Algebraic Number Theory

Rough solutions Example Sheet 4

1. From lectures we know that K is unramified at p if $p \nmid 2d$, since then $T^2 - d$ is separable mod p.

On the other hand, if $p \mid d$, then $T^2 - d$ is Eisenstein in $\mathbb{Q}_p[T]$, so K is ramified at p.

It remains to deal with $p = 2$.

If $2 \mid d$, then $T^2 - d$ is Eisenstein at 2 so K is ramified.

If $2 \nmid d$, then we have the following:

K unramified at 2 $\Leftrightarrow$ $d \equiv 1 \bmod 4$.

One can see this as follows:

Consider $\mathbb{Q}_2(\sqrt{d})$. Recall that

$\mathbb{Q}_2^\times = \langle 2 \rangle \times \langle -1 \rangle \times (1 + 4\mathbb{Z}_2)$ and

$(\mathbb{Q}_2^\times)^2 = \langle 4 \rangle \times (1 + 8\mathbb{Z}_2)$ from Q12,

Sheet 1.

If $d \equiv 1 \bmod 8$, then $d \in (\mathbb{Q}_2^\times)^2$, so

$\mathbb{Q}_2(\sqrt{d}) = \mathbb{Q}_2$ and so 2 is split in K. *

Recall that $\mathbb{Q}_2(\sqrt{5}) = \mathbb{Q}_2(\sqrt{-3}) =$

$= \mathbb{Q}_2(\zeta_3)$ is the unramified quadratic

extension of $\mathbb{Q}_2$, so $\mathbb{Q}_2(\sqrt{d})$ is

---

* This is an equivalence, i.e.

2 is split in K $\Leftrightarrow$ $d \equiv 1 \ (8)$

see solution to Q12, Ex Sheet 1.

unramified $\iff$ $d \in \mathbb{Q}_5^{\times 2}$ $\iff$

$\iff$ $d \equiv 5 \mod 8$.

2. (i) We have (from lectures)

$$(\mathbb{Z}/4)^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_4)|\mathbb{Q})$$

and p splits in $\mathbb{Q}(\zeta_4) \iff p \equiv 1 \ (4)$

(recall that p is odd).

On the other hand, ~~$\zeta_4^3 = -\zeta_4$~~

ζ_4 has minimal polynomial $T^2+1 \ / \mathbb{Q}$,

which is separable mod p, so p splits

in $\mathbb{Q}(\zeta_4) \iff \left(\frac{-1}{p}\right) = 1$.

Therefore $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \ (4)$,

which is equivalent to $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

From lectures, we know that for p, q odd,

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

where $p^* = (-1)^{\frac{p-1}{2}} p$. Therefore

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) =$$

$$= (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \left(\frac{p}{q}\right) \Longrightarrow$$

$$\Longrightarrow \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Using multiplicativity of the Legendre symbol.

(ii) For concreteness let's consider $\mathbb{Q}(\zeta_8)$ as a subfield of $\mathbb{C}$.

Then we can take $\zeta_8 = \frac{1+i}{\sqrt{2}}$.

Since $i = \zeta_8^2$, we see that

$\sqrt{2} \in \mathbb{Q}(\zeta_8)$.

From lectures we have

$$(\mathbb{Z}/8)^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_8)|\mathbb{Q})$$

~~so $\in [\mathbb{Q}(\zeta_8):\mathbb{Q}]$~~

Also $\zeta_8 + \zeta_8^{-1} = \frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}} = \sqrt{2}$

so $\mathrm{Gal}(\mathbb{Q}(\zeta_8)|\mathbb{Q}(\sqrt{2}))$ corresponds to

$\{\pm 1\} \subseteq (\mathbb{Z}/8)^\times$ (~~we did~~ ~~this~~ recall

the computation of $\mathrm{Gal}(\mathbb{Q}(\zeta_{8n}+\zeta_{8n}^{-1})|\mathbb{Q})$

from lectures).

