Last time:

* $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\mu_N)$, $\mu_N := \{x \in \overline{\mathbb{Q}} \mid x^N = 1\}$

↑ prim. N-th root of unity, e.g. $\zeta_N = e^{2\pi i/N}$

* $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq \mathrm{Aut}(\mu_N) \simeq (\mathbb{Z}/N)^\times$

* $(N, M) > 1 \Rightarrow \mathbb{Q}(\zeta_N) \cap \mathbb{Q}(\zeta_M) = \mathbb{Q}$

Set $\Phi_N(T) = \prod_{a \in (\mathbb{Z}/N)^\times} (T - \zeta_N^a) \in \mathbb{Z}[T]$

the N-th cyclotomic polynomial

$\Rightarrow$ $\Phi_N(T)$ (bec. $\Phi_N(\zeta_N) = 0$ and

$$[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \#(\mathbb{Z}/N)^\times = \deg \Phi_N(T))$$

$\Rightarrow$ $\Phi_N(T)$ min. poly of ζ_N

Aim: Calculate $\mathcal{O}_{\mathbb{Q}(\zeta_N)}$ and $\Delta_{\mathbb{Q}(\zeta_N)}$

Lemma: $\Delta_{\mathbb{Q}(\zeta_N)}$ divides $N^{\varphi(N)}$

Proof: $\Delta_{\mathbb{Q}(\zeta_N)} \mid \mathrm{Disc}(1, \zeta_N, \dots, \zeta_N^{\varphi(N)-1})$

/

$\mathrm{Disc}(\beta_1, \dots, \beta_n) = \mathrm{Disc}(\alpha_1, \dots, \alpha_n) \cdot \det C^2$, $(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n) \cdot C$ (Mat($\mathbb{Z}$))

Write $T^N - 1 = \Phi_N(T) \cdot F(T)$

$\Rightarrow N \cdot T^{N-1} = \Phi_N'(T) \cdot F(T) + \Phi_N(T) \cdot F'(T)$

$\Rightarrow N_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(\Phi_N'(\zeta_N)) \,\Big|\, N_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(N \cdot \zeta_N^{N-1}) = \pm N^{\varphi(N)}$

$\pm \mathrm{Disc}(1, \zeta_N, \dots, \zeta_N^{\varphi(N)-1})$ as $N_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(\zeta_N) = \pm 1$ ◻

Remark: We used $N_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(\zeta_N) = \pm 1$

More gen, $K/\mathbb{Q}$ number field

$\Rightarrow \mathcal{O}_K^\times = \{x \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(x) \in \mathbb{Z}^\times = \{\pm 1\}\}$

Namely, "$\subseteq$" ✓ $N_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$ ($x \cdot y = 1 \Rightarrow N(x) \cdot N(y) = 1$)

"$\supseteq$" $\pm 1 = N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x)$ ◻

(all lie in $\mathcal{O}_K$)

Corollary: p prime, $n \geq 1$, then

$$\mathcal{O}_{\mathbb{Q}(\zeta_{p^n})} = \mathbb{Z}[\zeta_{p^n}]$$

Proof: $\Phi_{p^n}(T+1)$ is Eisenstein at p ($\Rightarrow$ can use prop. from last time)

Included, $\Phi_{p^n}(T+1) \equiv T^{\varphi(p^n)} \mod p$ ($\zeta_{p^n} \equiv 1 \mod p$ as $\mathbb{F}_p$ has no non-trivial p^n-roots of p)

$$(T+1)^{p^n} - 1 = \Phi_N(T+1)\underbrace{\left((T+1)^{p^{n-1}} - 1\right)}$$

$(T+1)^{p^n} - 1$ = $p^n \cdot T + \ldots$

$\underbrace{\left((T+1)^{p^{n-1}} - 1\right)}$ = $p^{n-1} \cdot T + \ldots$

$\Rightarrow \Phi_{p^n}(1) = p$

~~$\Phi_{p^n}(T+1) = \Phi_{p^n}(T)$~~

$\Rightarrow$ $T^{p^n} - 1 = \Phi_{p^n}(T) \cdot (T^{p^{n-1}} - 1)$

Prop: K, L number fields, s.t. $K \cdot L = K \otimes_{\mathbb{Q}} L$

(Tian: $K \cap L = \mathbb{Q}$ ~~wrong~~)

Set $d := \gcd(\Delta_K, \Delta_L)$

Then $\mathcal{O}_{K \cdot L} \subseteq \frac{1}{d} \mathcal{O}_K \cdot \mathcal{O}_L$

Here: $\mathcal{O}_K \cdot \mathcal{O}_L = \langle x \cdot y \mid x \in \mathcal{O}_K, y \in \mathcal{O}_L \rangle_{\mathbb{Z}} \subseteq \mathcal{O}_{K \cdot L}$

