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:
  (i) α is an algebraic integer.
  (ii) $\mathbb{Z}[\alpha]$ is f.g. as a group.
  (iii) $\exists$ a subring $A \subset \mathbb{C}$ s.t. $\alpha \in A$ and A is f.g. as a group.
  (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,

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

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

↳ Exercise, can show with machinery so far.

- $\omega = e^{2\pi i/m}$. Then, $\Theta_{\mathbb{Q}[\omega]} = \mathbb{Z}[\omega]$. → 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. $(\omega := e^{2\pi i/p})$

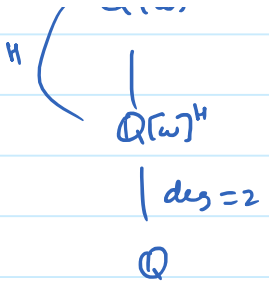
Then, $G = \mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ has order $p-1$ and is cyclic.

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

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

$\mathbb{Q}[\omega]$ / H

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



As we shall see,

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

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

Theorem. Let $n \geq 3$. $\omega := e^{2\pi i/n}$. Let $\eta \in \mathbb{Q}[\omega]$ be a root of unity. Then, $\eta^n = 1$ if n even, $\eta^{2n} = 1$ if n odd.

Proof. Suffices to prove when n even.
(n odd $\Rightarrow$ $(-\omega)$ primitive $2n^{th}$ 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 $\ell = \text{lcm}(m,n)$.
Thus, $\mathbb{Q}[\omega] \subseteq \mathbb{Q}\left[e^{2\pi i/\ell}\right] \subseteq \mathbb{Q}[\omega]$.
$\Rightarrow \varphi(m) = \varphi(\ell)$. ($\because m \mid \ell$.)
$\Rightarrow m = \ell$. ∎

Corollary. The fields $\left\{\mathbb{Q}\left[e^{2\pi i/m}\right]\right\}_{m \geq 2}$ 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 $\sigma_1, \dots, \sigma_n$ 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,

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

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

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

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

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

K | m | $\mathbb{Q}[\beta]$ | ℓ | $\mathbb{Q}$

Let $\theta_1, \ldots, \theta_\ell$ 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, $\alpha \neq 0$.

Then, $1/\alpha \in K$

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

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

They satisfy same polynomial.

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

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

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

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

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 $Tr_{L/K} : L \to K$ for number fields $K \subseteq L$.
Suppose we have extensions $K \subseteq L \subseteq M$. Then, we have

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

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

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

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

Theorem $\text{disc}(\alpha_1, \ldots, \alpha_n) = \det\left(Tr_{K/\mathbb{Q}}(\alpha_i \alpha_j)\right) \in \mathbb{Q}$.

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

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

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

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

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 $\mathbb{Q} \iff \mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0$.

Proof ($\Rightarrow$) clear. The rows in def^n 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 $\mathrm{disc} = 0$. Then, $\det \begin{pmatrix} \mathrm{Tr}(\alpha_1\alpha_1) & \cdots & \mathrm{Tr}(\alpha_1\alpha_n) \\ \vdots & & \vdots \\ \mathrm{Tr}(\alpha_n\alpha_1) & \cdots & \mathrm{Tr}(\alpha_n\alpha_n) \end{pmatrix} = 0.$

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

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

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

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 $\operatorname{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.

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,

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

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

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

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

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

$$= \det(\alpha_i^{j-1})^2$$

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

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

Vandermonde

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

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

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

$i : j \neq i$

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

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

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

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

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

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

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

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

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

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

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

(2 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 $p \equiv 1 \bmod 4$.

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

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

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

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

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

take N, note ω is unit ⇒
$$m^{\varphi(m)} \cdot (\pm 1) = N(f'(\omega)) \cdot N(g(\omega))$$

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

$$\therefore N(f'(\omega)) \mid m^{\varphi(m)}$$
$$\| \pm \operatorname{disc}(\omega)$$

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

Recall:

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

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 $\alpha_1, \ldots, \alpha_n$ of $K/\mathbb{Q}$.
Upon multiplication with appropriate (nonzero) integers, we may assume $\alpha_i \in \mathcal{O}_K$.