It follows that $\frac{(\mathbb{Z}/8)^\times}{\{\pm 1\}} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$

and that p splits in $\mathbb{Q}(\sqrt{2}) \iff$

$\iff p \equiv \pm 1 \bmod 8$

On the other hand $-1^2 - 2$ is separable mod p, so p splits in $\mathbb{Q}(\sqrt{2})$ $\iff$

$\iff \left(\frac{2}{p}\right) = 1$.

Therefore $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \ (8)$

Which is equivalent to $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

3. We know from lectures that

$$G^t(L_n|\mathbb{Q}_p) = \mathrm{Gal}(L_n|L_{m p^k})$$

when $k-1 < t \leq k$, $k = 0, 1, \ldots, e-1$,

and

$$G^0(L_n|\mathbb{Q}_p) = \mathrm{Gal}(L_n|L_m),$$

$$G^t(L_n|\mathbb{Q}_p) = 1 \quad \text{for} \quad t > e-1$$

We then have,

$$G^t(L_n'|\mathbb{Q}_p) \cong \frac{G^t(L_n|\mathbb{Q}_p)\,\mathrm{Gal}(L_n|L_n')}{\mathrm{Gal}(L_n|L_n')} =$$

$$= \begin{cases} \dfrac{\mathrm{Gal}(L_n|L_m)\,\mathrm{Gal}(L_n|L_n')}{\mathrm{Gal}(L_n|L_m')}, & t = 0, \\ \dfrac{\mathrm{Gal}(L_n|L_{m p^k})\,\mathrm{Gal}(L_n|L_n')}{\mathrm{Gal}(L_n|L_n')}, & k = 1, \ldots, e-1, \\ & k-1 < t \leq k, \\ 1, & t > e-1 \end{cases}$$

$$=$$

$$= \begin{cases} \mathrm{Gal}(L'_n \mid L'_n \cap L_m), & t = 0, \\ \mathrm{Gal}(L'_n \mid L'_n \cap L_{mp^k}), & k = 1, \dots, e-1, \\ & k-1 < t \le k \\ 1, & t > e-1. \end{cases}$$

(If one wants to analyse whether

$L'_n \cap L_{mp^k} = L_{mp^k}$ or L'_{mp^k}, or

when these are equal, it might be

useful to follow the suggestion in

the question)

4. We start with exp; we need to show that $\frac{x^n}{n!} \longrightarrow 0$ if $|x| < p^{-\frac{1}{p-1}}$.

Recall from the solution to Q11, sheet 1 that if $n = \sum_{i \geq 0} a_i p^i$ with $a_i \in \{0, \dots, p-1\}$, then

$$v_p(n!) = \frac{n - \sum_{i \geq 0} a_i}{p-1} \leq \frac{n}{p-1}$$

- In particular, $|n!| \geq p^{-\frac{n}{p-1}}$

and hence

$$\left| \frac{x^n}{n!} \right| \leq |x|^n p^{\frac{n}{p-1}} = \left(|x| p^{\frac{1}{p-1}} \right)^n$$

$\longrightarrow 0$ as $n \to \infty$ since

$|x| p^{\frac{1}{p-1}} < 1$ by assumption.

For $\log$, we need to show that $\left|\frac{x^n}{n}\right| \to 0$ if $|x| < 1$.

Note that we have $|n| \geq n^{-1}$, since $v_p(n) \leq \log_p(n)$ trivially.

Therefore

$$\left|\frac{x^n}{n}\right| \leq |x|^n \cdot n \longrightarrow 0 \quad \text{as } n \to \infty.$$

5. We claim that if $n > \frac{e}{p-1}$,

where e = ramification index of $K/\mathbb{Q}_p$

then

$$\pi_K^n \mathcal{O}_K \underset{\log}{\overset{\exp}{\rightleftarrows}} U_K^{(n)}$$

are well-defined homomorphisms and mutual inverses (and they are continuous).

Let $|\cdot|$ be the ext^n of $|\cdot|_p$ to K, and let $x \in \pi_K^n \mathcal{O}_K$.

Note that $|\pi_K^n| = p^{-n/e}$.

