Eine Woche, ein Beispiel

5.14. examples in ANT. ← Algebraic number theory

Goal: Calculate examples in ANT, containing:

$\mathbb{Q}(\sqrt{d})$ $\quad$ $\mathbb{Q}(\zeta_N)$ $\quad$ d square-free

$\mathbb{Q}[T]/(T^3-2)$ $\quad$ $\mathbb{Q}(\sqrt{5}, i)$ $\quad$ $\mathbb{Q}(\sqrt{-23})[T]/(T^3-T-1)$

...

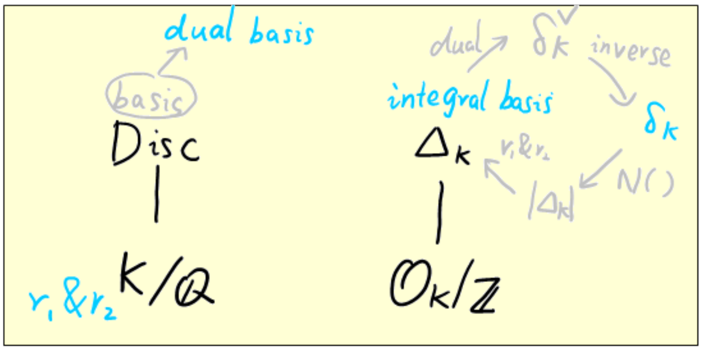
① K $\mathcal{O}_K$ Galois? If so, $Gal(K/\mathbb{Q})$ subgroup & subfield

② δ_K ↖ Δ_K: see the picture
ramification theory

③ $\mathcal{O}_K^\times$, $Cl(K)$, $\pi_1(\mathcal{O}_K)$

④ Gal ext ⇒ Frob element σ_p

⑤ local field K_p
places M_K



$N_{K/\mathbb{Q}}(x)$ $\quad$ $N_{K/\mathbb{Q}}(I)$ $\quad$ $N_{L/K}(I)$

$\delta_{K/\mathbb{Q}}$ K $\quad$ $\delta_{L/K}$ L

$\downarrow N_{K/\mathbb{Q}}$ $\quad$ $\downarrow N_{L/K}$

$\mathrm{Disc}_{K/\mathbb{Q}}(\alpha_1, \cdots \alpha_n)$ $\quad$ $\mathrm{Disc}_{K/\mathbb{Q}}$ $\mathbb{Z}$ $\quad$ $\mathrm{Disc}_{L/K}$ K

$K = \mathbb{Q}(\sqrt{d})$

1) All quartic extension of $\mathbb{Q}$ have form $\mathbb{Q}(\sqrt{d})$ $\quad r_1, r_2 = ?$

2) $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$

3) $Tr(\sqrt{d}) = 0 \quad Tr(\frac{\sqrt{d}+1}{2}) = 1 \quad N(\sqrt{d}) = -d \quad N(\frac{\sqrt{d}+1}{2}) = \frac{1-d}{4}$

4) a basis: $(\alpha_1, \alpha_2) = (1, \sqrt{d})$

the dual basis: $(\alpha_1^\vee, \alpha_2^\vee) = (\frac{1}{2}, \frac{1}{2\sqrt{d}})$

Recall how do we verify a basis (by Disc). the prop of Disc: "Verify"!

① $Disc(\alpha_1, \dots, \alpha_n) := \det(Tr_{K/\mathbb{Q}}(\alpha_i \alpha_j)) \overset{\text{taking } 1:1}{=} [\oplus_i \mathbb{Z}\alpha_i^\vee : \oplus_i \mathbb{Z}\alpha_i] = \det(\sigma_i(\alpha_j))^2$

② $Disc(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha))$ If $K = \mathbb{Q}[T]/(f) = \mathbb{Q}(\alpha)$

5) $$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\frac{\sqrt{d}+1}{2}] & d \equiv 1 \bmod 4 \\ \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \bmod 4 \end{cases}$$

Define $$\omega_d = \begin{cases} \frac{\sqrt{d}+1}{2} & d \equiv 1 \bmod 4 \\ \sqrt{d} & d \equiv 2,3 \bmod 4 \end{cases}$$

then $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z} \oplus \mathbb{Z}\omega_d$

6) $$D := \Delta_{\mathbb{Q}(\sqrt{d})} := Disc(1, \omega_d) = \begin{cases} d & d \equiv 1 \bmod 4 \\ 4d & d \equiv 2,3 \bmod 4 \end{cases}$$

7) Again use Lemma 1.3.7 / Prop 1.3.8 $\Rightarrow$ 5)

Recall how do we verify an integral basis (by Prop 1.3.8)

e.p. when $Disc(\beta_1, \dots, \beta_n)$ is square free, then $\{\beta_1, \dots, \beta_n\}$ is an integral basis.

