightarrow \ker(\log) \rightarrow \mathcal{U}(\mathbb{O}_k) \xrightarrow{\log} \log(\mathcal{U}(\mathbb{O}_k)) \rightarrow 0$$

splits. Thus,

$$U(\mathcal{O}_k) \cong \text{ker}(\log) \oplus \underset{\sim}{\log}(U(\mathcal{O}_k)).$$

{roots of unity in \mathcal{O}_k^\times }

We have $\log(U(\mathcal{O}_k)) \cong \mathbb{Z}^d$. Need to show $d = r+s-1$.

$d \leq r+s-1$ is clear since it is contained in \mathbb{N} .

Claim: $d \geq r+s-1$.

Proof: We construct $r+s-1$ units in $U(\mathcal{O}_k)$ which map to linearly independent elements in \mathbb{R}^{r+s} .

Lemma 1. For $k \in \{1, \dots, r+s\}$, given $0 \neq \alpha \in \mathcal{O}_k$, $\exists \beta \in \mathcal{O}_k \setminus \{\alpha\}$ s.t.

$$(i) |N_{K/\mathbb{Q}}(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc } \mathcal{O}_k|}.$$

$$(ii) \log(\alpha) = (a_1, \dots, a_{r+s}), \quad \log(\beta) = (b_1, \dots, b_{r+s}) \\ \text{and } b_i < a_i \text{ for all } i \neq k.$$

Lemma 2. Fix $k \in \{1, \dots, r+s\}$. $\exists u \in U(\mathcal{O}_k)$ s.t.

$$\log u = (a_1, \dots, a_{r+s}), \quad a_i < 0 \text{ for all } i \neq k. \\ (\log u)_i$$

Proof of Lem 2 using Lem 1: Pick $\alpha_1 \in \mathcal{O}_k \setminus \{0\}$.

By Lem 1: $\exists \alpha_2 \overset{\neq 0}{\in} \mathcal{O}_k$ s.t.

$$(i) |N_{K/\mathbb{Q}}(\alpha_2)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc } \mathcal{O}_k|},$$

$$(ii) (\log \alpha_2)_i < (\log \alpha_1)_i \text{ for all } i \neq k.$$

Continue doing this to get a sequence $(\alpha_i)_{i=1}^\infty$.

$$\text{Also, } \|\langle \alpha_i \rangle\| = |N_{K/\mathbb{Q}}(\alpha_i)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc } \mathcal{O}_k|}.$$

But there are only finitely many ideals of a given bound.
(Prime fact.)

$$\therefore \exists \langle \alpha_n \rangle = \langle \alpha_{n'} \rangle \text{ for some } n < n'.$$

$$\Rightarrow \alpha_n = \alpha_{n'} u \text{ for some } u \in U(\mathcal{O}_k).$$

Taking log does the job. □

Proof of $d \geq r+s-1$ assuming Lem 1:

For each $k \in \{1, \dots, r+s\}$, let u_k be as given by Lem 2.

Now, consider the images of u_1, \dots, u_{r+s} in \mathbb{R}^{r+s} put in a matrix as:

$$\begin{pmatrix} \log u_1 \\ \log u_2 \\ \vdots \\ \log u_{r+s} \end{pmatrix}$$

Note $\sum_{i=1}^{r+s} (\log u_k)_i = 0 \quad \therefore (\log u_k)_k > 0.$

$$\begin{pmatrix} \log u_1 \\ \vdots \\ \log u_{r+s} \end{pmatrix} = (a_{ij}).$$

- $a_{ii} > 0$ for all i .
- $a_{ij} < 0$ for all $i \neq j$.
- sum of entries in any row is 0.

Thus, we wish to show $\text{rank}(a_{ij}) = r+s-1$. (\leq is clear.)

We show that C_1, \dots, C_{r+s-1} are lin. indep. over \mathbb{R} .

Suppose not. Write

$$t_1 C_1 + \dots + t_{r+s-1} C_{r+s-1} = 0.$$

$$\text{Let } |t_k| = \max_i |t_i| > 0.$$

Divide by t_k to assume $t_k = 1$ and $t_i \leq 1 \forall i$.
 \leftarrow coordinate of $\sum t_i C_i = 0$:

$$t_1 a_{1,1} + \dots + t_{r+s-1} a_{r+s-1, r+s-1} = 0.$$

$$\therefore a_{r+s-1, r+s-1} = \sum_{i \neq k} t_i (-a_{r+s-1, i}) \leq \sum_{i \neq k} (-a_{r+s-1, i})$$

$$\Rightarrow a_{r+s-1, 1} + \dots + a_{r+s-1, r+s-1} \leq 0.$$

Add $a_{r+s-1, r+s}$ to get

$$0 \leq a_{r+s-1, r+s} < 0. \rightarrow \leftarrow$$

Thus, we have finished
the proof (modulo Lem 1). \blacksquare

Proof of Lemma 1: $n = r+2$.