By Q4 on this sheet, we need K for $\exp: \pi_K \mathcal{O}_K \to$ [illegible] to be well-defined. We have $|x| < p^{-1/p-1}$. We have $|x| \leq (|\pi_K^n|) = p^{-n/e}$ and

$$p^{-n/e} < p^{-1/p-1} \iff n > \frac{e}{p-1}.$$

Note that $\log : U_K^{(n)} \longrightarrow K$ is well-defined for all $n \geq 1$.

Continue to assume $n > \frac{e}{p-1}$.

Claim: $\exp\left(\pi_K^n \mathcal{O}_K\right) \subseteq U_K^{(n)}$,

$\log\left(U_K^{(n)}\right) \subseteq \pi_K^n \mathcal{O}_K$.

Proof: For exp, if $x \in \pi_K^n \mathcal{O}_K$,

then for $m \geq 1$,

$$\left|\frac{x^m}{m!}\right| \leq |x|^m \, p^{\frac{m-1}{p-1}} \leq p^{\frac{m-1}{p-1} - \frac{mn}{e}} <$$

$$< p^{\frac{(m-1)n}{e} - \frac{mn}{e}} = p^{-\frac{n}{e}}, \text{ so } \frac{x^m}{m!} \in \pi_K^n \mathcal{O}_K$$

$$\Rightarrow \exp(x) \in U_K^{(n)}.$$

For log, $\left|\frac{x^m}{m}\right| \leq \left|\frac{x^m}{m!}\right|$ so $\frac{x^m}{m} \in \pi_K^n \mathcal{O}_K$

$$\Rightarrow \log(1+x) \in \pi_K^n \mathcal{O}_K.$$

Now, the usual "power series computations" show that log & exp are homomorphisms and mutual inverses.

For the second part, we have

$$K^\times = \langle \pi_K \rangle \times \{[x] \mid x \in \mathcal{O}_K^\times\} \times U_K^{(1)} \cong$$

($[x]$: Teichmüller lifts)

$$\cong \mathbb{Z} \times \mathbb{Z}/q-1 \times U_K^{(1)} .$$

$$\left(\mathcal{O}_K^\times / \mathcal{O}_K^{(1)}\right)$$

Note that $U_K^{(1)}$ is a $\mathbb{Z}_p$-module under

$$z \circ (1+x)^n = (1+x)^z = \sum_{n=0}^{\infty} \binom{z}{n} x^n ;$$

$$\binom{z}{n} = \frac{z(z-1)\cdots(z-n+1)}{n!} , \quad z \in \mathbb{Z}_p$$

note that this $\mathbb{Z}_p$-module structure extends

the natural $\mathbb{Z}$-module (i.e abelian group) structure, and is continuous, in that if $z_n \to z$ in $\mathbb{Z}_p$, then

$$(1+x)^{z_n} \longrightarrow (1+x)^z.$$

Now if $n > \frac{e}{p-1}$, $U_K^{(n)} \subseteq U_K^{(1)}$ is a $\mathbb{Z}_p$-submodule and log & exp are isomorphisms of $\mathbb{Z}_p$-modules (we have

$$\exp(zx) = \exp\left(\lim_{n\to\infty} z_n x\right) =$$

$$= \lim_{n\to\infty} \exp(z_n x) = \lim_{n\to\infty} \exp(x)^{z_n} =$$

$$= \exp(x)^z$$

if $z_n \to z$ and $z_n \in \mathbb{Z}_{\geq 0}$ and similarly for log)

It follows that $U_K^{(n)} \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ so

since $U_K^{(1)}/U_K^{(n)}$ is finite, $U_K^{(1)}$ is a finitely generated $\mathbb{Z}_p$-module of rank $[K:\mathbb{Q}_p] \Rightarrow$

$$\Rightarrow U_K^{(1)} \cong \mathbb{Z}/p^a \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$$

for some $a \in \mathbb{Z}_{>0}$.