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

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

Theorem $K/\mathbb{Q}$ → deg n.
$\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ basis of $K/\mathbb{Q}$.
$d := \operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z} \setminus \{0\}$.
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. $\sum_{i=1}^{n} \mathbb{Z}\alpha_i \subseteq \mathcal{O}_K \subseteq \sum_{i=1}^{n} \mathbb{Z}\frac{\alpha_i}{d}$. — (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.

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

Then, $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}(\beta_1, \ldots, \beta_n)$

Thus, $\operatorname{disc}(\mathcal{O}_K) := \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ 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 $K/\mathbb{Q} \longrightarrow \deg n$.

$\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$: 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

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

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

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

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

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

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

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

By Cramer's rule,

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

$$y_j = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha) & \cdots \\ \vdots & \ddots & \vdots & \ddots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha) & \cdots \end{pmatrix} \quad (j\text{-th column})$$

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

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

$\Uparrow \qquad \Uparrow$

$\mathbb{Q} \qquad \mathbb{A}$

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

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

Then $d \mid m_j^2$ ... $\blacksquare$

Then, $d \mid m_j^2$, as desired. ∎

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.

- $m \equiv 2, 3 \ (4)$. $\{1, \sqrt{m}\}$ → 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) $\operatorname{disc}(\omega) = \prod_{i<j} (\alpha_i - \alpha_j)^2$ ($\alpha_i \to$ conjugates of ω)

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

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

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

(ii) 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 $j < i$.

Then, 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) $N_{\mathbb{Q}[1-\omega]/\mathbb{Q}}(1-\omega) = \prod_{\substack{k=1 \\ p \nmid k}}^{p} (1-\omega^k)$ ← n factors

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

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

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

→ p for all $i < n$.

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

$\rightarrow \dfrac{p}{(1-\omega)^j} \in \mathbb{Z}[\omega]$ for all $j \leq n$.

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

$p \in \mathcal{O}_K$

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

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

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

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

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

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

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

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

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

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

$\| \quad p^{+i}$

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

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

Exercise 2.27. $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$: lin. indep / $\mathbb{Q}$
$\{\alpha_1, \dots, \alpha_n\}$ is an integral basis of $\mathcal{O}_K$
$\iff \operatorname{disc}(\alpha_1, \dots, \alpha_n) = \operatorname{disc}(K)$.

Soln. ($\Rightarrow$) by def^n.
($\Leftarrow$) Let $H = \langle \alpha_1, \dots, \alpha_n \rangle$.
Then, H is free of rank n.
By earlier exercise, $\operatorname{disc}(H) = |G/H|^2 \cdot \operatorname{disc}(G)$.
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
  $KL \longrightarrow$ the compositum is also a number field.

$\mathcal{O}_K \cdot \mathcal{O}_L \subseteq \mathcal{O}_{KL}$.
Equality may not hold.

Example. $K = \mathbb{Q}[\sqrt{3}]$, $L = \mathbb{Q}[\sqrt{7}]$.
$\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$, $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$.
$\mathcal{O}_K \cdot \mathcal{O}_L = \mathbb{Z}[\sqrt{3}, \sqrt{7}]$.
$(3 \equiv 7 \equiv 1 \pmod 4)$

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

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

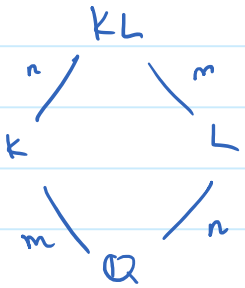
Recall: $\varphi(m) = \varphi(m_1)\varphi(m_2)$ since $\gcd(m_1, m_2) = 1$.