8) $$\delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} (\sqrt{d}) & d \equiv 1 \bmod 4 \\ (2\sqrt{d}) & d \equiv 2,3 \bmod 4 \end{cases}$$

ED

$d = -1$

$\delta_{\mathbb{Q}(i)} = (2) = (1+i)^2$

$1+i$	3	$2+i$, $2-i$	7	11	$3+2i$, $3-2i$
| 2	|	\ /	|	|	\ /
2	3	5	7	11	13

$d = -2$

$\delta_{\mathbb{Q}(\sqrt{2}i)} = (\sqrt{-2})^3$

$\sqrt{2}i$	$1+\sqrt{2}i$, $1-\sqrt{2}i$	5	7	$3+\sqrt{2}i$, $3-\sqrt{2}i$	13
| 2	\ /	|	|	\ /	|
2	3	5	7	11	13

$d = -3$

$\delta_{\mathbb{Q}(\sqrt{3}i)} = (\sqrt{-3})$

2	$\sqrt{3}i$	5	$\frac{1+3\sqrt{3}i}{2}$, $\frac{1-3\sqrt{3}i}{2}$	11	$1+2\sqrt{3}i$, $1-2\sqrt{3}i$
|	| 2	|	\ /	|	\ /
2	3	5	7	11	13

$d = 2$

$\delta_{\mathbb{Q}(\sqrt{2})} = (\sqrt{2})^3$

$\sqrt{2}$	3	5	$5-3\sqrt{2}$, $5+3\sqrt{2}$	11	13	$5+2\sqrt{2}$, $5-2\sqrt{2}$
| 2	|	|	\ /	|	|	\ /
2	3	5	7	11	13	17

$d = 3$

$\delta_{\mathbb{Q}(\sqrt{3})} = (1+\sqrt{3})^2(\sqrt{3})$

$1+\sqrt{3}$	$\sqrt{3}$	5	7	$8+5\sqrt{3}$, $8-5\sqrt{3}$	$4+\sqrt{3}$, $4-\sqrt{3}$
| 2	| 2	|	|	\ /	\ /
2	3	5	7	11	13

The following calculation need the theory of frobenius element.

9) Legendre Symbol

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv 1, 7 \mod 8 \\ -1 & p \equiv 3, 5 \mod 8 \end{cases}$$

10) Quadratic reciprocity law (p, q odd prime, $p \neq q$)

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) \quad \text{i.e.} \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

11) Remification

$p = 2$:	$D \not\equiv 1 \mod 4$	ramified
	$D \equiv 1 \mod 8$	split
	$D \equiv 5 \mod 8$	inert
p odd:	$p \mid D$	ramified
	$\left(\frac{D}{p}\right) = 1$	split
	$\left(\frac{D}{p}\right) = -1$	inert

$\mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{d})}$ $\quad d>0$ $\qquad N(\varepsilon_0)$

$\sqrt{2} = [1, \overline{2}]$ $\quad 1+\sqrt{2}$ $\quad -$

$\sqrt{3} = [1, \overline{1, 2}]$ $\quad 2+\sqrt{3}$ $\quad +$

$\sqrt{5} = [2, \overline{4}]$ $\quad 2+\sqrt{5} = \left[\frac{1}{2}(1+\sqrt{5})\right]^3$ $\quad -$

$\sqrt{6} = [2, \overline{2, 4}]$ $\quad 5+2\sqrt{6}$ $\quad +$

$\sqrt{7} = [2, \overline{1,1,1,4}]$ $\quad 8+3\sqrt{7}$ $\quad +$

$\sqrt{10} = [3, \overline{6}]$ $\quad 3+\sqrt{10}$ $\quad -$

$\sqrt{11} = [3, \overline{3, 6}]$ $\quad 10+3\sqrt{11}$ $\quad +$

$\sqrt{13} = [3, \overline{1,1,1,1,6}]$ $\quad 18+5\sqrt{13} = \left[\frac{1}{2}(3+\sqrt{13})\right]^3$ $\quad -$

