Algebraic number theory midterm exam (at home)

There are 11 parts to this exam, and the total is 100 points. You are free to use all the results seen in class. Please do this at home midterm exam on your own. In order to get full points, you need to justify carefully your answers. Feel free to ask me if you do not understand some notation. You may use the following results without justification.

- Theorem: There is no finite extension K of $\mathbb{Q}$ which is unramified at every prime ideal of $\mathbb{Z}$ (this is a consequence of the Hermite–Minkowski inequality for $|\ \mathrm{Disc}_K\ |$).
- (Kummer theory) Let L be a field and $n \geq 1$ be an integer such that F contains n distinct nth roots of unity. Let M be a finite Galois extension of L such that $\mathrm{Gal}(M/L)$ is an abelian group of exponent n. Then there exists a finite subset $\Delta \subset L^\times/(L^\times)^n$ such that M is obtained by adjoining to L (all) nth roots of all elements of Δ.

  Notation: We shall fix implicitly an algebraic extension $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ for every prime $p \geq 2$. If $n \geq 1$ is an integer, we denote by ζ_n a primitive nth root in $\overline{\mathbb{Q}}$ or $\overline{\mathbb{Q}}_p$ depending on the context.

The Kronecker–Weber Theorem

The goal of this exam is to prove the Kronecker–Weber theorem:

Theorem 0.1 (Kronecker–Weber) *Let K be a finite abelian extension of $\mathbb{Q}$. Then there exists $n \geq 1$ such that $K \subset \mathbb{Q}(\zeta_n)$.*

We shall follow the following steps.

Q1 (5 points). Let $K/\mathbb{Q}$ be a Galois extension. Then $\mathrm{Gal}(K/\mathbb{Q})$ is generated by the set of inertia subgroups $I_\mathfrak{p}$ when $\mathfrak{p}$ goes through the primes of $\mathcal{O}_K$.

Q2 (5 points). Conclude that if $K/\mathbb{Q}$ is a finite abelian extension, then $[K : \mathbb{Q}] \leq \prod_{p \geq 2} e_p$ where p goes through the prime numbers and e_p is the ramification index of p in K.

Q3 (15 points). The local Kronecker–Weber theorem states that any finite abelian extension E of $\mathbb{Q}_p$ (where $p \geq 2$ is a prime) is contained in $\mathbb{Q}_p(\zeta_n)$ for some $n \geq 1$. The goal of this question is to prove that the local Kronecker–Weber theorem implies Theorem 0.1. You may proceed as follows (you can also use your own way if you wish). Let $K/\mathbb{Q}$ be finite abelian. For each prime p ramifying in K, let $\mathfrak{p}$ above p in K and let $n_p \geq 1$ such that $K_\mathfrak{p} \subset \mathbb{Q}_p(\zeta_{n_p})$ (by the local KW theorem). Let a_p be the p-adic valuation of n_p. Then we let $n := \prod_p p^{a_p}$. Prove that $K \subset \mathbb{Q}(\zeta_n)$.

The rest of this exam is thus devoted to prove the local KW theorem.

Q4 (5 points). Let L/K an unramified finite Galois extension, where L and K are finite extensions of $\mathbb{Q}_p$ (for some prime $p \geq 2$). Prove that $L = K(\zeta_n)$ for some $n \geq 1$ with $p \nmid n$.

Q5 (10 points). Prove that $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\alpha)$ for some $\alpha \in \mathbb{Q}_p(\zeta_p)$ with $\alpha^{p-1} = -p$.

Q6 (15 points). Prove the local KW theorem when $K/\mathbb{Q}_p$ is tamely ramified. (Hint: Let e be the ramification index of $K/\mathbb{Q}_p$. Prove that $e \mid p-1$ by proving that $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ is totally ramified. You may use the description of tamely ramified extensions we have seen in class.)

From now on, we assume that p is odd. The case $p = 2$ of the local KW theorem is proved in a similar way, and we shall not consider it. We assume that K is a wildly ramified finite abelian extension of $\mathbb{Q}_p$.

Q7 (5 points). Explain why it suffices to consider the case where $\mathrm{Gal}(K/\mathbb{Q}_p) \simeq \mathbb{Z}/p^m\mathbb{Z}$ for some $m \geq 1$ in order to prove the local KW theorem.

We thus assume from now on that $\mathrm{Gal}(K/\mathbb{Q}_p) \simeq \mathbb{Z}/p^m\mathbb{Z}$ for some $m \geq 1$.

Q8 (5 points). Let E_u be the unique unramified extension of $\mathbb{Q}_p$ with $\mathrm{Gal}(E_u/\mathbb{Q}_p) \simeq \mathbb{Z}/p^m\mathbb{Z}$. Let E_r be the unique subextension of $\mathbb{Q}_p(\zeta_{p^{m+1}})$ such that $\mathrm{Gal}(E_r/\mathbb{Q}_p) \simeq \mathbb{Z}/p^m\mathbb{Z}$. Justify the existence of E_u and E_r. Prove that if K is contained in $E_u \cdot E_r$ (the compositum of E_u and E_r in $\overline{\mathbb{Q}}_p$), then the local KW theorem holds for K.

Q9 (10 points). Assume for a contradiction that K is not contained in $E_u \cdot E_r$. Let L be the compositum of K and $E_u \cdot E_r$ in in $\overline{\mathbb{Q}}_p$. Prove that there exists some subextension E of L such that $\mathrm{Gal}(E/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$.

In the last part of this exam, we prove that there is no abelian extension E of $\mathbb{Q}_p$ with $\mathrm{Gal}(E/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$.

Q10 (10 points). Let L be a field of characteristic $\neq p$ and let $\zeta_p \in \overline{L}$ a primitive pth root of unity. Define a character $\omega : \mathrm{Gal}(L(\zeta_p)/L) \to (\mathbb{Z}/p\mathbb{Z})^\times$ by the formula $g(\zeta_p) = \zeta_p^{\omega(g)}$ for all $g \in \mathrm{Gal}(L(\zeta_p)/L)$. Let $a \in L(\zeta_p)^\times$ and let $M = L(\zeta_p, a^{1/p})$. Show that if M/L is abelian, then $g(a) \equiv a^{\omega(g)}$ (modulo $(L(\zeta_p)^\times)^p$). (This means that $g(a)$ is equal to $a^{\omega(g)}$ up to a pth power in $L(\zeta_p)$.)

Q11 (15 points). Prove that there is no extension E of $\mathbb{Q}_p$ with $\mathrm{Gal}(E/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$. (Hint: consider $E(\zeta_p)$ as an extension of $\mathbb{Q}_p(\zeta_p)$ and use Kummer theory.)

The Kronecker–Weber Theorem.

Q1. Let $p \in \mathbb{Z}$ be a prime number. Let $\mathfrak{P} \subset \mathcal{O}_K$ be a prime above p.

We define the decomposition group $D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$.

There is an epimorphism $\varphi : D_{\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} \,/\, \mathbb{Z}/(p))$.

Let $e = e(\mathfrak{P}|p)$, $f = f(\mathfrak{P}|p)$, $n = [K:\mathbb{Q}] = efr$.

Then $\#D_{\mathfrak{P}} = \frac{n}{r} = ef$ because $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the set of primes above p.

$I_{\mathfrak{P}} = \ker\varphi$; $\#I_{\mathfrak{P}} = \dfrac{\#D_{\mathfrak{P}}}{\#\mathrm{Gal}((\mathcal{O}_K/\mathfrak{P})/(\mathbb{Z}/(p)))} = \dfrac{ef}{f} = e$.

Let $K^{D_{\mathfrak{P}}}$ be the fixed field of $D_{\mathfrak{P}}$, $K^{I_{\mathfrak{P}}}$ be the fixed field of $I_{\mathfrak{P}}$.

Let $\mathfrak{P}' = \mathfrak{P} \cap K^{I_{\mathfrak{P}}}$, $\mathfrak{P}'' = \mathfrak{P} \cap K^{D_{\mathfrak{P}}}$. We have an epimorphism:

$$\psi : I_{\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}\left(\cancel{K/K^{I}}(\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_{K^{I_{\mathfrak{P}}}}/\mathfrak{P}')\right).$$

Because $I_{\mathfrak{P}}$ is exactly the decomposition group of the extension $K/K^{I_{\mathfrak{P}}}$.

