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:
  1. (i) α is an algebraic integer.
  2. (ii) $\mathbb{Z}[\alpha]$ is f.g. as a group.
  3. (iii) $\exists$ a subring $A \subset \mathbb{C}$ s.t. $\alpha \in A$ and A is f.g. as a group.
  4. (iv) $\exists$ a f.g. subgroup $A \subset \mathbb{C}$ with $A \neq 0$ s.t. $\alpha A \subseteq A$.

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

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

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

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
  Let $m \in \mathbb{Z}$ be square-free. Then,

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

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

↳ Exercise, can show with machinery so far.

- $\omega = e^{2\pi i/m}$. Then, $\mathcal{O}_{\mathbb{Q}[\omega]} = \mathbb{Z}[\omega]$. → will show later!

- Theorem: ① $[\mathbb{Q}[\omega] : \mathbb{Q}] = \varphi(m)$.

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

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

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 $(\mathbb{Z}/p^r)^\times$ is cyclic.

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

$(\mathbb{Z}/2^2)^* \cong C_2$,

$(\mathbb{Z}/2^n)^* \cong C_2 \times C_{2^{n-2}}$ for $n \geq 3$.

- $(\mathbb{Z}/p)^* \cong C_{p-1}$ $\forall p$ prime.

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

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

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

$\mathbb{Q}[\omega]^H$ is the unique quadratic

$$\begin{array}{c} \mathbb{Q}[\omega] \\ | \end{array} \; H$$

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

$$\begin{array}{c} \mathbb{Q}[\omega] \\ | \\ \mathbb{Q}[\omega]^H \\ |\ \deg = 2 \\ \mathbb{Q} \end{array}$$

As we shall see,

$$\mathbb{Q}[\omega]^H = \mathbb{Q}[\sqrt{\pm p}], \quad \begin{array}{l} + \text{ if } p \equiv 1\ (4), \\ - \text{ if } p \equiv 3\ (4). \end{array}$$

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 odd $\Rightarrow$ $(-\omega)$ primitive $2m^{th}$ root of 1.)
Let n be s.t. $\eta^n = 1$.
Suffices to show $n \mid m$.
By elementary group theory, $\mathbb{Q}[\omega]^\times$ contains an ℓ^{th} primitive root of 1, with $\ell = \operatorname{lcm}(m, n)$.

Thus, $\mathbb{Q}[\omega] \subset \mathbb{Q}[e^{2\pi i/\ell}] \subset \mathbb{Q}[\omega]$.
$\Rightarrow \varphi(m) = \varphi(\ell)$. $\because m \mid \ell$.
$\Rightarrow m = \ell$. ☒

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

Def^n. Let $K \subseteq \mathbb{C}$ be a degree n ext^n of $\mathbb{Q}$.
Let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of $K/\mathbb{Q}$ in $\mathbb{C}$.
Recall the functions trace and norm:

$$Tr_{K/\mathbb{Q}} : K \longrightarrow \mathbb{Q} \quad \text{and}$$
$$N_{K/\mathbb{Q}} : K \longrightarrow \mathbb{Q}$$

defined as

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

A priori, not clear why $Tr_{K/\mathbb{Q}}$ 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 $Tr_{K/\mathbb{Q}}$ is additive and $N_{K/\mathbb{Q}}$ is multiplicative. Thus, both are homomorphisms interpreted with correct domain and operation.

- Properties.

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

More generally:

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

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

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

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

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

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

$$\text{Ily } \quad N_{K/\mathbb{Q}}(\alpha) = (-1)^n f(0) \in \mathbb{Q}.$$

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

Let m and ℓ be the degrees as shown:

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

$n = m\ell$.

Let $\theta_1, \dots, \theta_\ell$ 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, $\mathrm{Tr}_{K/\mathbb{Q}}(\beta) = m \cdot \mathrm{Tr}_{\mathbb{Q}[\beta]/\mathbb{Q}}(\beta) \in \mathbb{Q}$ and

$$N_{K/\mathbb{Q}}(\beta) = \left(N_{\mathbb{Q}[\beta]/\mathbb{Q}}(\beta)\right)^m \in \mathbb{Q}.$$

now β plays the role of α.

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

Prop^n. Let K be a number field.

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

α 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, $1/\alpha \in K$.

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

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

They satisfy same polynomial.

$\therefore \alpha_2, \dots, \alpha_n \in \mathbb{A}$.

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

Also: $\min_{\mathbb{Q}} \alpha = x^n + a_{n-1} x^{n} + \cdots + a_1 x \pm 1.$

$\min_{\mathbb{Q}} 1/\alpha = x^n \pm (a_1 x^{n-1} + \cdots + a_{n-1} x + 1).$

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

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

Moreover, $U(\mathcal{O}_{\mathbb{Q}[\sqrt{m}]}) = \{\pm 1\}$ 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 $\sqrt{3} \notin \mathbb{Q}[2^{1/4}]$.

Transitivity. We can define $\mathrm{Tr}_{L/K} : L \to K$ for number fields $K \subseteq L$. Suppose we have extensions $K \subseteq L \subseteq M$. Then, we have

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

Defn. $K/\mathbb{Q} \to \deg n$.

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

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

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

We define the discriminant of $\alpha_1, \ldots, \alpha_n$ by

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

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

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

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

$$\begin{pmatrix} \vdots & \ddots & \vdots \\ \sigma_1\alpha_n & \cdots & \sigma_n\alpha_n \end{pmatrix}\begin{pmatrix} \vdots & & \vdots \\ \sigma_n\alpha_1 & \cdots & \sigma_n\alpha_n \end{pmatrix}$$

$$= \begin{pmatrix} \sum (\sigma_i\alpha_1)^2 & \cdots & \sum(\sigma_i\alpha_1)(\sigma_i\alpha_n) \\ \vdots & \ddots & \vdots \end{pmatrix}$$

$$= \begin{pmatrix} Tr(\alpha_1^2) & \cdots & Tr(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ & \cdots & \end{pmatrix}$$

Take det. ∎

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

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

$\alpha_1, \ldots, \alpha_n$ are lin. dep over $\mathbb{Q} \iff disc(\alpha_1, \ldots, \alpha_n) = 0$.

Proof. ($\Rightarrow$) clear. The rows in defⁿ of the matrix satisfy same dependency

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

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

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

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

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

we have

$$\mathrm{Tr}(\alpha_1 \alpha) = \mathrm{Tr}(\alpha_2 \alpha) = \cdots = \mathrm{Tr}(\alpha_n \alpha) = 0$$

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

$\because$ Tr is $\mathbb{Q}$-linear, this gives $\mathrm{Tr} \equiv 0$.

But $\mathrm{Tr}(1) = n \neq 0$. $\rightarrow\leftarrow$ $\blacksquare$

Lecture 4 (13-01-2022)

13 January 2022 17:27

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

Theorem Let $K = \mathbb{Q}[\alpha]$ be a deg n ext^n of $\mathbb{Q}$.
Let $f = \min_{\mathbb{Q}} \alpha \in \mathbb{Q}[x]$.
Let $\alpha_1, \dots, \alpha_n$ be the n conjugates of α in $\mathbb{C}$.
Then,

$$\mathrm{disc}(1, \alpha, \dots, \alpha^{n-1}) = \prod_{r<s} (\alpha_r - \alpha_s)^2$$

$$= \pm N_{K/\mathbb{Q}}(f'(\alpha)).$$

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

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

$$\mathrm{disc}(1, \alpha, \dots, \alpha^{n-1}) = \det(\sigma_i \alpha^{j-1})^2$$
$$= \det(\alpha_i^{j-1})^2$$

$$= \det\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

Vandermonde

$$= \prod_{i<j} (\alpha_i - \alpha_j)^2. \quad \text{--- } (1)$$

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

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

$$\Rightarrow f'(\alpha_i) = \prod (\alpha_i - \alpha_j). \quad \text{--- } (2)$$

$i : j \neq i$

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

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

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

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

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

Proof. $f = \dfrac{x^p - 1}{x - 1} = x^{p-1} + \cdots + 1.$

$$(x-1)f = x^{p-1} \Rightarrow f + (x-1)f' = p\,x^{p-1}$$

$$\Rightarrow f'(\omega) = \frac{p\omega^{p-1}}{\omega - 1} = \frac{p}{\omega(\omega-1)}$$

$$\Rightarrow N(f'(\omega)) = \frac{p^{p-1}}{1 \cdot p} = p^{p-2}.$$

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

$+$ iff $p \equiv 1, 2 \mod 4.$

(not possible)

Also note that $\mathbb{Q}[\omega]/\mathbb{Q}$ is a Galois ext^n. Thus, $\sigma_i \omega \in \mathbb{Q}[\omega]$ $\forall i$. $\therefore \det(\sigma_i \omega^{j-1}) \in \mathbb{Q}[\omega]$.

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

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

$+$ iff $p \equiv 1 \mod 4$.

Notation: Let $\alpha \in \mathbb{C}$ be algebraic of degree n.
Then, $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of $\mathbb{Q}[\alpha]/\mathbb{Q}$.

$$\operatorname{disc}(\alpha) := \operatorname{disc}_{\mathbb{Q}[\alpha]/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}).$$

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

Cor: Prime factors of $\operatorname{disc}(\omega)$ involve p only

we now show a similar result for non-primes.

Now, let $\omega := e^{2\pi i/m}$, $m > 2$ is any integer.
Let $f(x) := \min_{\mathbb{Q}}(\omega) \in \mathbb{Z}[x]$, $\deg(f) = \varphi(m)$.

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

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

$\frac{d}{dx}$

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

$x = \omega$

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

take N
note ω is unit

$$\Rightarrow m^{\varphi(m)} \cdot (\pm 1) = N(f'(\omega)) \cdot N(g(\omega))$$

$\mathbb{Z}[\omega]$
$\therefore g(\omega) \in \mathcal{O}_{\mathbb{Q}[\omega]}$
$\therefore N(g(\omega)) \in \mathbb{Z}$

$$\therefore \underbrace{N(f'(\omega))}_{= \pm \operatorname{disc}(\omega)} \mid m^{\varphi(m)}.$$

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

Recall :

Def^n. Let G be a f.g. abelian group.
G is said to be free if $G \simeq \mathbb{Z}^n$ for some $n \in \mathbb{N}_0$.
n is uniquely determined and is called the rank of G.
$\left(G/2G \cong (\mathbb{Z}/2\mathbb{Z})^n \quad \therefore n = \log_2 |G/2G| \right)$

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

- 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 $K/\mathbb{Q} \to$ deg n.
$\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ basis of $K/\mathbb{Q}$.
$d := \operatorname{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z} \setminus \{0\}$.
Every $\alpha \in \mathcal{O}_K$ can be written as

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d} \quad \text{— (3)}$$

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

Cor. ① $\displaystyle\sum_{i=1}^{n} \mathbb{Z}\alpha_i \subseteq \mathcal{O}_K \subseteq \sum_{i=1}^{n} \mathbb{Z}\frac{\alpha_i}{d}$. — (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 $\mathcal{O}_K = \sum \mathbb{Z}\alpha_i$.

Def^n. $\mathcal{O}_K$: free abelian group of rank n.
$\{\alpha_1, \dots, \alpha_n\}$, $\{\beta_1, \dots, \beta_n\}$ bases of $\mathcal{O}_K / \mathbb{Z}$.

Then, $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \operatorname{disc}(\beta_1, \dots, \beta_n)$
Thus, $\operatorname{disc}(\mathcal{O}_K) := \operatorname{disc}(\alpha_1, \dots, \alpha_n)$ 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 $\det(A^2) = 1$, we are done. ☒

Lecture 5 (17-01-2022)

17 January 2022 17:32

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

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

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

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

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

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

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

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

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

$$\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} = \underbrace{\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}}_{\in GL_n(\mathbb{C})} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

By Cramer's rule, $x_j = \dfrac{y_j}{\delta}$,

$$y_j = \begin{array}{c} \begin{array}{ccc} & j & \\ & \downarrow & \end{array} \\ \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha) & \cdots \\ \vdots & \ddots & \vdots & \ddots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha) & \cdots \end{vmatrix} \end{array}$$

$\delta^2 = d$, $\quad y_j \to$ alg. integer.

$$\therefore \; \underset{\mathbb{Q}}{\underset{\cap}{d x_j}} = \underset{\mathbb{A}}{\underset{\cap}{\delta y_j}}.$$

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

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

Then $d \mid m_j^2$ — desired.

Then, $d \mid m_j^2$, as desired. $\boxtimes$

Def^n. 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.

- $m \equiv 2, 3 \ (4)$. $\{1, \sqrt{m}\} \to$ integral basis.

$$\operatorname{disc}(K) = \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = (-2\sqrt{m})^2 = 4m.$$

$m \equiv 1 \ (4)$.

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

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) $\operatorname{disc}(\omega) = \prod_{i<j} (\alpha_i - \alpha_j)^2$ $\quad$ ($\alpha_i \longrightarrow$ conjugates of ω)

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

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

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

(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

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

$d := \operatorname{disc}(1-\omega)$, $m_i \in \mathbb{Z}$, $d \mid m_i^2$.

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

(iv) We saw that $\operatorname{disc}(\omega) \mid m^{\varphi(m)}$.

$\therefore \operatorname{disc}(\omega) = \pm p^s$.

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

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

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

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

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

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

(v) $$N_{\mathbb{Q}[1-\omega]/\mathbb{Q}}(1-\omega) = \prod_{\substack{k=1 \\ p \nmid k}}^{p^r} (1-\omega^k) \quad \leftarrow n \text{ factors}$$

$$= (1-\omega)^n \cdot f(\omega), \qquad f(\omega) \in \mathbb{Z}[\omega].$$

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

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

$\Rightarrow$ p ... for all $i < n$.

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

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

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

$\uparrow$

$\mathcal{O}_K$

$$\therefore \frac{m_{i-1}}{1-\omega} \in \mathcal{O}_K \setminus \mathbb{Z}[\omega]. \qquad p \nmid m_{i-1}.$$

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

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

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

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

$$\therefore f(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} \qquad y = x^{p^{r-1}}$$

$$= \frac{y^p - 1}{y - 1}$$

$$= y^{p-1} + \cdots + 1.$$

$$= (x^{p^r})^{p-1} + \cdots + 1.$$

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

$\parallel$

p

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

Lecture 6 (20-01-2022)

20 January 2022 17:29

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

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

$\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of $\mathcal{O}_K$

$\iff \text{disc}(\alpha_1, \ldots, \alpha_n) = \text{disc}(K)$.

Sol^n: ($\Rightarrow$) by def^n.

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

Then, H is free of rank n.

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

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

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 $\omega = \omega_{p^r}$.

- K, L : number fields
  $KL \to$ the compositum is also a number field.

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

Equality may not hold.

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

$\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$, $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$. $(3 \equiv 7 \equiv 1 \quad (4))$

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

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

Let $\alpha := \frac{\sqrt{3}+\sqrt{7}}{2}$. Then, $\alpha^2 = \frac{3+7+2\sqrt{21}}{4}$

$$\Rightarrow \alpha^2 = \frac{5+\sqrt{21}}{2}$$

$$\Rightarrow \left(\alpha^2 - \frac{5}{2}\right)^2 = \frac{21}{4}$$

$$\Rightarrow \alpha^4 - 5\alpha^2 + \frac{25}{4} - \frac{21}{4} = 0$$

$$\Rightarrow \alpha^4 - 5\alpha^2 + 1 = 0.$$

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

Theorem. Let K, L be number fields such that $[KL:\mathbb{Q}] = [K:\mathbb{Q}][L:\mathbb{Q}]$.

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

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 $\# \mathrm{pf}(m) \geq 2$. Write $m = m_1 m_2$ with $\gcd(m_1, m_2) = 1$.

m_i have fewer prime factors.

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

By ind^n,

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

Note: ① $\mathbb{Q}[\omega_1] \cdot \mathbb{Q}[\omega_2] = \mathbb{Q}[\omega]$.

Proof ($\subseteq$) is clear.

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

$$\omega_1^s \cdot \omega_2^r = \omega \in \mathbb{Q}[\omega_1]\cdot\mathbb{Q}[\omega_2].$$ ∎

② $[\mathbb{Q}[\omega]:\mathbb{Q}] = [\mathbb{Q}[\omega_1]:\mathbb{Q}]\,[\mathbb{Q}[\omega_2]:\mathbb{Q}]$.

$\because$ these two are coprime

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

③ $\gcd(\operatorname{disc}(\omega_1), \operatorname{disc}(\omega_2)) = 1$.

(we had seen that prime factors of $\operatorname{disc}(\omega_m)$ are a subset of those of m.)

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

$= \mathbb{Z}[\omega]$. use that $\omega^{-1} \in \mathbb{Z}[\omega]$. ∎

Proof of theorem

$$\begin{tikzcd}
 & KL \arrow[dl, dash, "n"'] \arrow[dr, dash, "m"] & \\
K \arrow[dr, dash, "m"'] & & L \arrow[dl, dash, "n"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

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

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

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

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

Pf. σ has n distinct extensions $\sigma_1, \ldots, \sigma_n : KL \to \mathbb{C}$.
Then, $\sigma_i|_L$ are all distinct.
Indeed $\sigma_i|_L = \sigma_j|_L \Rightarrow \sigma_i|_{KL} = \sigma_j|_{KL}$ $(\because \sigma_i|_K = \sigma = \sigma_j|_K)$

$\Downarrow$

$i = j$

$$\Downarrow$$
$$i = j.$$

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

$\therefore$ $\sigma_i|_L = \tau$ for some $i \in [n]$. $\boxtimes$

<u>Step 2.</u> Let $\{\alpha_1, \dots, \alpha_m\}$ be an integral basis of $\mathcal{O}_K$.
They are also a $\mathbb{Q}$-basis of K.
||^{ly} $\{\beta_1, \dots, \beta_n\}$ $\longrightarrow$ $\mathbb{Z}$-basis of $\mathcal{O}_L$ (& $\mathbb{Q}$-basis of L).

$$\Rightarrow \{\alpha_i \beta_j : i \in [m],\ j = [n]\} \subseteq \mathcal{O}_{KL}$$
is a basis of KL over $\mathbb{Q}$.

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

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

Clear denominators to write

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

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

<u>Aim:</u> $\mathcal{O}_{KL} \subseteq \frac{1}{d} \cdot \mathcal{O}_K \cdot \mathcal{O}_L$.

Suffices to prove that $r \mid d$. $(\because \alpha_i \in \mathcal{O}_K,\ \beta_j \in \mathcal{O}_L.)$
$$\overset{\shortparallel}{\gcd(\operatorname{disc}(K), \operatorname{disc}(L))}$$

Enough to show $r \mid \operatorname{disc}(K)$.

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

Let $\sigma_1, \dots, \sigma_m$: embeddings of KL/L in $\mathbb{C}$.
(Note that $\sigma_1|_K, \dots, \sigma_m|_K$ are the m embeddings of K in $\mathbb{C}$.)

$$\sigma_1 \alpha = \frac{1}{r} \sum_{i,j} m_{ij} \cdot (\sigma_1 \alpha_i) \cdot \beta_j .$$

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

Then, $\sigma_j(x_i) = x_i \quad \forall\, j \in [m]$.

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

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

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

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

Also, $\gamma_i, \delta \in \mathbb{A}$. $\therefore \underset{\underset{L}{\cap}}{x_i \delta^2} = \underset{\underset{\mathbb{A}}{\cap}}{\gamma_i \delta}$.

