

Eine Woche, ein Beispiel

5.14. examples in ANT. ← Algebraic number theory

Goal: Calculate examples in ANT, containing:

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

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

...

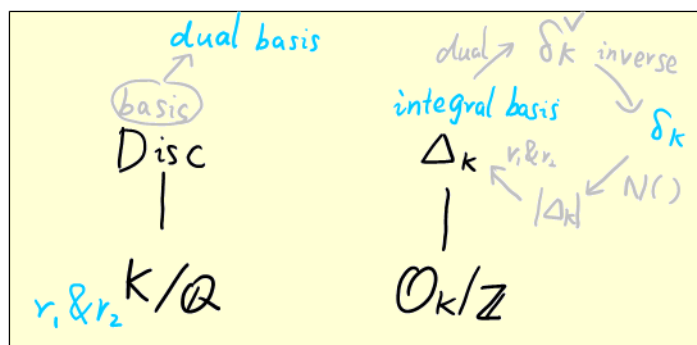
① K/\mathbb{Q} Galois? If so, $\text{Gal}(K/\mathbb{Q})$ subgroup & subfield

② $\delta_K \leftarrow \Delta_K$: see the picture
ramification theory

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

④ Gal ext \Rightarrow Frobenius element σ_p

⑤ local field K_p
places M_K



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

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

$$N_{L/K}(I)$$

\Rightarrow

$$\delta_{K/\mathbb{Q}} \xrightarrow{N_{K/\mathbb{Q}}} \delta_{K/\mathbb{Q}}$$

\Rightarrow

$$\delta_{L/K} \xrightarrow{N_{L/K}} \delta_{L/K}$$

$$\text{Disc}_{K/\mathbb{Q}}(a_1, \dots, a_n)$$

$$\text{Disc}_{K/\mathbb{Q}} \mathbb{Z}$$

$$\text{Disc}_{L/K} \mathbb{Z}$$

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

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

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

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

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

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

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

$$\textcircled{1} \text{Disc}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)) \stackrel{\text{taking 1-1}}{=} [\oplus \mathbb{Z} \alpha_i^\vee : \oplus \mathbb{Z} \alpha_i] = \det(\sigma_i(\alpha_j))^2$$

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

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

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

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

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

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

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

ED	$d = -1$	$1+i$	3	$2+i$	$2-i$	7	11	$3+2i$	$3-2i$
	$\delta_{\mathbb{Q}(i)} = (2) = (1+i)^2$	$\begin{vmatrix} 1 & 2 \\ 2 & 5 \end{vmatrix}$	1	$\backslash /$	1	1	$\backslash /$		
		2	3	5	7	11	13		
	$d = -2$	$\sqrt{2}i$	$1+\sqrt{2}i$	$1-\sqrt{2}i$	5	7	$3+\sqrt{2}i$	$3-\sqrt{2}i$	13
	$\delta_{\mathbb{Q}(\sqrt{2}i)} = (\sqrt{2})^3$	$\begin{vmatrix} 1 & 5 \\ 5 & 13 \end{vmatrix}$	$\backslash /$	1	1	$\backslash /$	1		
		2	3	5	7	11	13		
	$d = -3$	2	$\sqrt{3}i$	5	$\frac{1+3\sqrt{3}i}{2}$	$\frac{1-3\sqrt{3}i}{2}$	11	$1+2\sqrt{3}i$	$1-2\sqrt{3}i$
	$\delta_{\mathbb{Q}(\sqrt{3}i)} = (\sqrt{3})^3$	$\begin{vmatrix} 1 & 5 \\ 5 & 13 \end{vmatrix}$	$\backslash /$	1	$\backslash /$	1	$\backslash /$		
		2	3	5	7	11	13		
	$d = 2$	$\sqrt{2}$	3	5	$5-3\sqrt{2}$	$5+3\sqrt{2}$	11	13	$5+2\sqrt{2}$ $5-2\sqrt{2}$
	$\delta_{\mathbb{Q}(\sqrt{2})} = (\sqrt{2})^3$	$\begin{vmatrix} 1 & 5 \\ 5 & 13 \end{vmatrix}$	$\backslash /$	1	$\backslash /$	1	$\backslash /$		
		2	3	5	7	11	13	17	
	$d = 3$	$1+\sqrt{3}$	$\sqrt{3}$	5	7	$8+5\sqrt{3}$	$8-5\sqrt{3}$	$4+\sqrt{3}$	$4-\sqrt{3}$
	$\delta_{\mathbb{Q}(\sqrt{3})} = (1+\sqrt{3})^2(\sqrt{3})$	$\begin{vmatrix} 1 & 5 \\ 5 & 13 \end{vmatrix}$	$\backslash /$	1	$\backslash /$	$\backslash /$	$\backslash /$		
		2	3	5	7	11	13		

The following calculation need the theory of Frobenius element.