By the definition of $I_{\mathfrak{P}}$, we see that $\mathrm{Gal}(\mathcal{O}_K/\mathfrak{P} / \mathcal{O}_{K^{I_{\mathfrak{P}}}}/\mathfrak{P}')$ must be trivial, i.e.

$f(\mathfrak{P}|\mathfrak{P}') = 1$. Since $\mathfrak{P}$ is the only prime in $\mathcal{O}_K$ above $\mathfrak{P}'$, we have $e(\mathfrak{P}|\mathfrak{P}')\, f(\mathfrak{P}|\mathfrak{P}') = \#I_{\mathfrak{P}}$

Then we have $e(\mathfrak{P}|\mathfrak{P}') = e$. Thus $e(\mathfrak{P}'|p) = \dfrac{e(\mathfrak{P}|p)}{e(\mathfrak{P}|\mathfrak{P}')} = \dfrac{e}{e} = 1$.

~~Since $\mathfrak{P}$ is an arbitrary prime in $\mathcal{O}_K$ above~~ Let G be the group generated by the set of inertia subgroups $I_{\mathfrak{P}}$ when $\mathfrak{P}$ goes through the primes of $\mathcal{O}_K$. Clearly $K^G \subset K^{I_{\mathfrak{P}}}$ $\forall$ prime $\mathfrak{P} \subset \mathcal{O}_K$. By the previous discussion we see that p is unramified in K^G, $\forall p \in \mathbb{Z}$ prime.

Since there is no finite extension K of $\mathbb{Q}$ which is unramified at every prime ideal of $\mathbb{Z}$, K^G must be $\mathbb{Q}$. By Galois theory, $G = \mathrm{Gal}(K/\mathbb{Q})$. ☒.

Q2.

Let $p \in \mathbb{Z}$ be a prime, $\mathfrak{p} \in \mathcal{O}_K$ be a prime ideal above p. $\because D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$.

If $\mathfrak{p}' \subset \mathcal{O}_K$ be another prime above p. then $\mathfrak{p}' = \tau(\mathfrak{p})$ for some $\tau \in \mathrm{Gal}(K/\mathbb{Q})$.

$D_{\mathfrak{p}'} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}') = \mathfrak{p}'\} = \tau D_{\mathfrak{p}} \tau^{-1}$. Since $K/\mathbb{Q}$ is abelian, $D_{\mathfrak{p}'} = D_{\mathfrak{p}}$.

Consider $\varphi: D_{\mathfrak{p}} \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \,/\, \mathbb{Z}/(p))$. $I_{\mathfrak{p}} = \ker \varphi$.

$\varphi': D_{\mathfrak{p}'} \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p}' / \mathbb{Z}/(p))$, $I_{\mathfrak{p}'} = \ker \varphi'$.

Note that $\tau: K/\mathbb{Q} \to K/\mathbb{Q}$ induces an isomorphism.

$$\mathcal{O}_K/\mathfrak{p} \longrightarrow \mathcal{O}_K/\mathfrak{p}'$$

which fixes $\mathbb{Z}/(p)$. Then we have. $\tau^{-1} I_{\mathfrak{p}'} \tau \subset I_{\mathfrak{p}}$, $\tau I_{\mathfrak{p}} \tau^{-1} \subset I_{\mathfrak{p}'}$.

Thus $I_{\mathfrak{p}'} = \tau I_{\mathfrak{p}} \tau^{-1} = I_{\mathfrak{p}}$. We see $I_{\mathfrak{p}}$ only depends on $\mathfrak{p} \cap \mathbb{Z} = p$.

Let S be the set of primes that ramify in K. Then S is finite. Consider the product group $\prod_{p \in S} I_{\mathfrak{p}}$. Define $\phi: \prod_{p \in S} I_{\mathfrak{p}} \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$ by sending $(\chi_{\mathfrak{p}})_{p \in S} \in \prod_{p \in S} I_{\mathfrak{p}}$ to $\prod_{p \in S} \chi_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$. By Q1 and the fact that $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, we see that ϕ is a surjective homomorphism of groups. Thus

$$\begin{aligned} [K:\mathbb{Q}] = \#\,\mathrm{Gal}(K/\mathbb{Q}) &\le \#\prod_{p \in S} I_{\mathfrak{p}} \\ &= \prod_{p \in S} e_{\mathfrak{p}} \\ &= \prod_{p \ge 2} e_{\mathfrak{p}}. \end{aligned}$$

□.

Q3. We first prove that if $K/\mathbb{Q}$ is a finite abelian extension, $p \in \mathbb{Z}$ prime, $\mathfrak{p} \subset \mathcal{O}_K$ prime above p, then $K_{\mathfrak{p}}/\mathbb{Q}_p$ is a finite abelian extension. ------ (1).

Proof of (1): Assume $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Since $K/\mathbb{Q}$ is galois, $f(x)$ splits in K. Note that $K_{\mathfrak{p}} = \mathbb{Q}_p(\alpha)$. Let $\tilde{f}(x) \in \mathbb{Q}_p[x]$ be the minimal polynomial of α over $\mathbb{Q}_p$. Then $\tilde{f}(x) \mid f(x)$. We see that $\tilde{f}(x)$ splits in $K_{\mathfrak{p}}$. Thus $K_{\mathfrak{p}}/\mathbb{Q}_p$ is a galois extension.

Let $\varphi: \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$, $\sigma \longmapsto \sigma|_K$. It's a group homomorphism.

Let $\sigma \in \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$. Let $|\cdot|$ be the absolutely value on $K_{\mathfrak{p}}$. Define $|\cdot|'$ such that for $x \in K_{\mathfrak{p}}$, $|x|' = |\sigma(x)|$. Then $|\cdot|'$ is an absolute value extending the absolute value on $\mathbb{Q}_p$. Since $\mathbb{Q}_p$ is complete, by the uniqueness, $|x|' = |x| \ \forall x \in K_{\mathfrak{p}}$, i.e. $|x| = |\sigma(x)|$. Then we see that $\sigma: K_{\mathfrak{p}} \to K_{\mathfrak{p}}$ is continuous with respect to the topology induced by $|\cdot|$. Since K is dense in $K_{\mathfrak{p}}$, we see immediately that φ is injective. Since $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, $\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$ is abelian.

~~Let~~ Now we go back to the proof of Q3. Let S be the set of all primes in $\mathbb{Z}$ that are ramified in K. Let $p \in S$, Let $\mathfrak{P}$ be a prime in $\mathcal{O}_K$ above p. By (1), $K_{\mathfrak{P}}/\mathbb{Q}_p$ is abelian. By the local Kronecker Weber theorem, there exists $n_p \geq 1$ such that $K_{\mathfrak{P}} \subset \mathbb{Q}_p(\zeta_{n_p})$. Let a_p be the p-adic valuation of n_p. Let $n := \prod_{p \in S} p^{a_p}$. Let $E = K(\zeta_n)$. We are going to show $K \subset \mathbb{Q}(\zeta_n)$. Before doing that, we need some basis facts about cyclotomic extension of $\mathbb{Q}_p$.

Prop 1: Let K be a finite extension of $\mathbb{Q}_p$. Let ζ be a primitive n-th root of unity, $L = K(\zeta)$. Suppose $\gcd(n, p) = 1$. Then L/K is unramified.

Pf. ζ is a root of $x^n - 1$. Since $x^n - 1$ has no multiple roots in $\mathbb{F}_K$ (because $(x^n - 1, nx^{n-1}) = 1$, $n \neq 0$ in $\mathbb{F}_K$), L/K is unramified. ☒.

Prop 2: Let ζ be a primitive p^m-th root of unity. Then one has:

(i) $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ is totally ramified of degree $\varphi(p^m) = p^{m-1}(p-1)$.

(ii) $\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$.

(iii) $1 - \zeta$ is a prime element of ~~the valuation ring of~~ $\mathcal{O}_{\mathbb{Q}_p(\zeta)}$. $\mathcal{O}_{\mathbb{Q}_p(\zeta)}$ is the valuation ring.

(iv). $\mathcal{O}_{\mathbb{Q}_p(\zeta)} = \mathbb{Z}_p[\zeta]$.

Pf: Let $\phi: Gal(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \longrightarrow (\mathbb{Z}/p^m\mathbb{Z})^\times$

$\sigma \longmapsto a$, $\sigma(\zeta) = \zeta^a$.

ϕ is injective. Let $\phi(x) = \frac{x^{p^m}-1}{x^{p^{m-1}}-1} = x^{p^{m-1}(p-1)} + \cdots + x^{p^{m-1}} + 1$.