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

$\because \{\beta_1, \dots, \beta_m\}$ is a basis of $\mathcal{O}_L / \mathbb{Z}$, we get

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

$$\Rightarrow r \mid m_{ij} \cdot \mathrm{disc}(K) \quad \forall i, j.$$

by gcd $= 1$ hypothesis

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

∎

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

Exercise 2.30.: Let $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$.
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 $d_1 \mid d_2 \mid \cdots \mid d_{n-1}$, $f_i(x) \in \mathbb{Z}[x]$: 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 :

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

- If m is not squarefree, then write $m = hk^2$, with $\gcd(h, k) = 1$, h & k squarefree.
An integral basis of $\mathcal{O}_K$ is

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

EXAMPLES:
① $K = \mathbb{Q}[\sqrt[3]{2}]$. $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\} \to$ basis.
② $K = \mathbb{Q}[\sqrt[3]{4}]$. $\left\{1, \sqrt[3]{4}, \frac{\sqrt[3]{4^2}}{2}\right\}$
③ $K = \mathbb{Q}[\sqrt[3]{10}]$. $\left\{1, \sqrt[3]{10}, \frac{\sqrt[3]{10^2} + \sqrt[3]{10} + 1}{3}\right\}$.

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

Lecture 7 (24-01-2022)

24 January 2022 17:25

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

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

Moreover, the d_i are unique.

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

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

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

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

- $R_k := F_k \cap \mathcal{O}_K$ for $k = 1, \ldots, n$.

Note $R_n = F_n \cap \mathcal{O}_K = \mathcal{O}_K$.
$R_1 = \mathbb{Z}\frac{1}{d} \cap \mathcal{O}_K = \mathbb{Z}$.

$k=1$: $\{1\}$ is a basis for R_1. Let $k \geq 1$.
As induction hypothesis, assume we have gotten a basis for R_k as $\left\{1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{k-1}(\alpha)}{d_{k-1}}\right\}$ with the desired properties.

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

$\pi : F \quad \sum^{k+1} \mathbb{Z} \frac{\alpha^{i-1}}{} \longrightarrow \mathbb{Z}\frac{\alpha^k}{}$

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

to be the projection map.

Restrict π to the subgroup R_{k+1}.

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

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

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

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

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

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

alg. int.

$$\Downarrow$$

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

$$\Rightarrow \pi\Big(\underbrace{\frac{\alpha \cdot f_{k-1}(\alpha)}{d_{k-1}} - m\beta}_{\cap}\Big) = 0.$$

$$\mathcal{O}_K \cap F_k = R_k.$$

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

By induction hyp., $\left\{1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{k-1}(\alpha)}{d_{k-1}}\right\}$ 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

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

all of these

$$\left[\quad \alpha_{k-1} \qquad i=1 \qquad \alpha_{i-1} \right]$$

(all of these d_{i-1} divide d_{k-1})

$$= \frac{1}{m d_{k-1}} \underbrace{\left(\alpha f_{k-1}(\alpha) - \sum_{i=1}^{k} m_i' f_{i-1}(\alpha) \right)}_{\text{monic } \mathbb{Z}\text{-poly in } \alpha \text{ of deg} = k}$$

$$= \frac{f_k(\alpha)}{d_k}. \qquad (d_k := m \cdot d_{k-1})$$

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 $-d_k$)

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

is exact.

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

EXAMPLE. Let $K = \mathbb{Q}[\alpha]$ be a deg 5 ext^n, with $\alpha \in \mathcal{O}_K$.

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

(a) $\operatorname{disc}(\alpha) = \operatorname{disc}(1, \alpha, \dots, \alpha^4)$

$= \operatorname{disc}(1, \alpha, \alpha^2, \alpha^3, f_4(\alpha))$

$= \operatorname{disc}(1, \dots, f_3(\alpha), f_4(\alpha))$

$\vdots$

$= \operatorname{disc}(1, f_1(\alpha), f_2(\alpha), f_3(\alpha), f_4(\alpha))$

(f_4 is monic, use the other rows/columns of det)

$$\operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}\left(1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_4(\alpha)}{d_4} \right)$$

$$= \frac{1}{(d_1 \cdots d_4)^2} \operatorname{disc}(1, \dots, f_4(\alpha))$$

$$= \frac{\operatorname{disc}(\alpha)}{(d_1 \cdots d_4)^2}.$$

$\overline{(d_1 \cdots d_4)}^2$

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

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

$\therefore\ d_1^4 \mid \mathrm{disc}(\alpha)$.

$\overset{\text{Sly}}{\parallel}\ \ d_2^3 \mid \mathrm{disc}(\alpha),\quad d_3^2 \mid \mathrm{disc}(\alpha)$.

Chapter 3: Prime Decomposition in Number Rings.

Def^n. 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 $\alpha \in \mathrm{Frac}(A)$ 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 : $\mathfrak{p} \neq 0$ prime $\Rightarrow$ $\mathfrak{p}$ maximal

Let $0 \neq I \subseteq \mathcal{O}_K$ 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. $\therefore \beta \in \mathbb{A}$.

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

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

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

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

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

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

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.) ☒

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.

($R \to$ Dedekind)

Corollary: Define the equiv rel^n on $\{$non zero ideals of $R\}$ by
$I \sim I'$ if $\exists\, 0 \neq J \trianglelefteq R$ s.t. IJ and $I'J$ are principal.
Let $Cl(R) = R/\sim$. Then, multiplication of ideals in
$Cl(R)$ is well-defined. Moreover, the set of nonzero principal ideals
is an equivalence class and is the identity.

The above theorem tells us that $Cl(R)$ 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 $\Sigma = \{$ ideals $\neq 0$ that do not contain $\ldots\}$.
If $\Sigma \neq \emptyset$, then $\exists \underset{\neq 0}{\mathfrak{a}} \in \Sigma$ 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, $\exists y \in \operatorname{Frac}(R) \setminus R$ 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)

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

$$\langle a \rangle \not\supseteq \mathfrak{p}_1 \cdots \hat{\mathfrak{p}}_j \cdots \mathfrak{p}_r.$$

Pick a prime $\mathfrak{p} \supseteq \mathfrak{a}$.
Then, $\mathfrak{p} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$.
$\Rightarrow \mathfrak{p} \supseteq \mathfrak{p}_i$ for some i.

But nonzero primes are maximal. Thus $\mathfrak{p} = \mathfrak{p}_i$.
Wlog $\mathfrak{p} = \mathfrak{p}_1$.

By minimality, $\langle a \rangle \not\supseteq \mathfrak{p}_2, \dots, \mathfrak{p}_r$.
Pick $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus \langle \alpha \rangle$.

Then, $b\,\mathfrak{p}_1 \subseteq \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \langle a \rangle$.

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

Step 3. $I \neq 0$: proper ideal (if $I = R$, take $J = R$.)
Claim: $\exists J \underset{\text{ideal}}{\neq 0}$ s.t. IJ : principal ideal.

Proof. Pick $0 \neq \alpha \in I$.
$J := \{ \beta \in R : \beta I \subset \langle \alpha \rangle \}$
$= (\alpha : I)$.
Then, $J \neq 0$ is an ideal. ($\alpha \in J$.)
Also, $IJ \subseteq \langle \alpha \rangle$.
We show that $IJ = \langle \alpha \rangle$.

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

Clearly, $0 \neq \mathfrak{a}$.
We show $\mathfrak{a} = R$.
Assume $\mathfrak{a} \neq R$.
By step 2., let $y \in \mathrm{Frac}(R) \setminus R$ be s.t. $y\,\mathfrak{a} \subseteq R$.

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

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

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

$$\Rightarrow \quad yJ \subseteq R.$$

$$yJI = y\alpha\mathfrak{a} = \alpha(y\mathfrak{a}) \subseteq \alpha R = \langle \alpha \rangle.$$

$$\therefore \quad (y \cdot J) I \subseteq \langle \alpha \rangle$$

$yJ \subseteq R$

$$\Rightarrow \quad yJ \subseteq J$$

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

Thus, $\mathfrak{a} = R$ or $\frac{1}{\alpha} IJ = R.$

$$\therefore \quad IJ = \langle \alpha \rangle.$$

∎

Corollary 1. Let R : Dedekind Domain.
$Cl(R) := \{\text{nonzero ideals of } R\} / \sim$
class group of R

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

Then, $Cl(R)$ 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. $R = \mathbb{R}[x,y] / \langle x^2 + y^2 - 1 \rangle$ is a Dedekind domain.
$Cl(R)$ is then infinite. This does NOT happen for number rings, as we shall see later.

Corollary 2.

Def^n: 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, $IJ' \subseteq \langle \alpha \rangle$.

$\Rightarrow \mathfrak{a} := \frac{1}{\alpha} IJ'$: ideal of R.

Check $I = J\mathfrak{a}$. ∎

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

$IJ = IK \Rightarrow J = K$.

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

$\Rightarrow I'IJ = I'IK$

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

$\Leftrightarrow J = K$. ∎

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.

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

Also, I not prime.

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

$\Downarrow$ $P \mid I$ $\nearrow$

$I = PJ \subsetneq J$. Thus, J = product of primes.

$\Rightarrow I = PJ$ = —"— . $\rightarrow\leftarrow$

<u>Uniqueness:</u> $I = P_1 \cdots P_r$

$= Q_1 \cdots Q_s$.

$\Rightarrow Q_1 \cdots Q_s \subseteq P_1$. WLOG $Q_1 \subseteq P_1$.

$P_1 = Q_1$ by maximality. ... ∎

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 $I, J \trianglelefteq R$ be nonzero ideals.

We define

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

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, $n_i, m_i \geq 0$.

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 $I \mid \langle \alpha \rangle$ since R is a DD.

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

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

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

nonempty by unique factorisation

Note $\{P_i^{n_i+1}\}_1^r \cup \{Q_j\}_1^s$ are pairwise comaximal.

By CRT

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

$\exists \beta \in R$ s.t. $\beta \equiv \beta_i \mod P_i^{n_i+1} \quad \forall i \in \{1,\dots,r\}$,

$\equiv 1 \mod Q_j \quad \forall j \in \{1,\dots,s\}$.

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

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

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

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

T_j is not equal to any P_* or Q_* !

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

Remark. PID $\Rightarrow$ UFD.
$\not\Leftarrow$

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 $R \neq$ 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 $M \subsetneq R$ since $RP = P$ is not principal.

<u>Claim</u>: α is irreducible but not prime.

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

<u>Proof</u>. ① α is irred.

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 $P \mid \langle \beta \rangle$.

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, $\tilde{P} \supsetneq M$. This contradicts maximality of M. ※

② α is NOT prime.

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

Also, $M \subsetneq \langle \alpha \rangle$, $P \subsetneq \langle \alpha \rangle$.

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

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

We are now done. ☒

<u>EXAMPLES</u>. ① $\mathbb{Z} \subseteq \mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}(i)}$.

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

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

$\left(\dfrac{\mathbb{Z}[i]}{p\mathbb{Z}[i]} \cong \dfrac{\mathbb{Z}[x]}{\langle p, x^2+1 \rangle} \cong \dfrac{(\mathbb{Z}/p)[x]}{(x^2+1)} \leftarrow \text{field since } x^2+1 \text{ is irred in } \mathbb{Z}/p \text{ as } p \equiv 3\ (4). \right)$

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

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

Then, $a^2+b^2 = 0$ in $\mathbb{F}_p$.

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

$\therefore p\mathbb{Z}[i] = \langle p, a+ib\rangle\langle p, a-ib\rangle$.

Thus, $2 = \mathfrak{p}^2$, $\langle p\rangle = P$, $\langle p\rangle = P_1P_2$.

$p \equiv 3 \ (4)$ $\qquad p \equiv 1 \ (4)$

(2) $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}[\sqrt{-5}]}$

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

$\langle 3\rangle = \langle 3, \sqrt{-5}-1\rangle\langle 3, \sqrt{-5}+1\rangle$ $\qquad$ (look at $\mathbb{Z}[\sqrt{-5}]/\langle p\rangle$.)

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

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

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, Q : prime in S.

TFAE:

(i) $Q \mid PS$,

(ii) $Q \supseteq PS$,

(iii) $Q \supseteq P$,

(iv) $Q \cap R = P$,

(v) $Q \cap K = P$.

Proof. (i) $\Leftrightarrow$ (ii) is simple.

(ii) $\Leftrightarrow$ (iii) — " —.

(iv) $\Rightarrow$ (iii) obvious

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

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

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

$(iv) \Leftrightarrow (v)$: 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

$\Rightarrow \alpha \in \mathcal{O}_K = R$ ∎

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

EXAMPLE:

①
$$\begin{array}{cccccc} \mathbb{Q}[i] & \mathbb{Z}[i] & \langle 1+i \rangle & \langle 3 \rangle & \langle 2+i \rangle & \langle 2-i \rangle \\ | & | & | & | & \diagdown & \diagup \\ \mathbb{Q} & \mathbb{Z} & \langle 2 \rangle & \langle 3 \rangle & \multicolumn{2}{c}{\langle 5 \rangle} \end{array}$$

②
$$\begin{array}{cccccc} \mathbb{Q}[\sqrt{-5}] & \mathbb{Z}[\sqrt{-5}] & \langle 2, 1+\sqrt{-5} \rangle & \langle 3, 1+\sqrt{-5} \rangle & \langle 3, 1-\sqrt{-5} \rangle \\ | & | & | & \diagdown & \diagup \\ \mathbb{Q} & \mathbb{Z} & \langle 2 \rangle & \multicolumn{2}{c}{\langle 3 \rangle} \end{array}$$

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 $PS \subsetneq S$, pick any prime factor of PS (These are precisely all the Q)

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 $\gamma PS \subseteq S$

$\Rightarrow \gamma S \subseteq S$

$\Rightarrow \gamma \in S$.

$\therefore \gamma \in S \cap K \subseteq R$. $\rightarrow\leftarrow$ ∎

Def^n.

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

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

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

Then, $e(Q_i | P) := e_i$

$= $ ramification index of Q_i / P.

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

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

Examples. ①

$$\begin{array}{ccccc} \mathbb{Q}(i) & \mathbb{Z}[i] & \langle 1+i \rangle & \langle 3 \rangle & \langle 1+2i \rangle \quad \langle 1-2i \rangle \\ | & | & |\, e=2 & |\, e=1 & {}_1\diagdown \quad \diagup_1 \\ \mathbb{Q} & \mathbb{Z} & 2 & 3 & 5 \end{array}$$

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

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

$= 4 = 2^2.$

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

Suppose we have:

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

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

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

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

There is a ring map $\varphi : R \longrightarrow S/Q$ given by $R \hookrightarrow S \twoheadrightarrow S/Q$.
$\ker(\varphi) = R \cap Q = P$.

Def^n. $f(Q|P) = [S/Q : R/P]$.
= inertial degree of Q over P

Lecture 10 (03-02-2022)

03 February 2022 17:29

Def^n.

$$\begin{array}{ccc} Q_1 \cdots Q_r & S & L \\ \diagdown \ \diagup & | & | \\ P & R & K \end{array}$$

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

- $e(Q_i \mid P) = e_i$
  = ramification index of Q_i/P.
- $f(Q_i \mid P) = [S/Q_i : R/P]$ = inertial degree of Q_i/P.

  finite fields

Prop^n. (Multiplicative property of e and f).

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

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

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

f : usual field theory. ☺

EXAMPLE

$$\begin{array}{ccc} P & R & K \\ | & | & |\, m \\ p\mathbb{Z} & \mathbb{Z} & \mathbb{Q} \end{array} \qquad [K:\mathbb{Q}] = m.$$

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

Claim : $f \leq m$.

Proof. $f(P|_p \mathbb{Z}) = [R/P : \mathbb{Z}/p]$.

$R \simeq \mathbb{Z}^m$ (as groups)

$$\begin{array}{c} R/P \twoheadleftarrow (\mathbb{Z}/p\mathbb{Z})^m \\ \downarrow \\ \text{Cardinality } p^f. \end{array} \quad \therefore f \leq m. \quad \blacksquare$$

Def^n

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

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. $I + J = R$.

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

Thus, $\|IJ\| = |R/IJ| = |R/I| \cdot |R/J| = \|I\| \cdot \|J\|$.

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

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

By case 1, we get $\|I\| = \prod \|P_i^{n_i}\|$,

$\|J\| = \prod \|P_i^{m_i}\|$,

$\|IJ\| = \prod \|P_i^{m_i + n_i}\|$.

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

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

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

$\left(R/P \cong P^{n-1}/P^n \right)$ Inductively, we are done. ⊠

This finishes the proof. ⊠

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

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

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

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

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

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

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

Then,

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

Proof ① $K = \mathbb{Q}$:

$$\begin{array}{ccc} Q_1 \cdots Q_r & S & L \\ \backslash\ / & | & |\,n \\ p & \mathbb{Z} & \mathbb{Q} \end{array}$$

$pS = \prod_{1}^{r} Q_i^{e_i}$

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

$$\| \qquad\qquad$$

$$p^n = \prod_{i=1}^{r} \left(p^{f_i}\right)^{e_i}$$

S/Q_i is a $\mathbb{Z}/p$ vec. space of dim f_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 Suffices to prove for I prime by factoring I into primes.

Let $0 \neq P$ be a prime

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

Let $0 \neq P$ be a prime

<u>TS</u> : $\|PS\| = \|P\|^n$.

$$\begin{array}{ccc} \|PS\| & = & \|P\|^n \\ \| & & \| \\ |S/PS| & & |R/P|^n \end{array}$$

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

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

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

<u>Proof.</u> 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 $a_i \in P$ $\forall i$.

Then, $\underset{\neq 0}{I} := \langle a_1, \dots, a_{n+1} \rangle \subseteq P$.

Can choose $0 \neq I_1 \neq R$ s.t. $II_1 = \langle \theta \rangle$.

Thus, $\exists \gamma \in K \setminus R$ s.t. $\gamma I_1 \subseteq R$.

<u>Claim</u> : $\gamma I \nsubseteq P$.

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

End of Step 1.

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

$$pR = \prod_{i=1}^{r} P_i^{e_i}.$$

$$\begin{array}{ccc} & S & L \\ & | & |\,n \\ P & R & K \\ | & | & |\,m \\ p & \mathbb{Z} & \mathbb{Q} \end{array}$$

$$\dim_{R/P_i}(S/P_iS) =: n_i \le n,$$ by Step 1.

$$\|pS\| = p^{mn} \qquad \left(\because\ S/pS \cong \mathbb{Z}^{mn}/p\mathbb{Z}^{mn} \text{ as groups.}\right)$$

$$\| \qquad\qquad \prod_{i=1}^{r} \|P_iS\|^{e_i}$$

S/P_iS is a vec space over R/P_i of dim n_i

$$\| \qquad\qquad \prod_{i=1}^{r} \|P_i\|^{n_ie_i}$$

$f_i := f(P_i \mid p\mathbb{Z})$, $e_i = e(P_i \mid p\mathbb{Z})$.

$$\| \qquad\qquad \prod_{i=1}^{r} p^{f_in_ie_i}$$

Thus, $\sum f_i n_i e_i = mn$. —(*)

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

$$\sum e_if_i = m.$$

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

End of Step 2.

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

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

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

$f_i := f(Q_i \mid P)$

$$f_i := f(Q_i \mid P).$$

$$P \qquad R \qquad K$$

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

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

$$\|P\|^n = \prod_{i=1}^{f} \|P\|^{f_i e_i}$$

v. space blah blah...

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

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

Then,

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

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

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

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

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

$$\begin{array}{cc} T = \mathcal{O}_M & M \\ | & |_m \\ R & K \\ | & |_n \\ \mathbb{Z} & \mathbb{Q} \end{array}$$

Note $\sigma_i(T) \subseteq T$.

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

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

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

$$\|\alpha T\| = \|(\sigma_i \alpha) T\|$$

Lecture 11 (07-02-2022)

07 February 2022 17:32

Recall.

$$\begin{array}{ccc} S & & L \\ | & & |{\scriptstyle n} \\ R & & K \\ | & & | \\ \mathbb{Z} & & \mathbb{Q} \end{array}$$

① $I \neq 0$ ideal of R.

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

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

② $\|IS\| = \|I\|_R^n$.

③ $0 \neq \alpha \in R$,

$\|\langle \alpha \rangle\|_R = |N_{K/\mathbb{Q}}(\alpha)|$.

④ $0 \neq P$: prime of R.

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

Then, $\sum_1^r e_i f_i = n$.