$$E = \{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_{i1}| \leq c_i, 1 \leq i \leq r, \\ x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \dots\}$$

for c_1, \dots, c_{r+s} are picked in:

$$0 < c_i < e^{a_i} = \exp(a_i), \quad i \neq k \quad \text{and}$$

pick c_k s.t. $c_1 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{\text{disc } \mathcal{O}_K}.$

$$\begin{aligned} \text{vol}(E) &= 2^r c_1 \cdots c_r \cdot \pi^s c_{r+1} \cdots c_{r+s} \\ &= 2^r \pi^s \left(\frac{2}{\pi}\right)^s \sqrt{\text{disc } \mathcal{O}_K} = 2^{r+s} \sqrt{\text{disc } \mathcal{O}_K}. \\ &= 2^{r+s} \cdot 2^s \text{vol}(\mathbb{R}/\Lambda_{\mathcal{O}_K}) \\ &= 2^h \text{vol}(\mathbb{R}/\Lambda_{\mathcal{O}_K}). \end{aligned}$$

Thus, by our earlier result, we are done as E is compact, convex, centrally symmetric. \square

For $m > 1$ and $K = \mathbb{Q}[\sqrt{m}]$, we have $\mathcal{U}(\mathcal{O}_K) = \{\pm 1\} \times \langle u \rangle$.
 u is determined uniquely by imposing $u > 1$.
Such a u is called a fundamental unit.

Exercise (5.33). $m > 2$ sq. free.

Case 1. $m \equiv 2, 3 \pmod{4}$.

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$$

Choose $a \leq b$ smallest s.t. $b^2 m + 1$ or $b^2 m - 1$ is a square, say a^2 for $a \geq 0$. Then $a + b\sqrt{m}$ is the fund. unit.
 $\hookrightarrow (\text{show!})$

Case 2. $m \equiv 1 \pmod{4}$.

Pick smallest $b \geq 0$ s.t. $b^2 m \pm 1$ is a square, say a^2 .
 $(a \geq 0)$

Then, $\frac{a+b\sqrt{m}}{2}$ is the fund. unit.

Example. $\mathbb{Z}[\sqrt{3}]$. Want $3b^2 \pm 1 = a^2$.

$b=1$ and $a=2$ works. $\therefore 2+\sqrt{3}$ fund. unit.

$$\cdot \mathbb{Z}[\sqrt{5}] : \quad 5b^2 \pm 4 = a^2. \quad (1,1) \text{ works.}$$

$$\cdot \mathbb{Z}[\sqrt{94}] : \quad 2143295 + 22104\sqrt{94}.$$

$$\cdot \mathbb{Z}[\sqrt{95}] : \quad 31 + 4\sqrt{95}.$$

Lecture 19 (14-03-2022)

14 March 2022 17:29

Defn. $| \cdot | : K \rightarrow \mathbb{R}_{\geq 0}$ is an absolute value on K if

$$(i) |x| = 0 \Leftrightarrow x = 0.$$

$$(ii) |xy| = |x||y|.$$

$$(iii) \exists c > 0 \text{ s.t. } |x+y| \leq c \max(|x|, |y|).$$

Example. (Trivial absolute value)

$$|x| = \begin{cases} 0 &; x=0, \\ 1 &; x \neq 0. \end{cases}$$

Note:

$$|1| = 1.$$

For $x \in K^*$:

$$|x^{-1}| = |x|^{\gamma}.$$

$$|x| < 1 \Leftrightarrow |x^{-1}| > 1.$$

Assumption: We will consider only nontrivial values, i.e., $\exists x \in K^* \text{ s.t. } |x| \neq 1$.
Thus, $\exists x, y \in K^*$ s.t. $|x| < 1 < |y|$, by the calc. on right.

Defn. $| \cdot |, | \cdot |_1 : K \rightarrow \mathbb{R}_{\geq 0}$ are said to be equivalent if

$$(1) |x|_1 < 1 \Leftrightarrow |x| < 1 \quad \forall x \in K.$$

Theorem. The above is equivalent to: (2) $\exists s > 0$ s.t.

$$|x|_1 = |x|^s \quad \forall x \in K.$$

Proof. (2) \Rightarrow (1) is clear.

(1) \Rightarrow (2). Fix $y \in K$ s.t. $|y| > 1$.

let $x \in K^*$. Then, can write $|x| = |y|^{\alpha}$ for some $\alpha \in \mathbb{R}$.

let $\left(\frac{m_i}{n_i}\right) \in \mathbb{Q}^*$ be a sequence decreasing to α .

$$|x| = |y|^{\alpha} < |y|^{\frac{m_i}{n_i}}$$

$$\Rightarrow |x^{n_i}| < |y^{m_i}|$$

$$\Rightarrow \left| \frac{x^{n_i}}{y^{m_i}} \right| < 1$$

$$\Rightarrow \left| \frac{x}{y^{m_i/n_i}} \right| < 1$$

$$\Rightarrow |x|_1 < |y|^{m_i/n_i}.$$

Let $i \rightarrow \infty$ to get $|x|_i \leq |y|_i^\alpha$.