Proof: $(\alpha_1, \ldots, \alpha_n)$ int. basis of K, $(\beta_1, \ldots, \beta_m)$ of L

Let $x \in \mathcal{O}_{K \cdot L}$, and write

$$x = \sum_{i,j} \frac{x_{ij}}{r} \alpha_i \beta_j \quad , x_{ij}, r \in \mathbb{Z}$$

~~We may assume~~ $\gcd(x_{11}, \ldots, x_{nm}, r) = 1$

Show $\mathcal{O}_{K \cdot L} \subseteq \frac{1}{\Delta_K} \mathcal{O}_K \cdot \mathcal{O}_L$ (=) Claim by symmetry

$$\frac{1}{\Delta_K}\mathcal{O}_K\cdot\mathcal{O}_L \cap \frac{1}{\Delta_L}\mathcal{O}_K\cdot\mathcal{O}_L = \frac{1}{d}\mathcal{O}_K\cdot\mathcal{O}_L \quad)$$

Even ~~$\nmid \Delta_K$~~

Let $(\alpha_1^\vee,\dots,\alpha_n^\vee)$ be dual basis for $(\alpha_1,\dots,\alpha_n)$ under $\mathrm{Tr}_{K/\mathbb{Q}}$

$$\Rightarrow \mathrm{Tr}_{L\cdot K/L}(x\cdot\alpha_i^\vee) = \sum_{k,\ell}\frac{x_{k,\ell}}{r}\mathrm{Tr}_{L\cdot K/L}(\alpha_k\cdot\beta_\ell\cdot\alpha_i^\vee)$$

$$= \sum_{k,\ell}\frac{x_{k,\ell}}{r}\cdot\beta_\ell\cdot\underbrace{\mathrm{Tr}_{L\cdot K/L}(\alpha_k\cdot\alpha_i^\vee)}_{=\mathrm{Tr}_{K\otimes_{\mathbb{Q}}L/L}(\alpha_k\cdot\alpha_i^\vee)}$$

V K-vs., fin. dim
$f: V\to V$, L/K field ext.
$\Rightarrow \mathrm{Tr}_K(f) = \mathrm{Tr}_L(f\otimes_K L)$,
$f\otimes_K L: V\otimes_K L \to V\otimes_K L$

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_k\alpha_i^\vee) = \delta_{ik}$$

$$= \sum_{\ell}\frac{x_{i,\ell}}{r}\cdot\beta_\ell$$

$(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j}$

Now, $\alpha_i^\vee \in \frac{1}{\Delta_K}\mathcal{O}_K$ (by def. of Δ_K) ($\mathcal{O}_K \subseteq \mathcal{O}_K^\vee = \{y \mid \mathrm{Tr}(x\cdot y)\in\mathbb{Z}\ \forall x\in\mathcal{O}_K\}$
$\Rightarrow x\cdot\alpha_i^\vee \in \frac{1}{\Delta_K}\cdot\mathcal{O}_{K\cdot L}$ $\quad [\mathcal{O}_K^\vee:\mathcal{O}_K] = |\det(\ )| = |\Delta_K|$

$\Rightarrow \mathrm{Tr}_{L\cdot K/L}(x\cdot\alpha_i^\vee) \in \frac{1}{\Delta_K}\mathcal{O}_L$ (as $\mathrm{Tr}_{K\cdot L/L}(\mathcal{O}_{K\cdot L})\subseteq\mathcal{O}_L$)

$(\beta_1,\dots,\beta_m)$ $\mathbb{Z}$-basis of $\mathcal{O}_L$ $\Rightarrow \frac{x_{i,\ell}}{r}\in\frac{1}{\Delta_K}\cdot\mathbb{Z}$ $\forall i,\ell$ □
$(\leadsto \langle\beta_1,\dots,\beta_m\rangle_{\mathbb{Z}} = \mathcal{O}_L$

~~$\nmid \Delta_K$~~

Remark: The assumption $L \cdot K \cong K \otimes_{\mathbb{Q}} L$ is satisfied if

1) $L \cap K = \mathbb{Q}$, and one of $K/\mathbb{Q}$ or $L/\mathbb{Q}$ galois

2) $[L \cdot K : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$

Corollary: Assume that $L \cdot K = K \otimes_{\mathbb{Q}} L$ and $\gcd(\Delta_K, \Delta_L) = 1$

Then 1) $\mathcal{O}_{K \cdot L} = \mathcal{O}_K \cdot \mathcal{O}_L$

& 2) $\Delta_{K \cdot L} = \Delta_K^{[L:\mathbb{Q}]} \cdot \Delta_L^{[K:\mathbb{Q}]}$

(2) Exercise)

