16. Cyclotomic fields

$K = \mathbb{Q}(\mu)$, μ - prim. p^r-th root of unity, p - prime

Recall: 1) the min. poly of μ is

$$F = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}, \quad \deg F = p^{r-1}(p-1) = e$$

2) $Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times$

3) p is totally ramified in K.

Also recall, that for arbitrary number field a prime number q ramifies in this field, if and only if q divides the discriminant.

We have: $\mathbb{Z}[\mu] \subset \mathcal{O}_K$ a sublattice with basis $1, \mu, \dots, \mu^{e-1}$

$$D(1, \mu, \dots, \mu^{e-1}) = \left(\det(\sigma_i \mu^j)\right)^2, \text{ where}$$

see Thm. 4.5 in lecture 3 $\qquad$ $\sigma_i : K \hookrightarrow \mathbb{C}$ embeddings

Denote $\sigma_i(\mu) = \mu_i$; then $\mu_1 \dots \mu_e$ are all primitive p^2-th roots of unity in $\mathbb{C}$

We compute:

$$\det\begin{pmatrix} 1 & \mu_1 & \mu_1^2 & \cdots & \mu_1^{e-1} \\ 1 & \mu_2 & \mu_2^2 & \cdots & \mu_2^{e-1} \\ \vdots & & & & \\ 1 & \mu_e & \mu_e^2 & \cdots & \mu_e^{e-1} \end{pmatrix}$$

Vandermonde determinant

$$= \prod_{i<j} (\mu_j - \mu_i)$$

$$|D(1, \mu, \ldots, \mu^{e-1})| = \prod_{i<j} |\mu_j - \mu_i|^2 = \prod_{i \neq j} |\mu_i - \mu_j|$$

Note: $F = \prod_{i=1}^{e} (X - \mu_i)$ in $K[x]$

$$\Rightarrow F' = \sum_{i=1}^{e} \prod_{j: j\neq i} (X - \mu_j)$$

$$\Rightarrow F'(\mu_1) = \prod_{j: j \neq 1} (\mu_1 - \mu_j), \quad F'(\mu_2) = \prod_{j: j\neq 2} (\mu_2 - \mu_j) \ldots$$

$$\Rightarrow |D(1, \mu, \ldots, \mu^{e-1})| = \prod_{i=1}^{e} |F'(\mu_i)| =$$

$$= |N_{K/\mathbb{Q}}(F'(\mu))|$$

Since $F = \frac{X^{p^2} - 1}{X^{p^{2-1}} - 1} \Rightarrow X^{p^2} - 1 = F \cdot (X^{p^{2-1}} - 1)$

$$\Rightarrow p^2 X^{p^2 - 1} = F' \cdot (X^{p^{2-1}} - 1) + F \cdot p^{2-1} X^{p^{2-1} - 1}$$

$$\Rightarrow p^2 \underbrace{\mu^{p^2 - 1}}_{\mu^{-1}} = F'(\mu) \cdot (\mu^{p^{2-1}} - 1)$$

denote: $\zeta = \mu^{p^{2-1}}$ is a primitive p-th root of unity

$$F'(\mu) = \frac{p^r}{\mu\cdot(\zeta-1)}$$; $|N_{K/\mathbb{Q}}(\mu)| = 1$, because all Gal-conj. of μ have abs. val. 1.

$$|N_{K/\mathbb{Q}}(\zeta-1)| = |N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta-1)|^{[K:\mathbb{Q}(\zeta)]} = p^{p^{r-1}}$$

$$\Rightarrow |N_{K/\mathbb{Q}}(F'(\mu))| = \frac{p^{re}}{p^{p^{r-1}}} = p^{rp^{r-1}(p-1)-p^{r-1}}$$

$\Rightarrow D(1,\mu\ldots\mu^{e-1})$ is a power of p.

Since $D(1,\mu,\ldots,\mu^{e-1}) \overset{\text{Lemma 15.1}}{=} a^2 d_K$ for some integer a

$\Rightarrow d_K$ is also a power of p.

<u>Conclusion</u>: the only prime that ramifies in K is p.