$\sqrt{14} = [3, \overline{1,2,1,6}]$ $\quad 15+4\sqrt{14}$ $\quad +$

$\sqrt{15} = [3, \overline{1, 6}]$ $\quad 4+\sqrt{15}$ $\quad +$

$\sqrt{17} = [4, \overline{8}]$ $\quad 4+\sqrt{17}$ $\quad -$

$\sqrt{19} = [4, \overline{2,1,3,1,2,8}]$ $\quad 170+39\sqrt{19}$ $\quad +$

$\sqrt{21} = [4, \overline{1,1,2,1,1,8}]$ $\quad 55+12\sqrt{21} = \left[\frac{1}{2}(5+\sqrt{21})\right]^3$ $\quad +$

$\sqrt{29} = [5, \overline{2,1,1,2,10}]$ $\quad 70+13\sqrt{29} = \left[\frac{1}{2}(5+\sqrt{29})\right]^3$ $\quad -$

$\sqrt{37} = [6, \overline{12}]$ $\quad 6+\sqrt{37}$ $\quad -$

×	2	3	5	6	7
×	10	11	13	14	15
17	×	19	21	22	23
×	26	×	29	30	31
33	34	35	37	38	39
41	42	43	×	46	47
×	×	51	53	×	55
57	58	59	61	62	×
65	66	67	69	70	71

$Cl(K)$:

$(\mathbb{Z}/n\mathbb{Z})^\times$

$\downarrow$

Computing h by class number formula

$K \subseteq \mathbb{Q}(\zeta_N)$, $G = Gal(K/\mathbb{Q})$ abelian

$$\kappa = \prod_{\substack{\chi \in \widehat{G} \\ \chi \neq \chi_0 \\ \chi \to \text{prim}}} L(\chi, 1) \qquad \kappa = \frac{2^{r_1}(2\pi)^{r_2} R_K h}{w\, |\Delta_K|^{\frac{1}{2}}}$$

How to compute $L(\chi,1) \to h$?

$$\tau(\chi) = \sum_{m \in \mathbb{Z}/f\mathbb{Z}} \chi(m)\, \zeta_f^m$$

$$\tau_a(\chi) = \sum_{m \in \mathbb{Z}/f\mathbb{Z}} \chi(m)\, \zeta_f^{ma}$$

①
$$L(\chi,1) = -\frac{\chi(-1)\tau(\chi)}{f} \sum_{a=1}^{f-1} \bar{\chi}(a) \log(1-\zeta^a)$$

$$= \begin{cases} -\dfrac{\tau(\chi)}{f} \displaystyle\sum_{a=1}^{f-1} \bar{\chi}(a) \log\left(\sin \frac{\pi a}{f}\right) & \chi(-1) = 1 \\ \dfrac{\tau(\chi)\pi i}{f^2} \displaystyle\sum_{a=1}^{f-1} \bar{\chi}(a)\, a & \chi(-1) = -1 \end{cases}$$

② when $K = \mathbb{Q}(\sqrt{\Delta_K})$, then we know χ_{Δ_K} & $\tau(\chi_{\Delta_K})$ well.

with disc $= \Delta_K := \Delta$

(0) $Im\, \chi_\Delta \in \{-1, 0, 1\} \subseteq \mathbb{R}$

(a) $\chi_\Delta(-1) = sgn(\Delta)$

(b) $\chi_\Delta(2) = \begin{cases} (-1)^{\frac{\Delta^2-1}{8}} & \Delta_K \equiv 1 \bmod 4 \\ 0 & \Delta_K \equiv 3 \bmod 4 \text{ or } \Delta_K \text{ even} \end{cases}$

(c) $\chi_\Delta(p) = \left(\frac{d_K}{p}\right)$ $\quad$ p odd prime

(d) $\tau(\chi_\Delta) = \sqrt{\Delta_K} = \begin{cases} |\Delta_K|^{\frac{1}{2}} & \Delta_K > 0 \\ i\,|\Delta_K|^{\frac{1}{2}} & \Delta_K < 0 \end{cases}$

$$\Rightarrow h = \begin{cases} -\dfrac{1}{2\log(\varepsilon)} \displaystyle\sum_{a=1}^{|\Delta_K|-1} \chi_\Delta(a) \log\left(\sin\frac{\pi a}{\Delta}\right) = -\dfrac{1}{\log(\varepsilon)} \displaystyle\sum_{a=1}^{[\Delta/2]} \chi_{d_K}(a) \log\left(\sin\frac{\pi a}{\Delta}\right) & d_K > 0 \\ -\dfrac{1}{|d_K|} \displaystyle\sum_{a=1}^{|d_K|-1} \chi_{d_K}(a)\, a \cdot \dfrac{w}{2} \quad \text{or when } d_K < -4 & d_K < 0 \end{cases}$$