Then, $|x| = |y|^\alpha \Rightarrow |x|_i \leq |y|_i^\alpha$.

By considering an increasing sequence, we get the reverse inequality.

Thus,

$$|x| = |y|^\alpha \Rightarrow |x|_i = |y|_i^\alpha.$$

Thus, $\frac{\log |x|}{\log |x|_i}$ is constant for x s.t. $|x| \neq 1, 0$.
let this constant be s .

Thus, $|x| = |x|_i^s$ for all $x \in K$. □

Defn. Let $|\cdot|: K \rightarrow \mathbb{R}_{\geq 0}$ be an absolute value s.t.

$$|x+y| \leq |x| + |y|.$$

Then, $|\cdot|$ is said to be a valuation.

- $|\cdot|$ is said to be non-Archimedean if $|x+y| \leq \max(|x|, |y|)$.
- $|\cdot|$ is said to be Archimedean if not equivalent to any non-Archimedean valuation.

Example ① $K = \mathbb{R}$ or \mathbb{C} with usual $|\cdot|$.

Then, $|\cdot|$ is an valuation.

Claim: $|\cdot|^s$ is not non-Archimedean $\forall s$.

Prof. $|1+1|^s = 2^s$

$$\max(|1|, |1|) = 1.$$

$$2^s > 1 \text{ for all } s > 0. \quad \square$$

② Suppose K embeds within \mathbb{R} or \mathbb{C} (wlog, $K \subseteq \mathbb{C}$)

Then, we have an evaluation on K via restriction.

Then, this is again Archimedean since the above argument will go through.

Lemma. Let R : Dedekind domain, and $0 \neq p \in \text{Spec}(R)$.
Then, R_p is a local PID.

Proof. Local and ID is clear.

Let $x \in p \setminus p^2$.

$$\text{Then, } \langle x \rangle = p^{r_1} p_1^{r_1} \cdots p_t^{r_t} \text{ for } p_i \neq p.$$

Now, localising gives

$$xR_p = pR_p.$$

{ Now, since pR_p is also a DD, we see that
 $\text{Spec}(pR_p) = \{0, pR_p\}$. Thus, all ideals are principal. \square

Also, Any ideal I of R_p is of the form IR_p for an ideal $I \subset R$.

$$\text{Write } I = p^e p_1^{r_1} \cdots p_t^{r_t}. \text{ Localise to get } IR_p = (pR_p)^e = \langle x \rangle. \square$$

Defn. If R is a local PID, then R is a discrete valuation ring.
(DVR)

Example: R PID \Rightarrow Every localisation is a PID
 $\Rightarrow R_p$ is a DVR for all $p \in \text{Spec}(R)$.

More generally, R : DD $\Rightarrow R_p$ is a DVR for all primes p .

EXAMPLE OF NON-ARCHIMEDEAN VALUATION:

Let (R, ν) be a DVR which is not a field.

$$\nu = \langle \pi \rangle.$$

Given $a \in R \setminus \{0\}$, we can write $a = u \cdot \pi^n$ for some unit u
 $(; \text{we have } \langle a \rangle = \nu^n \text{ for some unique } n \geq 0.)$ and $n \geq 0$ (unique n).

Define $\nu: R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ by $\nu(a) = n$.

Fix $r \in (0, 1)$, and let $K = \text{Frac}(R)$.

$$\text{Define } 1: K \rightarrow \mathbb{R}_{\geq 0} \text{ by}$$

$$\frac{a}{b} \mapsto \begin{cases} r^{\nu(a) - \nu(b)}, & a \neq 0, \\ 1, & a = 0. \end{cases}$$

↓
independent
of generator
of ν

$$b \quad \left\{ \begin{array}{l} 0 \\ a = 0. \end{array} \right.$$

(This is well-defined.)

- $|0| = 0$.

- $|xy| = |x||y|$ is also clear.

- $|x+y| \leq \max(|x|, |y|)$.

Proof: We can write $x = u \cdot \pi^n$ and $y = v \cdot \pi^m$
 (Assume $x, y \neq 0$) for $u, v \in U(\mathbb{R})$ and $n, m \in \mathbb{Z}$.