Then $\phi(1) = p$. Note that $\phi(x) = \prod_{a\in(\mathbb{Z}/p^m\mathbb{Z})^\times} (x-\zeta^a)$, we have

$p = \prod_{a\in(\mathbb{Z}/p^m\mathbb{Z})^\times} (1-\zeta^a)$. $\forall a, b \in (\mathbb{Z}/p^m\mathbb{Z})^\times$, we can find $c \in \mathbb{Z}_+$ s.t. $ac \equiv b \bmod p^m$.

Then $\frac{1-\zeta^b}{1-\zeta^a} = \frac{1-\zeta^{ac}}{1-\zeta^a} \in \mathcal{O}_{\mathbb{Q}_p(\zeta)}$. Similarly, $\frac{1-\zeta^a}{1-\zeta^b} \in \mathcal{O}_{\mathbb{Q}_p(\zeta)}$. So $\frac{1-\zeta^a}{1-\zeta^b}$ is a unit.

$p = (1-\zeta)^{\varphi(p^m)} \cdot \prod_{a\in(\mathbb{Z}/p^m\mathbb{Z})^\times} \frac{1-\zeta^a}{1-\zeta}$. Note that $[\mathbb{Q}_p(\zeta):\mathbb{Q}_p] \le \deg \phi(x) = \varphi(p^m)$,

we see that $1-\zeta$ must be a prime in $\mathcal{O}_{\mathbb{Q}_p(\zeta)}$ and it is the unique prime above p.

p is totally ramified in $\mathbb{Q}_p(\zeta)$. And $[\mathbb{Q}_p(\zeta):\mathbb{Q}_p] = \varphi(p^m) = \#(\mathbb{Z}/p^m\mathbb{Z})^\times$

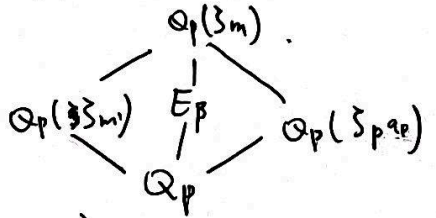
So ϕ is an isomorphism. Since the residue field of $\mathbb{Q}_p(\zeta)$ is equal to the residue field of $\mathbb{Q}_p$ (because the extension is totally ramified), and $1-\zeta$ is a uniformizer of $\mathbb{Q}_p(\zeta)$, by what we have proved in Homework , $\mathcal{O}_{\mathbb{Q}_p(\zeta)} = \mathbb{Z}_p[1-\zeta]$

$= \mathbb{Z}_p[\zeta]$ ☒.

Since $E/\mathbb{Q}_p$ is the compositum of two abelian extension $K/\mathbb{Q}_p$, $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$, $E/\mathbb{Q}_p$ is abelian. Let β be the prime above p in E, $\mathfrak{p}$ be the prime above p in K and $p = \beta \cap K$. Let E_β be the completion of E with respect to β.

Since $E = K(\zeta_n)$, we have $E_\beta = K_\mathfrak{p}(\zeta_n)$. Then $E_\beta = K_\mathfrak{p}(\zeta_n) \subset \mathbb{Q}_p(\zeta_{np}, \zeta_n)$

$= \mathbb{Q}_p(\zeta_m)$ for some $m \in \mathbb{Z}_{>0}$ where $m = p^{a_p} m'$, $(p, m') = 1$.



By prop(1), $e(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{p^{a_p}})) = 1$. By prop(2), $e(\mathbb{Q}_p(\zeta_{p^{a_p}})/\mathbb{Q}_p) = \varphi(p^{a_p})$.

Thus $e(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = \varphi(p^{a_p})$. Thus $e(E_\beta/\mathbb{Q}_p) \le \varphi(p^{a_p})$.

Let e_p be the ramification index of p in E. Since completion does not change ramification index, $e_p = e(E_\beta/\mathbb{Q}_p) \le \varphi(p^{a_p})$.

Note that $E = K(\zeta_n)$, $n = \prod_{p \in S} p^{q_p}$, p ramifies in $\mathbb{Q}(\zeta_n)$ if and only if $p \mid n$. We see S is the exactly the set of primes that ramifies in E.

Then by Q2, $[E:\mathbb{Q}] \le \prod_{p>2} e_p = \prod_{p \in S} e_p \le \prod_{p \in S} \varphi(p^{q_p}) = \varphi(n)$.

But $E \supset \mathbb{Q}(\zeta_n)$, $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$. We must have $[E:\mathbb{Q}] = \varphi(n)$, $E = \mathbb{Q}(\zeta_n)$.

Thus $K \subset E = \mathbb{Q}(\zeta_n)$ ☒.

Q4. Let $\mathbb{F}_L/\mathbb{F}_K$ be the residue field extension. Since K is a finite extension of $\mathbb{Q}_p$, $\mathbb{F}_K = \mathbb{F}_q$ for some $q = p^k$, $k \in \mathbb{Z}_{>0}$. $\mathbb{F}_L = \mathbb{F}_{q^f}$, $f \in \mathbb{Z}_{>0}$.

Note that $(X^{q^r}-X, (X^{q^r}-X)') = (X^{q^r}-X, q^r \cdot X^{q^r-1}) = (X^{q^r}-X, -1) = 1$ in $\mathbb{F}_q$, we see that $X^{q^r}-X$ has no multiple roots in $\mathbb{F}_q$. Let α be the generator of $\mathbb{F}_L^\times$. Then $\mathbb{F}_L = \mathbb{F}_K(\alpha)$. Since $X^{q^r}-X$ splits in $\mathbb{F}_{q^r} = \mathbb{F}_L$ and has no multiple roots, we can apply Hensel's lemma and see there exists $\hat{\alpha} \in \mathcal{O}_L$ s.t. $\overline{\hat{\alpha}} = \alpha$. ($\overline{\hat{\alpha}}$ is the image of $\hat{\alpha}$ in $\mathbb{F}_L$). and $\hat{\alpha}$ is a root of $X^{q^r}-X$. By what we have proved in class, $L = K(\hat{\alpha})$. ~~Then~~ $\hat{\alpha}$ must be an n-th root of unity for some n.

Note that $n \mid q^r-1$, we see $p \nmid n$. ☒

Q5. It's trivial for $p=2$ since $\zeta_2 = -1$. Now we assume $p \geq 3$.

Let $f(x) = X^{p-1}+p$ and $\alpha_1 \cdots \alpha_{p-1}$ be its roots in $\overline{\mathbb{Q}_p}$.

Let $\pi = 1-\zeta_p$ be the uniformizer in $\mathbb{Q}_p(\zeta_p)$. We have $|p| = |1-\zeta_p|^{p-1} = |\pi|^{p-1}$.

$f'(x) = (p-1)X^{p-2}$. Then $|\alpha_i-\alpha_1|\cdots|\alpha_i-\alpha_{i-1}|\cdot|\alpha_i-\alpha_{i+1}|\cdots|\alpha_i-\alpha_{p-1}| = |f'(\alpha_i)| = |\alpha_i|^{p-2} = |\pi|^{p-2}$

Note that for $i \neq j$, $|\alpha_i-\alpha_j| \leq \max\{|\alpha_i|, |\alpha_j|\} = |\pi|$, then $|\alpha_i-\alpha_1|\cdots|\alpha_i-\alpha_{p-1}| \leq |\pi|^{p-2}$.

Then all the ~~inqua~~ inequalities must be equalities, i.e. $\forall i \neq j$, $|\alpha_i-\alpha_j| = |\pi|$.

Now we consider $|\pi-\alpha_1|\cdots|\pi-\alpha_{p-1}| = |f(\pi)|$.. Since $\frac{X^p-1}{X-1} = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times}(X-\zeta_p^a)$, we have $p = (1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1})$ by taking $X=1$.

$$\begin{aligned} f(\pi) &= \pi^{p-1}+p \\ &= \pi^{p-1} + \pi^{p-1}\cdot\frac{1-\zeta_p}{1-\zeta_p}\cdot\frac{1-\zeta_p^2}{1-\zeta_p}\cdots\frac{1-\zeta_p^{p-1}}{1-\zeta_p} \\ &= \pi^{p-1}\left(1+\frac{\pi}{\pi}\cdot\frac{1-(1-\pi)^2}{\pi}\cdots\frac{1-(1-\pi)^{p-1}}{\pi}\right) \\ &= \pi^{p-1}\left(1+\prod_{k=1}^{p-1}\frac{1-(1-\pi)^k}{\pi}\right) \end{aligned}$$

Note that $\frac{1-(1-\pi)^k}{\pi} = \frac{1-\sum_{i=0}^{k}\binom{k}{i}(-\pi)^i}{\pi} = k+\pi\cdot a_k$, where $a_k \in \mathcal{O}_{\mathbb{Q}_p(\zeta_p)}$.