Corollary $0 \neq \alpha \in R$. Suppose $|N_{K/\mathbb{Q}}(\alpha)| = p \in \mathbb{Z}$ 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). ∎

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

$m = p^r$.

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

Proof.

Let $f(x) = \min_{\mathbb{Q}}(\omega)$

$$= \frac{x^{p^r}-1}{x^{p^{r-1}}-1}$$

$$= y^{p-1} + \cdots + y + 1 \quad \text{for } y = x^{p^{r-1}}.$$

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

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

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

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

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

Suppose $\langle 1-\omega \rangle = \prod_{i}^{r} Q_i^{e_i}$ for primes $Q_i \subseteq \mathbb{Z}[\omega]$.

Then, $p\mathbb{Z}[\omega] = \left(\prod_{i}^{r} Q_i^{e_i}\right)^n$.

But also, $\sum e_i n f_i = n$.

$\Rightarrow r = 1, \ e_1 = f_1 = 1$. $\therefore \langle 1-\omega \rangle = Q_1 \in \operatorname{Spec}$.

Def^n.

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

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

② $\alpha = 2^{1/3}$

Let $P = \langle \alpha \rangle$.

$$\begin{array}{ccc} P & \mathbb{Z}[\alpha] & \mathbb{Q}[\alpha] \\ | & | & |\, 3 \\ p = 2 & \mathbb{Z} & \mathbb{Q} \end{array}$$

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

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

$5\mathbb{Z}[\alpha] = Q_1 Q_2.$

$Q_1 = \langle 5, \alpha + 2\rangle,$

$Q_2 = \langle 5, \alpha^2 + 3\alpha - 1\rangle.$

$$\frac{\mathbb{Z}[x]}{\langle 5, x^3-2\rangle} = \frac{\mathbb{F}_5[x]}{\langle x^3-2\rangle} = \frac{\mathbb{F}_5[x]}{\langle x+2\rangle\langle x^2+3x-1\rangle}.$$

③ $\alpha^3 = \alpha + 1.$

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

$\operatorname{disc}(1, \alpha, \alpha^2) \to$ square free. $\therefore\ \mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha].$

$23R = PQ^2$ as $\dfrac{\mathbb{Z}[x]}{\langle 23\rangle} = \dfrac{\mathbb{F}_{23}[x]}{\langle x^3 - x - 1\rangle}$

$P = \langle 23, \alpha - 3\rangle,$ $\qquad = \dfrac{\mathbb{F}_{23}[x]}{\langle (x-3)(x-10)^2\rangle}.$

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

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

$1 \cdot f(P \mid 23) + 2 \cdot f(Q \mid 23) = 3. \qquad \therefore\ f(P \mid 23) = f(Q \mid 23) = 1.$

Note: Different ramification indices!

Theorem. Assume L/K is Galois.

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

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

primes in $L \equiv$ primes in $\mathcal{O}_L$

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

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

$\because P$ 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.

$$x \equiv 1 \mod \sigma Q \quad \forall \sigma \in G.$$
$$\equiv 0 \mod Q'.$$

$$\underset{\substack{\cap \\ R}}{N_{L/K}(x)} = \prod_{\sigma \in G} \sigma(x)$$

$$\left(\begin{array}{l} x \equiv 1 \mod \sigma Q \quad \forall \sigma \\ \quad \Updownarrow \\ \sigma(x) \equiv 1 \mod \sigma Q \quad \forall \sigma \end{array} \right)$$

$$\equiv \begin{cases} 1 & \mod Q \\ 0 & \mod Q' \end{cases}$$

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

But then $N_{L/K}(x) \in Q$. $\rightarrow\leftarrow$

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

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

Proof. $Q_1 \cdots Q_r$ S L

$\quad\ \ \backslash | /$ $\quad |$ $\quad |\, n$.

$\quad\quad P$ $\quad R$ $\quad K$

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

apply σ: Pick 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 ...

$$\begin{array}{ccc} S & \xrightarrow[\cong]{\sigma} & S \\ | & & | \\ Q_1 & \longrightarrow & Q_2 \end{array}$$

$\therefore S/Q_1 \cong S/Q_2$.

$\Rightarrow f_1 = f_2$. ∎

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

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

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

② $\langle 23 \rangle = PQ^2$.
23 is ramified in $\mathbb{Q}[\alpha]$.

① $|\mathrm{disc}(R)| = p$. p was ramified.
② $|\mathrm{disc}(R)| = 23$. 23 was ramified.

Theorem Suppose p is ramified in R.
Then, $p \mid \mathrm{disc}(R)$.

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

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

<u>Proof</u>. Let P: prime in R s.t. $e(P|p) > 1$.
$pR = P \cdot I$ s.t. $P \mid I$.
↳ I is a product of all primes P_i over p.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis of R.
Let $\alpha \in I \setminus pR$. ($\alpha \in P_i$ $\forall$ P_i over p.)
$\alpha = \sum m_i \alpha_i \notin pR$.

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

$$\begin{aligned}\mathrm{disc}(\alpha, \alpha_2, \ldots, \alpha_n) &= \mathrm{disc}\left(\sum m_i \alpha_i, \alpha_2, \ldots, \alpha_n\right) \\ &= \mathrm{disc}(m_1\alpha_1, \alpha_2, \ldots, \alpha_n) \\ &= m_1^2 \, \mathrm{disc}(\alpha_1, \ldots, \alpha_n)\end{aligned}$$

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

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 $\mathbb{C}$.

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

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

$$\begin{array}{ccccccc} T_{1,1} \cdots T_{1,m_1} & \cdots & T_{r,1} \cdots T_{r,m_r} \\ \backslash \;\; / & & \backslash \;\; / \\ P = P_1 & \cdots & P_r \\ & \backslash \;\; / & \\ & p & \end{array}$$

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

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

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

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

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

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

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

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

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

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.

$$\begin{array}{ccc} R & & \mathbb{Q}(\alpha) \\ | & & |_n \\ \mathbb{Z} & & \mathbb{Q} \end{array}$$

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

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

③
$$\begin{array}{c} L \\ n \big| \\ K \\ \big| \\ \mathbb{Q} \end{array}$$

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 $K = \mathbb{Q}[\sqrt{m}]$, $m \in \mathbb{Z}$ square free.

$R = \mathcal{O}_K$.

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.

($\because \sum e_i f_i = 2$)

- $p \mid m$.

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

- $p \nmid m$.
  - $p = 2$, m odd.

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

  - $p > 2$, m arbitrary

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

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

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.

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

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

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

$\hookrightarrow$ prime

$\operatorname{disc}(\mathbb{Z}[\beta]) = \operatorname{disc}(\beta) \mid n^{\varphi(n)}$.

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

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

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

$$\begin{tikzcd} \mathbb{Q}[\beta] \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

Galois. Thus, $f(Q_i \mid p) = f$ is constant.

$$s = \frac{\varphi(n)}{\operatorname{ord}_n(p)}.$$

$$\begin{tikzcd} & \mathbb{Q}[\omega] \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}[\alpha] \arrow[dr, dash] & & \mathbb{Q}[\beta] \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd} \qquad \begin{tikzcd} \langle 1-\alpha \rangle^{\varphi(p^r)} \arrow[dr, dash] & & Q_1 \cdots Q_s \arrow[dl, dash] \\ & p\mathbb{Z} & \end{tikzcd}$$

For each $i \in [s]$, fix a prime $P_i \subseteq \mathbb{Z}[\omega]$ over Q_i.

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

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

$$\begin{tikzcd} P_1 \arrow[d, dash] & \cdots & P_r \arrow[d, dash] \\ Q_1 \arrow[dr, dash] & \cdots & Q_r \arrow[dl, dash] \\ & p\mathbb{Z} & \end{tikzcd} \qquad \begin{tikzcd} \mathbb{Z}[\omega] \arrow[d, dash] \\ \mathbb{Z}[\beta] \arrow[d, dash] \\ \mathbb{Z} \end{tikzcd}$$

$$e\left(P_i \mid p\mathbb{Z}\right) = e\left(P_i \mid \langle 1-\alpha\rangle\right) e\left(\langle 1-\alpha\rangle \mid p\mathbb{Z}\right)$$

$$e\left(\langle 1-\alpha\rangle \mid p\mathbb{Z}\right) = \varphi(p^r)$$

$$\Rightarrow e(P_i \mid p) \geqslant \varphi(p^r).$$

$$f\left(P_i \mid p\right) = f\left(P_i \mid Q_i\right) \cdot f\left(Q_i \mid p\right)$$

$$\Rightarrow f\left(P_i \mid p\right) \geqslant f = \mathrm{ord}_n(p).$$

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

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

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

$$\varphi(m) \geqslant \sum \varphi(p^r) \cdot f$$

$$\varphi(m) = \varphi(p^r)\,\varphi(n)$$

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

Thus, equality everywhere.

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

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

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

Theorem. $L = K[\alpha]$ for some $\alpha \in S$.

$R[\alpha] \subseteq S$.

free abelian groups of mn

$$\begin{array}{ccc} S & & L \\ | & & |\,n \\ R & & K \\ | & & |\,m \\ \mathbb{Z} & & \mathbb{Q} \end{array}$$

Thus, the group $S/R[\alpha]$ is finite (and abelian).

Thus, the group $S/_{R[\alpha]}$ is finite (and abelian). $\mathbb{Z}$ $\mathbb{Q}$

Let $p \in \mathbb{Z}$ and take $P \in \operatorname{Spec}(R)$ over p.
Assume $p \nmid \left| S/_{R[\alpha]} \right|$. Let $g(x) = \min_K(\alpha) \in R[x]$.

We have the natural projection $R[x] \twoheadrightarrow R/P\,[x]$, $h \mapsto \bar{h}$.
$R[\alpha] \cong R[x]/\langle g(x) \rangle$.

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,
$$PS = \prod Q_i^{e_i}.$$
Also, $f(Q_i | P) = f_i$.

Proof (Sketch). Claims:

① Either $Q_i = S$ or $Q_i \in \operatorname{Spec}(S)$ and $\left|S/_{Q_i}\right| = \left|R/P\right|^{\deg(\bar{g}_i)}$.

② $Q_i + Q_j = S$ for $i \neq j$. $\bar{h}_i \bar{g}_i + \bar{h}_j \bar{g}_j = 1$
lift to $R[x]$. Put $x = \alpha$. ∎

Exercise

③ $PS \mid Q_1^{e_1} \cdots Q_r^{e_r}$.

Assume the claims.
Wlog assume that $Q_1, \ldots, Q_s$ are proper and $Q_{s+1} = \cdots = Q_r = S$.
Then, $F(Q_i | P) = f_i = \deg \bar{g}_i$ for $i \in [s]$.

Also, $PS \mid Q_1^{e_1} \cdots Q_s^{e_s}$.

$\therefore PS = Q_1^{d_1} \cdots Q_s^{d_s}$ for some $0 \leq d_i \leq e_i$.

But $n = \sum_{1}^{s} d_i \cdot f_i \leq \sum_{i=1}^{s} e_i \cdot f_i \leq \sum_{i=1}^{r} e_i f_i = n.$

$\therefore$ All are equalities and $s = r$.

Lecture 13 (14-02-2022)

14 February 2022 17:25

Theorem. $K = \mathbb{Q}[\omega]$, $\omega = e^{2\pi i/n}$, $p \in \mathbb{Z}$ prime.

Suppose $p \nmid n$. (p: unramified)

$p\mathbb{Z}[\omega] = P_1 \cdots P_r$.

$f(P_i | p) = f = \mathrm{ord}_n(p)$. ($f(P_i|p)$ is constant since Galois ext^n.)

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^n of degree f over $\mathbb{F}_p$.

In fact, $\mathrm{Gal}(\mathbb{Z}[\omega]/P, \mathbb{F}_p) = \langle \tau \rangle$ is cyclic of order f, where τ is the Frobenius map $x \mapsto x^p$.

Also, $\mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong (\mathbb{Z}/n)^*$ under

$(\omega \mapsto \omega^a) \longleftrightarrow \bar{a}$. (Here, $(a,n)=1$.)

As $(p,n)=1$, we have the automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ given by $\sigma(\omega) = \omega^p$.

Then, $o(\sigma) = \mathrm{ord}_n(p)$, in view of the above isomorphism.

To show: $f = \mathrm{ord}_n(p)$

Enough to show: $\sigma^a = id \Leftrightarrow \tau^a = id$.

Note: • $\sigma^a = id \Leftrightarrow \sigma^a(\omega) = \omega \Leftrightarrow \omega^{p^a} = \omega \Leftrightarrow \omega^{p^a-1} = 1 \Leftrightarrow p^a \equiv 1 \bmod n$

• $\tau^a = id \Leftrightarrow \tau^a(\bar\omega) = \bar\omega \Leftrightarrow \bar\omega^{p^a} = \bar\omega \Leftrightarrow \omega^{p^a} = \omega \bmod P$

define $\bar\omega$ by $\dfrac{\mathbb{Z}[\omega]}{P} = \mathbb{F}_p[\bar\omega]$

Let $b = (p^a \bmod n)$.

Clearly $b \neq 0$, as $(p,n)=1$.

Claim. If $\omega^b = \omega \bmod P$, then $b=1$.

Proof. If $b>1$, note

$n = (1-\omega)(1-\omega^2)\cdots(1-\omega^{n-1})$.

if $b>1$, then $1-\omega^{b-1} \in P$ as $\omega(1-\omega^{b-1}) \in P$.

Thus, $n \in P$. Also, $p \in P$. As $(n, p) = 1$, we have $1 \in P$. ⊠

Thus, $\omega^{p^a} = \omega \mod p \iff \omega^b = \omega \mod p \iff b = 1$. ⊠

Def^n. Let $K/\mathbb{Q}$ be Galois.

$$\begin{array}{ccc} P & \mathcal{O}_K & K \\ | & | & |\,n \\ p & \mathbb{Z} & \mathbb{Q} \end{array}$$

$G = Gal(K/\mathbb{Q})$.

$p\mathcal{O}_K = (P_1 \cdots P_r)^e, \quad f := f(P_i/p)$.

$n = ref$.

Let P lie over p, i.e., $P = P_i$ for some $i \in [r]$

D_P = decomposition group of P

$= \{\sigma \in G : \sigma P = P\}$

(We had shown that G acts transitively on $\{P_1, \ldots, P_r\}$.)

stabiliser of P.

$$|\text{orbit of } P| = [G : D_P]$$

$$\underset{r}{\parallel} \qquad\qquad \parallel \qquad\qquad \frac{ref}{|D_P|}$$

Prop^n. Thus, $\boxed{|D_P| = ef.}$ Hence, $\boxed{[K^{D_P} : \mathbb{Q}] = r.}$ ⊠

$k(P) = \mathcal{O}_K/P$: residue field of P

(nonzero primes are max'l)

$\mathcal{O}_K/P$ is a Galois ext^n of $\mathbb{Z}/p = \mathbb{F}_p$.

$Gal(k(P)/\mathbb{F}_p) = \langle \tau \rangle$, where τ is the Frobenius automorphism.

Let $\sigma \in D_P$.

$$\begin{tikzcd} \mathcal{O}_K \arrow[r, "\sigma"] \arrow[d] & \mathcal{O}_K \arrow[d] \\ \mathcal{O}_K/P \arrow[r, "\bar{\sigma}"] & \mathcal{O}_K/P \\ \bar{x} \arrow[r, mapsto] & \overline{\sigma(x)} \end{tikzcd}$$

(well defined since $\sigma(P) = P$.)

This is an isomorphism.

Thus, we get a natural map

$$\begin{array}{ccc} D_P & \xrightarrow{\varphi} & \mathrm{Gal}\left(k(P)/\mathbb{F}_p\right) \\ \sigma & \longmapsto & \bar{\sigma}. \end{array}$$

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. $D_P \leq G = \mathrm{Gal}(K/\mathbb{Q})$. Let $D := D_P$.
K/K^D is Galois with Galois group $D = D_P$.

$$\begin{array}{c} K \\ | \\ K^D \\ | \\ \mathbb{Q} \end{array}$$

As usual, $K^D = \{x \in K : \sigma x = x \ \forall \sigma \in D\}$.

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. $\mathrm{Gal}(K/K^D) = D$.
D acts transitively on the set of primes of $\mathcal{O}_K$ lying over $P \cap K^D$.

$$\begin{array}{ccc} P & & K \\ | & & | \\ P \cap K^D & & K^D \\ | & & | \\ p & & \mathbb{Q} \end{array}$$

D fixes P.
$\Rightarrow P$ is the only prime of $\mathcal{O}_K$ lying over $P \cap K^D$.

Conversely, suppose F is s.t. P is the only prime of $\mathcal{O}_K$ lying over $P \cap \mathcal{O}_F$.

$$\begin{array}{c} K \\ | \\ F \\ | \\ \mathbb{Q} \end{array}$$

Then, $\mathrm{Gal}(K/F) \leq G$ fixes P.
$\Rightarrow \mathrm{Gal}(K/F) \subseteq D$ ← Fund. Galois Thm.
$\Rightarrow K^D \subseteq F$. ☒

Lemma 3. Let $\mathfrak{p} = P \cap \mathcal{O}_{K^D}$.
As e, f, n are multiplicative, so is $r = \underline{n}$.

$$\begin{array}{c} K \\ |\,ef \end{array}$$

Lemma 3. Let $\mathfrak{P} = P \cap \mathcal{O}_{K^D}$.

As e, f, n are multiplicative, so is $r = \frac{n}{ef}$.

\# of primes lying over

$$\begin{array}{ccc} P & & K \\ | & & |\, ef \\ \mathfrak{P} & & K^D \\ | & & |\, r \\ p & & \mathbb{Q} \end{array}$$

As $r(K/\mathfrak{P}) = 1$, we get $r(K^D/p) = r$.

Thus, $[K^D : \mathbb{Q}] = r(K^D/p)$. Hence, $e(\mathfrak{P}/p) = f(\mathfrak{P}/p) = 1$.

In turn,

$$e(P/p) = e(P/\mathfrak{P}), \quad f(P/p) = f(P/\mathfrak{P}).$$

∎

Back to the homomorphism $\varphi : D_P \longrightarrow \mathrm{Gal}(k(P)/\mathbb{F}_p)$.

$$\mathrm{Gal}(k(P)/\mathbb{F}_p) = \langle \tau \rangle : \text{order } f = f(P/p)$$

τ: Frobenius

Theorem. φ is surjective.

Pf. $k(P) = \mathbb{F}_p[\bar{a}]$, for some $\bar{a} \in k(P) = \mathcal{O}_K/P$.

Choose a lift $a \in \mathcal{O}_K$ 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, $f(x) \in \mathcal{O}_{K^D}[x]$.

Note that we saw $f(\mathfrak{P}/p) = 1$. Thus, $\mathcal{O}_{K^D}/\mathfrak{P} \cong \mathbb{F}_p$.

$$\begin{array}{cccccc} & & & P & & K \\ f & e & 1 & | & & |\, ef \\ & & & \mathfrak{P} & & K^D \\ 1 & e & r & | & & |\, r \\ & & & p & & \mathbb{Q} \end{array}$$

Going modulo $\mathfrak{P}$: $\tilde{f}(x) = \prod_{\sigma \in D} (x - \tilde{\sigma} a) \in \mathbb{F}_p[x]$.

$\sigma \in D_{\mathfrak{p}}$

$$\mathbb{Z} \subseteq \mathcal{O}_{K^D} \subseteq \mathcal{O}_K.$$

$$\mathbb{Z}/p \cong \mathcal{O}_{K^D}/\mathfrak{p} \subseteq \mathcal{O}_K/P.$$

Going modulo P: $\bar{f}(x) = \prod_{\sigma \in D_P} (x - \bar{\sigma a}) \in \mathbb{F}_p[x]$.

$\bar{a}$: 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, $\bar{a}^p = \tau(\bar{a})$ is also a root of $\min_{\mathbb{F}_p}(\bar{a})$.

(as τ is an aut)

Thus, $\exists\, \sigma \in D_p$ s.t. $\overline{\sigma a} = \tau(\bar{a})$.

