Last time: $K/\mathbb{Q}$, $n := [K:\mathbb{Q}]$ ①

* $\alpha_1, \dots, \alpha_n \in K$ basis

$$\Rightarrow \mathrm{Disc}(\alpha_1,\dots,\alpha_n) := \det\big(\underbrace{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)}_{\text{non-deg.}}\big)$$

"discriminant of $\alpha_1, \dots, \alpha_n$"

* If $\langle \alpha_1, \dots, \alpha_n \rangle_{\mathbb{Z}} = \mathcal{O}_K$ ($\mathcal{O}_K$ free over $\mathbb{Z}$ of rank $n$)

$\Rightarrow \Delta_K := \mathrm{Disc}(\alpha_1,\dots,\alpha_n)$ ~ independent of choice of $\alpha_1, \dots, \alpha_n$

Namely, $(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n) \cdot C$, $C \in \mathrm{Mat}_{n\times n}(\mathbb{Q})$

$$\Rightarrow \mathrm{Disc}(\beta_1,\dots,\beta_n) = \mathrm{Disc}(\alpha_1,\dots,\alpha_n) \cdot \underbrace{\det C^2}_{\substack{=1 \text{ if} \\ \langle \beta_1,\dots,\beta_n\rangle_{\mathbb{Z}} = \mathcal{O}_K}}$$

* Why $\Delta_K$? $\Delta_K$ is a way to measure "complexity" of $K$ (more later)

Will prove: If $|\Delta_K| = 1 \Rightarrow K = \mathbb{Q}$.

* $n = 2$, $K = \mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}$ squarefree

$$\Rightarrow \Delta_K = \begin{cases} D, & D \equiv 1 \ (4) \\ 4D, & D \equiv 2,3 \ (4) \end{cases}$$

* $K = \mathbb{Q}(\alpha)$, $f$ = min. Poly of $\alpha$

$\Rightarrow \mathrm{Disc}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n\cdot(n-1)}{2}} \cdot N_{K/\mathbb{Q}}(f'(\alpha))$

Lemma: $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$, basis of $K$ over $\mathbb{Q}$.

Then:

$(\beta_1, \ldots, \beta_n)$ is not an integral basis

$\Leftrightarrow$ ex. prime $p$ with $p^2 \mid \mathrm{Disc}(\beta_1, \ldots, \beta_n)$

and $x_i \in \{0, \ldots, p-1\}$ for $i = 1, \ldots, n$, s.t.

not all of $x_i$ are zero and $\sum x_i \beta_i \in p\mathcal{O}_K$

$\Leftrightarrow$ ex. prime $p$ with $p^2 \mid \mathrm{Disc}(\beta_1, \ldots, \beta_n)$

and the residue classes $\bar{\beta}_1, \ldots, \bar{\beta}_n \in \mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p^n$

are linearly dependent over $\mathbb{F}_p$

Proof: Second "$\Leftrightarrow$" ✓

"$\Leftarrow$" ✓ as each $\mathbb{Z}$-basis of $\mathcal{O}_K$ reduces

to an $\mathbb{F}_p$-basis of $\mathcal{O}_K/p\mathcal{O}_K$

"$\Rightarrow$" Choose some integral basis $(\alpha_1, \ldots, \alpha_n)$

Then ex. $C \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$ with

$(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n) \cdot C$

$(\beta_1, \ldots, \beta_n)$ int. basis iff $\det C = \pm 1$

$\Rightarrow$ exists prime $p \mid \det C$

$\Rightarrow$ $p^2 \mid \mathrm{Disc}(\beta_1,\dots,\beta_n) = \det C^2 \cdot \overbrace{\mathrm{Disc}(\alpha_1,\dots,\alpha_n)}^{\Delta_K}$

& $\bar{\beta}_1,\dots,\bar{\beta}_n \in \mathcal{O}_K/p\mathcal{O}_K$ are not linearly independent as $\bar{C}$ is not invertible $\square$

Proposition: $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$, and $f(T) \in \mathbb{Z}[T]$ its min. polynomial. Assume that for each prime $p$ with $p^2 \mid \mathrm{Disc}(1,\alpha,\dots,\alpha^{n-1})$, there exists some integer $i \in \mathbb{Z}$ (depending on $p$), such that $f(T+i)$ is an Eisenstein polynomial for $p$.