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

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

Thus, by theorem, we get $\mathcal{O}_{\mathbb{Q}[\omega]} = \mathbb{Z}[\omega_1] \cdot \mathbb{Z}[\omega_2] = \mathbb{Z}[\omega]$ (same proof as earlier. use that $\omega^{-1} \in \mathbb{Z}[\omega]$. ∎)

Proof of theorem



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

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

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

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

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

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

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

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

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

Suffices to prove that $r \mid d$. $\left(\because \alpha_i \in \mathcal{O}_K,\ \beta_j \in \mathcal{O}_L.\right)$

$d = \gcd(\mathrm{disc}(K), \mathrm{disc}(L))$

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

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

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 $\mathbb{C}$.)

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

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, $x_i = \frac{\gamma_i}{\delta}$ in the usual way.

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

Also, $\gamma_i, \delta \in A$. $\therefore x_i \delta^2 = \gamma_i \delta$ (with $x_i \delta^2 \in L$, $\gamma_i \delta \in A$)

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

$\because \{\beta_1, \dots, \beta_m\}$ 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 $K = \mathbb{Q}[\sqrt[3]{2}]$. $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$ → basis.

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

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

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, $\exists\, f_1(x), \dots, f_{n-1}(x) \in \mathbb{Z}[x]$ monic with $\deg(f_i) = i$ and integers $d_1, \dots, d_{n-1} \in \mathbb{Z}_{>0}$ with $d_1 \mid d_2 \mid \cdots \mid d_{n-1} \neq 0$ such that

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

Moreover, the d_i are unique.

Proof $\{1, \alpha, \dots, \alpha^{n-1}\}$: 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 $k = 1, \dots, n$.

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 $\left\{1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{k-1}(\alpha)}{d_{k-1}}\right\}$ with the desired properties.

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

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

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

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 $\beta \in R_{k+1}$.

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

$$\Downarrow$$

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

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

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

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 d_i divide the

$\llcorner \quad a_{k-1} \qquad\qquad i=1 \qquad\qquad a_{i-1} \lrcorner$

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

$$= \frac{1}{m d_{k-1}} \Big(\alpha f_{k-1}(\alpha) - \sum_{i=1}^{k} m_i' \, f_{i-1}(\alpha) \Big)$$

monic $\mathbb{Z}$-poly in α 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 $e_K t^h$, 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) $\operatorname{disc}(\alpha) = \operatorname{disc}(1, \alpha, \dots, \alpha^4)$

$= \operatorname{disc}(1, \alpha, \alpha^2, \alpha^3, f_4(\alpha))$ (f_4 is monic, use the other rows/columns of det)

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

$\vdots$

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

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

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

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

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

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

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

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

$\| \quad d_2^3 \mid \operatorname{disc}(\alpha)$, $d_3^2 \mid \operatorname{disc}(\alpha)$.

d_1^4

Chapter 3: Prime Decomposition in Number Rings.

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

(i) A is Noetherian, i.e., every ideal of A is finitely generated.

(ii) All nonzero prime ideals of A are maximal.

(iii) A is integrally closed, i.e., if $\alpha \in \operatorname{Frac}(A)$ 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. $\therefore \beta \in \mathbb{A}$.
$\therefore \beta \in \mathcal{O}_K$.
$\therefore m = \beta\alpha \in I$.
$\Rightarrow (m) \subseteq \langle \alpha \rangle$.

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

$(\mathbb{Z}/m\mathbb{Z})^n$: 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. $m\beta \in \mathcal{O}_K$.
$\therefore \mathrm{Frac}(\mathcal{O}_K) = K$.

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" on $\{$nonzero 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, $\exists\, y \in \mathrm{Frac}(R) \setminus R$ 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.)

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

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

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 $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus \langle a \rangle$.

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: $\exists J \neq 0$ ideal 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 $\to\leftarrow$.)