As τ is determined by $\bar{a}$, we see that $\tau \in \operatorname{im}(\varphi)$.

As $\langle \tau \rangle = \operatorname{Gal}(k(P)/\mathbb{F}_p)$, we are done. ∎

We have the exact sequence

$$1 \longrightarrow I_p \longrightarrow D_p \xrightarrow{\varphi} \operatorname{Gal}(k(P)/\mathbb{F}_p) \longrightarrow 1,$$

where $I_p = \ker \varphi$

$= $ inertial group of P

$= \{\sigma \in D_p \mid \bar{\sigma} = \mathrm{id}_{k(P)}\}$

$= \{ \quad\quad \mid \bar{\sigma}(\bar{x}) = \bar{x} \quad \forall\, \bar{x}\}$

$= \{ \quad\quad \mid \sigma(x) = x \mod P \quad \forall\, x\}$.

- $$|I_p| = \frac{|D_p|}{|\operatorname{Gal}(k(P)/\mathbb{F}_p)|} = \frac{ef}{f} = e.$$

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.

$$D_P \xrightarrow[\simeq]{\varphi} \mathrm{Gal}(k(P)/\mathbb{F}_p) = \langle \tau \rangle$$

$\hookrightarrow$ Frobenius.

$\exists!$ $\mathrm{Frob}_P \in D_P$ called the Frobenius element such that $\overline{\mathrm{Frob}_P} = \tau$.

Thus, Frob_P is the unique map s.t.

$$\mathrm{Frob}_P(x) = x^p \mod P,$$

for all $x \in \mathcal{O}_K$.

Lemma. Let $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$.

Then, σP lies over p.

$$\mathrm{Frob}_{\sigma P} = \sigma \,\mathrm{Frob}_P\, \sigma^{-1}.$$

Proof. Let $x \in \mathcal{O}_K$.

Then,

$$(\mathrm{Frob}_P\, \sigma^{-1})(x) = (\sigma^{-1}(x))^p \mod P.$$

That is,

$$\mathrm{Frob}_P(\sigma^{-1} x) - \sigma^{-1}(x^p) \in P \qquad \forall x \in \mathcal{O}_K.$$

Apply σ to get

$$\sigma \,\mathrm{Frob}_P(\sigma^{-1} x) - x^p \in \sigma P \qquad \forall x \in \mathcal{O}_K.$$

By uniqueness, $\sigma \,\mathrm{Frob}_P\, \sigma^{-1} = \mathrm{Frob}_{\sigma P}$. ∎

Defn. • If $K/\mathbb{Q}$ is Galois and $p \in \mathbb{Z}$ unramified, then $\{\mathrm{Frob}_{P_i} : i = 1, \dots, r\}$ is a conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$.

If $K/\mathbb{Q}$ is abelian, the conjugacy class has a single element, denoted $\left(\frac{K \mid \mathbb{Q}}{p}\right)$.

Artin symbol

- $\left(\frac{K \mid \mathbb{Q}}{-}\right) : \left\{ \begin{matrix} \text{unramified} \\ \text{primes} \end{matrix} \right\} \longrightarrow G.$

Extend this to a group homomorphism of a free abelian group

$$\bigoplus_{p \text{ unramified}} \mathbb{Z}[p] \longrightarrow G$$

Artin's Conjecture

$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$: profinite group, inverse limit of finite groups

Topology on $\bar{\mathbb{Q}}/\mathbb{Q}$:
Neighbourhoods of 1: $\{ \mathrm{Gal}(\bar{\mathbb{Q}}/K) \mid K/\mathbb{Q} : \text{finite} \}$

$GL_n(\mathbb{C})$: give it the discrete topology.

Want: n-dimensional complex representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, i.e., a continuous homomorphism

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_n(\mathbb{C}).$$

That is, $K = \bar{\mathbb{Q}}^{\ker \rho}$ should be a finite ext^n of $\mathbb{Q}$.

ρ factors as

$$\begin{tikzcd} \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \arrow[rr, "\rho"] \arrow[dr, "\text{restriction}"'] & & GL_n(\mathbb{C}) \\ & \mathrm{Gal}(K/\mathbb{Q}) \arrow[ur, "\rho'"'] & \end{tikzcd}$$

As $\mathrm{Gal}(K/\mathbb{Q})$ is finite, so is $\mathrm{im}(\rho)$.

- ρ is a representation $\Rightarrow$ $\mathrm{im}(\rho)$ is finite.
  ($\not\Leftarrow$) not true, i.e., if $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ 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 $\left(\frac{K/\mathbb{Q}}{p}\right)$ denote the obvious conjugacy class.

  Then, $\rho'\left(\left(\frac{K/\mathbb{Q}}{p}\right)\right)$ lie in a conjugacy class of $\mathrm{GL}_n(\mathbb{C})$.

  Thus, it makes to talk about its characteristic polynomial, $F_p(x) \in \mathbb{C}[x]$.

$$F_p(x) = x^n + a_1 x^{n-1} + \cdots \pm \det(\rho'(\mathrm{Frob}_p)).$$

$$R_p(x) = x^n F_p\left(\frac{1}{x}\right) = 1 + a_1 x + \cdots \pm \det(\rho'(\mathrm{Frob}_p))\, x^n.$$

Artin's L-function for ρ:

$$L(\rho, s) := \prod_{\substack{p \in \mathbb{Z} \\ \text{unramified}}} \frac{1}{R_p(p^{-s})}, \qquad s \in \mathbb{C}.$$

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 $\mathbb{C} \setminus \{1\}$

Known: $n = 1$.

$n = 2$: Khare - Wintenberger.

$n \geq 3$: Open (?)

Lecture 15 (28-02-2022)

28 February 2022 17:29

Recall: **Def^n.** 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:

- $\left(\frac{-}{p}\right) : \mathbb{Z}_p \longrightarrow \{1, -1\}$ is a group homomorphism.
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 8, \\ -1 & \text{if } p \equiv \pm 3 \mod 8. \end{cases}$

Thm 1. (Gauss Quadratic Reciprocity)
Let p, q be distinct odd primes.
Then,
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} -1, & \text{if } p, q \equiv 3 \mod 4, \\ 1, & \text{else.} \end{cases}$$

Recall that: $\left(\frac{q}{p}\right) = 1 \iff q$ is a square mod p
$\iff \langle q \rangle$ is a product of two primes
in $\mathcal{O}_{\mathbb{Q}[\sqrt{\varepsilon(p)p}]}$, $\quad \varepsilon(p) = \begin{cases} 1 & p = 1\ (4) \\ -1 & p = -1\ (4) \end{cases}$

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: $\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{a}] \quad \overset{\text{disc}}{\rightsquigarrow} \quad 4a \end{cases}$

Proof. Two options: $\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{a}] & \overset{\text{disc}}{\rightsquigarrow} \quad 4a \\ \mathbb{Z}\left[\frac{1+\sqrt{a}}{2}\right] & \rightsquigarrow \quad a \end{cases}$

If $q \nmid a$, then $q \nmid \operatorname{disc}(\mathcal{O}_K)$. Thus, q is unramified. $\square$

Lecture 16 (03-03-2022)

03 March 2022 17:30

Theorem. $K/\mathbb{Q}$. $\{x_1, \dots, x_n\} \to \mathbb{Z}$-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. $\|I\| \le \lambda$.

Let $\sigma_1, \dots, \sigma_r$ be the real embeddings, i.e., $\sigma_i(K) \subseteq \mathbb{R}$.
The remaining embeddings will come in conjugate pairs, say
$\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}$. $\quad \sigma_{r+i}(K) \not\subseteq \mathbb{R}$.

Note $r + 2s = n = [K : \mathbb{Q}]$.

Define $f : K \longrightarrow \mathbb{R}^n$
$$\alpha \longmapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Re} \sigma_{r+1}(\alpha), \operatorname{Im} \sigma_{r+1}(\alpha), \dots, \operatorname{Re} \sigma_{r+s}(\alpha), \operatorname{Im} \sigma_{r+s}(\alpha)).$$

Evidently, f is an injective homomorphism (of abelian groups).
Let $R = \mathcal{O}_K$. $\quad f(R) \cong R \cong \mathbb{Z}^n$ 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 $\mathbb{R}$.

$$\begin{pmatrix} f(x_1) \\ \vdots \end{pmatrix} = \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_r(x_1) & \operatorname{Re}(\sigma_{r+1}(x_1)) & \cdots \\ \vdots & \ddots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$\begin{pmatrix} f(x_1) \\ \vdots \\ f(x_n) \end{pmatrix} = \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_r(x_1) & Re(\sigma_{r+1}(x_1)) & \cdots \\ \vdots & \ddots & \vdots & \vdots & \ddots \\ \sigma_1(x_n) & \cdots & \sigma_r(x_n) & Re(\sigma_{r+1}(x_n)) & \cdots \end{pmatrix}$$

$$\vdots\!\!/\!/ \ A$$

we show this has det $\neq 0$

Note: $[Re\ z \quad Im\ z] \xrightarrow{C_1 + iC_2} [z \quad Im\ z] \xrightarrow{-2iC_2} \frac{-1}{2i}[z \quad -2i\ Im\ z] \xrightarrow{C_2 + C_1} [z \quad \bar{z}]$

Doing the above shows that

$$\det(A) = \frac{1}{(-2i)^s} \det \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_r(x_1) & \sigma_{r+1}(x_1) & \overline{\sigma_{r+1}(x_1)} & \cdots & \sigma_{r+s}(x_1) & \overline{\sigma_{r+s}(x_1)} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \end{pmatrix}$$

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 $\mathbb{R}^n$ s.t.
(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 parallelotope:

$$\Sigma = \left\{ \sum_{i=1}^{n} \lambda_i v_i \ : \ 0 \leq \lambda_i < 1 \right\}.$$

The above naturally parameterises $\mathbb{R}^n / \Lambda$.

$$\operatorname{Vol}(\Lambda) := \left| \det \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right|.$$

The above is independent of choice of basis. $(GL_n(\mathbb{Z})\dots)$

$$\mathrm{Vol}(\mathbb{R}^n/\Lambda) := \mathrm{Vol}(\Lambda).$$

Back to $R = \mathcal{O}_K$. $x_1, \dots, x_n$ $\mathbb{Z}$-basis of $\mathcal{O}_K$.
$\Lambda_R := f(R)$. $f(x_1), \dots, f(x_n)$ basis of Λ_R over $\mathbb{Z}$.

$$\mathrm{Vol}(\mathbb{R}^n/\Lambda_R) = \left|\det\begin{pmatrix} f(x_1) \\ \vdots \\ f(x_n)\end{pmatrix}\right|$$

$$= \frac{1}{2^s}\sqrt{|\mathrm{disc}\ R|}.$$

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 $\mathbb{R}^n$.

Defn Λ: lattice in $\mathbb{R}^n$ $\to$ rank n.
$M \subseteq \Lambda$: sublattice (of rank n) if ....

$$\mathrm{Vol}(\mathbb{R}^n/M) = |\Lambda/M| \cdot \mathrm{Vol}(\mathbb{R}^n/\Lambda).$$

- 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 $GL_n(\mathbb{Z})$. One has det $\neq 0$. So does other.)
  Similarly, if $\Lambda' \leq \Lambda$ is a subgroup, Λ' is a free abelian group.
  Suppose $\mathrm{rank}_{\mathbb{Z}}(\Lambda') = n$. Then, Λ' is also a lattice

(One way: can pick a $\mathbb{Z}$-basis $\{v_1, \dots, v_n\}$ for Λ and $d_1, \dots, d_n \underset{\neq 0}{\in \mathbb{Z}}$ s.t. $\{d_1 v_1, \dots, d_n v_n\}$ is a $\mathbb{Z}$-basis for Λ'.)

- Λ_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, $f(I) = \Lambda_I$: sublattice of Λ_R.

Moreover, $\mathrm{Vol}(\Lambda_I) = \|I\| \cdot \mathrm{Vol}(\Lambda_R)$.

(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

$$f(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \mathrm{Re}(\sigma_{r+1}(\alpha)), \mathrm{Im}(\sigma_{r+1}(\alpha)), \dots).$$

$$N_{K/\mathbb{Q}}(\alpha) = \left(\prod_{i=1}^{r} \sigma_i(\alpha)\right)\left(\sigma_{r+1}(\alpha)\overline{\sigma_{r+1}}(\alpha)\right) \cdots \left(\sigma_{r+s}(\alpha)\overline{\sigma_{r+s}}(\alpha)\right)$$

$$= N(f(\alpha)).$$

Main Theorem. Let Λ be an n-dimensional lattice in $\mathbb{R}^n$.
Then, $\exists\, x \in \Lambda \setminus \{0\}$ s.t.

$$|N(x)| \leq \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^s \cdot \mathrm{Vol}(\mathbb{R}^n/\Lambda).$$

Proof in next class. First some applications.

Corollary. I: nonzero ideal in $R = \mathcal{O}_K$.
Then, $\exists\, \alpha \in I \setminus \{0\}$ s.t.

$$|N_{K/\mathbb{Q}}(\alpha)| \leq n! \left(\frac{4}{\cdot}\right)^s \|I\|$$

Then, $\exists \alpha \in I \setminus \{0\}$ s.t.

$$|N_{K/\mathbb{Q}}(\alpha)| \le \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \frac{\|I\|}{\sqrt{|\text{disc } R|}}.$$

Proof. Take $\Lambda = \Lambda_I$. Let $x = f(\alpha) \in \Lambda_I \setminus \{0\}$ be s.t.

$$\underset{\|}{|N(f(\alpha))|} = |N(x)| \le \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^s \text{Vol}\left(\mathbb{R}^n / I\right)$$

$$|N_{K/\mathbb{Q}}(\alpha)| = \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^s \cdot \|I\| \cdot \frac{1}{2^s} \sqrt{|\text{disc } R|}$$

$$n = \frac{!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\text{disc} R|} \cdot \|I\|.$$

Minkowski's Constant

Corollary. Every class C in $\mathcal{O}_K$ contains an ideal I s.t.

$$\|I\| \le \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\text{disc } R|}.$$

Proof. Pick $J (\neq 0)$ in C^{-1}. By previous thm, $\exists \alpha \in J$ s.t.

$$|N_{K/\mathbb{Q}}(\alpha)| \le \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\text{disc } R|} \cdot \|J\|.$$

$(\alpha) \subseteq J \Rightarrow \langle \alpha \rangle = JI$ for some I.

Necessarily, $I \in C$.

$$\therefore \quad |N_{K/\mathbb{Q}}(\alpha)| = \|\langle\alpha\rangle\| = \|I\| \cdot \|J\|$$
$$\wedge|$$
$$\frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \sqrt{|\text{dis } R|} \cdot \|J\|.$$

Cancelling $\|J\|$ gives $\|I\| \le \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\text{disc } R|}$. ∎

Lecture 17 (07-03-2022)

07 March 2022 17:28

Qn. K: number field.

Let $A \subseteq \mathcal{O}_K$ be a subring s.t. $\mathrm{Frac}(A) = K$.

In particular, if $A \subsetneq \mathcal{O}_K$, 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 $m \equiv 1 \bmod 4$ square free.

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.

$$N(x) \le \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^s \cdot \mathrm{vol}\left(\mathbb{R}^n / \Lambda\right).$$

N was defined as follows (in terms of r, s):

$$N((x_1, \ldots, x_n)) = x_1 \cdots x_r \cdot (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2),$$

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

$$\underbrace{\mathrm{vol}}_{\text{Lebesgue measure}}(E) > 2^n\, \mathrm{vol}(\mathbb{R}^n / \Lambda).$$

Then, $\exists\, x \overset{\neq 0}{\in} E \cap \Lambda$. Further, if E is compact, then one may relax above $>$ to $\geq$.

Proof. Let $\{v_1, \ldots, v_n\}$ 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 $\quad 0 < \mathrm{vol}(F) = \mathrm{vol}(\mathbb{R}^n/\Lambda) < \frac{1}{2^n}\mathrm{vol}(E) = \mathrm{vol}\left(\frac{1}{2}E\right).$

$$\frac{1}{2}E = \bigcup_{x\in\Lambda}\left((F+x) \cap \frac{1}{2}E\right).$$

Thus, $\quad \mathrm{vol}\left(\frac{1}{2}E\right) = \sum_{x\in\Lambda} \mathrm{vol}\left((F+x) \cap \frac{1}{2}E\right)$

$$= \sum_{x\in\Lambda} \mathrm{vol}\left(F \cap \left(\frac{1}{2}E - x\right)\right).$$

If $\left\{ F \cap \left(\frac{1}{2}E - x\right)\right\}_{x\in\Lambda}$ are pairwise disjoint, then

$$\mathrm{vol}\left(\frac{1}{2}E\right) = \mathrm{vol}\left(\bigsqcup_{x\in\Lambda} F \cap \left(\frac{1}{2}E - x\right)\right)$$

$$\leq \mathrm{vol}(F).$$

$\therefore \ \mathrm{vol}(F) < \mathrm{vol}(F). \quad \rightarrow\leftarrow$

Thus, $F \cap \left(\frac{E}{2} - x\right)$ and $F \cap \left(\frac{E}{2} - y\right)$ have nonempty intersection for some $x \neq y$, $x, y \in \Lambda$.

Thus, $\frac{1}{2}e - x = \frac{1}{2}e' - y \in F$ 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 $\mathrm{vol}(E) = 2^n \cdot \mathrm{vol}(\mathbb{R}^n/\Lambda)$, then

$$\mathrm{vol}\left(\left(1+\frac{1}{m}\right)E\right) = \left(1+\frac{1}{m}\right)^n \mathrm{vol}(E) > 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda).$$

also has (i) – (iii)

Thus, $\exists x_m \in \left(1+\frac{1}{m}\right)E \setminus\{0\}$ s.t. $x_m \in \Lambda$.

Now, $\{x_m\}_m \subseteq 2E \cap \Lambda \leftarrow$ finite set.

Then, $\exists M$ s.t. $x_M = x_m$ for infinitely many m.

$$\therefore \quad x_M \in \bigcap_{\text{inf many } m} \left(1+\tfrac{1}{m}\right) E = E.$$ ∎

Corollary Let $A \subseteq \mathbb{R}^n$ be convex, centrally symmetric, and compact.
(compact ⇒ closed ⇒ measurable)

Assume $|N(a)| \le 1 \quad \forall a \in A$.
Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank n.
Then, $\exists 0 \neq x \in \Lambda$ s.t.

$$|N(x)| \le \frac{2^n}{\operatorname{vol}(A)} \cdot \operatorname{vol}(\mathbb{R}^n/\Lambda).$$

Proof Let $t > 0$ be s.t. $t^n = \frac{2^n}{\operatorname{vol}(A)} \cdot \operatorname{vol}(\mathbb{R}^n/\Lambda)$.
Let $E = tA$. Then, E is ... $\operatorname{vol}(E) = t^n \operatorname{vol}(A) = 2^n \operatorname{vol}(\mathbb{R}^n/\Lambda)$.
By previous result, $\exists x \in E \setminus \{0\} \cap \Lambda$. Write $x = ta$ for $a \in A \setminus \{0\}$.
Note $|N(x)| = t^n |N(a)| \le t^n$. ∎

Theorem. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank n.
Then, $\exists x^{\neq 0} \in \Lambda$ s.t.

$$|N(x)| \le \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^s \cdot \operatorname{vol}(\mathbb{R}^n/\Lambda).$$

Proof (i) (Weaker version)
Let $A = \{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_i| \le 1, \ i \in \{1, \dots, r\},$
$x_{r+1}^2 + x_{r+2}^2 \le 1, \dots, x_{n-1}^2 + x_n^2 \le 1\}$.
compact, centrally symm., convex

$\forall a \in A: \quad |N(a)| \le 1$

$\therefore \quad \exists x^{\neq 0} \in \Lambda$ s.t.

$$|N(x)| \le \frac{2^n}{\operatorname{vol}(A)} \cdot \operatorname{vol}(\mathbb{R}^n/\Lambda).$$

Note that $\operatorname{vol}(A) = 2^r \cdot \pi^s$.

$$\therefore \quad |N(x)| \le \left(\frac{4}{\pi}\right)^s \operatorname{vol}(\mathbb{R}^n/\Lambda).$$

(ii) We pick a better A.

$$A = \{ \underline{x} \in \mathbb{R}^n : |x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \le n \}.$$

Again, same properties as before. Only convexity needs to be checked. Use AM-GM...