③ More restriction: $|\Delta_K| = p$ is an odd prime $\Rightarrow \Delta_K \equiv 1 \pmod 4$

R = Residue $\quad$ N = Non-residue $\quad$ $\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right) = \frac{n}{2^{n-1}}$

$\Delta_K = p \quad p \equiv 1 \pmod 4$:

$$\varepsilon^{2h} = \frac{\prod_{b \in N} \sin \frac{\pi b}{p}}{\prod_{a \in R} \sin \frac{\pi a}{p}} \Rightarrow \varepsilon^h = \frac{\sqrt{p}}{2^{\frac{p-1}{2}}} \left(\prod_{\substack{a \in R \\ a \leq \frac{p-1}{2}}} \sin \frac{\pi a}{p} \right)^{-2}$$

$\Delta_K = -p \quad p \equiv 3 \pmod 4 \quad p \neq 3$

$$h = \frac{1}{p}\left(\sum_{b \in N} b - \sum_{a \in R} a\right) = \frac{p-1}{2} - \frac{2}{p} \sum_{a \in R} a$$

e.g. $\Delta_k = -3 \quad p=3 \quad R=\{1\}$

$$h = 3\cdot\left(1-\tfrac{2}{3}\right)=1$$

$\Delta_k = -7 \quad p=7 \quad R=\{1,2,4\}$

$$h = 3 - \tfrac{2}{7}(1+2+4) = 1$$

$\Delta_k = -11 \quad p=11 \quad R=\{1,3,4,5,9\}$

$$h = 5 - \tfrac{2}{11}(1+3+\cdots) = 1$$

$\Delta_k = -19 \quad p=19 \quad R=\{1,4,5,6,7,9,11,16,17\}$

$$h = 7 - \tfrac{2}{19}(1+4+\cdots) = 1$$

$\left(\frac{2}{19}\right)=-1 \quad \left(\frac{3}{19}\right)=-1 \quad \left(\frac{5}{19}\right)=1 \quad \left(\frac{7}{19}\right)=1 \quad \left(\frac{11}{19}\right)=1 \quad \left(\frac{13}{19}\right)=-1 \quad \left(\frac{17}{19}\right)=1$

$\Delta_k = -23 \quad R=\{1\sim4,6,8,9,12,13,16,18\}$

$$h = 11 - \tfrac{2}{23}(1+2+\cdots) = 3$$

$\Delta_k = -31$

$R=\{1,2,4,5,7\sim10,14,16,18\sim20,25,28\}$

$$h = 15 - \tfrac{2}{31}(1+2+\cdots) = 3$$

$\Delta_k = -43$

$R=\{1,4,6,9-11,13\sim17,21,23-25,31,35,36,38,40,41\}$

$$h = 21 - \tfrac{2}{43}(1+4+\cdots) = 1$$

$\Delta_k = -67$

$$R=\left\{\begin{array}{l}1,4,6,9,10,14\sim17,19,21\sim26,29,33,\\ 35\sim37,39,40,47,49,54\sim56,59,60,62,64,65\end{array}\right\}$$

$$h = 33 - \tfrac{2}{67}(1+4+\cdots) = 1$$

$\Delta_k = -163$

$$R=\left\{\begin{array}{l}1,4,6,9,10,14\sim16,21,22,24\sim26,33\sim36,38\sim41,43,46,47,\\ 49,51,53\sim58,60\sim62,64,65,69,71,74,77,81,83\sim85,87,88,90,\\ 91,93,95\sim97,100,104,111,113,115,118,119,121,126,131\sim136,\\ 140,143\sim146,150\sim152,155,156,158,160,161\end{array}\right\}$$

$$h = 81 - \tfrac{2}{163}(1+4+\cdots) = 1$$

$\Delta_k = 5 \quad R=\{1,4\} \quad \varepsilon = \frac{1}{2}(1+\sqrt{5}) \quad h=1$

$$\frac{\sqrt{5}}{2^2}\;\frac{1}{(\sin\frac{\pi}{5})^2} = \frac{1}{2}(1+\sqrt{5}) = \varepsilon^h$$