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

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

$$\Rightarrow yJ \subseteq R.$$

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

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

($yJ \subseteq R$)

$$\Rightarrow yJ \subseteq J$$

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

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

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

Corollary 1. Let R : Dedekind Domain.

$Cl(R) := \{$ 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, $IJ' \subseteq \langle \alpha \rangle$.

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

Check $I = J\partial$. ∎

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

$IJ = IK \Rightarrow J = K$.

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

$\Rightarrow I'IJ = I'IK$

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

$\Leftrightarrow J = K$. ∎

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 $J \trianglelefteq R$.

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

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

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

Uniqueness: $I = P_1 \cdots P_r$

$= Q_1 \cdots Q_s$.

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

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

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 PID.

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

In the usual way, decompose in primes as:

$$I = \prod_{i=1}^{r} P_i^{n_i}, \quad \langle \alpha \rangle = \prod_{i=1}^{r} P_i^{m_i} \cdot \prod_{i=1}^{s} Q_j^{t_j}.$$

$(m_i \geq n_i \geq 1)$

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

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

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

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

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

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

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

↳ T_j is not equal to any P_* or Q_*!

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

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.

Claim: α is irreducible but not prime.

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

Proof. 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. □

EXAMPLES. 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.

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

$$\left(\frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]} \cong \frac{\mathbb{Z}[x]}{\langle p, x^2+1 \rangle} \cong \frac{(\mathbb{Z}/p)[x]}{(x^2+1)} \right)$$

← field since x^2+1 is irred in $\mathbb{Z}/p$ as $p \equiv 3 \ (4)$.

$p \equiv 1 \bmod 4 \Rightarrow p = \pi\bar{\pi}$ 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, $2 = p^2$, $\langle p\rangle = P$, $\langle p\rangle = P_1P_2$.

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

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

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

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

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

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

(look at $\mathbb{Z}[\sqrt{-5}]|_{\langle 7\rangle}$.)

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 only ($\subseteq$).

$\alpha \in Q \cap K$

$\Rightarrow \alpha \in S \cap K \Rightarrow$ α is alg. and in K

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

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

EXAMPLE:

① $\mathbb{Q}(i)$ — $\mathbb{Z}[i]$ — $\langle 1+i \rangle$ — $\langle 3 \rangle$ — $\langle 2+i \rangle$ — $\langle 2-i \rangle$

$\mathbb{Q}$ — $\mathbb{Z}$ — $\langle 2 \rangle$ — $\langle 3 \rangle$ — $\langle 5 \rangle$

② $\mathbb{Q}(\sqrt{-5})$ — $\mathbb{Z}[\sqrt{-5}]$ — $\langle 2, 1+\sqrt{-5} \rangle$ — $\langle 3, 1+\sqrt{-5} \rangle$ — $\langle 3, 1-\sqrt{-5} \rangle$

$\mathbb{Q}$ — $\mathbb{Z}$ — $\langle 2 \rangle$ — $\langle 3 \rangle$

Thm. ① Every prime Q of S lies over a unique prime P of R.

② Given a prime P in R, $\exists$ a prime Q in S lying over P.

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

② If $PS \subsetneq S$, 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 $\gamma PS \subseteq S$

$\Rightarrow \gamma S \subseteq S$

$\Rightarrow \gamma \in S$.

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

Defn.

S — L

P — R — K

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

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

Then, $e(Q_i \mid P) := e_i$

$=$ ramification index of Q_i/P.

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

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

Examples: ① $\mathbb{Q}(i)$ — $\mathbb{Z}[i]$ — $\langle 1+i \rangle$ — $\langle 3 \rangle$ — $\langle 1+2i \rangle$ — $\langle 1-2i \rangle$

$$\begin{array}{ccccccc} | & | & | e=2 & | e=1 & 1 \diagdown & \diagup 1 & \\ \mathbb{Q} & \mathbb{Z} & 2 & 3 & & 5 & \end{array}$$

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 post 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 $R \hookrightarrow S \twoheadrightarrow S/Q$.