Also check $|N(a)| \le 1$.

Apply AM-GM to the following n-quantities:

$|a_1|, \ldots, |a_n|, \sqrt{a_{r+1}^2 + a_{r+2}^2}, \sqrt{a_{r+1}^2 + a_{r+2}^2}, \ldots$

repeat twice

Finally, we are done once we show

$$\mathrm{vol}(A) = \frac{n^n}{n!} \cdot 2^r \cdot \left(\frac{\pi}{2}\right)^s.$$

Let $V_{r,s}(t) := \mathrm{vol}\left(\{ x \in \mathbb{R}^{r+2s} : |x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{r+2s-1}^2 + x_{r+2s}^2}\right) \le t \} \right).$

- $A = V_{r,s}(n)$ for $n = r + 2s$.
- $V_{r,s}(t) = t^{r+2s} \cdot V_{r,s}(1)$.

Claim: $V_{r,s}(1) = \dfrac{1}{(r+2s)!} \, 2^r \left(\dfrac{\pi}{2}\right)^s$

$$V_{r,s}(1) = 2\int_0^1 V_{r-1,s}(1-x)\,dx \qquad (\text{for } r \ge 1)$$

$$= 2\int_0^1 (1-x)^{r-1+2s} \, V_{r-1,s}(1)\,dx$$

$$= 2 \cdot \frac{1}{r+2s} \cdot V_{r-1,s}(1).$$

By induction, $V_{r,s}(1) = \dfrac{2^r}{(r+2s)(r-1+2s)\cdots(1+2s)} \cdot V_{0,s}(1)$

$$= \frac{2^r \, (2s)!}{} \, V_{0,s}(1).$$

$$= \frac{2^r}{(r+2s)!} (2s)! \quad V_{0,s}(1).$$

$$V_{0,s}(1) = \int_0^{2\pi}\int_0^{1/2} V_{0,s-1}(1-2r)\, r\,dr\,d\theta$$

$$= (2\pi) \int_0^{1/2} (1-2r)^{2(s-1)} \cdot r \cdot V_{0,s-1}(1)\, dr$$

$1-2r = u$
$dr = -\frac{du}{2}$

$$= (2\pi)\, V_{0,s-1}(1) \int_0^1 u^{2(s-1)} \left(\frac{1+x}{2}\right) \frac{dx}{2}$$

$$= \frac{\pi}{2(2s)(2s-1)} \quad V_{0,\, s-1}(1).$$

Again, proceed inductively to finally get the desired result. $\boxtimes$

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,

$$\mathcal{U}(\mathcal{O}_K) := \mathcal{O}_K^\times \cong W \times V$$

where $W = \{\text{roots of } 1 \text{ in } \mathcal{O}_K\} \to$ cyclic finite,

$V \cong \mathbb{Z}^{r+s-1}$.

Def^n. A basis of V is called a fundamental system of units in $\mathcal{O}_K$.

EXAMPLE. ① $K = \mathbb{Q}[\sqrt{m}]$, $m < 0$.

Then, $r = 0$, $s = 1$. Thus, $r + s - 1 = 0$, i.e., $\mathcal{O}_K^\times$ is finite.

② $K = \mathbb{Q}[\sqrt{m}]$, $m > 0$.

Then, $r = 2$, $s = 0$. $r + s - 1 = 1$. Thus, $\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$.

③ $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

$r = 4$, $s = 0$. $r + s - 1 = 3$. $\mathcal{O}_K = \{\pm 1\} \times \mathbb{Z}^3$.

$N(1 + \sqrt{2}) = N(2 + \sqrt{3}) = 1$. $N(\sqrt{2} + \sqrt{3}) = \pm 1$.

Proof of the Theorem: Let $\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$ be as usual.

We have the map

$$f : \mathcal{O}_K \setminus \{0\} \longrightarrow \Lambda_{\mathcal{O}_K} \setminus \{0\}$$
$$\alpha \longmapsto (\sigma_1 \alpha, \ldots, \sigma_r \alpha, \operatorname{Re}(\sigma_{r+1}\alpha), \operatorname{Im}(\sigma_{r+1}\alpha), \ldots).$$

Define

$$\log : \Lambda_{\mathcal{O}_K} \setminus \{0\} \longrightarrow \mathbb{R}^{r+s} \text{ as}$$
$$(x_1, \ldots, x_n) \longmapsto (\log|x_1|, \ldots, \log|x_r|, \log(x_{r+1}^2 + x_{r+2}^2), \ldots).$$

By abuse, denote the composition $\mathcal{O}_K \setminus \{0\} \xrightarrow{f} \Lambda \xrightarrow{\log} \mathbb{R}^{r+s}$ by $\log$.

Note $\log : \mathcal{O}_K \setminus \{0\} \longrightarrow \mathbb{R}^{r+s}$ is well-defined and

$$\alpha \longmapsto \left(\log|\sigma_1\alpha|, \dots, \log|\sigma_r\alpha|, \log|\sigma_{r+1}\alpha|^2, \dots, \log|\sigma_{r+s}\alpha|^2\right).$$

- $\log(\alpha\beta) = \log(\alpha) + \log(\beta)$, i.e., a monoid homomorphism.
  $(\log(1) = 0.)$

- $\log\big|_{\mathcal{U}(\mathcal{O}_K)}$ is a group homomorphism.

- $\log(\mathcal{U}(\mathcal{O}_K)) \subseteq H = \{\underset{\sim}{y} \in \mathbb{R}^{r+s} : y_1 + \dots + y_{r+s} = 0\}$.

- If $F \subseteq \mathbb{R}^{r+s}$ is bounded, then
  $\log^{-1}(F)$ is a finite set.
  (Bounded in lattice is finite. $\mathcal{O}_K \setminus \{0\} \xrightarrow{f} \Lambda_{\mathcal{O}_K} \setminus \{0\}$ is an iso.)

- $\underset{\ker(\log)}{\underset{\parallel}{\log^{-1}((0,\dots,0))}} \subset \mathcal{U}(\mathcal{O}_K^\times)$ is a finite subgroup.

  Thus, each element r in $\ker(\log)$ has finite order.
  $\therefore \ker(\log) \subseteq \{\text{roots of unity in } \mathcal{O}_K\}$
  $\supseteq$ is also clear since roots of unity go to roots of unity and have modulus 1.
  $\therefore \ker(\log) = \{\text{roots of unity in } \mathcal{O}_K\}$ is a finite group.

- $\log(\mathcal{U}(\mathcal{O}_K))$: subgroup of $\mathbb{R}^{r+s}$.
  If $\overset{\cup\!|}{S}$ is bdd, then $\log^{-1}(S)$ is finite.
  Thus, S is finite (since $|\ker| < \infty$.)

<u>Ex</u> (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, $\log(\mathcal{U}(\mathcal{O}_K))$ is a lattice in $\mathbb{R}^{r+s}$.
In particular, it is a free $\mathbb{Z}$-module. Thus, the s.e.s.

$$0 \to \ker(\log) \longrightarrow \mathcal{U}(\mathcal{O}_K) \xrightarrow{\log} \log(\mathcal{U}(\mathcal{O}_K)) \longrightarrow 0$$

splits. Thus,

$$\mathcal{U}(\mathcal{O}_K) \simeq \underset{\{\text{roots of unity in } \mathcal{O}_K\}}{\underset{\shortparallel}{\ker(\log)}} \oplus \log(\mathcal{U}(\mathcal{O}_K)).$$

We have $\log(\mathcal{U}(\mathcal{O}_K)) \cong \mathbb{Z}^d$. Need to show $d = r+s-1$.
$d \leq r+s-1$ is clear since it is contained in H.

Claim : $d \geq r+s-1$.

Proof We construct $r+s-1$ units in $\mathcal{U}(\mathcal{O}_K)$ which map to linearly independent elements in $\mathbb{R}^{r+s}$.

Lemma 1. For $k \in \{1,\dots,r+s\}$, given $0 \neq \alpha \in \mathcal{O}_K$, $\exists \beta \in \mathcal{O}_K \setminus \{0\}$ s.t.

(i) $|N_{K/\mathbb{Q}}(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc} \mathcal{O}_K|}$.

(ii) $\log(\alpha) = (a_1,\dots,a_{r+s})$, $\log(\beta) = (b_1,\dots,b_{r+s})$
and $b_i < a_i$ for all $i \neq k$.

Lemma 2. Fix $k \in \{1,\dots,r+s\}$. $\exists u \in \mathcal{U}(\mathcal{O}_K)$ s.t.

$$\log u = (a_1,\dots,a_{r+s}), \quad \underset{(\log u)_i}{\overset{}{\underset{\shortparallel}{a_i}}} < 0 \text{ for all } i \neq k.$$

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) $|N_{K/\mathbb{Q}}(\alpha_2)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc} \mathcal{O}_K|}$,

(ii) $(\log \alpha_2)_i < (\log \alpha_1)_i$ for all $i \neq k$.

Continue doing this to get a sequence $(\alpha_i)_{i=1}^{\infty}$.
Also, $\|\langle \alpha_i \rangle\| = |N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{\operatorname{disc} \mathcal{O}_K}$.
But there are only finitely many ideals of a given bound.
(Prime fact)

$\therefore \exists \langle \alpha_n \rangle = \langle \alpha_{n'} \rangle$ for some $n < n'$.

$\Rightarrow \alpha_n = \alpha_{n'} u$ for some $u \in \mathcal{U}(\mathcal{O}_K)$.

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 $\sum_{i=1}^{r+s} (\log u_k)_i = 0$. $\therefore (\log u_k)_k > 0$.

$$\begin{pmatrix} \log u_1 \\ \vdots \\ \log u_{r+s} \end{pmatrix} = (a_{ij}).$$

- $a_{ii} > 0$ for all i.
- $a_{ij} < 0$ for all $i \neq j$.
- sum of entries in any row is 0.

Thus, we wish to show $\operatorname{rank}(a_{ij}) = r+s-1$. ($\leq$ is clear.)
We show that $C_1, \dots, C_{r+s-1}$ are lin. indep. over $\mathbb{R}$.
Suppose not. Write

$$t_1 C_1 + \dots + t_{r+s-1} C_{r+s-1} = 0.$$

Let $|t_k| = \max |t_i| > 0$.
Divide by t_k to assume $t_k = 1$ and $t_i \leq 1 \ \forall i$.
k^{th} coordinate of $\sum t_i C_i = 0$:

$$t_1 a_{k,1} + \dots + t_{r+s-1} a_{k,r+s-1} = 0.$$

$$\therefore a_{k,k} = \sum_{i \neq k} t_i(-a_{k,i}) \leq \sum_{i \neq k} (-a_{k,i})$$

$$\Rightarrow a_{k,1} + \dots + a_{k,r+s-1} \leq 0.$$

Add $a_{k,r+s}$ to get

$$0 \leq a_{k,r+s} < 0. \quad \rightarrow\leftarrow$$

Thus, we have finished the proof (modulo Lem 1). $\blacksquare$

<u>Proof of lemma 1</u>: $n = r + 2s$.

$$E = \{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_i| \leq c_i, \quad 1 \leq i \leq r, \quad x_{r+1}^2 + x_{r+2}^2 \leq c_{i+1}, \dots\}$$

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. $c_1 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc} \mathcal{O}_K|}$.

$$\begin{aligned} \operatorname{vol}(E) &= 2^r c_1 \cdots c_r \cdot \pi^s c_{r+1} \cdots c_{r+s} \\ &= 2^r \pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc} \mathcal{O}_K|} = 2^{r+s} \sqrt{\operatorname{disc}(\mathcal{O}_K)}. \\ &= 2^{r+s} \cdot 2^s \operatorname{vol}(\mathbb{R}^n / \Lambda_{\mathcal{O}_K}) \\ &= 2^n \operatorname{vol}(\mathbb{R}^n / \Lambda_{\mathcal{O}_K}). \end{aligned}$$

Thus, by our earlier result, we are done as E is compact, convex, centrally symmetric. ∎

For sq. free $m > 1$ 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). $m \geq 2$ sq. free.

Case 1. $m \equiv 2, 3 \bmod 4$.

$\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$.

Choose $0 \leq b$ 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. (Show!)

Case 2. $m \equiv 1 \bmod 4$.

Pick smallest $b \geq 0$ s.t. $b^2 m \pm 4$ 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.

- $\mathbb{Z}[\sqrt{5}]$: $5b^2 \pm 4 = a^2$. $(1,1)$ works.

- $\mathbb{Z}[\sqrt{94}]$: $2143295 + 221064\sqrt{94}$.
- $\mathbb{Z}[\sqrt{95}]$: $31 + 4\sqrt{95}$.

Lecture 19 (14-03-2022)

14 March 2022 17:29

Defn. $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ is an absolute value on K (field) if

(i) $|x| = 0 \iff x = 0$.

(ii) $|xy| = |x||y|$.

(iii) $\exists\, c > 0$ s.t. $|x+y| \leq c \cdot \max(|x|, |y|)$.

Note:

$|1| = 1$.

- For $x \in K^\times$:

$|x^{-1}| = |x|^{-1}$.

$|x| < 1 \iff |x^{-1}| > 1$.

EXAMPLE. (Trivial absolute value)

$$|x| = \begin{cases} 0 & ; \quad x = 0, \\ 1 & ; \quad x \neq 0. \end{cases}$$

Assumption: We will consider only non-trivial values, i.e., $\exists\, x \in K^\times$ s.t. $|x| \neq 1$. Thus, $\exists\, x, y \in K^\times$ s.t. $|x| < 1 < |y|$, by the calc. on right.

Defn. $|\cdot|, \; |\cdot|_1 : K \longrightarrow \mathbb{R}_{\geq 0}$ are said to be equivalent if

① $\quad |x|_1 < 1 \iff |x| < 1 \quad \forall\, x \in K$.

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 $x \in K^\times$. Then, can write $|x| = |y|^\alpha$ for some $\alpha \in \mathbb{R}$.

Let $\left(\frac{m_i}{n_i}\right)_i \in \mathbb{Q}^{\#}$ be a sequence decreasing to α.

$$|x| = |y|^\alpha < |y|^{m_i/n_i}$$

$$\Rightarrow |x^{n_i}| < |y^{m_i}|$$

$$\Rightarrow \left|\frac{x^{n_i}}{y^{m_i}}\right| < 1$$

$$\Rightarrow \left|\frac{x^{n_i}}{y^{m_i}}\right|_1 < 1$$

$$\Rightarrow |x|_1 < |y|_1^{m_i/n_i}.$$

Let $i \to \infty$ to get $|x|_1 \le |y|_1^\alpha$.

Thus, $|x| = |y|^\alpha \implies |x|_1 \le |y|_1^\alpha$.

By considering an increasing sequence, we get the reverse ineq.

Thus,

$$|x| = |y|^\alpha \implies |x|_1 = |y|_1^\alpha.$$

Thus, $\dfrac{\log |x|}{\log |x|_1}$ is constant for x s.t. $|x| \neq 1, 0$.

Let this constant be s.

Thus, $|x| = |x|_1^s$ for all $x \in K$. ∎

Defn. Let $|\cdot| : K \to \mathbb{R}_{\ge 0}$ be an absolute value s.t.

$$|x+y| \le |x| + |y|.$$

Then, $|\cdot|$ is said to be a valuation.

- $|\cdot|$ is said to be non-Archimedean if $|x+y| \le \max(|x|, |y|)$.
- $|\cdot|$ 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 $\forall s$.

Proof. $|1+1|^s = 2^s$.

$\max(|1|, |1|) = 1$.

$2^s > 1$ for all $s > 0$. ∎

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 $0 \neq \mathfrak{p} \in \operatorname{Spec}(R)$.
Then, $R_\mathfrak{p}$ is a local PID.

Proof. Local and ID is clear.
Let $x \in \mathfrak{p} \setminus \mathfrak{p}^2$.
Then, $\langle x \rangle = \mathfrak{p}\,\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_t^{r_t}$ for $\mathfrak{p}_i \neq \mathfrak{p}$.
Now, localising gives

$$xR_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}.$$

Now, since $\mathfrak{p}R_\mathfrak{p}$ is also a DD, we see that
$\operatorname{Spec}(\mathfrak{p}R_\mathfrak{p}) = \{0, \mathfrak{p}R_\mathfrak{p}\}$. Thus, all ideals are principal. ∎

Alike. Any ideal $\neq 0$ of $R_\mathfrak{p}$ is of the form $IR_\mathfrak{p}$ for an ideal $0 \neq I \in R$.
Write $I = \mathfrak{p}^e\,\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_t^{r_t}$. Localise to get $IR_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^e = \langle x^e \rangle$. ∎

Defn. If R is a local PID, then R is a discrete valuation ring (DVR).

Example: · R PID $\Rightarrow$ Every localisation is a PID
$\Rightarrow$ $R_\mathfrak{p}$ is a DVR for all $\mathfrak{p} \in \operatorname{Spec}(R)$.

· More generally, R : DD $\Rightarrow$ $R_\mathfrak{p}$ is a DVR for all primes $\mathfrak{p}$.

EXAMPLE OF NON-ARCHIMEDEAN VALUATION:

Let $(R, \mathfrak{m})$ be a DVR which is not a field.
$\mathfrak{m} = \langle \pi \rangle$.
Given $a \in R \setminus \{0\}$, we can write $a = u \cdot \pi^n$ for some unit u
($\because$ We have $\langle a \rangle = \mathfrak{m}^n$ for some unique $n \geq 0$.) and $n \geq 0$ (unique n).
independent of generator of $\mathfrak{m}$

Define $v : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ by $v(a) = n$.

Fix $r \in (0,1)$, and let $K = \operatorname{Frac}(R)$.
Define $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ by

$$\frac{a}{b} \longmapsto \begin{cases} r^{v(a) - v(b)}, & a \neq 0 \\ \ldots & a = 0 \end{cases}$$

$$b \begin{cases} & \\ 0 & , \quad a = 0. \end{cases}$$

(This is well-defined.)

- $|0| = 0$.
- $|xy| = |x|\,|y|$ is also clear.
- $|x+y| \leq \max(|x|, |y|)$.

<u>Proof</u>: We can write $x = u \cdot \pi^n$ and $y = v \cdot \pi^m$
(Assume $xy \neq 0$) for $u, v \in \mathcal{U}(R)$ and $n, m \in \mathbb{Z}$.
Assume $n \geq m$.

$$x + y = u\pi^n + v\pi^m$$
$$= \pi^m v \underbrace{\left(\frac{u}{v}\pi^{n-m} + 1 \right)}_{\in R}$$

$\therefore\ x + y = u' \pi^\alpha$ for some $\alpha \geq m$.

$\therefore\ |x+y| = r^\alpha \leq r^m = \max(r^n, r^m) = \max(|x|, |y|)$. ☒

Lecture 20 (17-03-2022)

17 March 2022 17:31

Recall: $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ absolute value

if
- $|x| = 0 \iff x = 0$,
- $|xy| = |x||y|$,
- $|x+y| \leq C \max(|x|, |y|)$ for some $C > 0$.

We assume our absolute values are non-trivial: $\exists\, x \in K^\times$ 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
$$v : K \longrightarrow \mathbb{Z} \cup \{\infty\} \quad \text{s.t.}$$
- $v(x) = \infty \iff x = 0$,
- $v(xy) = v(x) + v(y)$, $\quad$ ($K^\times \to \mathbb{Z}$ is a group homom.)
- $v(x+y) \geq \min(v(x), v(y))$.