$\Delta_k = 13 \quad R=\{1,3,4,9,10,12\} \quad \varepsilon = \frac{1}{2}(3+\sqrt{13}) \quad h=1$

$$\frac{\sqrt{13}}{26}\cdot\frac{1}{(\sin\frac{\pi}{13}\cdot\sin\frac{3\pi}{13}\,\sin\frac{4\pi}{13})^2} = \frac{1}{2}(3+\sqrt{13}) = \varepsilon^h \Rightarrow \sin\frac{\pi}{13}\cdot\sin\frac{3\pi}{13}\cdot\sin\frac{4\pi}{13} = \frac{4\sqrt{13}}{2^3}\sqrt{\frac{1}{2}(\sqrt{13}-3)}$$

$\Delta_k = 17 \quad R=\{1,2,4,8,9,13,15,16\} \quad \varepsilon = 4+\sqrt{17} \quad h=1$

$$\frac{\sqrt{17}}{2^8}\;\frac{1}{(\sin\frac{\pi}{17}\sin\frac{2\pi}{17}\sin\frac{4\pi}{17}\sin\frac{8\pi}{17})^2} = 4+\sqrt{17} = \varepsilon^h$$

$$\Rightarrow \sin\frac{\pi}{17}\sin\frac{2\pi}{17}\sin\frac{4\pi}{17}\sin\frac{8\pi}{17} = \frac{1}{2^4}\sqrt{17-4\sqrt{17}}$$

$K = \mathbb{Q}[T]/(T^3-2) = \mathbb{Q}(\alpha)$ $\quad K/\mathbb{Q}$ not Galois.

1) $Tr(\alpha)=0 \quad Tr(\alpha^2)=0 \quad N(\alpha)=2 \quad N(\alpha^2)=4$

2) $Disc(1,\alpha,\alpha^2) = -N(3\alpha^2) = -3^3 \cdot 2^2$

$\therefore$ ① $\{1,\alpha,\alpha^2\}$ is a basis of $\mathbb{Q}(\alpha)$

② $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$, $\Delta_{\mathbb{Q}(\alpha)} = -3^3 \cdot 2^2$

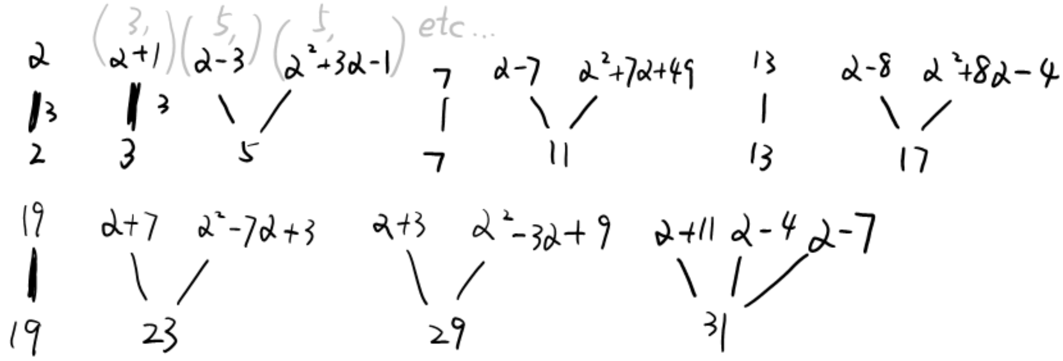
③ $r_1 = r_2 = 1$

3) the dual basis of $(\alpha_1,\alpha_2,\alpha_3) := (1,\alpha,\alpha^2)$ is

$(\alpha_1^\vee,\alpha_2^\vee,\alpha_3^\vee) = \left(\frac{1}{3}, \frac{1}{3\alpha}, \frac{1}{3\alpha^2}\right) = \left(\frac{1}{3}, \frac{\alpha^2}{6}, \frac{\alpha}{6}\right)$

$\delta_{\mathbb{Q}(\alpha)} = (3\alpha^2)$

4) ramification $(\alpha = \sqrt[3]{2})$



$K = \mathbb{Q}(\zeta_N)$

1) $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ Galois, $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$

$\mathbb{Q}(\zeta_N) = \mathbb{Q}[T]/\Phi_N(T)$ $\quad r_1 = 0$ except $N = 1, 2$

2) $\Delta_K \mid \mathrm{Disc}(1, \zeta, \cdots \zeta_N^{\phi(N)-1}) \Rightarrow \mathcal{O}_{\mathbb{Q}(\zeta_{p^n})} = \mathbb{Z}[\zeta_{p^n}]$

In general, $\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathbb{Z}[\zeta_N]$ by Cor 1.4.6.