$\ker(\varphi) = R \cap Q = P$.

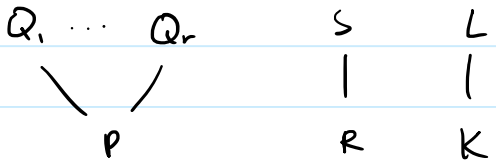
Def^n. $f(Q|P) = [S/Q : R/P]$.

= inertial degree of Q over P

Lecture 10 (03-02-2022)

03 February 2022 17:29

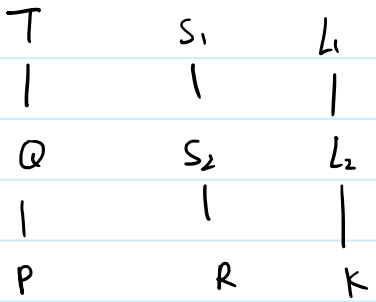
Defn.



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

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

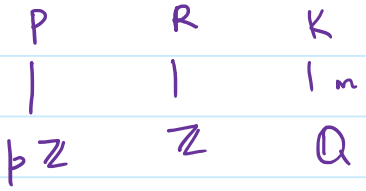
Prop^n. (Multiplicative property of e and f).



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

Proof. e : extend P to S_2 and then S_1.
f : usual field theory. ∎

EXAMPLE



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

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

Claim: $f \leq m$.

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

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

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

$\downarrow$

Cardinality p^f. $\therefore f \leq m$. ∎

Defn

R	K
$\vert$	$\vert^n$
$\mathbb{Z}$	$\mathbb{Q}$

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, $\|IJ\| = \left|R/_{IJ}\right| = |R/I| \cdot |R/J) = \|I\| \cdot \|J\|$.

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

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

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

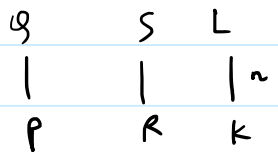
$\left(R/P \cong P^{n-1}/P^n.\right)$ Inductively, we are done. ∎

This finishes the proof. ∎

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

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

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

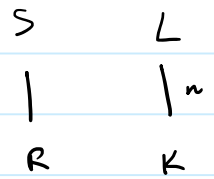


Cor. $e_i \leq n$, $f_i \leq n$ $\forall i$.

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

Then,

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



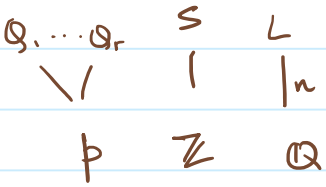
Proof ① $K = \mathbb{Q}$:

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

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

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

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



S/Q_i is a $\mathbb{Z}/p$ vec. space of dim f_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

IS: $\|PS\| = \|P\|^n$.

$\|PS\| = |S/PS|$ and $\|P\| = |R/P|$

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

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

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

Proof. Let $\bar{\alpha}_1, \ldots, \bar{\alpha}_{n+1} \in S/PS$, we wish to show that they are linearly dependent over R/P.

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

Thus, $\exists a_1, \ldots, a_{n+1} \in K$ 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, $I := \langle a_1, \ldots, a_{n+1} \rangle \subseteq P$.

$I \neq 0$

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

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

Claim: $\gamma I \notin P$.

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

End of Step 1.

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

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

$$\dim_{R/P_i}(S/P_iS) =: n_i \leq n,$$

by Step 1.

S	L
|	| n
P	R	K
|	|	| m
p	$\mathbb{Z}$	$\mathbb{Q}$

$$\|pS\| = p^{mn}$$

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

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

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

$$\prod_{i=1}^{r} \|P_i\|^{n_i e_i}$$

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

$$\prod_{i=1}^{r} p^{f_i n_i e_i}$$

Thus, $\sum f_i n_i e_i = mn.$ — (*)

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

$$\sum e_i f_i = m.$$

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

End of Step 2.