Thm: $\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathbb{Z}[\zeta_N]$

Proof: Ind. on the # of prime factors of N (using $\mathbb{Z}[\zeta_N] \cdot \mathbb{Z}[\zeta_M] = \mathbb{Z}[\zeta_{N \cdot M}]$ if $(N, M) = 1$)

Prop: $\Delta_{\mathbb{Q}(\zeta_{p^n})} = \pm p^{p^{n-1}(pn-n-1)}$

with "$-$" if $p \equiv 3(4)$ or $p^n = 4$ ($\rightsquigarrow p=2, n=2$)
"$+$" otherwise

Proof: If $p^n \geq 3 \Rightarrow r_1 = 0$

$\Rightarrow$ sign of $\Delta_K = (-1)^{r_2} = (-1)^{\frac{(p-1)\cdot p^{n-1}}{2}}$

Compute

$$|\Delta_K| = |\mathrm{Disc}(1, \zeta_{p^n}, \dots, \zeta_{p^n}^{\varphi(p^n)-1})|$$

$$= |N_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}(\Phi'_{p^n}(\zeta_{p^n}))|$$

~~[illegible]~~ with

$$\Phi_{p^n}(T) = \frac{T^{p^n}-1}{T^{p^{n-1}}-1} = \sum_{i=0}^{p-1} T^{p^{n-1}\cdot i}$$

$$\Rightarrow \Phi'_{p^n}(\zeta_{p^n}) = \sum_{i=1}^{p-1} p^{n-1}\cdot i \cdot \zeta_{p^n}^{p^{n-1}\cdot i - 1}$$

$$= p^{n-1} \cdot \zeta_{p^n}^{p^{n-1}-1} \cdot \sum_{i=1}^{p-1} i \, (\underbrace{\zeta_{p^n}^{p^{n-1}}}_{\text{prim. } p\text{-th root of unity}})^{i-1}$$

$$\Phi_p'(\zeta_p) \cdot \zeta_p = \zeta_{p^n}^{p^{n-1}}$$

$$\Phi_p'(\zeta_p) = \prod_{i=2}^{p-1} (\zeta_p - \zeta_p^i) = \zeta_p^{p-2} \cdot \prod_{i=1}^{p-2} (1 - \zeta_p^i)$$

$$\Rightarrow \left| N_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} (\Phi_{p^n}'(\zeta_{p^n})) \right|$$

$$= p^{p^{n-1}\cdot(p-1)(n-1)} \cdot \underbrace{\prod_{i=1}^{p-2} N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} (1-\zeta_p^i)}$$

$$= (*) \qquad = \left| N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} (1-\zeta_p^i) \right|^{p^{n-1}}$$

$$\| \; p^{p^{n-1}}$$

($\Phi_p(T+1)$ Eisenstein at p
$\Rightarrow$ min. Pol. of $\zeta_p^i - 1$, $i = 1, \dots, p-2$)

$$\Rightarrow (*)$$

$$= p^{\left(p^{n-1}\cdot(p-1)(n-1)+(p-2)\cdot(p^{n-1})\right.}$$

$$= p^{p^{n-1}\underbrace{(pn-n-p+1+p-2)}_{pn-n-1}}$$

□

2.2. Dedekind domains

Definition: An integral domain A is called a Dedekind domain if A is noetherian, integrally closed, and every non-zero prime ideal is maximal

Examples: 1) PID $\Rightarrow$ Dedekind domain, e.g. $\mathbb{Z}$, $k[T]$ (k field)
$\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$

2) $K/\mathbb{Q}$ number field $\Rightarrow$ $\mathcal{O}_K$ Dedekind domain

(noetherian ✓ $\mathrm{rk}_{\mathbb{Z}} \mathcal{O}_K < \infty$

int. closed ✓

$\mathfrak{p} \subseteq \mathcal{O}_K$ prime $\Rightarrow$ $\mathfrak{p} \cap \mathbb{Z} \subseteq \mathbb{Z}$ prime

If $\mathfrak{p} \cap \mathbb{Z} = \{0\} \Rightarrow \mathcal{O}_{K,\mathfrak{p}} \supseteq \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} = K$

Otherwise, $\mathfrak{p} \neq \cap \mathbb{Z} = (p)$, $p \subseteq \mathbb{Z}$ prime

But in $\mathcal{O}_{K/(p)}$ each prime ideal is maximal (as $\dim_{\mathbb{F}_p} \mathcal{O}_{K/(p)}$ is finite + chinese reminder theorem)

3) A Dedekind, S mult.

$\Rightarrow$ $S^{-1}A$ Dedekind (Exercise)

(e.g. $\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} \mid p \nmid n\}$)

4) $\mathbb{Z}[x]$ not Dedekind,

$\{0\} \subsetneq (x) \subsetneq (p, x)$ prime ideals