Then $f(\pi) = \pi^{p-1}\cdot(1+(p-1)!+\pi\cdot a)$ for some $a \in \mathcal{O}_{\mathbb{Q}_p(\zeta_p)} = \mathbb{Z}_p[\zeta_p]$.

By Wilson's theorem, $p \mid 1+(p-1)!$. Then $|f(\pi)| = |\pi|^{p-1}\cdot|1+(p-1)!+\pi\cdot a|$

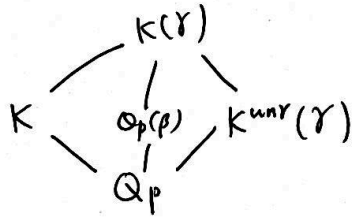
$< |\pi|^{p-1}$.

Then $|\pi-\alpha_i|<|\pi|$ for some i. Since $|\alpha_i-\alpha_j|=|\pi|$ for any $j\neq i$, by Kraser's lemma π belongs to α_i, i.e. $\mathbb{Q}_p(\alpha_i)\subset\mathbb{Q}_p(\pi)=\mathbb{Q}_p(\zeta_p)$. Since $f(x)$ is an Eisenstein polynomial, $f(x)$ is irreducible. Then $[\mathbb{Q}_p(\alpha_i):\mathbb{Q}_p]=\deg f=p-1$. We must have $\mathbb{Q}_p(\alpha_i)=\mathbb{Q}_p(\zeta_p)$. Thus there exists some $\alpha\in\mathbb{Q}_p(\zeta_p)$ such that $\mathbb{Q}_p(\zeta_p)=\mathbb{Q}_p(\alpha)$ and α is a root of $f(x)$ ☒.

Q6. Let $K/\mathbb{Q}_p$ be a tamely ramified abelian extension. Let $e=e(K/\mathbb{Q}_p)$ be the ramification index of $K/\mathbb{Q}_p$. We first prove that $e\mid p-1$.

Let $K^{unr}\subset K$ s.t. $K^{unr}/\mathbb{Q}_p$ is the maximal unramified extension contained in K. By Q4, $K^{unr}=\mathbb{Q}_p(\zeta_n)$ for some $(n,p)=1$. Then K/K^{unr} is tamely totally ramified of degree e. Then there exists a uniformizer $\pi\in K^{unr}$ s.t. K is obtained by adding a root α of the polynomial $X^e-\pi$ to K^{unr}, i.e. $K=K^{unr}(\alpha)$, $\alpha^e-\pi=0$.

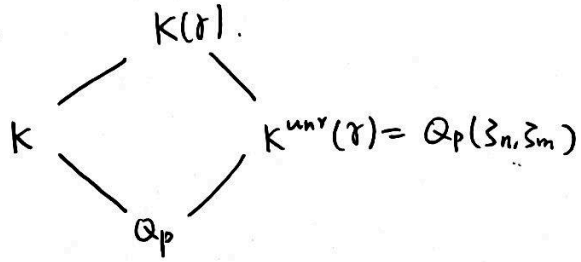
Since $K^{unr}/\mathbb{Q}_p$ is unramified, we have $|\pi|=|p|$. Let $u=\frac{\pi}{p}$. Then u is a unit in K^{unr}. Consider the polynomials X^e-p, X^e-u. Then $\exists\beta,\gamma$ s.t. $\alpha=\beta\gamma$, where β is some root of X^e-p, γ is some root of X^e-u. Consider $K^{unr}(\gamma)$. Since u is a unit and $(e,p)=1$, X^e-u has no multiple roots in the residue field of K^{unr}. So $K^{unr}(\gamma)/K^{unr}$ is unramified. By Q4, $K^{unr}(\gamma)=K^{unr}(\zeta_m)$ for some $(m,p)=1$. So $K^{unr}(\gamma)=\mathbb{Q}_p(\zeta_n,\zeta_m)$ is a cyclotomic extension of $\mathbb{Q}_p$.



We also see that $K(\gamma)=K^{unr}(\gamma,\beta)$. Since $K/\mathbb{Q}_p$, $K^{unr}(\gamma)/\mathbb{Q}_p$ are abelian extensions, $K(\gamma)/\mathbb{Q}_p$ is an abelian extension. Then $\mathbb{Q}_p(\beta)/\mathbb{Q}_p$ is abelian. Since β is a root of the irreducible polynomial $X^{p^e}-p$ (X^e-p is actually an Eisenstein polynomial, hence irreducible), X^e-p splits in $\mathbb{Q}_p(\beta)$. We have $\beta\cdot\zeta_e^i\in\mathbb{Q}_p(\beta)$ $\Rightarrow\zeta_e\in\mathbb{Q}_p(\beta)$. And since X^e-p is Eisenstein, $\mathbb{Q}_p(\beta)/\mathbb{Q}_p$ is totally ramified. So $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ is totally ramified. But ζ_e is a root of X^e-1, which has no multiple roots in $\mathbb{F}_p$, then $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ is unramified. Therefore $\mathbb{Q}_p(\zeta_e)=\mathbb{Q}_p$.

It remains to show that $\zeta_e \in \mathbb{Q}_p$ if and only if $e \mid p-1$. It's easy to see that If $e \mid p-1$, then $\zeta_e \in \mathbb{Q}_p$ because we have proved in class that $\zeta_{p-1} \in \mathbb{Q}_p$ by applying Hensel's lemma to $X^{p-1}-1$. Now assume $\zeta_e \in \mathbb{Q}_p$. Then X^e-1 splits in $\mathbb{Q}_p$. We see X^e-1 splits in $\mathbb{F}_p$ by modulo p. Then $\mathbb{F}_p^\times$ has an element of order e. Note that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, we must have $e \mid p-1$. ☒.

We continue the proof.



We have seen that $K(\gamma) = K^{unr}(\gamma, \beta) = \mathbb{Q}_p(\zeta_n, \zeta_m, \beta)$., where β is a root of $X^e - p$.

Let ζ_{2p-2} be the primitive $(2p-2)$-th root of unity. Then $\zeta_{2p-2}^{p-1} = -1$.

By Q5, $(\alpha \cdot \zeta_{2p-2})^{p-1} \equiv (-p)\cdot(-1) = p$. $\Rightarrow \left((\alpha \cdot \zeta_{2p-2})^{\frac{p-1}{e}}\right)^e = p$.

Thus $\beta = (\alpha \cdot \zeta_{2p-2})^{\frac{p-1}{e}} \cdot \zeta_e^i$ for some $i \in \mathbb{Z}$. Since $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\zeta_p)$, $\mathbb{Q}_p(\beta) \subset \mathbb{Q}_p(\zeta_{2p-2}^{\frac{p-1}{e}}, \zeta_e^i, \zeta_p)$. Then $K \subset K(\gamma) = \mathbb{Q}_p(\zeta_n, \zeta_m, \beta) \subset \mathbb{Q}_p(\zeta_n, \zeta_m, \zeta_{2p-2}^{\frac{p-1}{e}}, \zeta_e^i, \zeta_p)$.

$\subset \mathbb{Q}_p(\zeta_N)$ for some N large enough. ☒.

Q7. We first prove a lemma.

Lemma. Let K/F be finite Galois extension with Galois group

$$G = Gal(K/F) = G_1 \times \cdots \times G_r.$$

Then $K = K_1 \cdots K_r$ where $K_j = K^{H_j}$, $H_j = \prod_{i \neq j} G_i \times \{j\}$ at j.

Proof of the lemma: We prove by induction on r. If $r=1$, there is nothing to prove. If $r=2$, it suffices to prove $[K_1 \cdot K_2 : F] = [K:F]$. Given an element $x \in K_1 \cap K_2$, it is fixed by H_1 and H_2. Then x is fixed by $H_1 \cdot H_2 = G$. $\Rightarrow K_1 \cap K_2 = F$.

Since H_1, H_2 are normal subgroups of G, K_1/F, K_2/F are Galois extensions.