<u>Ring of integers of $K=\mathbb{Q}(\mu)$</u>

<u>Lemma 16.1</u> K – arbitrary number field. Let $R\subset \mathcal{O}_K$ be a sublattice with a basis $e_1,\ldots,e_n$ and $D(e_1\ldots e_n)=a^2 d_K$ for some $a\in\mathbb{Z}$. Then $\mathcal{O}_K \subset \frac{1}{a}R = \langle \frac{e_1}{a},\ldots,\frac{e_n}{a}\rangle$

Proof Let $z_1 \dots z_n$ be a basis of $\mathcal{O}_K$, s.t. $e_1' = d_1 z_1, \dots, e_n' = d_n z_n$ is a basis of R for some $d_i \in \mathbb{Z}$

$$D(e_1', \dots, e_n') = D(e_1, \dots, e_n)$$

$$\shortparallel$$

$$\left(\prod_{i=1}^{n} d_i\right)^2 D(z_1, \dots, z_n) = \left(\prod_{i=1}^{n} d_i\right)^2 \cdot d_K,$$

so $a = \prod_{i=1}^{n} d_i$; $\quad \frac{1}{a} R = \left\langle \frac{z_1}{\prod_{i \neq 1} d_i}, \dots \frac{z_n}{\prod_{i \neq n} d_i} \right\rangle \supset \mathcal{O}_K$ $\square$

In our case $D(1, \mu, \dots, \mu^{e-1}) = p^N$ for some $N \Rightarrow a$ is a power of p

$R = \mathbb{Z}[\mu]$, the elements of $\mathcal{O}_K$ are of the form $\sum_{i=0}^{e-1} \frac{a_i}{p^{k_i}} \mu^i$, $a_i \in \mathbb{Z}$

$1, \mu, \dots, \mu^{e-1}$ is a basis of R.

We choose another basis:

$$1, \underbrace{1-\mu}_{= \xi}, \underbrace{(1-\mu)^2}_{= \xi^2}, \dots \underbrace{(1-\mu)^{e-1}}_{= \xi^{e-1}}$$

exercise: show that this is also a basis.

Recall from last week

$$\mathfrak{p} = (\xi) = (1-\mu) \text{ is a prime}$$

ideal in $\mathcal{O}_K$; $\mathfrak{p} \cap \mathbb{Z} = (p)$

$p \cdot \mathcal{O}_K = (\xi)^e$

Assume that

$$\alpha = \sum_{i=0}^{e-1} \frac{a_i}{p^{k_i}} \xi^i \in \mathcal{O}_K \quad \text{for some } a_i \in \mathbb{Z}$$
$$(a_i, p) = 1$$

Localize $\mathcal{O}_K$ at $\mathfrak{p}$ and consider α as an element of the DVR $\mathcal{O}_{K,\mathfrak{p}}$

ξ is a uniformizer for $\mathcal{O}_{K,\mathfrak{p}}$ and we have a valuation:

$$\nu : K^\times \longrightarrow \mathbb{Z}$$
$$x = \xi^n y \text{ with } y \in \mathcal{O}_{K,\mathfrak{p}}^\times \Rightarrow \nu(x) = n$$

What is $\nu(\alpha)$?

$$\nu\left(\frac{a_i}{p^{k_i}} \xi^i\right) = \nu(a_i) - k_i \nu(p) + i$$

a_i is coprime to $p \Rightarrow a_i \notin \mathfrak{p}$

$$\Rightarrow a_i \in \mathcal{O}_{K,\mathfrak{p}}^\times \Rightarrow \nu(a_i) = 0$$

$\nu(p) = e$, because $p \cdot \mathcal{O}_K = (\xi^e)$

$$\Rightarrow p = \xi^e y \quad y \in \mathcal{O}_{K,\mathfrak{p}}^\times$$

$$\Rightarrow \nu\left(\frac{a_i}{p^{k_i}} \xi^i\right) = i - k_i e \equiv i \pmod e,$$

in particular the valuations of all summands are different

Lemma 16.2 Let A a DVR with field of fracts. F and valuation $\nu : F^\times \to \mathbb{Z}$. Let $x, y \in F^\times$ s.t. $\nu(x) \neq \nu(y)$. Then $\nu(x+y) = \min\{\nu(x), \nu(y)\}$