9) Legendre Symbol

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

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

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) Ramification

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

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

	$N(\varepsilon_0)$
$\sqrt{2} = [1, \overline{2}]$	$1 + \sqrt{2} \quad -$
$\sqrt{3} = [1, \overline{1, 2}]$	$2 + \sqrt{3} \quad +$
$\sqrt{5} = [2, \overline{4}]$	$2 + \sqrt{5} = \left[\frac{1}{2}(1 + \sqrt{5})\right]^3 -$
$\sqrt{6} = [2, \overline{2, 4}]$	$5 + 2\sqrt{6} \quad +$
$\sqrt{7} = [2, \overline{1, 1, 4}]$	$8 + 3\sqrt{7} \quad +$
$\sqrt{10} = [3, \overline{6}]$	$3 + \sqrt{10} \quad -$
$\sqrt{11} = [3, \overline{3, 6}]$	$10 + 3\sqrt{11} \quad +$
$\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$	$18 + 5\sqrt{13} = \left[\frac{1}{2}(3 + \sqrt{13})\right]^3 -$
$\sqrt{14} = [3, \overline{1, 2, 1, 6}]$	$15 + 4\sqrt{14} \quad +$
$\sqrt{15} = [3, \overline{1, 6}]$	$4 + \sqrt{15} \quad +$

$\sqrt{17} = [4, \overline{8}]$	$4 + \sqrt{17} \quad -$
$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}]$	$170 + 39\sqrt{19} \quad +$
$\sqrt{21} = [4, \overline{1, 1, 2, 1, 1, 8}]$	$55 + 12\sqrt{21} = \left[\frac{1}{2}(5 + \sqrt{21})\right]^3 +$
$\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$	$70 + 13\sqrt{29} = \left[\frac{1}{2}(5 + \sqrt{29})\right]^3 -$
$\sqrt{37} = [6, \overline{12}]$	$6 + \sqrt{37} \quad -$

x	2	3	5	6	7
x	10	11	13	14	15
17	x	19	21	22	23
x	26	x	29	30	31
32	33	34	35	37	38
41	42	43	x	46	47
x	x	51	53	x	55
57	58	59	61	62	x
65	66	67	69	70	71

$Cl(K)$:

Computing h by class number formula $K \subseteq \mathbb{Q}(\sqrt{N})$, $G = \text{Gal}(K/\mathbb{Q})$ abelian

$$K = \prod_{\substack{\chi \in \hat{G} \\ \chi \neq \chi_0}} L(\chi, 1)$$

$$K = \frac{2^r (2\pi)^r R_K h}{w |\Delta_K|^{\frac{1}{2}}}$$

$\chi \rightarrow \text{prim}$

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

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

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

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

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

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

with disc $= \Delta_K = \Delta$

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

(a) $\chi_{\Delta}(-1) = \text{sgn}(\Delta)$

(b) $\chi_{\Delta}(2) = \begin{cases} (-1)^{\frac{\Delta-1}{8}} \\ 0 \end{cases}$

$\Delta_K \equiv 1 \pmod{4}$

$\Delta_K \equiv 3 \pmod{4}$ or Δ_K even

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

p odd prime

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

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

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

$R = \text{Residue}$ $N = \text{Non-residue}$

$$\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right) = \frac{n}{2^{n-1}}$$

$\Delta_K = p$ $p \equiv 1 \pmod{4}$

$$\varepsilon^{2h} = \frac{\prod_{b \in N} \sin \frac{\pi b}{p}}{\prod_{a \in R} \sin \frac{\pi a}{p}}$$

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

$\Delta_K = -p$ $p \equiv 3 \pmod{4}$ $p \neq 3$

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

e.g.