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

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

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

S	L
|	| n
P	R	K

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

P	1
R	$\mid n$
K	

TS: $n = \sum_1^r f_i e_i$.

$$\|pS\| = \prod_1^r \|Q_i\|^{e_i}$$

$\|pS\| = \|p\|^n$ (v. space blah blah...)

$\prod_{i=1}^r \|p\|^{f_i e_i}$

$\therefore n = \sum f_i e_i$ ∎

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

Then,

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

R	K
$\mid$	$\mid n$
$\mathbb{Z}$	$\mathbb{Q}$

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 $M \to M$.

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

$T = \Theta_M$	M
$\mid$	$\mid m$
R	K
$\mid$	$\mid n$
$\mathbb{Z}$	$\mathbb{Q}$

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

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

Lecture 11 (07-02-2022)

07 February 2022 17:32

Recall:

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

① $I \neq 0$ ideal of R.

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

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

② $\|IS\| = \|I\|_R^n$.

③ $0 \neq \alpha \in R$,

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

④ $0 \neq P$: prime of R.

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

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

$m = p^r$.

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

Proof.

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

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

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

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

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

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

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

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

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

$\Rightarrow r = 1, \quad e_1 = f_1 = 1. \quad \therefore \langle 1-\omega \rangle = Q_1$ espec.

Def'.

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

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

② $\alpha = 2^{1/3}$

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

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

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

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

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

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

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

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

③ $\alpha^3 = \alpha + 1$.

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

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

$23R = P Q^2$ as $\frac{\mathbb{Z}[x]}{\langle 23\rangle} = \frac{\mathbb{F}_{23}[x]}{\langle x^3-x-1\rangle} = \frac{\mathbb{F}_{23}[x]}{\langle (x-3)(x-10)^2\rangle}$.

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

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

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

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

Note: Different ramification indices!

Theorem. Assume L/K is Galois.

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

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

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

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

Then, G acts on Σ and does so transitively.

Proof. Let $Q \in \Sigma$.

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

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

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

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

$\because$ 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.

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

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x)$$
$$\in R$$
$$\equiv \begin{cases} 1 \mod Q \\ 0 \mod Q' \end{cases}$$

$\left(x \equiv 1 \mod \sigma Q \ \forall \sigma \iff \sigma(x) \equiv 1 \mod \sigma Q \ \forall \sigma \right)$

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

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, $n = \Sigma e_i f_i = ref$.

Proof.

$$\begin{array}{ccc} Q_1 \cdots Q_r & S & L \\ \backslash | / & | & | \, n. \\ P & R & K \end{array}$$

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

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 ...

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

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

$\Rightarrow f_1 = f_2$. ∎

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

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

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

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

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

(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.)

Proof. Let P : prime in R s.t. $e(P \mid p) > 1$.
$pR = P \cdot I$ 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, $p \nmid m_1$.

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

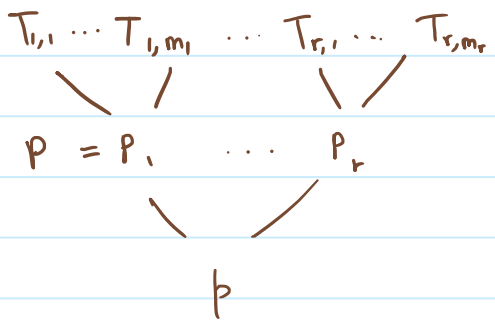
$= m_1^2 \operatorname{disc}(R)$.

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 $\mathbb{C}$.

S	L
$\vert$	$\vert$
R	K
$\vert$	$\vert n$
$\mathbb{Z}$	$\mathbb{Q}$

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



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

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

Corollary. ① $\alpha \in R$.
$f \in \mathbb{Z}[x]$ monic with $f(\alpha) = 0$.
If p is a prime such that $p \nmid N(f'(\alpha))$, then p is unramified.