Then there is an isomorphism $Gal(K_1 \cdot K_2/F) \cong Gal(K_1/F) \times Gal(K_2/F)$

Then $[K_1 \cdot K_2 : F] = \#\, Gal(K_1 \cdot K_2/F) = \#\, Gal(K_1/F) \cdot \#\, Gal(K_2/F) = [K_1 : F] \cdot [K_2 : F]$.

$= \#H_1 \cdot \#H_2 = \#G = [K:F]$.

We assume the lemma is true for $\leq r$ and consider the condition on $r+1$.

Suppose $H_j = \prod_{i \neq j} G_i \times \{1\}$ and $H_r' = \prod_{i \neq r, r+1} G_i \times \{1\}$ at r $\times \{1\}$ at $r+1$. Then by hypothesis.

$K = K_1 \cdots K_{r-1} \cdot K_r'$ where $K_j = K^{H_j}$ and $K_r' = K^{H_r'}$. Since $H_r' \leq H_r, H_{r+1}$,

$K_r, K_{r+1} \subseteq K_r'$. Moreover $Gal(K_r'/F) \cong Gal(K/F)/Gal(K/K_r') = G_r \times G_{r+1}$.

We see from the condition $r=2$ we have proved that $K_r' = K_r \cdot K_{r+1}$. Then $K = K_1 \cdots K_{r+1}$. ☒.

Now suppose $K/\mathbb{Q}_p$ is an abelian extension. Then $Gal(K/\mathbb{Q}_p)$ is an abelian group, it can be written as a product of cyclic groups whose orders are a power of a prime.

i.e. $Gal(K/\mathbb{Q}_p) = G_1 \times \cdots \times G_r$, $G_i = \mathbb{Z}/q^{m_k}\mathbb{Z}$, q is a prime, $k \geq 1$.

Then $K = K_1 \cdots K_r$, $K_j = K^{H_j}$, $H_j = \prod_{i \neq j} G_i \times \{1\}$ at j. $Gal(K_j/\mathbb{Q}_p) \cong Gal(K/\mathbb{Q}_p)/Gal(K/K_j)$

$\cong G_i$. So we only need to consider the case where $Gal(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^k\mathbb{Z}$. for some prime q. By Q6, if $q \neq p$, then $K/\mathbb{Q}_p$ is a tamely ramified and hence K is contained in some cyclotomic extension of $\mathbb{Q}_p$. So it suffices to consider the case where $Gal(K/\mathbb{Q}_p) \cong \mathbb{Z}/p^m\mathbb{Z}$ for some $m \geq 1$. ☒.

Q8. We have proved in class that there is a one-to-one correspondence between ~~unramif~~ finite unramified extensions of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}_p}$ and finite extensions of $\mathbb{F}_p$ in $\overline{\mathbb{F}_p}$. So there is a unique unramified extension E_u of $\mathbb{Q}_p$ corresponds to $\mathbb{F}_{p^{p^m}}$.

By prop2 proved in Q3, $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{m+1}})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$. Since $p \geq 3$, we know that $(\mathbb{Z}/p^{m+1}\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^m\mathbb{Z} \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$ is cyclic.

Hence there is a unique subgroup of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{m+1}})/\mathbb{Q}_p)$ of index $p-1$.

It corresponds to a subextension E_r. We have $\mathrm{Gal}(E_r/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{m+1}})/\mathbb{Q}_p) / \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{m+1}})/E_r) \cong \mathbb{Z}/p^m\mathbb{Z}$. Since $\mathbb{Q}_p(\zeta_{p^{m+1}})/\mathbb{Q}_p$ is totally ramified, $E_r/\mathbb{Q}_p$ is totally ramified.

By Q4, $E_u = \mathbb{Q}_p(\zeta_n)$ for some $n \geq 1$ with $(n,p)=1$. So if K is contained in $E_u \cdot E_r$, K is contained in $\mathbb{Q}_p(\zeta_n, \zeta_{p^{m+1}}) = \mathbb{Q}_p(\zeta_{n \cdot p^{m+1}})$, then the local KW theorem holds for K.

□.

Q9. Note that $(E_u \cap E_r)/\mathbb{Q}_p$ is both totally ramified and unramified. Then $E_u \cap E_r = \mathbb{Q}_p$. Since $E_u/\mathbb{Q}_p$, $E_r/\mathbb{Q}_p$ are Galois extensions, they are linearly disjoint.

~~If~~ Suppose $K \nsubseteq E_u \cdot E_r$, We first prove that $E_u \nsubseteq K \cdot E_r$., $E_r \nsubseteq K \cdot E_u$.

If $E_u \subset K \cdot E_r$, then $E_r \cdot E_u \subset K \cdot E_r$. Note that there is an injection

$$\mathrm{Gal}(K \cdot E_r / \mathbb{Q}_p) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}_p) \times \mathrm{Gal}(E_r/\mathbb{Q}_p)$$

we see that $[K \cdot E_r : \mathbb{Q}_p] \leq [K : \mathbb{Q}_p] \cdot [E_r : \mathbb{Q}_p] = [E_u : \mathbb{Q}_p] \cdot [E_r : \mathbb{Q}_p] = [E_u \cdot E_r : \mathbb{Q}_p]$

We must have $K \cdot E_r = E_r \cdot E_u \Rightarrow K \subset E_r \cdot E_u$. A contradiction. ~~So $K \nsubseteq K E_r E_u$.~~

So $E_u \nsubseteq K \cdot E_r$. Similarly, $E_r \nsubseteq K \cdot E_u$.

Consider the following group homomorphism

$$\varphi: \mathrm{Gal}(E_u \cdot E_r \cdot K / \mathbb{Q}_p) \longrightarrow \mathrm{Gal}(E_u/\mathbb{Q}_p) \times \mathrm{Gal}(E_r/\mathbb{Q}_p) \times \mathrm{Gal}(K/\mathbb{Q}_p)$$
$$\sigma \longmapsto (\sigma|_{E_u}, \sigma|_{E_r}, \sigma|_K)$$

It is injective. because if $\sigma|_{E_u}, \sigma|_{E_r}, \sigma|_K$ are identity maps, σ is a identity map.

We denote the image of $\mathrm{Gal}(E_u \cdot E_r \cdot K/\mathbb{Q}_p)$ by H, $H \cong \mathrm{Gal}(E_u \cdot E_r \cdot K/\mathbb{Q}_p)$.

H is a subgroup of $\mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$.

Since $K \not\subseteq Eu\cdot Er$, $Eu\cdot Er \neq Eu\cdot Er\cdot K$. Then $Gal(Eu\cdot Er\cdot K / Eu\cdot Er)$ is nontrivial

Let $\sigma \in Gal(Eu\cdot Er\cdot K/Eu\cdot Er)$, $\sigma \neq id$.. Then $\varphi(\sigma) = (id, id, \sigma|_K)$. Thus

H contains an element of the form $(0, 0, z)$. $\in \mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$.

$z \in \mathbb{Z}/p^m\mathbb{Z}$, $z \neq 0$.

Since $Eu \not\subseteq K\cdot Er$, $Er \not\subseteq K\cdot Eu$, we can similarly prove that H contains an element of the form $(0, y, 0)$ and of the form $(x, 0, 0)$ where $x, y \in \mathbb{Z}/p^m\mathbb{Z}$ are nonzero.

The group generated by $(x,0,0), (0,y,0), (0,0,z)$ is $\mathbb{Z}/p^{r_1}\mathbb{Z} \times \mathbb{Z}/p^{r_2}\mathbb{Z} \times \mathbb{Z}/p^{r_3}\mathbb{Z}$ where $p^{r_1}, p^{r_2}, p^{r_3}$ are the orders of x, y, z in $\mathbb{Z}/p^m\mathbb{Z}$. Thus H contains a subgroup isomorphic to $\mathbb{Z}/p^{r_1}\mathbb{Z} \times \mathbb{Z}/p^{r_2}\mathbb{Z} \times \mathbb{Z}/p^{r_3}\mathbb{Z}$. , $r_1, r_2, r_3 \geq 1$.

Note that the order of H is a power of p, so H is a product of cyclic groups whose orders are a power of p. i.e. $H \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$, $a_1 \ldots a_k \geq 1$.