Proof Let u be a uniformizer

Write $x = u^n a$, $a \in A^\times$

$y = u^m b$, $b \in A^\times$, $m \neq n$

assume $n < m \Rightarrow$

$$x + y = u^n(a + \underbrace{u^{m-n} b}_{\mathfrak{m}})$$

$a + u^{m-n} b \in A^\times \Rightarrow \nu(x+y) = n$

analogously for $m < n$. $\square$

In our case:

$$\nu(\alpha) = \nu\left(\sum_{i=0}^{e-1} \frac{a_i}{p^{k_i}} \zeta^i\right) = \min_{i=0\ldots e-1} \nu\left(\frac{a_i}{p^{k_i}} \zeta^i\right)$$

$$= \min_i (i - k_i e)$$

Note: if $\exists k_i > 0$, then

$i - k_i e < 0$ because $0 \le i \le e-1$

then $\nu(\alpha) < 0$ — contradicts the assumption $\alpha \in \mathcal{O}_K$

$\Rightarrow k_i \le 0 \Rightarrow \alpha \in \mathbb{Z}[\zeta]$

$$\mathbb{Z}[\zeta] = \mathbb{Z}[\mu]$$

<u>Conclusion:</u> $\mathcal{O}_K = \mathbb{Z}[\mu]$

<u>The general case:</u> μ — primitive n-th root of unity for arbitrary n

$K = \mathbb{Q}(\mu)$.

Decompose $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$, $p_i \ne p_j$, $i \ne j$

We may restrict to the case $n = p_1^{r_1} p_2^{r_2}$

the general case is done by induction on k similarly.

$\mu_1 = \mu^{p_2^{r_2}}$, $\mu_2 = \mu^{p_1^{r_1}}$

μ_1: prim. $p_1^{r_1}$-th root of unity; μ_2: prim. $p_2^{r_2}$-th root of unity

$\Rightarrow K$ contains the subfields

$K_1 = \mathbb{Q}(\mu_1)$ and $K_2 = \mathbb{Q}(\mu_2)$

K is generated by K_1 and K_2 (because $\mu = \mu_1^a \mu_2^b$ for some a, b: $a p_2^{r_2} + b p_1^{r_1} = 1$)

<u>Lemma 16.3</u> $K_1 \cap K_2 = \mathbb{Q}$

<u>Proof</u> Let $K_0 = K_1 \cap K_2$

If $K_0 \neq \mathbb{Q}$ then $d_{K_0} > 1 \Rightarrow \exists$ a prime number p_0 that ramifies in K_0 (corollary from Thm 15.5)

$K_0 \subset K_1 \Rightarrow p_0$ ramifies in K_1

The only prime that ramifies in K_1 is p_1

$\Rightarrow p_0 = p_1$.

$K_0 \subset K_2 \Rightarrow p_0 = p_2$ — contradiction: $p_1 \neq p_2$ $\square$

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

<u>Prop. 16.4</u> Assume K any number field, $K_1, K_2 \subset K$ subfields, Galois $/ \mathbb{Q}$.

$(d_{K_1}, d_{K_2}) = 1$, K is generated by K_1, K_2

Then:

1) The natural map $K_1 \otimes_{\mathbb{Q}} K_2 \longrightarrow K$ is an isomorphism $x \otimes y \longmapsto xy$

2) K is Galois $/\mathbb{Q}$,

$$Gal(K/\mathbb{Q}) \simeq Gal(K_1/\mathbb{Q}) \times Gal(K_2/\mathbb{Q})$$

3) If $\mathcal{O}_{K_1} = \langle \alpha_1 \dots \alpha_n \rangle$, $\mathcal{O}_{K_2} = \langle \beta_1, \dots, \beta_m \rangle$ as $\mathbb{Z}$-modules, then

$$\mathcal{O}_K = \langle \alpha_i \beta_j, \quad i = 1 \dots n, \ j = 1 \dots m \rangle$$

<u>Proof</u> 1) Similar to Lemma 16.3: $K_1 \cap K_2 = \mathbb{Q}$

Let $K_1 = \mathbb{Q}(\xi) = \frac{\mathbb{Q}[x]}{(f)}$, f - monic min. poly of ξ.