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

$$h = 3 - \frac{2}{3} = 1$$

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

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

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

$$h = 5 - \frac{2}{11}(1+3+\dots) = 1$$

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

$$h = 7 - \frac{2}{19}(1+4+\dots) = 1$$

$$\binom{2}{19} = -1 \quad \binom{3}{19} = -1 \quad \binom{5}{19} = 1 \quad \binom{7}{19} = 1 \quad \binom{11}{19} = 1 \quad \binom{13}{19} = -1 \quad \binom{17}{19} = 1$$

$$\Delta_k = -23 \quad R=\{1 \sim 4, 6, 8, 9, 12, 13, 16, 18\}$$

$$h = 11 - \frac{2}{23}(1+2+\dots) = 3$$

$$\Delta_k = -31$$

$$R=\{1, 2, 4, 5, 7 \sim 10, 14, 16, 18 \sim 20, 25, 28\}$$

$$h = 15 - \frac{2}{31}(1+2+\dots) = 3$$

$$\Delta_k = -43$$

$$R=\{1, 4, 6, 9 \sim 11, 13 \sim 17, 21, 23 \sim 25, 31, 35, 36, 38, 40, 41\}$$

$$h = 21 - \frac{2}{43}(1+4+\dots) = 1$$

$$\Delta_k = -67$$

$$R = \left\{ 1, 4, 6, 9, 10, 14 \sim 17, 19, 21 \sim 26, 29, 33, \right. \\ \left. 35 \sim 37, 39, 40, 47, 49, 54 \sim 56, 59, 60, 62, 64, 65 \right\}$$

$$h = 33 - \frac{2}{67}(1+4+\dots) = 1$$

$$\Delta_k = -163$$

$$R = \left\{ 1, 4, 6, 9, 10, 14 \sim 16, 21, 22, 24 \sim 26, 33 \sim 36, 38 \sim 41, 43, 46, 47, \right. \\ 49, 51, 53 \sim 58, 60 \sim 62, 64, 65, 69, 71, 74, 77, 81, 83 \sim 85, 87, 88, 90, \\ 91, 93, 95 \sim 97, 100, 104, 111, 113, 115, 118, 119, 121, 126, 131 \sim 136, \\ \left. 140, 143 \sim 146, 150 \sim 152, 155, 156, 158, 160, 161 \right\}$$

$$h = 81 - \frac{2}{163}(1+4+\dots) = 1$$

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

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

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

$$\frac{\sqrt{13}}{2^6} \frac{1}{(\sin \frac{\pi}{13} \cdot \sin \frac{3\pi}{13} \cdot \sin \frac{4\pi}{13})^2} = \frac{1}{2}(3+\sqrt{13}) = \varepsilon^h \Rightarrow \sin \frac{\pi}{13} \cdot \sin \frac{3\pi}{13} \cdot \sin \frac{4\pi}{13} = \frac{\sqrt{13}}{2^3} \sqrt{\frac{1}{2}(\sqrt{13}-3)}$$

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

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

$$\Rightarrow \sin \frac{\pi}{17} \sin \frac{2\pi}{17} \sin \frac{4\pi}{17} \sin \frac{8\pi}{17} = \frac{1}{24} \sqrt{17-4\sqrt{17}}$$

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

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

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

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

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

$$\textcircled{3} v_1 = v_2 = 1$$

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

$$2 \quad \begin{pmatrix} 3 \\ \alpha+1 \end{pmatrix} \begin{pmatrix} 5 \\ \alpha-3 \end{pmatrix} \begin{pmatrix} 5 \\ \alpha^2+3\alpha-1 \end{pmatrix} \text{ etc...}$$

$$\begin{array}{ccccccc} 13 & & & & & & \\ \downarrow & & & & & & \\ 2 & 3 & 5 & 7 & 11 & 13 & 17 \end{array}$$

$$\begin{array}{ccccccc} 19 & \alpha+7 & \alpha^2-7\alpha+3 & \alpha+3 & \alpha^2-3\alpha+9 & \alpha+11 & \alpha-4 & \alpha-7 \\ \downarrow & \swarrow \searrow & & \swarrow \searrow & & \swarrow \searrow & \swarrow \searrow & \\ 19 & 23 & & 29 & & 31 & & \end{array}$$

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

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

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

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

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

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

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

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

4) By Frobenius element,

$p \equiv 0 \pmod{N}$ ramified

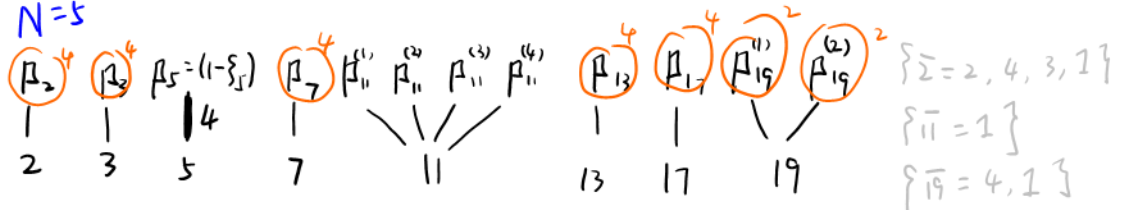
$p \equiv 1 \pmod{N}$ split

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

($N = p^k$ totally ramified)