R	$\mathbb{Q}(\alpha)$
$\vert$	$\vert n$
$\mathbb{Z}$	$\mathbb{Q}$

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

R	K
$\vert$	$\vert n$
$\mathbb{Z}$	$\mathbb{Q}$

③ L / n / k / $\mathbb{Q}$ 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.

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

  - $p > 2$, 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 $R = \frac{\mathbb{Z}[x]}{\langle x^2 - m \rangle}$ or $\frac{\mathbb{Z}[x]}{\langle x^2 - x - \left(\frac{m-1}{4}\right) \rangle}$ 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 $\alpha := \omega^n = \exp\left(\frac{2\pi i}{p^r}\right)$, $\beta := \omega^{p^r} = \exp\left(\frac{2\pi i}{n}\right)$.

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

↳ prime

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

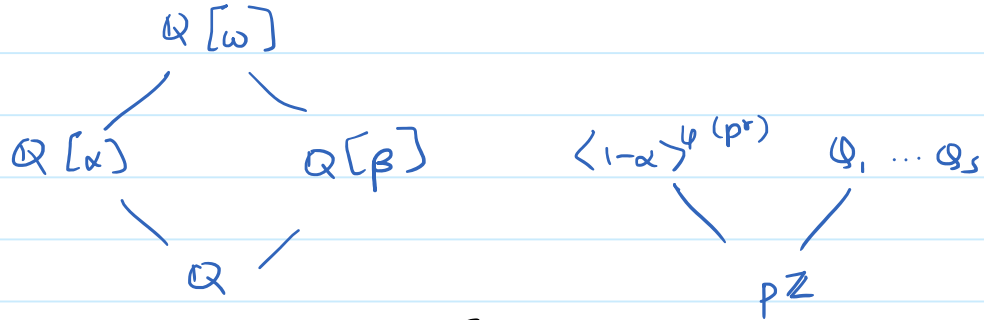
$(p, n) = 1 \Rightarrow p \nmid \operatorname{disc}(\mathbb{Z}[\beta])$.

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

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

$\mathbb{Q}[\beta]$ / $\mathbb{Q}$ Galois. Thus, $f(Q_i | p) = f$ is constant.

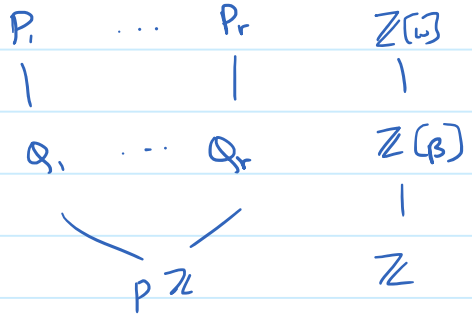
$$s = \frac{\varphi(n)}{\operatorname{ord}_n(p)}.$$



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



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

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

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

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

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

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

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

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

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

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

Thus, equality everywhere.

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

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 $s = \dfrac{\varphi(n)}{\mathrm{ord}_n(p)}$. $\square$

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

$R[\alpha] \subseteq S$.

↳ ↲ free abelian groups of rank mn

Thus, the group S/R is finite (and abelian).

S	L
1	n
R	K
1	m
$\mathbb{Z}$	$\mathbb{Q}$

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

Let $p \in \mathbb{Z}$ and take $P \in \mathrm{Spec}(R)$ over p.
Assume $p \mid |S/R[\alpha]|$. Let $g(x) = \min_{\mathbb{Q}}(\alpha) \in R[x]$.

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 $Q_i \in \mathrm{Spec}(S)$ and $|S/Q_i| = |R/P|^{\deg(\bar{g}_i)}$.
2. $Q_i + Q_j = S$ for $i \neq j$. $\to \bar{h}_i \bar{g}_i + \bar{h}_j \bar{g}_j = 1$
   ↳ lift to $R[x]$. Put $x = \alpha$. ∎
3. $PS \mid Q_1^{e_1} \cdots Q_r^{e_r}$.

Exercise ↖

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 $s = r$.