Then $\mathcal{O}_K \subset \mathbb{Z}[\alpha]$

Recall: $f(T) = T^n + a_1 \cdot T^{n-1} + \dots + a_n$ is called Eisenstein at $p$ if $p \mid a_i$ for $1 \le i \le n$ and $p^2 \nmid a_n$.

Proof: Note $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha - i]$ for $i \in \mathbb{Z}$.
Replacing $\alpha$ by $\alpha - i$ and using prev. Le
it suffices to see:

If $f(T) = T^n + a_1 T^{n-1} + \dots + a_n$ is Eisenstein for $p$, then for all $x_i \in \{0, \dots, p-1\}$, not all zero,

$$x = \frac{1}{p} \sum_{i=0}^{n-1} x_i \alpha^i \notin \mathcal{O}_K$$

Set $j = \min\{i \mid x_i \neq 0\}$. Then

$$N_{K/\mathbb{Q}}(x) = \underbrace{\frac{1}{p^n} \cdot N_{K/\mathbb{Q}}(\alpha)^j}_{} \cdot N_{K/\mathbb{Q}}\Big(\sum_{i=j}^{n-1} x_i \alpha^{i-j}\Big)$$

$$= \frac{(-1)^n \cdot a_n^j}{p^n} \in \mathbb{Q} \setminus \mathbb{Z}, \text{ as } p^2 \nmid a_n$$

Claim: $N_{K/\mathbb{Q}}\Big(\sum_{i=j}^{n-1} x_i \alpha^{i-j}\Big) \equiv \underset{\not\equiv 0}{x_j^n} \ (p)$

$(\leadsto N_{K/\mathbb{Q}}(x) \in \mathbb{Q} \setminus \mathbb{Z}$, i.e. $x \notin \mathcal{O}_K)$

Prf of claim: $\{\sigma_1, \dots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \mathbb{C})$

$$\Rightarrow N_{K/\mathbb{Q}}\Big(\sum_{i=j}^{n-1} x_i \alpha^{i-j}\Big) = \prod_{k=1}^{n} \big(x_j + x_{j+1} \sigma_k(\alpha)^{i-j} + \dots + x_{n-1} \cdot \sigma_k(\alpha)^{n-1-j}$$

Consider the polynomial

$$\prod_{k=1}^{n}\left(y_j + y_{j+1}\cdot\tilde{\sigma}_k^{i-j} + \dots + y_{n-1}\cdot\tilde{\sigma}_k^{n-1-j}\right)$$

$$\in \mathbb{Z}[y_j,\dots,y_{n-1},\tilde{\sigma}_1,\dots,\tilde{\sigma}_n]$$

It is invariant under permutations of the $\sigma_1,\dots,\sigma_n$

$\Rightarrow$ each monomial of $y_j,\dots,y_{n-1}$ has a coefficient which is a polynomial of the symmetric polynomials in the $\tilde{\sigma}_j$ and except for $y_j^n$ the coeff. has no constant term (set $\tilde{\sigma}_1,\dots,\tilde{\sigma}_n$ to 0)

Set $y_j = x_j$, $\tilde{\sigma}_k = \sigma_k(\alpha)$

$\Rightarrow$ coeff. of mon. ~~[illegible]~~ in $x_j$ are polynomials in the $a_i$

$$\Rightarrow \prod_{k=1}^{n}(x_j + \dots) \equiv x_j^n \ (p)$$

$\square$

Example: 1) $K=\mathbb{Q}(\alpha)$, $\alpha^3=2$

$f(T)=T^3-2$
$f'(T)=3\cdot T^2$

$$\Rightarrow \mathrm{Disc}(1,\alpha,\alpha^2) = (-1)^{\frac{n\cdot(n-1)}{2}}\cdot N_{K/\mathbb{Q}}(3\cdot\alpha^2)$$

$$= + 3^3\cdot 2^2$$

$\Rightarrow$ critical primes $2, 3$

$p = 2 \to f(T) = T^3 - 2$ Eisenstein at 2

$p = 3 \Rightarrow f(T-1) = T^3 - 3T^2 + 3T - 3$

Eisenstein at 3

$\Rightarrow \mathcal{O}_K = \mathbb{Z}[\alpha]$

2) $K = \mathbb{Q}(\alpha)$, $\alpha^3 - \alpha - 1 = 0$ Disc$(1, \alpha, \alpha^2)$ squarefree