$\deg(f) = [K_1 : \mathbb{Q}]$

$K = K_2(\xi)$ by assumption

Assume $f = f_1 \cdot f_2$ in $K_2[x]$

Coeff. of f_1 are in K_1 (because the roots of f_1 are in K_1, since K_1 is Galois $/\mathbb{Q}$), but also in K_2

$\Rightarrow f_1 \in \mathbb{Q}[x]$; analogously $f_2 \in \mathbb{Q}[x]$

$\Rightarrow$ either $\deg f_1 = 1$, or $\deg f_2 = 1$

$\Rightarrow f$ is irred in $K_2[x]$

$\Rightarrow K \simeq \dfrac{K_2[x]}{(f)} \Rightarrow [K:\mathbb{Q}] = [K_1:\mathbb{Q}]\cdot[K_2:\mathbb{Q}]$

$\Rightarrow K_1 \otimes_{\mathbb{Q}} K_2 \longrightarrow K$ is an isomorphism, because it is surj. by assumption and both sides have the same dimension.

2) $Gal(K_1/\mathbb{Q}) \times Gal(K_2/\mathbb{Q})$ acts on $K_1 \otimes K_2$

$(g_1, g_2) \quad (g_1,g_2)\cdot x\otimes y = g_1 x \otimes g_2 y$

$\Rightarrow Gal(K_1/\mathbb{Q}) \times Gal(K_2/\mathbb{Q}) \hookrightarrow Gal(K/\mathbb{Q})$ is an isomorph. since both groups have the same order. $[K:\mathbb{Q}]$

3) $\alpha_i\beta_j$ span a sublattice in $\mathcal{O}_K$

$\Rightarrow$ any element of $\mathcal{O}_K$ is of the form

$x = \sum_{i,j} \frac{d_{ij}}{c_{ij}} \alpha_i\beta_j$ for some $d_{ij}, c_{ij} \in \mathbb{Z}$, $(d_{ij}, c_{ij}) = 1$

Write $\gamma_i = \sum_j \frac{d_{ij}}{c_{ij}} \beta_j$, then $x = \sum_i \alpha_i \gamma_i$

Let $\sigma_1 \dots \sigma_n$ be elements of $Gal(K_1/\mathbb{Q})$. They act on K fixing K_2 (see above)

$\sigma_\ell x = \sum_i \gamma_i\, \sigma_\ell(\alpha_i) \in \mathcal{O}_K$, or in matrix form:

$$(*)\quad \underbrace{\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n) \end{pmatrix}}_{A} \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = \begin{pmatrix} \sigma_1(x) \\ \vdots \\ \sigma_n(x) \end{pmatrix}$$

$$(\det A)^2 = d_{K_1} \qquad \det A \in \mathcal{O}_{K_1}$$

Multiplying $(*)$ by A^+ (see a lemma in Lecture 4) $\qquad A^+ \cdot A = \det A \cdot \mathrm{Id}$

$$\Rightarrow \det A \cdot \gamma_i \in \mathcal{O}_K$$

$$\Rightarrow (\det A)^2 \gamma_i = d_{K_1} \cdot \gamma_i \in \mathcal{O}_{K_2}$$

$$d_{K_1} \cdot \gamma_i = \sum_j \underbrace{\frac{d_{ij}}{c_{ij}} \cdot d_{K_1}}_{\in \mathbb{Z}} \cdot \beta_j \in \mathcal{O}_{K_2}$$

$\Rightarrow c_{ij}$ divide d_{K_1}

analogously c_{ij} divide d_{K_2}

but $(d_{K_1}, d_{K_2}) \Rightarrow c_{ij} = \pm 1$ $\qquad \square$