Lemma. Let $v : K \to \mathbb{Z} \cup \{\infty\}$ be an exponential valuation.
Then, for any $c \in (0,1)$, the map
$$|\cdot|_v : K \longrightarrow \mathbb{R}_{\geq 0} \quad \text{defined by}$$
$$x \longmapsto c^{v(x)}$$
is a non-Archimedean valuation.

Proof. Easy check ☒

Example. Let R be a Dedekind domain (not a field).
Let $\mathfrak{p} \neq 0$ be a prime ideal of R.
Define, for $x \neq 0$,
$$v_{\mathfrak{p}}(x) = \text{power of } \mathfrak{p} \text{ in the prime factorisation of } x.$$
Extend this to $K^\times$ 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 $v_p(x+y) \geq \min(\ldots)$.

To check that, we localize at p to get

$xR_p = (\pi^n)$, $yR_p = (\pi^m)$, where

$pR_p = (\pi)$, $n = v_p(x)$, $m = v_p(y)$.

Then, $x = u\cdot\pi^n$, $y = v\cdot\pi^m$ with $n \geq m$.

Then, $\pi^m \mid (x+y)$.

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

Lemma. Let $|\cdot| : K \to \mathbb{R}_{\geq 0}$ be a non-Archimedean valuation.

Let $R := \{x \in R : |x| \leq 1\}$,

$p := \{x \in R : |x| < 1\}$.

Then, (R, p) is a local ring.

Proof. By non-Arch.: $x, y \in K$ satisfy

$|x+y| < \min(|x|, |y|)$.

$\therefore$ R closed under $+$.

$0, 1 \in R$ ✓ $|xy| = |x||y|$. $\therefore$ R is a ring.

$\|^{ly}$ p is an ideal.

We claim: $R \setminus p$ = units of R.

($\supseteq$) Clear since $1 \notin p$. Thus, p is a proper ideal.

($\subseteq$) Let $x \in R\setminus p$. Then, $|x| = 1$.

Thus, x is a unit in K with $|x^{-1}| = 1$.

$\therefore$ $x^{-1} \in R$. ∎

Note: If $x \in K^\times$, then either x or $x^{-1} \in K$.

Def^n. R is a valuation ring if R is a domain such that for any $0 \neq x \in \mathrm{Frac}(R)$, one of x or x^{-1} is in R.

(Lemma contd.) Further, if R is a DVR, then $|K^\times| \simeq \mathbb{Z}$.
↳ image of $K^\times$ under $|\cdot|$

Proof $\mathfrak{p} = (\pi)$. If $u \in \mathcal{U}(R)$ then $|u| = 1$.
$x \in R \setminus \{0\}$: $x = u \cdot \pi^n$.
$\Rightarrow |x| = |\pi|^n$ for $n \geq 0$.
Finally, for $\frac{x}{y} \in K^\times$, we have

$$\left|\frac{x}{y}\right| = |\pi|^{n-m}.$$

Thus, $|K^\times|$ is generated by $|\pi|$. ∎

Conversely, if $|K^\times|$ is cyclic ($\simeq \mathbb{Z}$), then R is a DVR.

Proof We already know that R is a local ring with max'l ideal $\mathfrak{p}$. Need to show $\mathfrak{p}$ is principal.
Let $\phi : |K^\times| \xrightarrow{\sim} \mathbb{Z}$ be an isomorphism.
Let $x \in K^\times$ 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: $\langle x \rangle = \mathfrak{p}$. (In turn, $\phi(|R \setminus \{0\}|) = \mathbb{Z}_{\geq 0}$.)
Proof ($\subseteq$) $x \notin \mathcal{U}(R)$ as $\phi|x| \neq 0$. $\therefore x \in \mathfrak{p}$
($\supseteq$) Let $y \in \mathfrak{p}$. 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. $|\cdot| : K \to \mathbb{R}_{\geq 0}$: valuation.
Can consider the image of $\mathbb{Z}$ in K, call it $\mathbb{Z}|_K$.
$|\cdot|$ is non-Archimedean iff $|\mathbb{Z}|_K|$ is bounded.

Proof ($\Rightarrow$) $|1 + \cdots + 1| \leq |1|$.
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.

$$|x+y|^n = |(x+y)^n| = \left| \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i} \right|$$

triangle inequality since $|\cdot|$ is a valuation

$$\leq \sum_{i=0}^{n} \left|\binom{n}{i}\right| |x|^i |y|^{n-i}$$

$$\leq r \cdot (n+1) \max(|x|^n, |y|^n).$$

$$\Rightarrow |x+y| \leq r^{1/n} (n+1)^{1/n} \max(|x|, |y|).$$

Let $n \to \infty$ to get

$$|x+y| \leq \max(|x|, |y|).$$ ∎

Valuations of $\mathbb{Q}$:

- For $p \geq 2$ prime, we have the evaluation

$$|\cdot|_p = c^{v_p}, \qquad c \in (0,1), \text{ where}$$

$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ exponential valuation is defined as

$$v_p\left(p^t \frac{m'}{n'}\right) := t \quad \text{for } (p, m'n') = 1.$$

$$(v_p(0) := \infty)$$

One choice of c is $\frac{1}{p}$.

$$|\cdot|_p = \left(\frac{1}{p}\right)^{v_p}$$ 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

$$|x|_p \le 1 \iff \frac{1}{p^{v_p(x)}} \le 1 \iff v_p(x) \geq 0 \iff x \in \mathbb{Z}_{(p)}.$$

$\therefore \mathbb{Z}_{(p)}$ 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 $x \in \mathbb{Q}^\times$,

$$\prod_{p \in \text{Primes} \cup \{\infty\}} |x|_p = 1.$$

(Have picked a representative from each class.)

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

$$|p|_p = \frac{1}{p}, \quad |p|_\infty = p, \quad |p|_q = 1$$

for primes $q \neq p$. ∎

Def^n. K: field.
An equivalence class $\mathfrak{p}$ of valuations on K is called a prime in K.
$\mathfrak{p}$ 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 $|\,|_{\mathfrak{p}} \in \mathfrak{p}$ s.t.

$$\prod_{\substack{\mathfrak{p}:\text{ primes}\\ \text{in } \mathbb{Q}}} |x|_{\mathfrak{p}} = 1.$$

Proof of theorem: Let $|\cdot|$ be a valuation on $\mathbb{Q}$.

Fix $m, n \geq 2$. Then, $\exists r \in \mathbb{N} \cup \{0\}$ s.t.

$$n^r \leq m < n^{r+1}.$$

$$m = a_0 + a_1 n + \cdots + a_r n^r \quad \text{for } a_i \in \{0, 1, \ldots, n-1\}.$$

$$N = \max\{1, |n|\}.$$

$$\begin{aligned}
\therefore |m| &\leq \sum |a_i|\,|n^i| \\
&\leq \sum |a_i|\, N^i \\
&\leq \sum (a_i |1|)\, N^i \\
&\leq \sum a_i\, N^i
\end{aligned}$$

$$\begin{aligned}
\Rightarrow |m| &\leq (r+1)\cdot n \cdot N^r \\
&\leq \left(1 + \frac{\log m}{\log n}\right) \cdot n \cdot N^{\log m / \log n}.
\end{aligned}
\qquad \left(\begin{aligned} & n^r \leq m \\ \Rightarrow\ & r \leq \log m / \log n. \end{aligned} \right)$$

Thus, $$|m^s| \leq \left(1 + \frac{s \log m}{\log n}\right) n \cdot N^{s \log m / \log n}.$$

$$\Rightarrow |m| \leq \left(1 + s\frac{\log m}{\log n}\right)^{1/s} \cdot n^{1/s} \cdot N^{\log m / \log n}.$$

Let $s \longrightarrow \infty$ to get

$$\boxed{|m| \leq N^{\log m / \log n}.}$$

Case 1. $|k| > 1$ for all $k > 1$.

Then, $N = \max\{1, |n|\} = |n|$.

Thus,

$$|m| \leq |n|^{\log m / \log n}.$$

Thus,

$$|m| \le |n|^{\log m/\log n}$$

$$\Rightarrow |m|^{1/\log m} \le |n|^{1/\log n}.$$

But interchanging $m \leftrightarrow n$ shows $|m|^{1/\log m} = |n|^{1/\log n}$ for all $m, n > 1$.

Let this constant be C.

Then, $|m| = C^{\log m}$.

Also, $|-m| = |m|$.

$$\therefore |m| = C^{\log |m|_\infty} \quad \forall\ m \in \mathbb{Z}\setminus\{0\}.$$

Write $C = e^{\alpha}$ gives

$$|m| = |m|_\infty^{\alpha} \quad \forall\ m \in \mathbb{Z}\setminus\{0\}.$$

This finishes the proof.

Case 2. $|n| \le 1$ for some $n > 1$.

Then, $N = 1$. $\therefore |m| \le 1 \quad \forall\ m > 1$.

$\Rightarrow |\mathbb{Z}| \le 1$.

$\therefore |\cdot|$ is non-Archimedean.

Let $R \subseteq \mathbb{Q}$ be the valuation ring of $|\cdot|$.

$R = \{x \in \mathbb{Q} : |x| \le 1\}$.

Let $\mathfrak{p} = \{x \in \mathbb{Q} : |x| < 1\} \subseteq R$

Note that $\mathfrak{p} \ne 0$ since nontrivial valuation.

Also, $\mathfrak{p} \cap \mathbb{Z}$ is a nonzero prime ideal.

$\therefore \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p \geq 2$.

$\therefore p \in \mathfrak{p}$.

Also, if $m \in \mathbb{Z}$ with $p \nmid m$, then $m \notin \mathfrak{p}$.

$\therefore m$ is a unit.

$\therefore \mathbb{Z}_{(p)} \subseteq R \subseteq \mathbb{Q}$.

Claim: $|\cdot|$ is equiv to $|\cdot|_p$.

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.

$$\therefore |x| = |p^r| \cdot \left|\frac{m}{n}\right|$$

Then, m and n are units in R.

$$\therefore |x| = |p^r| \cdot \Big|\underbrace{\frac{m}{n}}_{=1}\Big|$$

$$= |p|^r . \qquad \blacksquare$$

Then, we're done. $\blacksquare$

Reference: - Algebraic Number Theory by Janusz.
- Online notes by James Milne.

Lecture 21 (21-03-2022)

21 March 2022 17:11

Completion:

K: field, $|\cdot|: K \to \mathbb{R}_{\geq 0}$ valuation on K.

this induces a metric

want to complete field w.r.t. this $d(x,y) = |x-y|$

Let $(a_n)_n$ be a Cauchy sequence in K (wrt $|\cdot|$).

That is, $\forall \varepsilon > 0$ $\exists N \in \mathbb{N}$ s.t. $|a_n - a_m| < \varepsilon$ $\forall n, m \geq N$.

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

$$\lim_{n\to\infty} |a_n - a| = 0.$$

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 $\mathcal{C}$ be the set of all Cauchy sequences in K.

Let $\mathcal{Y}$ 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 $\mathcal{C}$.

This make $(\mathcal{C}, +, \cdot)$ a ring with $1 = (1)_n$ and $0 = (0)_n$.

Moreover, $\mathcal{Y}$ is an ideal in $\mathcal{C}$.

Defn. $\hat{K} = \mathcal{C}/\mathcal{N}$: ring.

Claim. $\hat{K}$ is a field.

Proof. Let $(a_n)_n \in \mathcal{C} \setminus \mathcal{N}$. $(|a_n|)_n$ is Cauchy in $\mathbb{R}$. Thus, it has a limit a. Furthermore, $a > 0$ since $(a_n)_n \notin \mathcal{N}$.

Thus, $|a_n| \geq \frac{a}{2} > 0$ for $n \gg 0$.

Define $b_n = \dfrac{1}{a_n}$ for $n \gg 0$. ($|b_n|$ converges to $1/a$. Thus, Cauchy.)

Then, $(a_n b_n)_n$ is eventually 1.

Thus, $(a_n b_n)_n = 1$ modulo $\mathcal{N}$. ∎

We have the map $i : K \to \hat{K}$, $a \mapsto (a)_n$.

$i(1) = 1$, thus i is injective.

i is a ring homom. in fact.

Valuation on $\hat{K}$:

Define $|\cdot|_0 : \mathcal{C} \to \mathbb{R}_{\geq 0}$ by
$$(a_n)_n \longmapsto \lim_{n\to\infty} |a_n|.$$

- $|(a_n)_n|_0 = 0 \iff (a_n)_n \in \mathcal{N}$.
- $$|(a_n b_n)_n|_0 = \lim_{n\to\infty} |a_n||b_n| = \left(\lim_{n\to\infty} |a_n|\right)\left(\lim_{n\to\infty} |b_n|\right) = |(a_n)_n|_0 \, |(b_n)_n|_0.$$
- $$|(a_n + b_n)_n|_0 = \lim_{n\to\infty} |a_n + b_n| \leq \lim_{n\to\infty} |a_n| + \lim_{n\to\infty} |b_n| = |(a_n)_n|_0 + |(b_n)_n|_0.$$

$|\cdot|_0$ makes sense modulo $\mathcal{N}$. 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 $\hat{K}$.

$\forall n: u^{(n)} = (x_k^{(n)})_k$

$\hookrightarrow$ Cauchy in K.

Given $\varepsilon > 0$, $\exists N$ s.t.

$$|u^{(n)} - u^{(m)}| < \varepsilon \quad \forall n, m \geq N$$

$$\| $$

$$\lim_{k \to \infty} |x_k^{(n)} - x_k^{(m)}| < \varepsilon. \qquad (*)$$

Step 1. Fix n. $u^{(n)} \in \mathcal{C}$.

$\exists N_n$ s.t. $|x_q^{(n)} - x_r^{(n)}| < \frac{1}{n} \quad \forall q, r \geq N_n$.

Replacing $(x_k^{(n)})_k$ by $(x_{k+N_n}^{(n)})_k$, we may assume

$$|x_q^{(n)} - x_r^{(n)}| < \frac{1}{n} \quad \forall q, r.$$

Note that $(x_k^{(n)})_k - (x_{k+N_n}^{(n)})_k \in \mathfrak{N}$.

Step 2. Let $u := (x_1^{(n)})_n$. Note that u is a sequence in K.

We show $u \in \mathcal{C}$ and $\lim_{n \to \infty} |u^{(n)} - u| = 0$.

Thus, $u^{(n)} \longrightarrow u \in \hat{K}$ and we are done.

(i) $u \in \mathcal{C}$.

Proof Let $\varepsilon > 0$ be given.

$$|x_1^{(n)} - x_1^{(m)}| \le |x_1^{(n)} - x_q^{(n)}| + |x_q^{(n)} - x_q^{(m)}| + |x_q^{(m)} - x_1^{(m)}|$$

$(*)$

$$\le \frac{1}{n} + \frac{\varepsilon}{3} + \frac{1}{m} < \varepsilon$$

for $n, m \gg 0$.

(ii) $x^{(n)} \to x$.

Proof. $$|x^{(n)} - x| = \lim_{k \to \infty} |x_k^{(n)} - x_1^{(k)}|.$$

Given $\varepsilon > 0$:

$$|x_k^{(n)} - x_1^{(k)}| \le \underbrace{|x_k^{(n)} - x_1^{(n)}|}_{\le \frac{1}{n}} + \underbrace{|x_1^{(n)} - x_1^{(k)}|}_{\le \varepsilon/2}.$$

since $x \in \mathcal{C}$

This gives (ii).

We are done ∎

Def^n. $(K, |\cdot|)$: field with a valuation.

$(\hat{K}, |\cdot|_0)$: complete field w.r.t. $|\cdot|_0$.

$i : K \to \hat{K}$ 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 $f : (K, |\cdot|) \to (L, |\cdot|')$ be a homomorphism, i.e., $f : K \to L$ is a ring homom and $|x| = |fx|'$ $\forall x \in K$.

Then, $\exists! \hat{f} : \hat{K} \to \hat{L}$ ring homom s.t. $|u| = |\hat{f}u|'$ $\forall u \in \hat{K}$.

Further, $i' \circ f = \hat{f} \circ i$.

$$\begin{array}{ccc} (K, |\cdot|) & \xrightarrow{f} & (L, |\cdot|') \\ {\scriptstyle i}\downarrow & \circlearrowright & \downarrow{\scriptstyle i'} \end{array}$$

$$\begin{array}{ccc} & & \\ i \downarrow & \circlearrowright & \downarrow i' \\ (\hat{K}, |\cdot|) & \xrightarrow[\hat{f}]{} & (\hat{L}, |\cdot|') \end{array}$$

Here, $\hat{K}$ and $\hat{L}$ 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 $\hat{f}([(a_n)_n]) := [(fa_n)_n] \in \hat{L}$.

All desired properties are easy to see. ∎

Corollary. The completion of $(K, |\cdot|)$ is unique up to unique isomorphism.

EXAMPLES. ① $(\mathbb{Q}, |\cdot|_\infty)$.

Completion is $\mathbb{R}$.

② $(\mathbb{Q}, |\cdot|_p) \to p$-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 $(\mathbb{Q}, |\cdot|_p)$.

Lecture 22 (24-03-2022)

24 March 2022 17:23

Theorem. $(R, \mathfrak{p})$: DVR. $K = \mathrm{Frac}(R)$.

$\mathfrak{p} = (\pi)$ and $K = \{u \cdot \pi^k : u \in R^\times, k \in \mathbb{Z}\}$.

Fix $c \in (0,1)$.

Then, $|\cdot| : K \to \mathbb{R}_{\geq 0}$ defined by

$u \cdot \pi^k \longmapsto c^k$ is a non-Archimedean $\mathfrak{p}$-adic valuation on K.

Let $(K_\mathfrak{p}, |\cdot|)$ be the completion.

(This will again be non-Archimedean since $|\mathbb{Z} \cdot 1_{K_\mathfrak{p}}| = |\mathbb{Z} \cdot 1_K|$ is bounded.)

Then, define the associated objects $\hat{R} := \{x \in K_\mathfrak{p} : |x| \leq 1\}$

$\hat{\mathfrak{p}} := \{x \in \hat{R} : |x| < 1\}$.

We also use $\hat{K}$ for $K_\mathfrak{p}$.

Then, (i) $\hat{R}$ is a DVR,

(ii) $\hat{\mathfrak{p}} = \pi \hat{R}$.

Proof. (i) Recall $\hat{R}$ is a DVR iff $|K_\mathfrak{p}^\times| \simeq \mathbb{Z}$.

Let $\alpha \in K_\mathfrak{p}^\times$. Let $(a_n)_n \in K^\mathbb{N}$ be s.t. $[(a_n)_n] = \alpha$.

$$0 \neq |\alpha| = \lim_{n\to\infty} |a_n| = \lim_{n\to\infty} c^{k_n} \quad \text{for some integer sequence } (k_n)_n.$$

Since $c \in (0,1)$, it is forced that $(k_n)_n$ is eventually constant.

Wlog, $|a_n| = c^k$ for fixed $k \in \mathbb{Z}$ and all $n \geq 1$.

$\therefore$ $|\alpha| = c^k$ for some $k \in \mathbb{Z}$.

The above is true for all $\alpha \in K^\times$.

$\therefore$ $|\hat{K}^\times| = \mathbb{Z}$.

(ii) As $\hat{R}$ is a DVR, write $\hat{\mathfrak{p}} = x\hat{R}$.

$\pi \in \hat{\mathfrak{p}}$ since $|\pi| < 1$.

Write $|x| = c^m$. $|x| < 1 \Rightarrow m \in \mathbb{Z}_{>0}$.

$(m \in \mathbb{Z})$

Also, $|\pi| = 1$. $\therefore$ $\left|\frac{x}{\pi^m}\right| = 1$

In general, if $(R, \mathfrak{p})$ is a DVR and $\mathfrak{p} = (\pi)$, then π is a prime and hence irreducible.

$\Rightarrow$ $x = u \cdot \pi^m$ for some $u \in \mathcal{U}(\hat{R})$.

But x is irred in $\hat{R}$.