In detail, Proposition 3.5.3. — The Frobenius element $\sigma_l \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is given by $\sigma_l(\zeta_N) = \zeta_N^l$. The decomposition group of each \mathfrak{l}_i is $D_{\mathfrak{l}_i} = \langle l \rangle \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$, 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 $N \mid (l^f - 1)$.

e.g. $N=5$



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

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

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

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

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}	$1-x^4+x^8-x^{12}+x^{16}-x^{20}+x^{24}$

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

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}	$1+x^4-x^{12}-x^{16}+x^{24}-x^{32}-x^{36}+x^{44}+x^{48}$

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

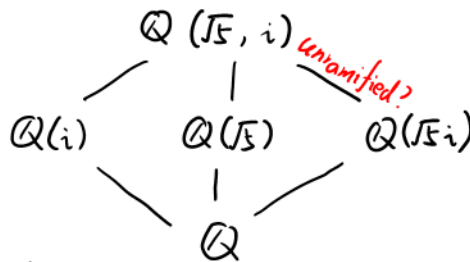
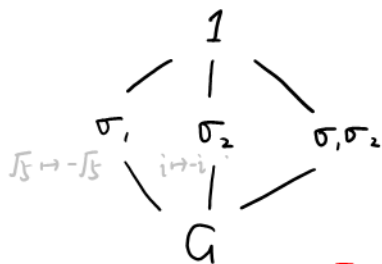
Φ_{25}	$1+x^5+x^{10}+x^{15}+x^{20}$
Φ_{49}	$1+x^7+x^{14}+x^{21}+x^{28}+x^{35}+x^{42}$
Φ_{121}	$1+x^{11}+x^{22}+x^{33}+x^{44}+x^{55}+x^{66}+\dots+x^{110}$

50 以内 乘积: $\Phi_{27} \Phi_{33} \Phi_{35} \Phi_{39} \Phi_{45}$

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

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

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



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

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

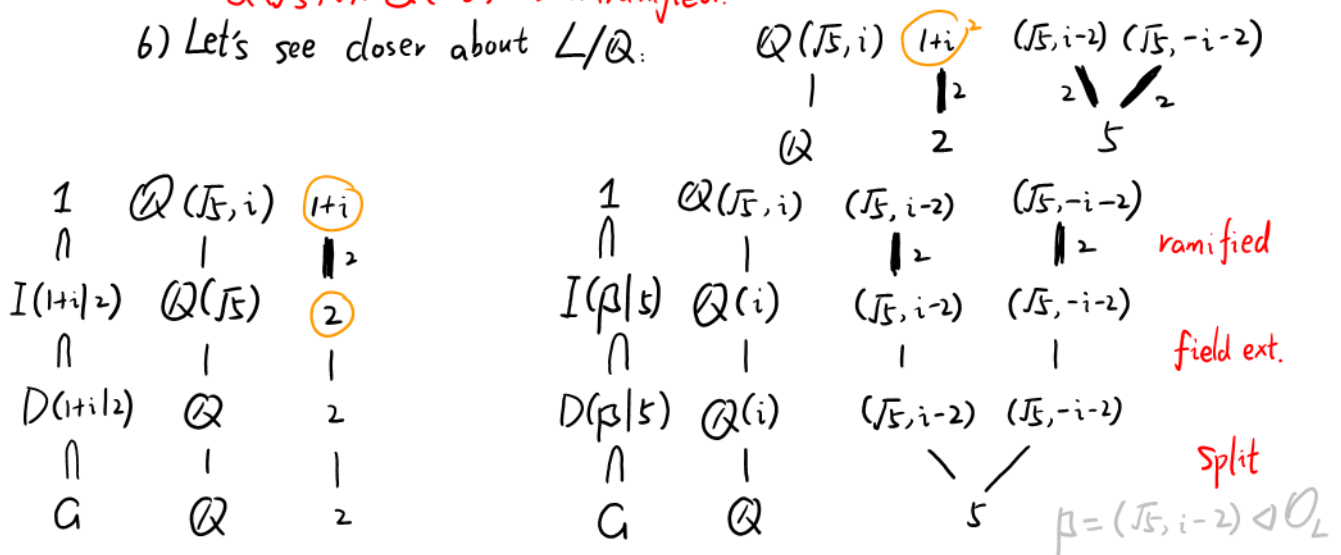
$\delta_{\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}} = (2\sqrt{-5})$ $\Delta_{\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}} = 2^4 \cdot 5^2$