3) $\Delta_{\mathbb{Q}(\zeta_{p^n})} = \pm p^{p^{n-1}(pn-n-1)}$ $\quad$ minus: $p \equiv 3 \pmod 4$ or $p=2, n=2$

when $N = p_1^{n_1} \cdots p_k^{n_k}$, by Prop 3.3.7.3.

$$\Delta_{\mathbb{Q}(\zeta_N)} = (-1)^{t_N}\left[p_1^{\left(n_1 - \frac{n_1 - 1}{p_1}\right)} \cdots p_k^{\left(n_k - \frac{n_k - 1}{p_k}\right)}\right]^N \qquad t_N = \begin{cases} 0 & N = 1, 2 \\ \frac{\phi(N)}{2} & N > 2 \end{cases}$$

4) By Frobenius element,

$p \equiv 0 \pmod N$ ramified $\quad$ ($N = p^k$ totally ramified)

$p \equiv 1 \pmod N$ split

$p \not\equiv 0, 1 \pmod N$ inert

In detail, ***Proposition 3.5.3.*** — *The Frobenius element $\sigma_l \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is given by $\sigma_l(\zeta_N) = \zeta_N^l$. The decomposition group of each $\mathfrak{l}_i$ is $D_l = \langle l \rangle \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$, and the residue degree $f(\mathfrak{l}_i|l)$ is the order of l in $(\mathbb{Z}/N\mathbb{Z})^\times$, that is, the minimal integer $f > 0$ such that $N|(l^f - 1)$.*

e.g $\quad N = 5$

$\{\bar{2} = 2, 4, 3, 1\}$

$\{\overline{11} = 1\}$

$\{\overline{19} = 4, 1\}$

The minimal polynomial $\Phi_N(x)$ of $\zeta_N \in \mathbb{Q}[\zeta_N]$

Table[{n, Cyclotomic[n, x]}, {n, 0, 50}]

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

$N = 2^n p$: $\varphi(N) = 2^{\min\{0,n-1\}}(p-1)$

Φ_2 $1+x$	Φ_3 $1+x+x^2$	Φ_5 $1+x+x^2+x^3+x^4$	Φ_7 $1+x+x^2+x^3+x^4+x^5+x^6$
Φ_4 $1+x^2$	Φ_6 $1-x+x^2$	Φ_{10} $1-x+x^2-x^3+x^4$	Φ_{14} $1-x+x^2-x^3+x^4-x^5+x^6$
Φ_8 $1+x^4$	Φ_{12} $1-x^2+x^4$	Φ_{20} $1-x^2+x^4-x^6+x^8$	Φ_{28} $1-x^2+x^4-x^6+x^8-x^{10}+x^{12}$
Φ_{16} $1+x^8$	Φ_{24} $1-x^4+x^8$	Φ_{40} $1-x^4+x^8-x^{12}+x^{16}$	Φ_{56} $1-x^4+x^8-x^{12}+x^{16}-x^{20}+x^{24}$

$N = 2^n \cdot 3 \cdot p$, $p = 3, 5, 7$: $\varphi(N) = 2^{\min\{1,n\}}(p-1)$

Φ_9 $1+x^3+x^6$	Φ_{15} $1-x+x^3-x^4+x^5-x^7+x^8$	Φ_{21} $1-x+x^3-x^4+x^6-x^8+x^9-x^{11}+x^{12}$
Φ_{18} $1-x^3+x^6$	Φ_{30} $1+x-x^3-x^4-x^5+x^7+x^8$	Φ_{42} $1+x-x^3-x^4+x^6-x^8-x^9+x^{11}+x^{12}$
Φ_{36} $1-x^6+x^{12}$	Φ_{60} $1+x^2-x^6-x^8-x^{10}+x^{14}+x^{16}$	Φ_{84} $1+x^2-x^6-x^8+x^{12}-x^{16}-x^{18}+x^{22}+x^{24}$
Φ_{72} $1-x^{12}+x^{24}$	Φ_{120} $1+x^4-x^{12}-x^{16}-x^{20}+x^{28}+x^{32}$	Φ_{168} $1+x^4-x^{12}-x^{16}+x^{24}-x^{32}-x^{36}+x^{44}+x^{48}$