It follows that

$$K^\times \cong \mathbb{Z} \times \mathbb{Z}/q-1 \times \mathbb{Z}/p^a \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$$

as desired, as topological groups even, where $\mathbb{Z}$, $\mathbb{Z}/q-1$ & $\mathbb{Z}/p^a$ have the discrete topology and the product has the product topology.

To see that any finite index subgroup then $K^\times$ is open it suffices to show

Hat any finite index subgroup of $\mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ is open. Set $d = [K:\mathbb{Q}_p]$ and let $H \leq \mathbb{Z}_p^d$ have index N.

Then $N\mathbb{Z}_p^d \leq H$ and $N\mathbb{Z}_p^d = p^{v_p(N)}\mathbb{Z}_p^d$ is open in $\mathbb{Z}_p^d$, so H is open (H is the union of all $N\mathbb{Z}_p^d$-cosets in H, all of which are open).

6. We start by computing the class group of K.

The Minkowski bound is

$$\sqrt{56}\left(\frac{4}{\pi}\right)\frac{2}{4} = \frac{2\sqrt{56}}{\pi} < 5,$$

($\sqrt{56}$: discriminant)

so Cl_K are generated by (ideals above primes) of norms 2 and 3.

One checks that $\mathcal{O}_K = \mathbb{Z}[2\sqrt{-14}]$

(by directly deciding when $x+y\sqrt{-14}$, $x,y \in \mathbb{Q}$, is an algebraic integer),

so Dedekind's theorem implies that

$$2\mathcal{O}_K = \underbrace{(2, \sqrt{-14})^2}_{\mathfrak{p}_2^2}$$

and $$3\mathcal{O}_K = \underbrace{(3, 1+\sqrt{-14})}_{\mathfrak{p}_3}\underbrace{(3, 1-\sqrt{-14})}_{\mathfrak{p}_3}$$

(here $X^2+14 \equiv X^2 \bmod 2$, $X^2+14 \equiv (X-1)(X+1) \bmod 3$)

Write $\mathfrak{p}_2 = (2, 1+\sqrt{-14})$

~~the element $2+\sqrt{-14}$ has norm 18~~,

$\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3'$ are not principal,

since no element has norm 2 or 3.

the element $2+\sqrt{-14}$ has norm 18

$$\Rightarrow (2+\sqrt{-14}) = \begin{cases} \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3' & \text{or} \\ \mathfrak{p}_2\mathfrak{p}_3^2 & \text{or} \\ \mathfrak{p}_2\mathfrak{p}_3'^2 \end{cases}$$

But $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3' = \mathfrak{p}_2 \neq 1$ in Cl_K,

~~so either~~ and $(2+\sqrt{-14}) = 1$ in Cl_K,

so this can't be.

We deduce that $\mathfrak{p}_2 = \mathfrak{p}_3^2 = \mathfrak{p}_3'^2 \neq 1$,

(using $\mathfrak{p}_2^2 = 1$) in Cl_K, so

$Cl_K \cong \mathbb{Z}/4$, generated by $\mathfrak{p}_3$

Next, we prove that $L|\mathbb{Q}$, and hence $L|K$, is Galois.

Claim: $L|\mathbb{Q}$ is the splitting field of T^4+2T^2-7.

Pf: ~~We have~~ Set $\beta = 2\sqrt{2}-1$, $\beta' = -2\sqrt{2}-1$ and let $\gamma = \sqrt{2\sqrt{2}-1}$ i.e. the generator of $L|K$ by definition.

We have $\beta+\beta' = -2$, $\beta\beta' = -7$

$$\Rightarrow (T^2-\beta)(T^2-\beta') = T^4+2T^2-7$$

so $\pm\gamma$ is a root of T^4+2T^2-7.