Assume $n \geq m$.

$$\begin{aligned} x + y &= u\pi^n + v\pi^m \\ &= \pi^m v \left(\underbrace{\frac{u\pi^{n-m}}{v} + 1}_{\in \mathbb{R}} \right) \end{aligned}$$

$$\begin{aligned} \therefore x + y &= u' \pi^\alpha \text{ for some } \alpha \geq m. \\ \therefore |x+y| &= r^\alpha \leq r^m = \max(r^m, rv) = \max(|x|, |y|). \quad \square \end{aligned}$$

Lecture 20 (17-03-2022)

17 March 2022 17:31

Recall: $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$ absolute value

if $\cdot |x| = 0 \Leftrightarrow x = 0$,

$$\cdot |xy| = |x||y|,$$

$$\cdot |x+y| \leq C \max(|x|, |y|) \text{ for some } C > 0.$$

We assume our absolute values are non-trivial: $\exists x \in K^* \text{ s.t. } |x| \neq 1$.

Further if $|x+y| \leq |x| + |y|$, then $|\cdot|$ is a valuation on K .

Called non-Archimedean if $|x| + |y| \leq \max(|x|, |y|)$. Else, Archimedean.

Defn. An exponential valuation is a map

$$v : K \rightarrow \mathbb{Z} \cup \{\infty\} \text{ s.t.}$$

$$\cdot v(x) = \infty \Leftrightarrow x = 0,$$

$$\cdot v(xy) = v(x) + v(y), \quad (K^* \rightarrow \mathbb{Z} \text{ is a group homom.})$$

$$\cdot v(x+y) \geq \min(v(x), v(y)).$$

Lemma. Let $v : K \rightarrow \mathbb{Z} \cup \{\infty\}$ be an exponential valuation.

Then, for any $c \in (0, 1)$, the map

$$|\cdot|_v : K \rightarrow \mathbb{R}_{\geq 0} \text{ defined by}$$
$$x \mapsto c^{v(x)}$$

is a non-Archimedean valuation.

Proof. Easy check \square

Example. Let R be a Dedekind domain (not a field).

Let $p \neq 0$ be a prime ideal of R .

Define, for $x \neq 0$,

$v_p(x) = \text{power of } p \text{ in the prime factorisation of } x$.

Extend this to K^* by

$$v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y).$$

Finally, $v_p(0) := \infty$. Then, v_p is an exp. val.

Only nontrivial part is $v_p(x+y) \geq \min(\dots)$

To check that, we localise at p to get

$$xR_p = (\pi^n), \quad yR_p = (\pi^m), \quad \text{where}$$

$$pR_p = (\pi), \quad n = v_p(x), \quad m = v_p(y).$$

Then, $x = u \cdot \pi^n, \quad y = v \cdot \pi^m$ with $n \geq m$.

$$\text{Then, } \pi^m \mid (n+y).$$

$$\text{Thus, } v_p(x+y) \geq m = \min(v_p(x), v_p(y)).$$

This extends to $x, y \in K$ as well.

This $| \cdot |_p = c^{v_p}$ is a non-Archimedean valuation.

If $c, c' \in (0, 1)$, then the two valuations are equivalent

$$\overbrace{\hspace{780pt}}^x$$

Lemma: Let $| \cdot |: K \rightarrow \mathbb{R}_{\geq 0}$ be a non-Archimedean valuation.

$$\text{let } R := \{x \in K : |x| \leq 1\},$$

$$\mathfrak{p} := \{x \in R : |x| < 1\}.$$

Then, (R, \mathfrak{p}) is a local ring.

Proof. By non-Arch.: $x, y \in K$ satisfy

$$|x+y| \leq \min(|x|, |y|).$$

$\therefore R$ closed under $+$.

$$0, 1 \in R \quad |xy| = |x||y|. \quad \therefore R \text{ is a ring.}$$

\mathfrak{p} is an ideal.

We claim: $R \setminus \mathfrak{p} = \text{units of } R$.

(\supseteq) Clear since $1 \notin \mathfrak{p}$. Thus, \mathfrak{p} is a proper ideal.

(\subseteq) Let $x \in R \setminus \mathfrak{p}$. Then, $|x| = 1$.

Thus, x is a unit in K with $|x^{-1}| = 1$.

$$\therefore x^{-1} \in R.$$

□

Note: If $x \in k^*$, then either x or $x^{-1} \in k$.

Defn. R is a valuation ring if R is a domain such that for any $0 \neq x \in \text{Frac}(R)$, one of x or x^{-1} is in R .

(Lemma)
(contd.) Further, if R is a DVR, then $|k^*| \cong \mathbb{Z}$.
↳ image of k^* under l-l

Proof. $p = (\pi)$. If $u \in \mathcal{U}(R)$ then $|u| = 1$.

$$x \in R \setminus \{0\} : x = u \cdot \pi^n.$$

$$\Rightarrow |x| = |\pi|^n \text{ for } n \geq 0.$$

Finally, for $\frac{x}{y} \in k^*$, we have

$$\left| \frac{x}{y} \right| = |\pi|^{n-m}.$$

Thus, $|k^*|$ is generated by $|\pi|$. □

Conversely, if $|k^*|$ is cyclic ($\cong \mathbb{Z}$), then R is a DVR.