$N = p^2$: $\varphi(N) = (p-1)p$

Φ_{25} $1+x^5+x^{10}+x^{15}+x^{20}$

Φ_{49} $1+x^7+x^{14}+x^{21}+x^{28}+x^{35}+x^{42}$

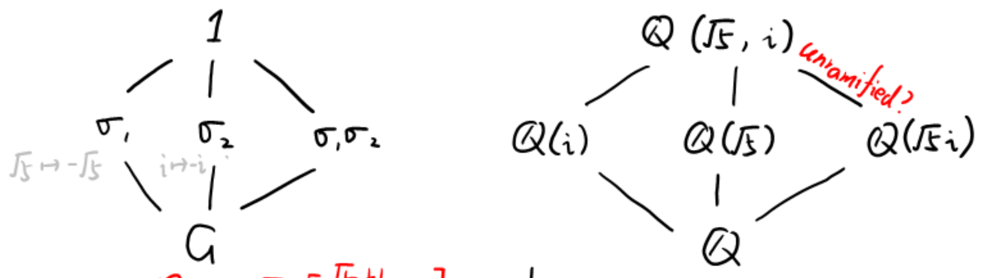
Φ_{121} $1+x^{11}+x^{22}+x^{33}+x^{44}+x^{55}+x^{66}+\cdots+x^{110}$

50以内剩： Φ_{27} Φ_{33} Φ_{35} Φ_{39} Φ_{45}

$K=\mathbb{Q}(\sqrt{-5})$ $L=\mathbb{Q}(\sqrt{5},i)$ purpose: L/K is unramified by discuss $L/\mathbb{Q}$

1) $\mathcal{O}_K=\mathbb{Z}[\sqrt{-5}]$ $\mathcal{O}_L \supseteq \mathbb{Z}[\frac{\sqrt{5}+1}{2}, i]$

2) $L/\mathbb{Q}$ Galois, $Gal(L/\mathbb{Q})=\{1,\sigma_1,\sigma_2,\sigma_1\sigma_2\}$



3) $\mathcal{O}_L=\mathbb{Z}[\frac{\sqrt{5}+1}{2}, i]$ by

https://math.stackexchange.com/questions/299710/on-the-ring-of-integers-of-a-compositum-of-number-fields

4) take $(\alpha_1,\alpha_2,\alpha_3,\alpha_4)=(1,i,\sqrt{5},i\sqrt{5})$

the integral basis $(\beta_1,\beta_2,\beta_3,\beta_4)=(1,i,\frac{\sqrt{5}+1}{2}, i\frac{\sqrt{5}+1}{2})$

then $(\alpha_1^\vee,\alpha_2^\vee,\alpha_3^\vee,\alpha_4^\vee)=(\frac{1}{4},\frac{1}{4i},\frac{1}{4\sqrt{5}},\frac{1}{4\sqrt{5}i})$

$(\beta_1^\vee,\beta_2^\vee,\beta_3^\vee,\beta_4^\vee)=(\frac{1}{4}-\frac{1}{4\sqrt{5}}, -i(\frac{1}{4}-\frac{1}{4\sqrt{5}}), \frac{1}{2\sqrt{5}}, -i\cdot\frac{1}{2\sqrt{5}})$

$\delta_{\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}}=(2\sqrt{5})$ $\Delta_{\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}}=2^4\cdot 5^2$

$\Delta_{L/\mathbb{Q}}=Disc_{L/\mathbb{Q}}(\beta_1,\beta_2,\beta_3,\beta_4)=\frac{1}{4^2}Disc_{L/\mathbb{Q}}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)=4^2\cdot 5^2$

5) Since $\delta_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}=(2\sqrt{5})\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} \Rightarrow \delta_{\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}(\sqrt{-5})}=\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$

$\therefore$ $\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}(\sqrt{-5})$ is unramified.

6) Let's see closer about $L/\mathbb{Q}$:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{5},i) & (1+i)^2 & (\sqrt{5},i-2)\ \ (\sqrt{5},-i-2) \\ | & \|\,2 & 2\ \backslash\ \ /\ 2 \\ \mathbb{Q} & 2 & 5 \end{array}$$

$$\begin{array}{ccc} 1 & \mathbb{Q}(\sqrt{5},i) & (1+i) \\ \cap & | & \|\,2 \\ I(1+i|2) & \mathbb{Q}(\sqrt{5}) & (2) \\ \cap & | & | \\ D(1+i|2) & \mathbb{Q} & 2 \\ \cap & | & | \\ G & \mathbb{Q} & 2 \end{array}$$

$$\begin{array}{ccccl} 1 & \mathbb{Q}(\sqrt{5},i) & (\sqrt{5},i-2) & (\sqrt{5},-i-2) & \\ \cap & | & \|\,2 & \|\,2 & \text{ramified} \\ I(\beta|5) & \mathbb{Q}(i) & (\sqrt{5},i-2) & (\sqrt{5},-i-2) & \\ \cap & | & | & | & \text{field ext.} \\ D(\beta|5) & \mathbb{Q}(i) & (\sqrt{5},i-2) & (\sqrt{5},-i-2) & \\ \cap & | & \backslash & / & \text{split} \\ G & \mathbb{Q} & \multicolumn{2}{c}{5} & \end{array}$$