We have $\sqrt{2} = \frac{\beta+1}{2}$, and $\sqrt{-4} \in K \subseteq L$, so $\sqrt{-7} \in L$, and $\left(\frac{\sqrt{-7}}{\gamma}\right)^2 = \frac{-7}{\beta} = \beta'$, so

$\pm \frac{\sqrt{-7}}{6}$ are the other two roots of $T^4 + 2T^2 - 7$

This shows that L contains the splitting field, and running the calculations shows that $L = \mathbb{Q}(\sqrt{6}, \sqrt{2}, \sqrt{-7})$ is contained in the splitting field. □

Next we show that L/K is unramified. For this, we use the following lemma:

Lemma: Let F be a number field and let $u \in \mathcal{O}_F$ be a non-square. Let $\mathfrak{p}$ be a prime of F with $u \notin \mathfrak{p}$, and let $E = F(\sqrt{u})$

Then $\mathfrak{p}$ is unramified in E if either

(a) $2 \notin \mathfrak{p}$ or

(b) $2 \in \mathfrak{p}$ and $\exists\, b, c \in \mathcal{O}_F$ s.t. $u = b^2 - 4c$.

Pf: If (a) holds, then the discriminant of $T^2 - u$, which is $-4u$, is not in $\mathfrak{p}$, so $T^2 - u$ is seperable mod $\mathfrak{p}$ $\Rightarrow$ E unramified at $\mathfrak{p}$.

If (b) holds, then E is also the splitting field of $T^2 + bT + c$ over F, and this has discriminant $u \notin \mathfrak{p}$, so it's seperable mod $\mathfrak{p}$ and hence E is unramified at $\mathfrak{p}$. $\square$

We now use this.

Set $M = K(\sqrt{2}) \subseteq L$.

Note that M/K is quadratic and that $M = K(\sqrt{-7})$ (since $\sqrt{-M} \in K$) as well.

Let $\mathfrak{p}$ be a prime in K.

If $2 \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified in $M = K(\sqrt{2})$ by the Lemma.

If $2 \in \mathfrak{p}$, we use the description $M = K(\sqrt{-7})$ and that $-7 = 1^2 - 4 \cdot 2$ to conclude that M/K is unramified at $\mathfrak{p}$ by criterion (b) in the Lemma.

In conclusion, M/K is unramified everywhere.

It remains to show that L/M is quadratic and unramified everywhere.

L/M quadratic

This is equivalent to $[L:\mathbb{Q}] = 8$.

First, we can check by direct calculation that $\gamma \notin \mathbb{Q}(\sqrt{2})$, so

$[\mathbb{Q}(\gamma):\mathbb{Q}(\sqrt{2})] = 2 \Rightarrow$

$\Rightarrow [\mathbb{Q}(\gamma):\mathbb{Q}] = 4 \leq [L:\mathbb{Q}]$.

If we have equality, then $\mathbb{Q}(\gamma) = L$, but $\mathbb{Q}(\gamma)$ is not Galois since it has both real and complex embeddings. Get $L \supsetneq \mathbb{Q}(\gamma)$ and $[L:\mathbb{Q}] = 8$.

L/M unramified everywhere

We use the lemma. Note that $L = M(\sqrt{\beta}) = M(\sqrt{\beta'})$, and that, since $\beta + \beta' = -2$ and $\beta\beta' = -7$, $(\beta, \beta') \supseteq (2, 7) = (1)$ so

β and β' are coprime

Let $\mathfrak{q}$ be a prime of H.

If $2, \beta \notin \mathfrak{q}$, then $\mathfrak{q}$ is unramified in $L = H(\sqrt{\beta})$ by the lemma.

If $2 \in \mathfrak{q}$, $\beta \notin \mathfrak{q}$, then since $\beta = (1+\sqrt{2})^2 - 4 \cdot 1$, criterion (b) of the lemma shows that $\mathfrak{q}$ is unramified.

If $\beta \in \mathfrak{q}$, then $\beta' \notin \mathfrak{q}$ (by coprimality), and moreover $2 \notin \mathfrak{q}$ ($2, \beta \in \mathfrak{q} \Rightarrow \beta' \in \mathfrak{q}$ ##)

so the lemma implies that $\mathfrak{q}$ is unramified in $L = H(\sqrt{\beta'})$.