Proof. We already known that R is a local ring with max'l ideal p . Need to show p is principal.

Let $\phi: |k^*| \cong \mathbb{Z}$ be an isomorphism.

Let $x \in k^*$ be s.t. $\phi(|x|) = 1$.

If $x \notin R$, then $x^{-1} \in R$. By replacing ϕ with $-\phi$, assume $x \in R$. $\therefore \mathbb{Z}_{\geq 0} \subseteq |R \setminus \{0\}|$. Thus, equality must hold. (why?)

Claim: $(x) = p$. (In turn, $\phi(|R \setminus \{0\}|) = \mathbb{Z}_{\geq 0}$)

Proof. (\subseteq) $x \in \mathcal{U}(R)$ as $\phi(|x|) \neq 0$. $\therefore x \in p$

(\supseteq) let $y \in p$. let $n := \phi(|y|)$.
 $(\because y^{-1} \notin R, n > 0)$ $\therefore \phi(|x^{-n}y|) = 0$

$$\therefore |x^{-n}y| = 1.$$

$\therefore x^{-n}y$ is a unit in R , we are done. □

Lemma:

$| \cdot | : K \rightarrow \mathbb{R}_{\geq 0}$: valuation.

Can consider the image of \mathbb{Z} in K , call it $\mathbb{Z}|_K$.

$| \cdot |$ is non-Archimedean if $|\mathbb{Z}|_K|$ is bounded.

Proof: (\Rightarrow) $|1 + \dots + 1| \leq |1|$.

Also, $| -1 | = 1 \therefore |n| \leq 1$ for all $n \in \mathbb{Z}|_K$.

(\Leftarrow) Suppose $r \in \mathbb{R}$ is an upper bound of $|\mathbb{Z}|_K$.

$r \geq 1$ as $|1| = 1$.

WTS: $|x+y| \leq \max\{|x|, |y|\}$ for all x, y .

$$\begin{aligned}
 |x+y|^n &= |(x+y)^n| = \left| \sum_{i=0}^n \binom{n}{i} x^i y^{n-i} \right| \quad \text{triangle inequality} \\
 &\leq \sum_{i=0}^n \left| \binom{n}{i} \right| |x|^i |y|^{n-i} \quad \text{since } | \cdot | \text{ is a valuation} \\
 &\leq r \cdot (n+1) \max(|x|^n, |y|^n).
 \end{aligned}$$

$$\Rightarrow |x+y| \leq r^{\frac{1}{n}} (n+1)^{\frac{1}{n}} \max(|x|, |y|).$$

Let $n \rightarrow \infty$ to get

$$|x+y| \leq \max(|x|, |y|). \quad \blacksquare$$

Valuations of \mathbb{Q} :

- For $p \geq 2$ prime, we have the evaluation

$$| \cdot |_p = c^{\nu_p}, \quad c \in (0, 1), \text{ where}$$

$\nu_p : \mathbb{Q} \rightarrow \mathbb{Z} \cup \{\infty\}$ exponential valuation is defined as

$$\nu_p\left(p^t \frac{m'}{n'}\right) := t \quad \text{for } (p, m'n') = 1.$$

$$(\nu_p(0) := \infty)$$

One choice of c is $\frac{1}{p}$.

$| \cdot |_p = \left(\frac{1}{p}\right)^{\nu_p}$ is called the p -adic valuation on \mathbb{Q} .

As noted, this is a non-Archimedean valuation.

Thus, we can talk about the valuation ring of $| \cdot |_p$.

For $x \in \mathbb{Q}^\times$, note that

$$|x|_p \leq 1 \Leftrightarrow \frac{1}{p^{\nu_p(x)}} \leq 1 \Leftrightarrow \nu_p(x) \geq 0 \Leftrightarrow x \in \mathbb{Z}(p).$$

$\therefore \mathbb{Z}(p)$ is a DVR.

- Theorem. • Any non-Archimedean valuation on \mathbb{Q} is equivalent to a p -adic valuation.
• Any Archimedean valuation on \mathbb{Q} is equivalent to the restriction of absolute value on \mathbb{R} .

Corollary. (Product Theorem)

Define $| \cdot |_p$ as earlier, let $| \cdot |_\infty$ be restriction of usual $| \cdot |$ on \mathbb{R} to \mathbb{Q} .
Then, for all $x \in \mathbb{Q}^\times$,

$$\prod_{p \in \text{Primes of } \mathbb{Q}} |x|_p = 1. \quad \begin{matrix} (\text{Have picked a representative}) \\ (\text{from each class.}) \end{matrix}$$

Proof (of corollary). Note that the product above is finite for any $x \in \mathbb{Q}^\times$.