$\Rightarrow \operatorname{Disc}(1, \alpha, \alpha^2) = -23 \overset{\&}{\Rightarrow} \mathcal{O}_K = \mathbb{Z}[\alpha]$

$\qquad\qquad\qquad\qquad\qquad\qquad \parallel$

$\qquad\qquad\qquad = \det(\operatorname{Tr}_{K/\mathbb{Q}}(\alpha^i \alpha^j))$

Indeed,

$\operatorname{Tr}(1) = 3$

$\operatorname{Tr}(\alpha) = 0$

$\operatorname{Tr}(\alpha^2) = 2$ (Use that $\alpha^2$ is repr. by matrix $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ in basis $1, \alpha, \alpha^2$ bec. $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$ )

$\operatorname{Tr}(\alpha^3)$

$\parallel$

$\operatorname{Tr}(\alpha + 1) = 3$

$\operatorname{Tr}(\alpha^4) = \operatorname{Tr}(\alpha^2 + \alpha) = 2$

Now,

$$\operatorname{Disc}(1, \alpha, \alpha^2) = \det\begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix} = 3 \cdot (-5) + 2 \cdot (-4) = -23$$

⚠ Not all $\mathcal{O}_K$ can be gen. by one element, e.g. $K = \mathbb{Q}(\sqrt{17}, \sqrt{10})$
(Exercise)

Recall $\pm a_i$ = symmetric polynomials in $\theta_k(\alpha)$

$$f(T) = T^n + a_1 T^{n-1} + \dots + a_n = \prod_{k=1}^{n} (T - \theta_k(\alpha))$$

~~If~~ $b$ = monomial in the $x_j, \dots, x_{n-1}$

Know: $\mathbb{Z}[\tilde{\theta}_1, \dots, \tilde{\theta}_n]^{S_n}$

$\Rightarrow$ coeff. in $b$ is symmetric polynomial in the $a_i$ $(a_0 = 1)$

$b = y_j^n$

Last time:
$\mathcal{O}_K$ free of rank $n$ over $\mathbb{Z}$

$\Rightarrow$ ex. $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ over $\mathbb{Z}$.

Claim: $\alpha_1, \dots, \alpha_n \in K$ basis of $K$ over $\mathbb{Q}$

Proof: ~~$\mathrm{Frac}(\mathcal{O}_K) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K = K$~~

Suffices to see that $\alpha_1, \dots, \alpha_n$ are l. ind. over $\mathbb{Q}$ ✓

Def: 1) $\sigma: K \hookrightarrow \mathbb{C}$ is called a real embedding if $\sigma(K) \subseteq \mathbb{R}$

$r_1 := \# \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$ number of real embeddings

2) $\sigma: K \hookrightarrow \mathbb{C}$ is called a complex embedding if $\sigma(K) \nsubseteq \mathbb{R}$

(note $\bar{\sigma}: K \hookrightarrow \mathbb{C}, x \mapsto \overline{\sigma(x)}$ cpl. conj. is another, distinct complex embedding)

$$r_2 := \frac{\# \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) - \# \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})}{2}$$

= number of pairs of complex conj. complex embeddings

Note: $n = r_1 + 2 \cdot r_2 \quad (n = \# \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}))$

Proposition: $\Delta_K$ has sign $(-1)^{r_2}$

(note that the sign of $\Delta_K$ can be read of from $\underbrace{\text{any}}_{\mathrm{Disc}(\alpha_1, \dots, \alpha_n) \text{ for}}$ $\mathbb{Q}$-basis $\alpha_1, \dots, \alpha_n$ of $K$)

Proof: $\{ \underbrace{\sigma_1, \dots, \sigma_{r_1}}_{\text{real emb}}, \sigma_{r_1+1}, \underset{\bar{\sigma}_{r_1+1}}{\overset{\shortparallel}{\sigma_{r_1+2}}}, \dots\dots, \underset{\bar{\sigma}_{r_1+2r_2-1}}{\overset{\shortparallel}{\sigma_{r_1+2r_2}}} \}$