We claim that $k \geq 3$. If $k \leq 2$. We count the number of elements of H whose order divides p. i.e. $\#\{h \in H \mid ph = 0\} := N$. When $k=1$., $H \cong \mathbb{Z}/p^{a_1}\mathbb{Z}$. Then $N = p^{a_1}$.. When $k=2$, $H \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z}$. Then $N = \#\{h \in H \mid ph = 0\}$

$= \#\{h_1 \in \mathbb{Z}/p^{a_1}\mathbb{Z} \mid ph_1 = 0\} \cdot \#\{h_2 \in \mathbb{Z}/p^{a_2}\mathbb{Z} \mid ph_2 = 0\} = p^2$: But since H contains a subgroup isomorphic to $\mathbb{Z}/p^{r_1}\mathbb{Z} \times \mathbb{Z}/p^{r_2}\mathbb{Z} \times \mathbb{Z}/p^{r_3}\mathbb{Z}$, N must not be smaller than $\#\{w \in \mathbb{Z}/p^{r_1}\mathbb{Z} \times \mathbb{Z}/p^{r_2}\mathbb{Z} \times \mathbb{Z}/p^{r_3}\mathbb{Z} \mid pw = 0\}$.

$= \#\{w_1 \in \mathbb{Z}/p^{r_1}\mathbb{Z} \mid pw_1 = 0\} \cdot \#\{w_2 \in \mathbb{Z}/p^{r_2}\mathbb{Z} \mid pw_2 = 0\} \cdot \#\{w_3 \in \mathbb{Z}/p^{r_3}\mathbb{Z} \mid pw_3 = 0\}$.

$= p^3$. A contradiction.

So $k \geq 3$. Let H_i be the cyclic subgroup of $\mathbb{Z}/p^{a_i}\mathbb{Z}$ of order $p^{a_i - 1}$., $i = 1, 2, 3$.

Let $M = H_1 \times H_2 \times H_3 \times \mathbb{Z}/p^{a_4}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$. be the subgroup of H.

Since $H \cong Gal(Eu\cdot Er\cdot K/\mathbb{Q}_p)$, we regard M as a subgroup of $Gal(Eu\cdot Er\cdot K/\mathbb{Q}_p)$.

Let E be fixed field of M, i.e. $E = L^M$, where $L = Eu\cdot Er\cdot K$.

Then $Gal(E/\mathbb{Q}_p) \cong Gal(L/\mathbb{Q}_p) / Gal(L/E) \cong H/M$

$$\cong \frac{\mathbb{Z}/p^{a_1}\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z} \times \mathbb{Z}/p^{a_3}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}}{H_1 \times H_2 \times H_3 \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}}$$

$$\cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Q10. Let $\alpha = a^{1/p}$ be a root of $X^p - a$. For any $g \in \mathrm{Gal}(L(\zeta_p)/L)$, we can extend it to $\tilde{g} \in \mathrm{Gal}(L(\zeta_p, \alpha)/L)$ such that $\tilde{g}|_{L(\zeta_p)} = g$.

We can ω to $\omega : \mathrm{Gal}(L(\zeta_p, \alpha)/L) \to (\mathbb{Z}/p\mathbb{Z})^\times$, $\tilde{g}(\zeta_p) = \zeta_p^{\omega(\tilde{g})}$.

It suffices to prove $\tilde{g}(a) \equiv a^{\omega(\tilde{g})}$ modulo $(L(\zeta_p)^\times)^p$ $\forall\, \tilde{g} \in \mathrm{Gal}(L(\zeta_p, \alpha)/L)$ because $\tilde{g}(a) = \tilde{g}|_{L(\zeta_p)}(a)$, $\omega(\tilde{g}) = \omega(\tilde{g}|_{L(\zeta_p)})$. Note that $a = \alpha^p$, then it suffices to prove that $\tilde{g}(\alpha) \equiv \alpha^{\omega(\tilde{g})}$ modulo $L(\zeta_p)^\times$, i.e. $\tilde{g}(\alpha) \cdot \alpha^{-\omega(\tilde{g})} \in L(\zeta_p)^\times$

For any $\sigma \in \mathrm{Gal}(L(\zeta_p, \alpha)/L(\zeta_p))$,

$$\begin{aligned}\sigma\left(\tilde{g}(\alpha) \cdot \alpha^{-\omega(\tilde{g})}\right) &= \sigma(\tilde{g}(\alpha)) \cdot \sigma(\alpha)^{-\omega(\tilde{g})} \\ &= \tilde{g}(\sigma(\alpha)) \cdot \sigma(\alpha)^{-\omega(\tilde{g})} \qquad (M/L = L(\zeta_p, \alpha)/L \text{ is abelian})\end{aligned}$$

Since σ fixes $L(\zeta_p)$, $\sigma(\alpha)$ is also a root of $X^p - a$. Suppose $\sigma(\alpha) = \alpha \cdot \zeta_p^i$ for some $i \in \mathbb{Z}$.

Then $$\begin{aligned}\tilde{g}(\sigma(\alpha)) \cdot \sigma(\alpha)^{-\omega(\tilde{g})} &= \tilde{g}(\alpha \cdot \zeta_p^i) \cdot (\alpha \cdot \zeta_p^i)^{-\omega(\tilde{g})} \\ &= \tilde{g}(\alpha) \cdot \tilde{g}(\zeta_p)^i \cdot \alpha^{-\omega(\tilde{g})} \cdot \zeta_p^{-i\omega(\tilde{g})} \\ &= \tilde{g}(\alpha) \cdot \zeta_p^{\omega(\tilde{g}) \cdot i} \alpha^{-\omega(\tilde{g})} \cdot \zeta_p^{-i\omega(\tilde{g})} \\ &= \tilde{g}(\alpha) \cdot \alpha^{-\omega(\tilde{g})}.\end{aligned}$$

So $\tilde{g}(\alpha)$ is fixed by $\mathrm{Gal}(L(\zeta_p, \alpha)/L(\zeta_p))$. So ~~$\tilde{g}(\alpha) \in L(\zeta_p)$~~ $\tilde{g}(\alpha) \cdot \alpha^{-\omega(\tilde{g})} \in L(\zeta_p)$

Since $a \neq 0$, then $\alpha \neq 0$, $\tilde{g}(\alpha) \cdot \alpha^{-\omega(\tilde{g})} \neq 0$, $\tilde{g}(\alpha) \cdot \alpha^{-\omega(\tilde{g})} \in L(\zeta_p)^\times$. ☒

Q11. Since $E(\zeta_p)/\mathbb{Q}_p$ is the compositum of two abelian extensions $E/\mathbb{Q}_p$, $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$, $E(\zeta_p)/\mathbb{Q}_p$ is abelian. Then $E(\zeta_p)/\mathbb{Q}_p(\zeta_p)$ is Galois. We have an injective homomorphism

$$\varphi: \mathrm{Gal}(E(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \longrightarrow \mathrm{Gal}(E/\mathbb{Q}_p).$$
$$\sigma \longmapsto \sigma|_E$$

So $\mathrm{Gal}(E(\zeta_p)/\mathbb{Q}_p(\zeta_p))$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^3$. Note that $[E(\zeta_p):\mathbb{Q}_p(\zeta_p)] = \frac{[E(\zeta_p):\mathbb{Q}_p]}{[\mathbb{Q}_p(\zeta_p):\mathbb{Q}_p]}$

$= \frac{[E(\zeta_p):E]\cdot[E:\mathbb{Q}_p]}{[\mathbb{Q}_p(\zeta_p):\mathbb{Q}_p]} = \frac{[E(\zeta_p):E]\cdot p^3}{p-1}$, we see $p^3 \mid [E(\zeta_p):\mathbb{Q}_p(\zeta_p)]$.

So $[E(\zeta_p):\mathbb{Q}_p(\zeta_p)]$ must be p^3 and we have $\mathrm{Gal}(E(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \cong (\mathbb{Z}/p\mathbb{Z})^3$.

Then $E(\zeta_p)/\mathbb{Q}_p(\zeta_p)$ is a Kummer extension. By Kummer theory, there exists $a_1,\dots,a_s \in \mathbb{Q}_p(\zeta_p)$ such that $E(\zeta_p) = \mathbb{Q}_p(\zeta_p, a_1^{1/p}, \dots, a_s^{1/p})$. Let a be one of the a_i's. Let $M = \mathbb{Q}_p(\zeta_p, a^{1/p})$. Then $M/\mathbb{Q}_p$ is a subextension of $E(\zeta_p)/\mathbb{Q}_p$ and hence abelian. Define $\omega: \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \to (\mathbb{Z}/p\mathbb{Z})^\times$ by the formula $g(\zeta_p) = \zeta_p^{\omega(g)}$ for all $g \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$. By prop 2 in Q3, we see ω is an isomorphism.