- Since valuations are multiplicative, it suffices to prove it for primes and ± 1 . (Clear for ± 1 since $|\pm 1|_p = 1 \forall p$)
- Thus, we now prove it for primes p .

But note

$$|p|_p = \frac{1}{p}, \quad |p|_\infty = p, \quad |p|_q = 1 \quad \text{for primes } q \neq p. \quad \square$$

Defn. K : field.

An equivalence class \mathcal{F} of valuations on K is called a prime in K .
 \mathcal{F} is called a finite prime if it consists of non-Arch. valuations,

and an infinite prime otherwise.

- The Product Theorem is a corollary in the sense that we can pick a "normalised" representative $\prod_{p \in P} p$ s.t.

$$\prod_{\substack{p: \text{ primes} \\ \text{in } \mathbb{Q}}} |x|_p = 1.$$

Proof of theorem: Let $| \cdot |$ be a valuation on \mathbb{Q} .

Fix $m, n \geq 2$. Then, $\exists r \in \mathbb{N} \cup \{\infty\}$ s.t.

$$n^r \leq m < n^{r+1}.$$

$$m = a_0 + a_1 n + \dots + a_r n^r \quad \text{for } a_i \in \{0, 1, \dots, n-1\}.$$

$$N = \max \{|1|, |m|\}.$$

$$\therefore |m| \leq \sum |a_i| N^i$$

$$\leq \sum |a_i| N^i$$

$$\leq \sum (a_i |1|) N^i$$

$$\leq \sum a_i N^i$$

$$\Rightarrow |m| \leq (r+1) \cdot n \cdot N^r$$

$$\leq \left(1 + \frac{\log m}{\log n}\right) \cdot n \cdot N^{\log m / \log n}.$$

$$\begin{aligned} n^r &\leq m \\ \Rightarrow r &\leq \frac{\log m}{\log n}. \end{aligned}$$

$$\text{Thus, } |m^s| \leq \left(1 + \frac{s \log m}{\log n}\right) n \cdot N^{s \log m / \log n}.$$

$$\Rightarrow |m| \leq \left(1 + s \frac{\log m}{\log n}\right)^s n^s N^{\log m / \log n}.$$

Let $s \rightarrow \infty$ to get

$$|m| \leq N^{\log m / \log n}.$$

Case 1. $|R| > 1$ for all $R > 1$.

Then, $N = \max \{|1|, |m|\} = |m|$.

Thus,

$$|m| \leq |m|^{\log m / \log n}.$$

Thus,

$$|m| \leq |n| \stackrel{\log m / \log n}{\Rightarrow} |m|^{\frac{1}{\log m}} \leq |n|^{\frac{1}{\log n}}.$$

But interchanging $m \leftrightarrow n$ shows $|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{\log n}}$ for all $m, n > 1$.

Let this constant be C .

$$\text{Then, } |m| = C^{\log m}.$$

$$\text{Also, } |m| = |m|.$$

$$\therefore |m| = C^{\log |m|} \quad \forall m \in \mathbb{Z} \setminus \{0\}.$$

$$\text{Write } C = e^\alpha \text{ gives } |m| = |m|^\alpha \quad \forall m \in \mathbb{Z} \setminus \{0\}.$$

This finishes the proof.

Case 2. $|n| \leq 1$ for some $n > 1$.

$$\text{Then, } N=1. \quad \therefore |m| \leq 1 \quad \forall m > 1.$$

$$\Rightarrow |\mathbb{Z}| \leq 1.$$

$\therefore \mathbb{Z}$ is non-Archimedean.

Let $R \subseteq \mathbb{Q}$ be the valuation ring of \mathbb{Z} .
"

$$\{x \in \mathbb{Q} : |x| \leq 1\}.$$

$$\text{Let } p = \{x \in \mathbb{Q} : |x| < 1\} \subseteq R$$

Note that $p \neq 0$ since nontrivial valuation.

Also, $p \cap \mathbb{Z}$ is a nonzero prime ideal.

$$\therefore p \cap \mathbb{Z} = p\mathbb{Z} \text{ for some prime } p \geq 2.$$

$$\therefore p \subseteq p.$$

Also, if $m \in \mathbb{Z}$ with $p \nmid m$, then $m \notin p$.

$\therefore m$ is a unit.

$$\therefore \mathbb{Z}(p) \subseteq R \subseteq \mathbb{Q}.$$

Claim: \mathbb{Z} is equiv to $\mathbb{Z}(p)$.

Proof. Given $x \in \mathbb{Q} \setminus \{0\}$, write $x = p^r \frac{m}{n}$ with $(p, mn) = 1$.