$= \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \mathbb{C})$

$\alpha_1, \dots, \alpha_n$ integral basis of $K$

Recall $\Delta_K = \det(\sigma_i(\alpha_j))^2$

Now, $\overline{\det(\sigma_i(\alpha_j))} = (-1)^{r_2} \cdot \det(\sigma_i(\alpha_j))$

by numb. of $\sigma_i$'s

$\Rightarrow \Delta_K = \underbrace{\det(\sigma_i(\alpha_j))\overline{\det(\sigma_i(\alpha_j))}}_{>0} \cdot (-1)^{r_2} \Rightarrow$ Claim. $\square$

## 1.4. Cyclotomic fields

$N \geq 1$, set $\zeta_N \in \mathbb{C}$ prim. $N$-th. root of unity, e.g.

$$\zeta_N = e^{2\pi i/N}$$

$\mathbb{Q}(\zeta_N) = N$-th. cyclotomic field

More canonically, $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\mu_N)$, where

$$\mu_N = \{x \in \overline{\mathbb{Q}} \mid X^N = 1\}$$

($\rightsquigarrow \mathbb{Q}(\zeta_N)$ Galois over $\mathbb{Q}$)

Why consider these?

* Accessible class of examples
* $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong \mathrm{Aut}(\mu_N) \cong (\mathbb{Z}/N)^\times$ canonically

$\Rightarrow \mathbb{Q}(\zeta_N)/\mathbb{Q}$ abelian ext. of $\mathbb{Q}$

* Kronecker-Weber: $K/\mathbb{Q}$ abel. ext. $\Rightarrow \exists N \geq 1$, s.t. $K \subseteq \mathbb{Q}(\zeta_N)/\mathbb{Q}$
(not to be proved in this lecture)

* Concretely ($n=2$), $K/\mathbb{Q}$ quadratic $\Rightarrow \exists N \geq 1$, s.t. $K \subseteq \mathbb{Q}(\zeta_N)/\mathbb{Q}$

$\rightsquigarrow$ arithmetic consequences for $K$, (like Gauss reciprocity law)

Proposition: $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong \mathrm{Aut}(\mu_N) \cong (\mathbb{Z}/N)^*$

Proof: Clear: $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ acts on $\mu_N \subseteq \mathbb{Q}(\mu_N)$

$\Rightarrow$ Get hom. $\psi: \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \to \mathrm{Aut}(\mu_N) \underset{\uparrow}{\cong} (\mathbb{Z}/N)^*$

canonically (induced $\mathbb{Z} \to \mathrm{End}(\mu_N)$)

$\psi$ inj. as $\mu_N$ gen. $\mathbb{Q}(\mu_N)$

Let $d \in \mathbb{Z}$ with $(d, N) = 1$

Write $d = p_1 \cdot \ldots \cdot p_k$ with $p_i$ prime

$\Rightarrow (p_i, N) = 1$

Suff. to show: If $p$ prime with $(p, N) = 1$, then $p \in (\mathbb{Z}/N)^*$ is in image of $\psi$, i.e. $\zeta_N^p$ Galois conj. to $\zeta_N$

Let $f(T)$ min poly of $\zeta_N$. Write

$$T^N - 1 = f(T) \cdot g(T) \quad , g(T) \in \mathbb{Z}[T]$$

Assume $\zeta_N^p$ not conj. to $\zeta_N \Rightarrow g(\zeta_N^p) = 0$

$\Rightarrow f(T) \mid g(T^p)$. Set $\bar{f}, \bar{g} \in \mathbb{F}_p[T]$ as the reductions of $f, g$.