7. Let $K = \mathbb{Q}(\sqrt{-23})$, $p \neq 23$.

Recall from lectures that

$$\mathcal{O}_K = \mathbb{Z}[\alpha], \quad \alpha = \frac{1+\sqrt{-23}}{2}$$

and that

$$N(x+y\alpha) = x^2 + xy + 6y^2$$

Thus $p = x^2 + xy + 6y^2$ has a solution if and only if p splits into two principal prime ideals in K.

First, note that p splits in K $\iff$ T^2+23 splits mod p $\iff$ T^2+23 has a root in $\mathbb{F}_p$.

Next, recall from lectures that the Hilbert class field of K is

M is the splitting field of $T^3 - T + 1$, which is an S_3-extension of $\mathbb{Q}$.

Let $L/\mathbb{Q}$ be an ext^n obtained by adjoining a root of $T^3 - T + 1$.

Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$ dividing p.

Then, from lectures, $\mathfrak{p}$ is principal $\iff$ $\mathfrak{p}$ is totally split in M/K.

Therefore, $p = x^2 + xy + 6y^2$ has a solution $\iff$ p is totally split in $M/\mathbb{Q}$. $\iff$ p totally split in $L/\mathbb{Q}$ and $K/\mathbb{Q}$

$\iff$ $T^3 - T + 1$ and $T^2 + 23$ have roots in $\mathbb{F}_p$.

8. Let H be the Hilbert class field of K.

From lectures, we know that $[H:K] = h_K$, and that H/K is everywhere unramified and the real places stay real.

Note that all places of K are real, so all places of H are real.

Claim: HL/L is everywhere unramified, and $[HL:L] = h_K$.

Proof: HL/L is everywhere unramified since H/K is.

To check that $[HL:L] = h_K$,

we need to check that

$H \cap L = K$. But this is

clear since all places of

H are real, so all places of

$H \cap L$ are real $\Rightarrow$ $H \cap L \subseteq K$

(and $K \subseteq H \cap L$ trivially)

Moreover, HL/L is Galois since H/K is,

and $Gal(H/K) \xrightarrow{\sim} Gal(HL/L)$ so

HL/L is abelian.

It follows that HL is contained

in the Hilbert class field H of L

(since H is the maximal abelian ext^n of

L which is unramified everywhere)

so $h_K = [HL : L] \mid [H : L] = h_L$.

9. (i) We have

$$\mathrm{Art}_{\mathbb{Q}_p} : \mathbb{Q}_p^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}_p^{ab} \mid \mathbb{Q}_p)$$

$$\downarrow$$

$$\mathrm{Gal}(K \mid \mathbb{Q}_p)$$

and the induced map

$$\mathbb{Q}_p^\times \longrightarrow \mathrm{Gal}(K \mid \mathbb{Q}_p)$$

is surjective with kernel $N(K \mid \mathbb{Q}_p)$

Since $\mathrm{Art}_{\mathbb{Q}_p}(\mathbb{Z}_p^\times) = \mathrm{Gal}(\mathbb{Q}_p^{ab} \mid \mathbb{Q}_p^{ur}) \leq$

$$\leq \mathrm{Gal}(\mathbb{Q}_p^{ab} \mid K)$$

we must have $\mathbb{Z}_p^\times \leq N(K \mid \mathbb{Q}_p)$

Thus $N(K \mid \mathbb{Q}_p)$ corresponds to a subgroup of $\mathbb{Q}_p^\times / \mathbb{Z}_p^\times \cong \mathbb{Z}$ of index f, of which there is only one,

so $N(K \mid \mathbb{Q}_p) = \langle p^f \rangle \times \mathbb{Z}_p^\times$.

(ii) $N_{L|\mathbb{Q}_p}(1-\zeta_{p^n}) =$

$$= \prod_{a \in (\mathbb{Z}/p^n)^\times} (1-\zeta_{p^n}^a) = \Phi_{p^n}(1) = p$$

Therefore, $N(L|\mathbb{Q}_p)$ is a subgroup of $\mathbb{Q}_p^\times$ which contains p, and has index $p^{n-1}(p-1)$ by local class field theory; so $N(L/\mathbb{Q}_p)$ corresponds to a subgroup of $\mathbb{Q}_p^\times/\langle p\rangle \cong \mathbb{Z}_p^\times$ of index $p^{n-1}(p-1)$.