Then, m and n are units in R .

$$\therefore |x| = |p^r| \cdot |m|$$

Then, m and n are units in \mathbb{R} .

$$\therefore |x| = |p^r| \cdot \left| \prod_{i=1}^n m_i^{e_i} \right|$$
$$= |p|^r.$$

◻

They are done.

◻

- Reference:
- Algebraic Number Theory by Janusz.
 - Online notes by James Milne.

Lecture 21 (21-03-2022)

21 March 2022 17:11

Completion:

K : field, $|\cdot|: K \rightarrow \mathbb{R}_{\geq 0}$ valuation on K .

Let $(a_n)_n$ be a Cauchy sequence in K (wrt $|\cdot|$). ↳ this induces a metric
want to complete field w.r.t. this
 $d(x, y) = |x - y|$

That is, $\forall \varepsilon > 0 \exists N \in \mathbb{N}$ s.t. $|a_n - a_m| < \varepsilon \quad \forall n, m \geq N$.

Ex. If $(a_n)_n$ is Cauchy in K , then $(|a_n|)_n$ is Cauchy in \mathbb{R}

We say that a_n converges to $a \in K$ if

$$\lim_{n \rightarrow \infty} |a_n - a| = 0.$$

↳ limit in \mathbb{R}

Defn. $(K, |\cdot|)$ is a complete field if every Cauchy sequence in K converges in K .

Example : $(\mathbb{Q}, |\cdot|_\infty)$ is not complete.

Completion of $(K, |\cdot|)$:

Let ℓ be the set of all Cauchy sequences in K .

Let γ be the set of all Cauchy sequences converging to 0.

Ex. $(a_n)_n, (b_n)_n$ Cauchy in $K \Rightarrow (a_n + b_n)_n$ and $(a_n b_n)_n$ are Cauchy in K .

Thus, we have obvious definitions of $+$ and \cdot on ℓ .

This make $(\ell, +, \cdot)$ a ring with $1 = (1)_n$ and $0 = (0)_n$.

Moreover, γ is an ideal in ℓ .

Dfn. $\hat{K} = \mathcal{C}/\gamma$: ring.

Claim. \hat{K} is a field.

Proof. Let $(a_n)_n \in \mathcal{C} \setminus \gamma$. $(|a_n|)_n$ is Cauchy in \mathbb{R} . Thus, it has a limit a . Furthermore, $a > 0$ since $(a_n)_n \notin \gamma$. Thus, $|a_n| \geq \frac{a}{2} > 0$ for $n \gg 0$.

Define $b_n = \frac{1}{a_n}$ for $n \gg 0$. ($|b_n|$ converges to γ .)
Thus, $(a_n b_n)_n$ is Cauchy.

Then, $(a_n b_n)_n$ is eventually 1.

Thus, $(a_n b_n)_n \equiv 1 \pmod{\gamma}$. \square

We have the map $i : K \rightarrow \hat{K}$, $a \mapsto (a)_n$.
 $i(1) = 1$, thus i is injective.
 i is a ring homom. in fact.

Valuation on \hat{K} :

Define $|\cdot|_0 : \mathcal{C} \rightarrow \mathbb{R}_{\geq 0}$ by
 $(a_n)_n \mapsto \lim_{n \rightarrow \infty} |a_n|$.

$$\cdot |(a_n)_n|_0 = 0 \Leftrightarrow (a_n)_n \in \gamma.$$

$$\cdot |(a_n b_n)_n|_0 = \lim_{n \rightarrow \infty} |a_n||b_n|$$

$$= \left(\lim_{n \rightarrow \infty} |a_n| \right) \left(\lim_{n \rightarrow \infty} |b_n| \right) = |(a_n)_n|_0 |(b_n)_n|_0.$$

$$\cdot |(a_n + b_n)_n|_0 = \lim_{n \rightarrow \infty} |a_n + b_n|$$

$$\leq \lim_{n \rightarrow \infty} |a_n| + \lim_{n \rightarrow \infty} |b_n| = |(a_n)_n|_0 + |(b_n)_n|_0.$$

$|\cdot|_0$ makes sense modulo γ . This defines a valuation on \hat{K} .

Also, for $x \in K$,

$$|i(x)|_0 = |x|.$$

Thus, $\|\cdot\|_0$ restricts to $\|\cdot\|$ on K (identified appropriately).

Claim: $(\hat{K}, \|\cdot\|_0)$ is complete. We simply denote $\|\cdot\|_0$ as $\|\cdot\|$.

Proof: Let $(u^{(n)})_n$ be a Cauchy seq. in \hat{K} .

$$x_n : u^{(n)} = (x_k^{(n)})_k$$

↪ Cauchy in K .