$\Rightarrow \bar{f}(T) \mid \bar{g}(T^p) \underset{\text{Frob.}}{=} \bar{g}(T)^p$. Let $\alpha \in \bar{\mathbb{F}}_p$ be a root of $\bar{f}$

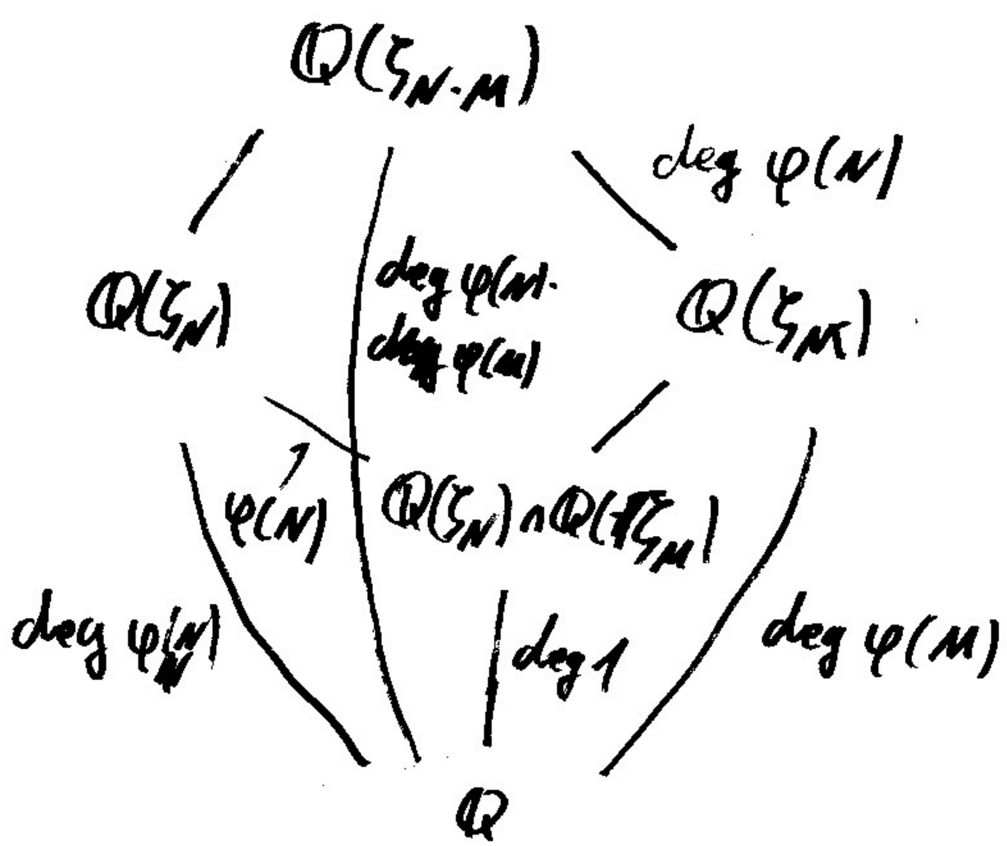
$\Rightarrow T - \alpha \mid \bar{g}(T) \quad \Rightarrow (T-\alpha)^2 \mid \bar{f}(T) \cdot \bar{g}(T) = \underline{\underline{T^N - 1}}$

But $T^N - 1 \in \mathbb{F}_p[T]$ is sep. as its deri. is $N \cdot T^{N-1}$ and $(p, N) = 1$ $\square$

Corollary: $N, M \geq 2$ integers with $\gcd(N, M) = 1$.

Then $\mathbb{Q}(\zeta_N) \cap \mathbb{Q}(\zeta_M) = \mathbb{Q}$

Proof: Set $\varphi(M) = (\mathbb{Z}/_{M\mathbb{Z}})^\times$




$N, M$ coprime $\Rightarrow \varphi(N\cdot M) = \varphi(N)\cdot\varphi(M)$

$G \supseteq H, N$

$\Rightarrow H\cdot N/N \cong H/H\cap N$

For fields

$\Rightarrow$ ~~K/k~~ let $L, M$ two sep. ext. of $K$

$\Rightarrow [L\cdot M : L] = [M : L\cap M]$

Next aim: $\mathcal{O}_{\mathbb{Q}(\zeta_N)}$, $\Delta_{\mathbb{Q}(\zeta_N)}$

Why $K := \mathbb{F}_p(T) \subseteq \mathbb{F}_p(T^{\frac{1}{p}}) =: L$ insep. $\quad L[X] \ni f(X) = X^p - T$

$\alpha = T^{\frac{1}{p}} \Rightarrow f(X) = X^p - T \in K[X] = (X - T^{\frac{1}{p}})^p$

$p\cdot X^{p-1} = 0 \in K[X]$