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

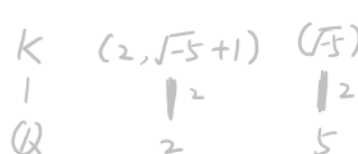
5) Since $\delta_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}} = (2\sqrt{-5}) \mathcal{O}_{\mathbb{Q}(\sqrt{-5})} \Rightarrow \delta_{\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})} = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$

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

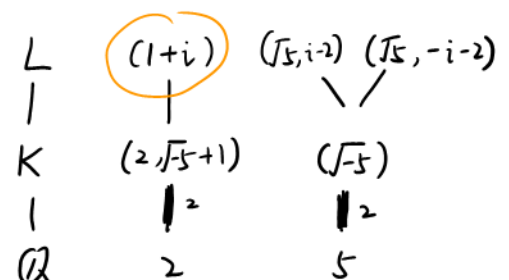
6) Let's see closer about L/\mathbb{Q} :



while K/\mathbb{Q} :



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



Local field

Teichmüller lift for $K = \mathbb{Q}_5$

$$\begin{aligned}
 [1] &= 1 & 1 &= [1] \\
 + [2] &= 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \dots & 2 &= [2] + [4] \cdot 5 + [3] \cdot 5^2 + [4] \cdot 5^3 + [2] \cdot 5^4 + \dots \\
 &\quad (2, 1, 2, 1, 3, 4, 2, 3, 0, 3, \dots) \\
 - [3] &= 3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + \dots & 3 &= [3] + [2] \cdot 5 + [1] \cdot 5^2 + [4] \cdot 5^3 + [2] \cdot 5^4 + \dots \\
 &\quad (3, 3, 2, 3, 1, 0, 2, 1, 4, 1, \dots) \\
 - [4] &= 4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots & [4] &= [4] + [1] \cdot 5 \\
 &\quad (4, 4, 4, 4, \dots)
 \end{aligned}$$

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

$$\begin{aligned}
 f(x) &= 5x^6 + x^5 + 3x^4 - x^3 - 2x + 3 \in \mathbb{Z}_5[x] \\
 \bar{f}(x) &= (x^2 - 2) \cdot (x^3 - 2x^2 + x + 1) := \bar{g}(x) \bar{h}(x) \in \mathbb{F}_5[x] \quad \pi = 5 \\
 \begin{cases} g_0(x) = x^2 - 2 \\ h_0(x) = x^3 - 2x^2 + x + 1 \end{cases} &\Rightarrow \begin{cases} f - g_0 h_0 = 5(x^6 + x^4 - x^2 + 1) := \pi f_1 & f_1 \in \mathbb{Z}_5[x] \\ a g_0 + b h_0 \equiv 1 \pmod{\pi} & \text{where } a, b \in \mathbb{Z}_5[x] \\ \begin{cases} a(x) = -2x^2 + 2x + 3 \\ b(x) = 2x + 2 \end{cases} \\ b f_1 = u g_0 + v & \text{where } u, v \in \mathbb{Z}_5[x] \\ \begin{cases} u(x) = 2x^5 + 2x^4 + 6x^3 + 6x^2 + 10x + 10 \\ v(x) = 22x + 22 \end{cases} \end{cases}
 \end{aligned}$$

$$\Rightarrow (a f_1 + u h_0) g_0 + v h_0 \equiv f_1 \pmod{\pi}$$

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

$$q_0(x) := \text{"deg} \leq 5 \text{ of } (a f_1 + u h_0)(x)" = 5x^6 + 11x^4 - 9x^2 + 22x + 13$$

$$\text{Let } g_1 = g_0 + \pi p_0 \quad h_1 = h_0 + \pi q_0$$

$$\begin{aligned}
 \Rightarrow g_1 h_1 &= f + \pi (g_0 h_0 - f) + \pi (p_0 h_0 + q_0 g_0) + \pi^2 p_0 q_0 \\
 &\equiv f + \pi (p_0 h_0 + q_0 g_0 - f) \equiv f \pmod{\pi^2}
 \end{aligned}$$

$$g_1 = x^2 + 110x + 108$$

$$h_1 = 55x^4 + x^3 - 47x^2 + 111x + 66$$