By Q10, $g(a) \equiv a^{\omega(g)} \pmod{(\mathbb{Q}_p(\zeta_p)^\times)^p}$ for any $g \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$.

Suppose $a = \pi^i \cdot u$ where $i \in \mathbb{Z}_{\geq 0}$ and $|u| = 1$. Here $\pi = \zeta_p - 1$ is the uniformizer of $\mathbb{Q}_p(\zeta_p)$. Note that $|g(a)| = |a|$ for any $g \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$, we see that $|g(a)\cdot a^{-\omega(g)}|$

$= |a|^{1-\omega(g)} = |x|^p$ for some $x \in \mathbb{Q}_p(\zeta_p)^\times$. Then $p \mid i(1-\omega(g))$ for any ~~$g \in \mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$~~ $g \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$. We may chouse g such that $\omega(g) = 2$. Then $p \mid i$.

Since we can replace a by $a\cdot(\pi^{-i/p})^p = u$, we can assume a is a unit without loss of generality, let $a = u$. be a unit. Next we will give some basic facts about unit group and higher unit group of $\mathbb{Q}_p(\zeta_p)$.

Let $U = \{x \in \mathbb{Z}_p[\zeta_p] \mid x \equiv 1 \bmod \pi\}$ be the unit group. Let $U^{(n)} = \{x \in \mathbb{Z}_p[\zeta_p] \mid x \equiv 1 \bmod \pi^n\}$ $n \in \mathbb{Z}_{\geq 1}$ ~~$U^{(n)} = \{x \in \mathbb{Z}_p[\zeta_p] \mid x \equiv 1 \bmod \pi^n\}$~~ $n \in \mathbb{Z}_{\geq 1}$

$\pi = \zeta_p - 1$ is the uniformizer of $\mathbb{Q}_p(\zeta_p)$. Here are some propositions.

Prop: (1) $U^{(n)}$ is a multiplicative group.

(2) For any unit $u \in \mathbb{Q}_p(\zeta_p)$, there exists a power of $p-1$-th primitive root of unity, say ζ_{p-1}^i, such that $\zeta_{p-1}^i \cdot u \in U$

(3) $U^{(p+1)} = (U)^p$. where $(U)^p = \{ x^p \mid x \in U \}$.

Proof of the propositions: (1) For $x \in U^{(n)}$, $x-1 \in (\pi)^n$. Then $x^{-1}-1 = \frac{1-x}{x} \in (\pi)^n$

Thus $x^{-1} \in U^{(n)}$. For $x, y \in U^{(n)}$, we have $xy \equiv 1 \cdot 1 \equiv 1 \bmod \pi^n \Rightarrow xy \in U^{(n)}$.

Thus $U^{(n)}$ is a group.

(2) Note that $Q_p(\zeta_p)/Q_p$ is totally ramified, the residue field of $Q_p(\zeta_p)$ is equal to that of Q_p, say $\mathbb{F}_p$. We have seen in class that $0, \zeta_{p-1}, \zeta_{p-1}^2, \dots \zeta_{p-1}^{p-1}$ is a set of representatives of Q_p mod p, then it is also a set of representatives of $Q_p(\zeta_p)$ mod π.

Since $x \notin (\pi)$, $x \equiv \zeta_{p-1}^i \pmod{\pi}$ for some $i \in \mathbb{Z} \Rightarrow \zeta_{p-1}^{-i} x \in U$.

(3) $(U)^p \subseteq U^{(p+1)}$: Let $u \in U$. Then $u \equiv 1 \bmod \pi$. Suppose $u = 1 + c_1\pi + c_2\pi^2 + \dots$ for $c_i \in \mathbb{Z}/\{0, 1, 2, \dots p-1\}$. Note that $\zeta_p^n = (1+\pi)^n = 1 + n\pi + \binom{n}{2}\pi^2 + \dots$. Choose $n = p - c_1$ we have $\zeta_p^{p-c_1} = 1 + (p-c_1)\pi + \binom{n}{2}\pi^2 + \dots \equiv 1 - c_1\pi \bmod \pi^2$. Thus $\zeta_p^{p-c_1} \cdot u \equiv (1+c_1\pi)(1-c_1\pi)$ $\equiv 1 \bmod \pi^2$. Then we have proved the fact that for any $u \in U$, there exists n such that $u \cdot \zeta_p^n \equiv 1 \bmod \pi^2$. Let $u_1 = u \cdot \zeta_p^n = 1 + \pi^2 m$ for some $m \in \mathbb{Z}_p[\zeta_p]$

Then $u_1^p = (1+\pi^2 m)^p = \sum_{k=0}^{p} \binom{p}{k} (\pi^2 m)^k = 1 + \sum_{k=1}^{p-1} \binom{p}{k} (\pi^2 m)^k + (\pi^2 m)^p$. Note that

$p \mid \binom{p}{k}$ for $1 \le k \le p-1$. Since $|p| = |\pi|^{p-1}$, we have $\pi^{p+1} \mid \sum_{k=1}^{p-1} \binom{p}{k} (\pi^2 m)^k + (\pi^2 m)^p$

Then $u_1^p \equiv 1 \bmod \pi^{p+1} \Rightarrow u^p = (u_1 \cdot \zeta_p^{-n})^p = u_1^p \equiv 1 \bmod \pi^{p+1}$.

So $u^p \in U^{(p+1)}$. $\forall u \in U$. $\Rightarrow (U)^p \subseteq U^{(p+1)}$.

$U^{(p+1)} \subseteq (U)^p$: Let $a \in U^{(p+1)}$. Consider $f(x) = X^p - a$. It suffices to prove $f(x)$ has a root in U. We first prove $f(x)$ has a root in $Q_p(\zeta_p)^\times$.

Let $\alpha_1 \sim \alpha_p$ be roots of $f(x)$. Then $f(x) = (x-\alpha_1)\cdots(x-\alpha_p)$. We may assume $\alpha_i = \alpha_1 \cdot \zeta_p^{i-1}$ $i = 1, 2 \cdots p$. Then $|\alpha_i - \alpha_j| = |\alpha_1 \cdot \zeta_p^{i-1} - \alpha_1 \cdot \zeta_p^{j-1}| = |\alpha_1| \cdot |\zeta_p^{i-1} - \zeta_p^{j-1}| = |1 - \zeta_p^{i-j}| = |\pi|$ for $i \neq j \pmod{p}$. Note that $|1-\alpha_1| \cdots |1-\alpha_p| = |f(1)| = |1-a| \le |\pi|^{p+1} < |\pi|^p$.

Then there exists i such that $|1-\alpha_i| < |\pi| = |\alpha_i - \alpha_j| \ \forall j \neq i$. Since $a \in U^{(p+1)} \subset Q_p(\zeta_p)$ we see $\{\alpha_j\}_{j \neq i}$ contains the set of conjugates of α_i (here the conjugate is with respect to the base field $Q_p(\zeta_p)$). By Krasner's lemma, 1 belongs to α_i and $\alpha_i \in Q_p(\zeta_p)(1) = Q_p(\zeta_p)$

Then $f(x)$ has a root in $Q_p(\zeta_p)^\times$. The root must be a unit, because $|a| = 1$.

Let u be a root of X^p-a. By (2), we can find $i\in\mathbb{Z}$ and $u'\in U$ such that $u=u'\cdot\zeta_{p-1}^i$. Then $(u'\cdot\zeta_{p-1}^i)^p=u^p=a\equiv 1 \bmod \pi^{p+1}$. We have proved in the inclusion $(U)^p\subseteq U^{(p+1)}$ that $(u')^p\equiv 1 \bmod \pi^{p+1}$. Then $\zeta_{p-1}^{pi}\equiv 1 \bmod \pi^{p+1}$.

$\Rightarrow \zeta_{p-1}^{i}\equiv 1 \bmod \pi^{p+1}$. $\Rightarrow \zeta_{p-1}^{i}\equiv 1 \bmod \pi$. $\Rightarrow i\equiv 0 \bmod (p-1)$. So $u=u'\in U$.

Then for any $a\in U^{(p+1)}$, X^p-a has a root u in U. Other roots are in the form of $u\cdot\zeta_p^i$. Since $\zeta_p\equiv 1 \bmod \pi$, we see all the roots of X^p-a are in U. Thus $U^{(p+1)}\subseteq (U)^p$. ☒.