$\therefore$ $m = 1$ and $x\hat{R} = \pi\hat{R}$. ☒

Porism. Same setup as earlier:

$$(R, \mathfrak{p}) \rightsquigarrow |\cdot|_{\mathfrak{p}} \xrightarrow{\text{completion}} \hat{K} \rightsquigarrow (\hat{R}, \hat{\mathfrak{p}}) \text{ DVR}.$$

① Given $\alpha \in \hat{K}^\times$, there is a Cauchy sequence $(a_n)_n \in K^{\mathbb{N}}$ s.t.

$$\alpha = [(a_n)_n] \quad \text{and} \quad |\alpha| = |a_n| \quad \forall n \in \mathbb{N}.$$

Moreover, $|K^\times| = |\hat{K}^\times|$.

② Given $\alpha \in \mathcal{U}(\hat{R})$, we have $|\alpha| = 1$.

Thus, $\exists$ Cauchy $(a_n)_n \in K^{\mathbb{N}}$ s.t. $|a_n| = 1$ $\forall n \in \mathbb{N}$.

(In particular, $a_n \in \mathcal{U}(R)$ $\forall n$.)

Cor. ③ Under the inclusion $R \hookrightarrow \hat{R}$, $\hat{\mathfrak{p}}$ is the ideal generated by $\mathfrak{p}$. Moreover, $R/\mathfrak{p}^n \cong \hat{R}/\hat{\mathfrak{p}}^n$ for all $n \geq 1$.

Example. ① $R = \mathbb{Z}_{\langle p \rangle}$. $p \geq 2$ prime. $\operatorname{Frac}(R) = \mathbb{Q}$.

$$|p|_p = \frac{1}{p}.$$

$\mathbb{Q}_p$ = completion of $\mathbb{Q}$ wrt $|\cdot|_p$ $\rightarrow$ p-adic field

$\mathbb{Z}_p$ = valuation ring of $\mathbb{Q}_p$ $\rightarrow$ p-adic integers

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p$$

$$\mathfrak{p} = p\mathbb{Z} \rightsquigarrow \hat{\mathfrak{p}} = p\mathbb{Z}_p$$

$$\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \quad \text{for } n \geq 1.$$

$\therefore$ $\mathbb{Z}_p/p^n\mathbb{Z}_p$ is finite $\forall n$.

② $R = \mathbb{F}_p[t]$, $f \in R$ monic irred, $K = \mathbb{F}_p(t)$.

$\mathfrak{Q} = \langle f \rangle$. Similar results as before.

Proof of Corollary ③ Suffices to prove: (i) $\hat{R} = R + \hat{\mathfrak{p}}^n$. $\Big\} \Rightarrow \dfrac{\hat{R}}{\ } - \dfrac{R + \hat{\mathfrak{p}}^n}{\ }$

Proof of Corollary ③ Suffices to prove: (i) $\hat{R} = R + \hat{\mathfrak{p}}^n$, (ii) $R \cap \hat{\mathfrak{p}}^n = \mathfrak{p}^n$. $\Rightarrow \frac{\hat{R}}{\hat{\mathfrak{p}}^n} = \frac{R+\hat{\mathfrak{p}}^n}{\hat{\mathfrak{p}}^n} \cong \frac{R}{\mathfrak{p}^n} = \frac{R}{R\cap\hat{\mathfrak{p}}^n}$

Let $\alpha \in \hat{R} \setminus \hat{\mathfrak{p}}$. Then, $|\alpha| = 1$. Write $\alpha = [(a_n)_n]$ with $|a_n| = 1$ $\forall n$, $a_n \in K$.

Can assume $|a_n - a_{n+1}| \leq \frac{1}{2}$ $\forall n$.

As $|\cdot|$ is non-arch, we get

$$|a_1 - a_n| \leq \frac{1}{2} \quad \forall n.$$

Taking $n \to \infty$ gives $|a_1 - \alpha| \leq 1/2 < 1$.

$\therefore a_1 - \alpha \in \hat{\mathfrak{p}}$.

$$\therefore \hat{R} = R + \hat{\mathfrak{p}}$$
$$\Rightarrow \pi\hat{R} = \pi R + \pi\hat{\mathfrak{p}}$$
$$\Rightarrow \hat{\mathfrak{p}} = \mathfrak{p} + \pi\hat{\mathfrak{p}}$$

$$\Rightarrow \hat{R} = R + \mathfrak{p} + \pi\hat{\mathfrak{p}}$$
$$= R + \hat{\mathfrak{p}}^2.$$

Continue to get $\hat{R} = R + \hat{\mathfrak{p}}^n$ $\forall n$.

$$\hat{\mathfrak{p}}^n \cap R = \{x \in \hat{K} : |x| \leq c^n\} \cap R$$
$$= \{x \in R : |x| \leq c^n\} = \mathfrak{p}^n. \quad \blacksquare$$

Power Series Representation of Elements

$(R, \mathfrak{p})$: DVR $\quad (K, |\ |) \quad \mathfrak{p} = \pi R$

$(\hat{R}, \hat{\mathfrak{p}})$: DVR $\quad (\hat{K}, |\ |) \quad \hat{\mathfrak{p}} = \pi\hat{R}$

Fix a set S of coset representatives of $R/\mathfrak{p}$ with $0 \in S$.

$$R = \bigsqcup_{s \in S} (s + \mathfrak{p}).$$

Given any sequence $(s_i)_i \in S^{\mathbb{N}}$, and $v \in \mathbb{Z}$.

$$a_n := \pi^{v}(s_0 + s_1 \pi + \cdots + s_n \pi^n) \in K$$

for all $n \geq 1$.

If $n < m$, then

$$a_m - a_n = \pi^{v}(s_{n+1} \pi^{n+1} + \cdots + s_m \pi^m).$$

$$\Rightarrow |a_m - a_n| = c^t \quad \text{for some } t \geqslant v + n + 1.$$

Thus, $(a_n)_n \in K^{\mathbb{N}}$ is Cauchy.

$$[(a_n)_n] =: \pi^{v}(s_0 + s_1 \pi + \cdots).$$

(Looking at K as a subset of $\hat{K}$, we have:

$$\lim_{n \to \infty} \pi^{v}(s_0 + s_1 \pi + \cdots + s_n \pi^n) = \lim_{n \to \infty} a_n = [(a_n)_n].)$$

Theorem. Every $\alpha \in \hat{K}^{\times}$ can be represented UNIQUELY as a power series

$$\pi^{v}(s_0 + s_1 \pi + s_2 \pi + \cdots) \quad \text{for } s_i \in S,\ s_0 \neq 0,\ v \in \mathbb{Z}.$$

Proof. Write $\alpha = u \cdot \pi^{v}$. $v \in \mathbb{Z}$ is fixed as $|\alpha| = c^{v}$ and $u \in \mathcal{U}(\hat{R})$ is fixed.

Note that $|\pi^{v}(s_0 + s_1 \pi + \cdots)| = c^{v}$. Thus, v is unique.

Suffices to prove that $u \in \mathcal{U}(\hat{R})$ can be uniquely written as

$$s_0 + s_1 \pi + s_2 \pi^2 + \cdots.$$

Note $\hat{R}/\hat{\mathfrak{p}} \simeq R/\mathfrak{p}$.

Note $\quad \hat{R}/\hat{\mathfrak{p}} \simeq R/\mathfrak{p}$.

$$u + \hat{\mathfrak{p}} \longmapsto s_0 + \mathfrak{p} \quad \text{for some unique } s_0 \in S.$$

$s_0 \neq 0$ since $u \notin \hat{\mathfrak{p}}$.

Now, $u - s_0 \in \mathfrak{p}$. Look at image of $u - s_0$ in $\hat{R}/\hat{\mathfrak{p}}^2 \cong R/\mathfrak{p}^2$

to get s_1 s.t.

$$u - s_0 \equiv s_1 \mod \hat{\mathfrak{p}}^2.$$

We proceed to get $s_0, s_1, s_2, \ldots$ s.t.

$$u - s_0 - s_1 - \cdots - s_n \in \mathfrak{p}^{n+1}.$$

Thus, $|u - s_0 - s_1 - \cdots - s_n| < c^{n+1} \longrightarrow 0$.

Uniqueness left as exercise. ∎

Example. $\mathbb{Z}_{\langle p \rangle} \quad \mathbb{Q}_p$.

$$\begin{array}{cc} \mathbb{Z}_{\langle p\rangle} & \mathbb{Q}_p \\ \uparrow & \uparrow \\ \mathbb{Z} & \mathbb{Q} \end{array}$$

$p = 3$. $\quad S = \{0, 1, 2\}$.

$|8|_3 = 1$.

$$8 = 3^0(2 + 2 \cdot 3 + 0 \cdot 3^2 + 0 \cdot 3^3 + \cdots)$$

polynomial rep.

$$-1 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$$

(not saying all same) power series

$$\frac{1}{8} = 2 + 2 \cdot 3 + \cdots$$

$\left(\frac{1}{8} \equiv 2 \mod 3\right)$

$\left(\frac{1}{8} = 2 + 3 \cdot \left(-\frac{5}{8}\right)\right)$

$\left(-\frac{5}{8} = 2 + 3 \cdot \left(-\frac{23}{8}\right)\right)$

$$-\frac{1}{8} = \frac{1}{1 - 3^2} = 1 + 3^2 + 3^4 + 3^6 + \cdots$$

$$F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n].$$

Qn. Does F have any integer solution?

Qn. Does F have $\mathbb{Z}_p$-solutions for all primes p?

Lemma. Fix a prime p.
F has a $\mathbb{Z}_p$-solution iff F has a solution in $\mathbb{Z}/p^n$ for all $n \geq 1$.

Proof. ($\Rightarrow$) Simple. Go modulo p^n.
(Note that $v \geq 0$ for elements in $\mathbb{Z}_p$.)
($\Leftarrow$) Assume $n=1$ for ease of notation. Similar for higher variables.
Let $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ be a solution of F.
Write

$$x_1 = s_{0,1},$$
$$x_2 = s_{0,2} + s_{1,2}\, p,$$
$$x_3 = s_{0,3} + s_{1,3}\, p + s_{2,3}\, p^2, \ \ldots$$

If the columns were constant, then could have gotten a solution.

Exercise. $\square$

Exercise: $x^2 = 2$ has a solution in $\mathbb{Z}_7$.

Lecture 23 (28-03-2022)

28 March 2022 17:31

Extension of Nonarchimedean Valuations

$(R, \mathfrak{p})$: DVR, $K = \mathrm{Frac}(R)$.

$|\cdot|_{\mathfrak{p}}$: $\mathfrak{p}$-adic evaluation on R. $(\mathfrak{p} = \langle \pi \rangle)$

$K = \{u \cdot \pi^n : u \in \mathcal{U}(R), n \in \mathbb{Z}\}$.

$v_{\mathfrak{p}}(u \pi^n) = n$, $|x| = c^{v_{\mathfrak{p}}(x)}$ for some $c \in (0,1)$

$L/K \longrightarrow$ separable extension.

R' = integral closure of R in L.

$\hookrightarrow$ Dedekind domain (Why? Same proof as for $\mathcal{O}_L$ can be imitated? We do have R is a PID.)

Note that any maximal ideal of R' contracts to a max'l ideal of R and hence, contracts to $\mathfrak{p}$ $\therefore$ There are only finitely many maximal ideals in R'.

$$\mathfrak{p} R' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \quad \text{prime fac.}$$

$$\mathrm{Max}(R') = \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}.$$

Prop^n. Any Dedekind domain with finitely many prime ideals is a PID.

Proof. Pick $x_1 \in \mathfrak{P}_1 \setminus \mathfrak{P}_1^2$.

$\exists\, z \in R'$ s.t. (CRT)

$$z \equiv x_1 \mod \mathfrak{P}_1^2,$$
$$z \equiv 1 \mod \mathfrak{P}_i \quad \text{for } i \geq 2.$$

Write $\langle z \rangle = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_r^{a_r}$.

The congruences gives $a_1 = 1$ and $a_i = 0$ for $i \geq 2$.

$\therefore \mathfrak{P}_1 = \langle z \rangle$.

Similarly, $\mathfrak{P}_2, \dots, \mathfrak{P}_r$ is principal.

$\therefore R'$ is a PID. ∎

Prop^n With setup as above:

① $(L, |\cdot|_{\mathfrak{p}_i})$: nonarch. valuation.

$$|\cdot|_{\mathfrak{p}_i}\Big|_K \text{ is equivalent to } |\cdot|_{\mathfrak{p}}$$

② If $|\cdot|$ is a (nonarchimedean) valuation on L which is equivalent to $|\cdot|_{\mathfrak{p}}$ on K, then $|\cdot|$ is equivalent to $|\cdot|_{\mathfrak{p}_{i_0}}$ for some i.

③ $\{|\cdot|_{\mathfrak{p}_i}\}_i$ are pairwise inequivalent.

Thus, the above tells us exactly how many ways there are to extend a valuation.

④ $R_i :=$ valuation ring of $|\cdot|_{\mathfrak{p}_i}$
$= \{x \in L : |x|_{\mathfrak{p}_i} \leq 1\}$.

$\mathfrak{p}_i = \langle \pi_i \rangle$.

$$L = \{u \cdot \pi_i^m : m \in \mathbb{Z}, u \in U(R_i)\}.$$

$R_i = R'_{\mathfrak{p}_i}$.

Proof. ① For $\pi \in K$ generating $\mathfrak{p}$, we have

$$\pi R' = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$
$$\Rightarrow \pi R'_{\mathfrak{p}_i} = (\mathfrak{p}_i R'_{\mathfrak{p}_i})^{e_i}$$
$$\Rightarrow \pi R_i = (\mathfrak{p}_i R_i)^{e_i}$$
$$\Rightarrow v_{\mathfrak{p}_i}(\pi) = e_i.$$

$$\Rightarrow |\pi|_{\mathfrak{p}_i} = c_i^{e_i} \qquad (\text{where } c_i := |\pi_i|)$$

Conclude.

② By replacing with an equiv. valuation, we may assume $|x| = |x|_{\mathfrak{p}}$ for $x \in K$.

$R_0 =$ valuation ring of $|\cdot|$
$= \{x \in L : |x| \leq 1\}$.

$R \subseteq R_0$.

Claim: $R' \subseteq R_0$.

Proof. If $x' \in R' \setminus \{0\}$, then

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \quad \text{for } a_i \in R.$$

If $x \notin R_0$, then $x^{-1} \in \mathfrak{m}$. $\to$ max'l ideal of R_0

$$\Rightarrow \quad 1 = -\underbrace{(a_1 x^{-1} + \cdots + a_0 x^{-n})}_{\in \mathfrak{m}}.$$

$\therefore 1 \in \mathfrak{m}$ $\to\leftarrow$. Thus, $R' \subseteq R_0$. ∎

Thus, $\mathfrak{m} \cap R' = \mathfrak{p}_i$ for some i. $(\because \mathfrak{m} \cap R = \mathfrak{p})$

$\Rightarrow \quad R' \setminus \mathfrak{p}_i \subseteq R_0 \setminus \mathfrak{m}$

$\Rightarrow \quad R' \setminus \mathfrak{p}_i \subseteq \mathcal{U}(R_0)$

Thus, $R'_{\mathfrak{p}_i} \subseteq R_0$. (as elements outside $\mathfrak{p}_i$ are already units in R_0)

Claim: $R'_{\mathfrak{p}_i} = R_0$.

After claim, it follows $|\cdot| \sim |\cdot|_{\mathfrak{p}_i}$ since same valuation rings.

Proof of claim is an exercise.
$\hookrightarrow$ Use that val. ring is max'l local ring.

③ Valuation rings are distinct. ∎

Theorem $(K, |\cdot|)$: nonarchimedean, complete valuation field.
Assume that the valuation ring R is a DVR.
Let R' and L be as before.

$$\begin{tikzcd} R' \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash, "n"] \\ (R, \mathfrak{p}) \arrow[r, dash] & K \end{tikzcd}$$

Then, there exists a unique extension of $|\cdot|$ to L. (up to equivalence)

One explicit representative is

$$|y| := |N_{L/K}(y)|_{\mathfrak{p}}^{1/n}.$$

Theorem $(R, \mathfrak{p})$: DVR. $K = \mathrm{Frac}(R)$.
Suppose K is a number field. Let R' and L be as before.

$$\begin{tikzcd} R' \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash] \\ R \arrow[r, dash] & K \end{tikzcd}$$

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

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

$$\begin{array}{ccc} K & & L \\ | & & | \\ R & — & k \end{array}$$

$|\cdot|_{\mathfrak{P}_1}, \ldots, |\cdot|_{\mathfrak{P}_r}$ are inequivalent valuations of L that restrict to $|\cdot|_{\mathfrak{p}}$ on K.

Let $P \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$.

$$\begin{array}{cc} K_{\mathfrak{p}}, & L_P \\ | & | \\ \hat{R} & \hat{R}' \\ | & | \\ \hat{\mathfrak{p}} & \hat{P} \end{array}$$

completions

- $\mathfrak{p} = \pi R$, $\hat{\mathfrak{p}} = \pi\hat{R}$. • Similarly, $P = \pi' R'$, $\hat{P} = \pi' \hat{R}'$.
- $e(P|\mathfrak{p}) = e(\hat{P} | \hat{\mathfrak{p}})$. (Localize.)
- $f(P|\mathfrak{p}) = f(\hat{P} | \hat{\mathfrak{p}})$.

Theorem. (Ostrowski's Theorem)

$(K, |\cdot|)$: Complete Archimedean valuation.

Then, K is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ (as fields) and $|\cdot|$ is equivalent to the corresponding absolute value on $\mathbb{R}$ or $\mathbb{C}$.

Sketch. Arch valuation $\Rightarrow$ char$(K) = 0$.

$\therefore \mathbb{Q} \hookrightarrow K$.

$\Rightarrow \hat{\mathbb{Q}} \hookrightarrow K$

$\cong$

$\mathbb{R}$

One then shows that every element of K satisfies a quadratic equation over $\mathbb{R}$.

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

$\sigma_1, \ldots, \sigma_r$: real embeddings of K.

$\sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$: complex embeddings of K.

Then,

$$|\cdot|_i : K \to \mathbb{R}_{\geq 0} \quad \text{for } i = 1, \ldots, r+s$$

$$x \mapsto |\sigma_i x|.$$

(i) $|\cdot|_1, \dots, |\cdot|_{r+s}$ are not equivalent.

(ii) These are all Archimedean valuations of K.

Proof (i) Given $i \in [r+s]$, $\exists\, u \in \mathcal{U}(\mathcal{O}_K)$ s.t.

$$\log|\sigma_j u| < 0 \quad \text{for } j \neq i,$$
$$\log|\sigma_i u| > 0.$$

$$\Rightarrow |\sigma_j u| < 1 \text{ for } j \neq i \text{ and } |\sigma_i u| > 1.$$

$$\therefore\ |\ |_i \not\sim |\ |_j.$$

(ii) $|\cdot|$: Arch. val. on K.

Complete $(K, |\cdot|)$ to $(\hat{K}, |\cdot|)$.

By Ostrowski, we may assume $(\hat{K}, |\cdot|) = (\mathbb{R}, |\cdot|)$ or $(\mathbb{C}, |\cdot|)$.

But $K \hookrightarrow \hat{K}$ and we already know all embeddings of K in $\mathbb{R}$ or $\mathbb{C}$.

$$\therefore\ |\ |_K = |\ |_i \text{ for some } i$$ ∎

Thus, we now know all Archimedean and non-Archimedean valuations on a number field (since we know those for $\mathbb{Q}$).

Product formula for Number Fields.

For $x \in \mathbb{Q}^\times$, we had

$$\prod_{p:\ \text{primes of } \mathbb{Q}} |x|_p = 1.$$

(Here, each $|\cdot|_p$ was normalised suitably.)