$\beta=(\sqrt{5},i-2)\triangleleft\mathcal{O}_L$

while $K/\mathbb{Q}$:

$$\begin{array}{ccc} K & (2,\sqrt{-5}+1) & (\sqrt{-5}) \\ | & \|\,2 & \|\,2 \\ \mathbb{Q} & 2 & 5 \end{array}$$

$L/K/\mathbb{Q}$:

$$\begin{array}{ccc} L & (1+i) & (\sqrt{5},i-2)\ \ (\sqrt{5},-i-2) \\ | & | & \backslash\ \ / \\ K & (2,\sqrt{-5}+1) & (\sqrt{-5}) \\ | & \|\,2 & \|\,2 \\ \mathbb{Q} & 2 & 5 \end{array}$$

Local field

Teichmüller lift for $K=\mathbb{Q}_5$

$[1]=1$ $\qquad$ $1=[1]$

$i\ \ [2]=2+1\cdot 5+2\cdot 5^2+1\cdot 5^3+3\cdot 5^4+\cdots$ $\qquad$ $2=[2]+[4]\cdot 5+[3]\cdot 5^2+[4]\cdot 5^4+[2]\cdot 5^5+\cdots$

$(2,1,2,1,3,4,2,3,0,3,\cdots$

$-i\ \ [3]=3+3\cdot 5+2\cdot 5^2+3\cdot 5^3+\cdots$ $\qquad$ $3=[3]+[2]\cdot 5+[1]\cdot 5^2+[4]\cdot 5^3+[2]\cdot 5^4+\cdots$

$(3,3,2,3,1,0,2,1,4,1,\cdots$

$-1\ \ [4]=4+4\cdot 5+4\cdot 5^2+4\cdot 5^3+\cdots$ $\qquad$ $[4]=[4]+[1]\,5$

$(4,4,4,4,\cdots)$

e.g of Hensel's lemma for $K=\mathbb{Q}_5$

$f(x)=5x^6+x^5+3x^4-x^3-2x+3 \in \mathbb{Z}_5[x]$

$\bar{f}(x)=\overline{(x^2-2)}\cdot\overline{(x^3-2x^2+x+1)} := \bar{g}(x)\bar{h}(x) \in \mathbb{F}_5[x]$ $\qquad \pi=5$

$$\begin{cases} g_0(x)=x^2-2 \\ h_0(x)=x^3-2x^2+x+1\end{cases} \Rightarrow \begin{cases} f-g_0h_0=5(x^6+x^4-x^2+1):=\pi f_1 \qquad f_1\in\mathbb{Z}_5[x] \\ ag_0+bh_0\equiv 1 \pmod{\pi} \quad \text{where } a,b\in\mathbb{Z}_5[x] \\ \qquad \begin{cases} a(x)=-2x^2+2x+3 \\ b(x)=2x+2\end{cases} \\ bf_1=ug_0+v \qquad \text{where } u,v\in\mathbb{Z}_5[x] \\ \qquad \begin{cases} u(x)=2x^5+2x^4+6x^3+6x^2+10x+10 \\ v(x)=22x+22\end{cases}\end{cases}$$

$\Rightarrow (af_1+uh_0)g_0+vh_0\equiv f_1 \mod \pi$

$p_0(x):=v(x)=22x+22$

$q_0(x):=$ "deg ≤ 5 of $(af_1+uh_0)(x)$" $=\cancel{5x^6}+11x^4-9x^2+22x+13$

Let $g_1=g_0+\pi p_0 \qquad h_1=h_0+\pi q_0$ $\qquad$ $g_1=x^2+110x+108$

$\Rightarrow g_1h_1=f+(g_0h_0-f)+\pi(p_0h_0+q_0g_0)+\pi^2p_0q_0$ $\qquad$ $h_1=55x^4+x^3-47x^2+111x+66$

$\equiv f+\pi(p_0h_0+q_0g_0-f)\equiv f \pmod{\pi}$