Now we go back to the proof of Q11. For u unit, we can find i such that $u\cdot\zeta_{p-1}^i=u_1\in U$ by (2). Then we can replace u by $u\cdot(\zeta_{p-1}^i)^p=u\cdot\zeta_{p-1}^i=u_1\in U$. So we may assume $u\in U$. Then by Q10, for any $g\in Q_p(\zeta_p)/Q_p$, we have $g(u)\equiv u^{w(g)}$ modulo $(Q_p(\zeta_p)^\times)^p$. Since $u\in U$, $g(u)\in U$. (because $g((\pi))=(\pi)$)

$\Rightarrow g(u)\cdot u^{-w(g)}\in U$. On the other hand, $g(u)\cdot u^{-w(g)}=x^p$ for some $x\in Q_p(\zeta_p)^\times$.

$\Rightarrow |x|^p=|g(u)\cdot u^{-w(g)}|=1$. So $|x|=1$, x is a unit. Then $x=\zeta_{p-1}^j x'$ for some $x'\in U$. $\Rightarrow (\zeta_{p-1}^j x')^p=\zeta_{p-1}^j (x')^p\in U$. Since $(x')^p\in U^{(p+1)}\subset U$, $\zeta_{p-1}^j\in U$.

So $j\equiv 0 \bmod (p-1)$. So $x\in U$. $\Rightarrow g(u)\equiv u^{w(g)}$ modulo $(U)^p$.

By (3), we have $g(u)\equiv u^{w(g)}$ modulo $U^{(p+1)}$. ~~i.e. $\exists\, y_g\in U^{(p+1)}$ such that $g(u)=u^{w(g)}\cdot y_g$~~ We have proved before that $\exists\, i$ s.t. $u\cdot\zeta_p^i=u_1\equiv 1 \bmod \pi^2$.

So $g(u_1)=g(u\cdot\zeta_p^i)=g(u)\cdot g(\zeta_p)^i\equiv u^{w(g)}\cdot\zeta_p^{w(g)i}\equiv (u\cdot\zeta_p^i)^{w(g)}\equiv u_1^{w(g)}$ modulo $U^{(p+1)}$.

Write $u_1=1+c_r\pi^r+c_{r+1}\pi^{r+1}+\cdots$ with $c_i\in\{0,1,\cdots p-1\}$, $c_r\neq 0$.

Note that $g(\pi)=g(\zeta_p-1)=g(\zeta_p)-1=\zeta_p^{w(g)}-1=(1+\pi)^{w(g)}-1$, we have

$$\frac{g(\pi)}{\pi}=\frac{\sum_{k=1}^{w(g)}\binom{w(g)}{k}\cdot\pi^k}{\pi}\equiv w(g) \bmod \pi$$ So $g(u_1)=1+c_r g(\pi)^r+c_{r+1}g(\pi)^{r+1}+\cdots$

$$=1+c_r\cdot\pi^r\cdot\left(\frac{g(\pi)}{\pi}\right)^r+O(\pi^{r+1})=1+c_r w(g)^r\cdot\pi^r+O(\pi^{r+1})$$

We have $1+c_r w(g)^r\pi^r+O(\pi^{r+1})\equiv u_1^{w(g)}=1+c_r w(g)\cdot\pi^r+O(\pi^{r+1})$ modulo $(U^{(p+1)})$

$\Rightarrow 1+c_r w(g)^r\cdot\pi^r+O(\pi^{r+1})=\left(1+c_r w(g)\pi^r+O(\pi^{r+1})\right)(1+\pi^{p+1}m)$ for some $m\in\mathbb{Z}_p[\zeta_p]$.

If $r \geq p+1$, $u_1 \in U^{(p+1)}$. If $r < p+1$, by comparing the coefficients of π^r on both sides, we have $C_r \omega(g)^r \equiv C_r \omega(g) \bmod \pi$. We can choose g such that $\omega(g)$ is the generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Since $\omega(g)^{r-1} \equiv 1 \bmod \pi$, we have $(p-1) \mid (r-1)$ because $\{0, 1, 2 \cdots p-1\}$ is a set of representatives modulo π. Since $u_1 \equiv 1 \bmod \pi^2$, $r \geq 2$. $\Rightarrow r = p$.

$\Rightarrow u_1 \in U^{(p)} \setminus U^{(p+1)}$.

Fact: $U^{(n)}/U^{(n+1)} \cong \mathcal{O}/(\pi)$. where $\mathcal{O} = \mathbb{Z}_p[\zeta_p]$ is the valuation ring. It is a group homomorphism., where $U^{(n)}/U^{(n+1)}$ is a multiplicative group, $\mathcal{O}/(\pi)$ is an additive group.

Proof of the fact: Consider the homomorphism.

$$\varphi: U^{(n)} \longrightarrow \mathcal{O}/(\pi).$$
$$1 + \pi^n a \longmapsto a \pmod{\pi}.$$

First we verify it is an homorphism. $\varphi((1+\pi^n a)(1+\pi^n b)) = \varphi(1 + \pi^n(a+b) + \pi^{2n} ab)$

$= a+b \pmod{\pi} = a \pmod{\pi} + b \pmod{\pi} = \varphi(1+\pi^n a) + \varphi(1+\pi^n b)$, $\varphi(1) = 0$

It is easy to see $\ker \varphi = U^{(n+1)}$. Thus we have $U^{(n)}/U^{(n+1)} \cong \mathcal{O}/(\pi)$ since φ is surjective.

Here $\mathcal{O}/(\pi) \cong \mathbb{Z}/p\mathbb{Z}$. $\varphi(1+\pi^n) = 1$ is the generator of the cyclic group $\mathbb{Z}/p\mathbb{Z}$. Thus $1+\pi^n$ generates the group $U^{(n)}/U^{(n+1)}$.

So far, we have proved that:

- $M/\mathbb{Q}_p$ is a subextension of $E(\zeta_p)/\mathbb{Q}_p$ where $M = \mathbb{Q}_p(\zeta_p, a^{1/p})$ for some $a \in \mathbb{Q}_p(\zeta_p)$.
- we can replace a by some $u \in U$, i.e. $\exists\, u \in U$, s.t. $a \equiv u \bmod (\mathbb{Q}_p(\zeta_p)^\times)^p$.
- we can find i s.t. $u \cdot \zeta_p^i = u_1 \equiv 1 \bmod \pi^2$.
- $u_1 \in U^{(p+1)}$. or $u_1 \in U^{(p)} \setminus U^{(p+1)}$. And since $U^{(p)}/U^{(p+1)} \cong \mathbb{Z}/(p)$, $U^{(p)}/U^{(p+1)}$ is generated by $1+\pi^p$, $u_1 \equiv (1+\pi^p)^j$ for some j modulo $U^{(p+1)} = (U)^p$.

Therefore, we can finally replace a by some $\zeta_p^{-i} \cdot (1+\pi^p)^j$, $i, j \in \mathbb{Z}$, i.e.

$a \equiv \zeta_p^{-i} (1+\pi^p)^j$ modulo $(\mathbb{Q}_p(\zeta_p)^\times)^p$

So $\mathbb{Q}_p(\zeta_p, a^{1/p}) = \mathbb{Q}_p(\zeta_p, (\zeta_p^{-i}(1+\pi^p)^j)^{1/p}) \subset \mathbb{Q}_p(\zeta_p, \zeta_p^{1/p}, (1+\pi^p)^{1/p})$ for any $a \in \{a_1 \dots a_s\}$. Thus $E(\zeta_p) \subset \mathbb{Q}_p(\zeta_p, \zeta_p^{1/p}, (1+\pi^p)^{1/p})$.

But $[\mathbb{Q}_p(\zeta_p, \zeta_p^{1/p}, (1+\pi^p)^{1/p}) : \mathbb{Q}_p] \leq [\mathbb{Q}_p(\zeta_p, \zeta_p^{1/p}) : \mathbb{Q}_p(\zeta_p)] \cdot [\mathbb{Q}_p(\zeta_p, (1+\pi^p)^{1/p}]$

$\leq p \cdot p = p^2$

$[E(\zeta_p) : \mathbb{Q}(\zeta_p)] = \#(\mathbb{Z}/p\mathbb{Z})^3 = p^3$

A contradiction! Therefore, there is no extension E of $\mathbb{Q}_p$ with $\mathrm{Gal}(E/\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^3$

囚.

Xu Song

2023.5.27