The only subgroup of $\mathbb{Z}_p^\times$ of index $p^{n-1}(p-1)$ is $1+p^n\mathbb{Z}_p$.

(this can be seen e.g. by induction on n, using that $1+p^n\mathbb{Z}_p \cong p^n\mathbb{Z}_p$ via the exponential)

Therefore $N(L/\mathbb{Q}_p) = \langle p\rangle \times (1+p^n\mathbb{Z}_p)$

(iii) Now let $K/\mathbb{Q}_p$ be finite abelian.

Since $N(K/\mathbb{Q}_p) \leq \mathbb{Q}_p^\times$ is open and of finite index, we can find f, n s.t.

$$N(K/\mathbb{Q}_p) \supseteq \langle p^f \rangle \times (1+p^n\mathbb{Z}_p)$$

But

$$\langle p^f \rangle \times (1+p^n\mathbb{Z}_p) =$$

$$= \left(\langle p^f \rangle \times \mathbb{Z}_p^\times\right) \cap \left(\langle p \rangle \times (1+p^n\mathbb{Z}_p)\right)$$

$$= N(K_f/\mathbb{Q}_p) \cap N(L_n/\mathbb{Q}_p) =$$

$$= N(K_f L_n/\mathbb{Q}_p) = N(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p),$$

where $K_f = \mathbb{Q}_p(\zeta_{p^f-1})$ is the unique unramified ext^n of deg f, $L_n = \mathbb{Q}_p(\zeta_{p^n})$ and $m = p^n(p^f-1)$

Therefore $N(K/\mathbb{Q}_p) \supseteq N(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p)$

which implies that $K \subseteq \mathbb{Q}_p(\zeta_m)$.

10. (i) $X^{p-1} - \zeta_p$ is Eisenstein @ π,

so K_ζ is totally ramified of

degree $p-1$.

If $\alpha \in K_\zeta$ is a root of $X^{p-1} - \zeta_p$,

then the other roots are $\alpha\zeta^i$, $i = 0, \dots, p-2$

which are also in K_ζ, so $K_\zeta / \mathbb{Q}_p$ is

Galois.

(ii) Let $K/\mathbb{Q}_p$ be totally ramified

of degree $p-1$ and let $\pi \in K$ be

a uniformizer.

Then $\pi^{p-1} = pu$ for some $u \in \mathcal{O}_K^\times$.

Since $\psi_K = \psi_p$, $u = \zeta v$

for some $(p-1)$th root of 1 ζ and

$v \in 1 + \pi\mathcal{O}_K$.

~~Claim~~ The polynomial

$X^{p-1} - v \in \mathcal{O}_K[X]$

has a root modulo π $(X=1)$

and is seperable mod π, so by

Hensel's lemma $\exists\ b \in \mathcal{O}_K^\times$ s.t

$$b^{p-1} = v$$

Summing up, we have

$$\pi^{p-1} = p\zeta b^{p-1} \Longrightarrow$$

$$\Longrightarrow (\pi b^{-1})^{p-1} = p\zeta \Longrightarrow$$

$$\Longrightarrow K_\zeta \subseteq K \Longrightarrow K_\zeta = K \text{ since}$$

the degrees match.