Now, if K is a number field, then we want to pick a representative suitably so that

$$\prod_{\mathfrak{p}:\ \text{primes of } K} |x|_{\mathfrak{p}} = 1 \quad \text{for all } x \in K^\times.$$

$$\shortparallel$$

$$\Big(\prod |x|_{\mathfrak{p}}\Big) \cdot \Big(\prod |x|_{\mathfrak{p}}\Big)$$

$$\left(\prod_{\mathfrak{p}\text{: non Arch.}} |x|_{\mathfrak{p}}\right) \cdot \left(\prod_{\mathfrak{p}\text{: Arch.}} |x|_{\mathfrak{p}}\right)$$

$$= \left(\prod_{\substack{p \geq 2 \\ \text{prime in } \mathbb{Z}}} \underbrace{\prod_{\mathfrak{p} \in \{\text{primes over } p\}} |x|_{\mathfrak{p}}}_{\text{normalise so that } |N_{K/\mathbb{Q}}(x)|_p}\right) \cdot \left(\underbrace{\prod_{i=1}^{r+s} |x|_i}_{|N_{K/\mathbb{Q}}(x)|_\infty}\right)$$

Then use result over $\mathbb{Q}$.

For the Archimedean ones, it is easy:

$|\cdot|_1, \ \ldots, \ |\cdot|_r, \ |\cdot|_{r+1}^2, \ \ldots, \ |\cdot|_{r+s}^2$ does the job.

For non-Archi : $|\cdot|_{p_i} \rightsquigarrow |\cdot|_{p_i}^{1/e_if_i}$.

Lecture 24 (31-03-2022)

31 March 2022 17:35

$\mathbb{Q}_p^* = \{ p^m(s_0 + s_1 p + \cdots) : m \in \mathbb{Z}, \ s_i \in \{0, \ldots, p-1\}, s_0 \neq 0\}.$

$\mathbb{Z}_p = \{0\} \cup \{ \quad$ — " — $: m \geq 0,$ — " — $\}.$

$= \{ s_0 + s_1 p + \cdots : s_i \in \{0, \ldots, p-1\}\}.$

$$\mathbb{Z}/p \xleftarrow{\lambda_1} \mathbb{Z}/p^2 \xleftarrow{\lambda_2} \mathbb{Z}/p^3 \leftarrow \cdots$$

λ_i : natural projections

$$\varprojlim_n \mathbb{Z}/p^n = \{ (x_n) = \prod_{n \geq 1} \mathbb{Z}/p^n : \lambda_n x_{n+1} = x_n \ \forall n \}.$$

Then,

$$\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n$$

$$s_0 + s_1 p + s_2 p^2 + \cdots \longleftrightarrow (s_0, s_0 + s_1 p, \ldots).$$

- $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right].$

- $\mathbb{Z}_p \cong \mathbb{Z}[x]/\langle x - p \rangle.$

$$\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}_p$$
$$x \longmapsto p.$$

(Note $\sum_{i=0}^{\infty} a_i p^i$ converges in $\mathbb{Z}_p$ for any choice!)

Clearly, $x - p \in \ker \varphi$.

Suppose $f(x) = \sum a_i x^i \in \ker \varphi$.

Then, $\sum_{i \geq 0} a_i p^i = 0.$

$$\Rightarrow \sum_{i=0}^{n-1} a_i p^i = 0 \quad \text{in } \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p.$$

Let $b_{n-1} = -\frac{1}{p^n}\left(\sum_{i=0}^{n-1} a_i p^i \right) \in \mathbb{Z}$ for $n \geq 1$.

$$b_0 = -\frac{1}{p} a_0; \qquad a_0 = -pb_0.$$

$$b_n = -\frac{1}{p^{n+1}}\left(\sum_{i=0}^{n} a_i p^i\right)$$

$$= \frac{b_{n-1}}{p} - \frac{a_n}{p} \implies a_n = b_{n-1} - pb_n \quad \text{for } n \geq 1.$$

Thus, $(x-p) \mid f(x)$.

- $(K, |\cdot|_p)$: complete wrt nonArch. valuation.

Assume $(\mathcal{O}, \mathfrak{p})$: dvr, valuation ring

$\mathfrak{p} = \pi\mathcal{O}$. Fix a set $S \subseteq R$ of coset reps. of $\mathfrak{p}$

$K^\times = \left\{ \pi^m \left(\sum_{i\geq 0} s_i \pi^i \right) : s_i \in S, \ s_0 \neq 0 \right\}$

$\mathcal{O} = \cdots$

$$\mathcal{O}/\mathfrak{p} \xleftarrow{\lambda_1} \mathcal{O}/\mathfrak{p}^2 \xleftarrow{\lambda_2} \cdots$$

$$\varprojlim_n \mathcal{O}/\mathfrak{p}^n \simeq \mathcal{O}. \qquad (*)$$

On $\mathcal{O}/\mathfrak{p}^n$, we give it the discrete topology.

Give $\prod \mathcal{O}/\mathfrak{p}^n$ the product topology.

Give $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$ the subspace topology.

$(*)$ is even a homeomorphism ($\mathcal{O}$ has a metric).

Thus, we have an isomorphism as topological rings.

Def^n. $(K, |\cdot|)$: complete, $|\cdot|$: nonarch.

Assume $(\mathcal{O}, \mathfrak{p})$, the valuation ring is a DVR.

K is said to be a local field if $\mathcal{O}/\mathfrak{p}$ is a finite field.

Theorem. Any local field is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.

Laurent series $= \mathbb{F}_p[t][\frac{1}{t}] = \mathrm{Frac}(\mathbb{F}_p[[t]])$

- $(K, |\cdot|)$: Local field
  $(\mathcal{O}, \mathfrak{p})$: DVR
  $\mathcal{O}/\mathfrak{p}$: finite field
  $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$.

  $\therefore \mathcal{O}/\mathfrak{p}^n$ is finite.

  $\mathcal{O} \cong \varprojlim \mathcal{O}/\mathfrak{p}^n$. $\to$ each $\mathcal{O}/\mathfrak{p}^n$ is finite. Thus, compact
  $\hookrightarrow \prod \mathcal{O}/\mathfrak{p}^n$ is compact.
  $\hookrightarrow \mathcal{O}$ is compact as $\mathcal{O}$ is complete with $\prod \mathcal{O}/\mathfrak{p}^n$.

  $\mathcal{O}, \mathfrak{p}, \mathfrak{p}^2, \dots$: system of nbds of 0.
  For $a \in K$, $a + \mathcal{O}$, $a+\mathfrak{p}$, $a+\mathfrak{p}^2, \dots$ is a system...
  $a + \mathcal{O}$ compact nbd.
  $\therefore K$ is locally compact.

Eg. $\mathbb{Q}_p$: locally compact
$\mathbb{Z}_p$: compact.

Theorem: (Hensel's Lemma)
$(K, \mathfrak{p})$: complete $|\cdot|$ nonarch
$(\mathcal{O}, \mathfrak{p})$: val. ring.
$R = \mathcal{O}/\mathfrak{p}$.
$f(x) \in \mathcal{O}[x]$ is primitive if $f(x) \neq 0$ and $\max_i \{|a_i|\} = 1$.
Then, if $\bar{f} = \bar{g}\bar{h} \mod p$ with $\gcd(\bar{g}, \bar{h}) = 1$, then $\exists\, g, h \in \mathcal{O}[x]$ s.t.

$$f = gh, \quad \bar{g} = g \bmod p, \quad \bar{h} = h \bmod p, \quad \deg g = \deg \bar{g}.$$

($\deg h \neq \deg \bar{h}$ is possible.)

Corollary. $f = x^{p-1} - 1 \in \mathbb{Z}_p[x]$.

$\bar{f} \in \mathbb{F}_p[x]$ has distinct linear factors.

Thus, $\mathbb{Z}_p$ contains $(p-1)^{\text{th}}$ roots of unity.

Proof. $\mathcal{O}[x] \longrightarrow (\mathcal{O}/\mathfrak{p})[x]$.

Let $g_0, h_0 \in \mathcal{O}[x]$ be lifts of $\bar{g}, \bar{h}$ of same deg.

$\deg g_0 = \deg \bar{g} =: m$. $\quad d := \deg f$.

$\deg h_0 = \deg \bar{h} = \deg \bar{f} - \deg \bar{g} \leq d - m$.

$f = g_0 h_0 \mod \mathfrak{p}$

$\langle \bar{g}, \bar{h} \rangle = 1$ in $\mathcal{O}/\mathfrak{p}[x]$

$\Rightarrow \bar{a}\bar{g} + \bar{b}\bar{h} = \bar{1}$ for some $\bar{a}, \bar{b} \in \mathcal{O}/\mathfrak{p}[x]$

$\Downarrow$

$a g_0 + b h_0 - 1 \in \mathfrak{p}[x]$ for some $a, b \in \mathcal{O}[x]$.

Among all nonzero coeffs of $f - g_0 h_0$ and $a g_0 + b h_0 - 1$, pick one with max val., say π.

If α is a coeff of one of those polys, then

$$|\alpha| \leq |\pi|$$

$$\Rightarrow \left|\frac{\alpha}{\pi}\right| \leq 1$$

$$\Rightarrow \frac{\alpha}{\pi} \in \mathcal{O}$$

$$\Rightarrow \alpha \in \pi\mathcal{O}.$$

$\therefore$ $f - g_0 h_0 \in \pi\mathcal{O}[x]$,

$a g_0 + b h_0 - 1 \in \pi\mathcal{O}[x]$.

Want:

$$g = g_0 + p_1\pi + p_2\pi^2 + \cdots,$$

$$h = h_0 + q_1\pi + q_2\pi^2 + \cdots,$$

$p_i, q_i \in \mathcal{O}[x]$, $\deg p_i < m$, $\deg q_i \leq d - m$

s.t. $g_n := g_0 + p_1\pi + \cdots + p_n\pi^n$,

$h_n := h_0 + q_1\pi + \cdots + q_n\pi^n$

satisfy $f - g_n h_n \in \pi^{n+1}\mathcal{O}[x]$.

$$\Rightarrow \lim_{n\to\infty}(f - g_n h_n) \in \bigcap_{n\geq 1}(\pi^n) = 0.$$

$$ \overset{\shortparallel}{f - gh}$$

Rest exercise. ☺

Cor. $(K, |\cdot|)$: complete, non Arch.

$(\mathcal{O}, \mathfrak{p})$.

$f(x) = a_0 + \cdots + a_n x^n \in K[x]$ with $a_0 a_n \neq 0$.

If f is irreducible, then

$$|f| := \max_i \{|a_i|\} = \max\{|a_0|, |a_n|\}.$$

Proof. We may $a_i \in \mathcal{O}$ $\forall i$.

If $|f| = |a_i|$ for some $0 < i < n$, then divide by a_i

so $|f| = |a_i| = 1$.

Then, $\bar{f} \neq 0 \bmod \mathfrak{p}$. ☹

Lecture 25 (04-04-2022)

04 April 2022 17:31

Theorem (Ostrowski's Theorem)

K: complete field wrt Archimedean valuation $|\cdot|_K$.
Then, $\exists$ an isomorphism $\sigma : K \to \mathbb{R}$ or $\mathbb{C}$ and $s \in (0,1]$
s.t.
$$|x|_K = |\sigma x|^s.$$

Proof As K is Archimedean, $\mathrm{char}(K) = 0$.
We have $\mathbb{Q} \subseteq K$. We had already noted all Arch. valuations on $\mathbb{Q}$. Thus,
$$|x|_K = |x|_\infty^s \quad \forall x \in \mathbb{Q}$$
for some $s \in (0,1]$.
(for $s > 1$, $|\cdot|_\infty^s$ won't be a valuation on $\mathbb{Q}$.)

We have $\mathbb{Q} \hookrightarrow K$.
We may complete $\mathbb{Q}$ w.r.t. $|\cdot|_\infty^s$ and get
$$\hat{\mathbb{Q}} \hookrightarrow K. \qquad \hat{\mathbb{Q}} \cong \mathbb{R}.$$
(We will have $|x|_K = \underbrace{|x|}_{\text{usual valuation}}{}^s$ for $x \in \mathbb{R} \subseteq K$.)

Claim: $K \cong \mathbb{R}$ or $\mathbb{C}$.

Proof We show that any $\xi \in K$ satisfies a quadratic equation over $\mathbb{R}$.
Fix $\xi \in K$.
Define $f : \mathbb{C} \to \mathbb{R}_{\geq 0}$ by
$$z \mapsto |\xi^2 - \underbrace{(z+\bar{z})}_{}\xi + \underbrace{z\bar{z}}_{}|_K.$$
these are linear

f is continuous. Moreover $\lim_{z\to\infty} f(z) = \infty$ as $|\cdot|_K$ is Arch.

Thus, f has a minimum on $\mathbb{C}$, say m.

Let $S = \{ z \in \mathbb{C} : f(z) = m \}$.

Note that S is nonempty, closed, and bounded.

$\exists z_0 \in S$ of maximum absolute value, i.e., $|z| \leq |z_0| \; \forall z \in S$.

If $m = 0$, then we are done as ξ satisfies

$$x^2 - (z_0 + \bar{z}_0) x + z_0 \bar{z}_0 \in \mathbb{R}[x].$$

Suppose $m > 0$. Pick ε s.t. $0 < \varepsilon^s < m$.

Define $g(x) = x^2 - (z_0 + \bar{z}_0) x + z_0 \bar{z}_0 + \varepsilon$.

$\hookrightarrow$ does not have real roots!

Let $z_1, \bar{z}_1 \in \mathbb{C}$ be the roots of $g(x)$.

Then, $z_1 \bar{z}_1 = z_0 \bar{z}_0 + \varepsilon$, i.e., $|z_1|^2 = |z_0|^2 + \varepsilon$.

$\therefore z_1 \notin S$.

$\Rightarrow f(z_1) > m$.

For any $n \geq 1$, define

$$\begin{aligned} G(x) &= (g(x) - \varepsilon)^n - (-\varepsilon)^n \in \mathbb{R}[x]. \\ &= (x^2 - (z_0 + \bar{z}_0) x + z_0 \bar{z}_0)^n - (-\varepsilon)^n \qquad (*) \\ &= \prod_{i=1}^{2n} (x - \alpha_i) = \prod_{i=1}^{2n} (x - \bar{\alpha}_i). \end{aligned}$$

Also, $G(z_1) = 0$. Assume $\alpha_1 = z_1$.

$$G(x)^2 = \prod_{i=1}^{2n} (x - \alpha_i)(x - \bar{\alpha}_i)$$

$$= \prod_{i=1}^{2n} \left(x^2 - (\alpha_i + \bar{\alpha}_i) x + \alpha_i \bar{\alpha}_i \right)$$

$$\Rightarrow |G(\xi)|_K^2 = \prod_{i=1}^{2n} |\xi^2 - (\alpha_i + \bar{\alpha}_i)\xi + \alpha_i \bar{\alpha}_i|_K$$

$$= \prod_{i=1}^{2n} f(\alpha_i) \geq f(\alpha_1) \cdot m^{2n-1}. \qquad \text{---} (1)$$

OTOH, $(*)$ gives

$$|G(\xi)|_K = |(\xi^2 - (z_0 + \bar{z}_0)\xi + z_0 \bar{z}_0)^n - (-\varepsilon)^n|_K$$

$$\leq |\xi^2 - (z_0+\bar{z}_0)\xi + z_0\bar{z}_0|_k^n + |-\varepsilon|_k^n$$
$$= m^n + |\varepsilon|_k^n$$
$$= m^n + \varepsilon^{ns}.$$

Thus, $|G(\xi)|_k^2 \leq (m^n + \varepsilon^{ns})^2.$ —— (2)

(1) and (2) give us
$$f(\alpha_1)\, m^{2n-1} \leq (m^n + \varepsilon^{ns})^2$$
$$\Rightarrow \frac{f(\alpha_1)}{m} \leq \left(1 + \left(\frac{\varepsilon^s}{m}\right)^n\right)^2$$

Take $n \to \infty$ to get $f(\alpha_1) \leq m.$
$$\begin{array}{c} f(\alpha_1) \\ \parallel \\ f(z_1) \end{array}$$

This is the desired contradiction. ☒

Thus, we are done. ☒

QRL: p, q odd primes. $\chi_q(p) := \left(\frac{p}{q}\right).$

Then, $\chi_q(p) = \chi_p(q) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$

Q. Let $d \in \mathbb{N}$. What are all primes p s.t. d is a quadratic residue mod p.

$Q_d = \{p \in \mathbf{P} : d$ is a quadratic residue mod $p\}.$

↳ set of positive primes

$$Q_1 = Q_4 = Q_9 = \cdots = \mathbf{P}.$$

$$Q_2 = \{p \in P : \chi_p(2) = 1\}$$
$$= \{p \in P : (-1)^{\frac{p^2-1}{8}} = 1\}$$
$$= \{p \in P : p \equiv 1, 7 \bmod 8\}.$$

$d=5$: $\chi_p(5) = \chi_5(p)\,(-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}$ ← for p odd

$= \chi_5(p)$

$= 1 \quad \text{iff} \quad p \equiv \pm 1 \ (5).$

Need to check mod 2 separately.

$$Q_5 = \{p \in P : p = \pm 1 \mod 5\} \cup \{2\}.$$

$d = 11$:

$$\chi_p(11) = \chi_{11}(p) \cdot (-1)^{5 \cdot \left(\frac{p-1}{2}\right)}$$

$$= \chi_{11}(p) \cdot (-1)^{\frac{p-1}{2}}$$

$$= \begin{cases} \chi_{11}(p) & p = 1 \ (4) \\ -\chi_{11}(p) & p = -1 \ (4) \end{cases}$$

$\chi_{11}(p) = 1 \longleftrightarrow p = 1, 4, 9, 5, 3$

$\chi_{11}(p) = -1 \longleftrightarrow p = 2, 6, 7, 8, 10$

$$\mathbb{Z}/4 \times \mathbb{Z}/11 \xrightarrow{\simeq} \mathbb{Z}/44$$

$1, \quad \{1, 3, 4, 5, 9\}$

$3, \quad \{2, 6, 7, 8, 10\}$

$(1, 1) \longmapsto 1$

$(0, 1) \longmapsto 12$

$(1, 0) \longmapsto -11 = 33$

$(1, 3) \longmapsto -11 + 36 = 25$

$(1, 4) \longmapsto 37$

$(1, 5) \longmapsto 5$

$\vdots$

This gives us 10 residue classes mod 44.

Thm. ① Let $a \in \mathbb{N}$. TFAE:

(i) $P \setminus Q_a$ is finite, i.e., a is a square modulo

all but finitely many primes.
(ii) a is a square.

② $S \subseteq \mathbb{N}$ finite.
Then, $\exists$ infinitely many primes p s.t. every element of S is a quadratic residue mod p.

③ $\Pi \subseteq P$ finite set of primes.
Let $\varepsilon : \Pi \longrightarrow \{\pm 1\}$ be any function.
Then, $\exists$ infinitely many primes p s.t.

$$\chi_p(q) = \varepsilon(q) \quad \text{for all } q \in \Pi.$$

Notation: $\Pi(a)$ = prime factors of a = $\{p \in P : p \mid a\}$.

Proof. ① (ii) $\Rightarrow$ (i) clear.
(i) $\Rightarrow$ (ii) Assume a is squarefree.
We show $a = 1$.
If $a > 1$, write $\Pi(a) = \{q_1, \dots, q_n\}$.
Define $\varepsilon : \Pi(a) \longrightarrow \{\pm 1\}$ by

$$q_1 \longmapsto -1$$
$$q_i \longmapsto +1 \quad \text{for } i \geq 2.$$

By ③, $\exists$ inf many primes p s.t.

$$\chi_p(q_i) = \begin{cases} -1, & i = 1, \\ 1, & i > 1. \end{cases}$$

$$\therefore \chi_p(a) = -1 \quad \text{for inf many primes.} \rightarrow\leftarrow$$

② Also follows if we assume ③.

③ Use Dirichlet's Theorem:

$$AP(a, b) := \{a + nb : n \geq 0\} \quad \text{for } a, b \in \mathbb{N}.$$

Then, $|AP(a, b) \cap P| = \infty \iff \gcd(a, b) = 1$.
($\Leftarrow$) is the interesting direction.

Stein's Lecture Notes: Quadratic Residues