Given $\epsilon > 0$, $\exists N$ s.t.

$$|u^{(n)} - u^{(m)}| < \epsilon \quad \forall n, m \geq N$$

||

$$\lim_{k \rightarrow \infty} |x_k^{(n)} - x_k^{(m)}| < \epsilon. \quad (*)$$

Step 1. Fix n . $x^{(n)} \in \ell$.

$$\exists N_1$$
 s.t. $|x_q^{(n)} - x_r^{(n)}| < \frac{1}{n} \quad \forall q, r \geq N_1$

Replacing $(x_k^{(n)})_k$ by $(x_{k+N_1}^{(n)})_k$, we may assume

$$|x_q^{(n)} - x_r^{(n)}| < \frac{1}{n} \quad \forall q, r.$$

Note that $(x_k^{(n)})_k - (x_{k+N_1}^{(n)})_k \in \eta$.

Step 2. Let $u := (x_i^{(n)})_n$. Note that u is a sequence in K .

We show $u \in \ell$ and $\lim_{n \rightarrow \infty} |u^{(n)} - u| = 0$.

Thus, $u^{(n)} \rightarrow u \in \hat{K}$ and we are done.

(i) $u \in \ell$.

Proof.

$$\begin{aligned}
 & \text{Let } \varepsilon > 0 \text{ be given.} \\
 |x_i^{(n)} - x_i^{(m)}| & \leq |x_i^{(n)} - x_q^{(n)}| + |x_q^{(n)} - x_q^{(m)}| \\
 & \quad + |x_q^{(m)} - x_i^{(m)}| \\
 & \leq \frac{1}{n} + \frac{\varepsilon}{3} + \frac{1}{m} < \varepsilon
 \end{aligned}$$

for $n, m > 0$.

(ii) $x^{(n)} \rightarrow x$.

$$\underline{\text{Proof.}} \quad |x^{(n)} - x| = \lim_{k \rightarrow \infty} |x_k^{(n)} - x_k^{(k)}|.$$

Given $\varepsilon > 0$:

$$\begin{aligned}
 |x_k^{(n)} - x_k^{(k)}| & \leq \underbrace{|x_k^{(n)} - x_1^{(n)}|}_{\leq \frac{1}{n}} + \underbrace{|x_1^{(n)} - x_1^{(k)}|}_{\leq \varepsilon/2}, \\
 & \text{since } n \in \mathbb{N}
 \end{aligned}$$

This gives (ii).

We are done \square

Defn. $(K, |\cdot|)$: field with a valuation.

$(\hat{K}, |\cdot|_0)$: complete field w.r.t. $|\cdot|_0$.

$i: K \rightarrow \hat{K}$ embedding s.t. $|x| = |i(x)|_0$ for all $x \in K$.

$i(K)$ is dense in \hat{K} .

Then, $(\hat{K}, |\cdot|_0)$ is called a completion of $(K, |\cdot|)$.

Thm. Every $(K, |\cdot|)$ has a completion.

Proof. Content of earlier discussion

Uniqueness of Completion up to Isomorphism:

Lemma. Let $f: (K, |\cdot|) \rightarrow (L, |\cdot|')$ be a homomorphism,

i.e., $f: K \rightarrow L$ is a ring homom and $|x| = |f(x)|'$ $\forall x \in K$.

Then, $\exists! \hat{f}: \hat{K} \rightarrow \hat{L}$ ring homom s.t. $|u| = |\hat{f}(u)|' \forall u \in \hat{K}$.

further, $i' \circ f = \hat{f} \circ i$.

$$\begin{array}{ccc}
 (K, |\cdot|) & \xrightarrow{f} & (L, |\cdot|') \\
 i \downarrow & \Downarrow & \downarrow i' \\
 \hat{K} & & \hat{L}
 \end{array}$$

$$i \downarrow \quad \quad \quad \downarrow i' \\ (\widehat{K}, |\cdot|) \xrightarrow[\widehat{f}]{} (\widehat{L}, |\cdot|')$$

Here, \widehat{K} and \widehat{L} are defined via Cauchy sequences as earlier.

Proof. Let $(a_n)_n$ be Cauchy in K .

Then, $(fa_n)_n$ is Cauchy in L .

Moreover, the class of $(fa_n)_n$ depends only on the class of $(a_n)_n$.

Define $\widehat{f}([\{a_n\}_n]) := [\{fa_n\}_n] \in \widehat{L}$.

All desired properties are easy to see. \square

Corollary. The completion of $(K, |\cdot|)$ is unique up to unique isomorphism.

EXAMPLES. ① $(\mathbb{Q}, |\cdot|_\infty)$.

Completion is \mathbb{R} .

② $(\mathbb{Q}, |\cdot|_p) \rightarrow p\text{-adic valuation}$.
non-Archimedean.

The completion is denoted \mathbb{Q}_p .

Note $|p^n| = \frac{1}{p^n}$ for $n \in \mathbb{N}$.

$\therefore (p^n)_n$ is a null sequence in $(\mathbb{Q}, |\cdot|_p)$.