(iii) : Since K_ζ contains a root of $X^{p-1} = p\zeta$, we have $-p\cdot\zeta \in N(K_\zeta | \mathbb{Q}_p)$

So $N(K_\zeta | \mathbb{Q}_p)$ has index $p-1$ and by local class field theory (note that $K_\zeta | \mathbb{Q}_p$ is

abelian:

$$\mathrm{Gal}(K_\zeta | \mathbb{Q}_p) \xrightarrow{\alpha} \{1, \zeta, \dots, \zeta^{p-2}\}$$

$$\sigma \longmapsto \frac{\sigma\alpha}{\alpha}$$

where α is a root of $X^{p-1} - \zeta_p$)

and contains $-p\zeta \Rightarrow$

$$\Rightarrow \quad N(K_\zeta | \mathbb{Q}_p) = \langle -p\zeta \rangle \times (1 + p\mathbb{Z}_p)$$

(here we argue as in Q9(ii):

we have $\mathbb{Q}_p^\times = \langle -p\zeta \rangle \times \mathbb{Z}_p^\times$

↑ unit number

so $N(K_\zeta | \mathbb{Q}_p)$ corresponds to the unique subgroup of $\mathbb{Q}_p^\times / \langle -p\zeta \rangle \cong \mathbb{Z}_p^\times$ of index $p-1$).

Since $N(\mathbb{Q}_p(\zeta_p) | \mathbb{Q}_p) = \langle p \rangle \times (1 + p\mathbb{Z}_p)$

by Q9(ii), we get that

$$\mathbb{Q}_p(\zeta_p) = K_{-1}.$$

11. Set $M = K(\zeta_n) = K \cdot \mathbb{Q}(\zeta_n)$

Since $K/\mathbb{Q}$ & $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ are unramified outside S, $M/\mathbb{Q}$ is unramified outside S.

Let $p \in S$, take $\mathfrak{p}$ in K above p and $\mathfrak{q}$ in M above $\mathfrak{p}$.

Then

$$M_{\mathfrak{q}} = K_{\mathfrak{p}}(\zeta_n) \subseteq$$

$$\subseteq \mathbb{Q}_p(\zeta_{n_p}, \zeta_n)$$

and $M_{\mathfrak{q}} \supseteq \mathbb{Q}_p(\zeta_{p^{e_p}})$.

Since $\mathbb{Q}_p(\zeta_{n_p}, \zeta_n) \mid \mathbb{Q}_p(\zeta_{p^{e_p}})$ is unramified (it is generated by roots of unity of order prime to p),

$M_{\mathfrak{q}} / \mathbb{Q}_p(\zeta_{p^{e_p}})$ is unramified and

hence $M_{\mathfrak{q}} = \mathbb{Q}_p(\zeta_{p^{e_p} n'}) =$

$$= \mathbb{Q}_p(\zeta_{p^{e_p}}) \cdot \mathbb{Q}_p(\zeta_{n'})$$

for some n' with $(n', p) = 1$.

It follows that the inertia group

$I_p = I_{\mathfrak{q}|p}$ satisfies

$$I_p \cong \mathrm{Gal}\left(M_{\mathfrak{q}} \,|\, \mathbb{Q}_p(\zeta_{n'})\right) \cong \mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{p^{r_p}}) \,|\, \mathbb{Q}_p\right)$$

($\mathbb{Q}_p(\zeta_{n'})$ = max unramified subext^n of $M_{\mathfrak{q}}$)

so $\#I_p = \varphi(p^{r_p})$

(φ = Euler φ-function)

(recall that, since $M|\mathbb{Q}$ is abelian, $I_{\mathfrak{q}|p}$ is independent of $\mathfrak{q}$).

Let I be the product of all the I_p, for $p \in S$, inside $\mathrm{Gal}(H|\mathbb{Q})$

The fixed field of I is an ext^n of $\mathbb{Q}$ which is unramified everywhere.

By Minkowski's theorem the fixed field must be $\mathbb{Q}$, so

$$I = \mathrm{Gal}(M/\mathbb{Q})$$

But $$\#I \leq \prod_{p \in S} \#I_p = \prod_{p \in S} \varphi(p^{e_p}) =$$

$$= \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$$

Since $M \supseteq \mathbb{Q}(\zeta_n)$, it follows that we must have an equality, and that $M = \mathbb{Q}(\zeta_n)$ as desired.

We then conclude that

$$K \subseteq K(\zeta_n) = M = \mathbb{Q}(\zeta_n),$$

as desired.