ALGEBRAIC NUMBER THEORY-SUMMER SCHOOL NOTES

YE TIAN

Contents

1. Ideal Class Groups

1.1. **Ideal class groups and unit groups.** Let K be a number field. Denote $\mathrm{Cl}(K)$ be its ideal class group and $\mathcal{O}_K^\times$ be its group of units.

Theorem 1.1. *We have*

(1) $\mathrm{Cl}(K)$ *is a finite abelian group.*
(2) $\mathcal{O}_K^\times \cong \mathbb{Z}^{r_1+r_2-1}\times\mu(K)$, *where* r_1, r_2 *are the number of real and complex places of* K, $\mu(K)$ *is the set of roots of unity in* K, *which is a finite cyclic group.*

Summary. (1) Note that for any $M\geq 1$, there exist only finite many integral ideals of $\mathcal{O}_K$ with norm bounded by M. Thus enough to show exists M_K such that for any fractional ideal $\mathfrak{a}$, exists $\alpha\in\mathfrak{a}$ such that $\mathrm{N}(\alpha\mathfrak{a}^{-1})<M_K$. A fractional ideal $\mathfrak{a}$ can be viewed as a lattice in $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\simeq\mathbb{R}^n$ here $n=[K:\mathbb{Q}]$. Consider the following centrally symmetric convex connected region

$$U_t=\Big\{(x,y)\in\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}|\ \sum_{i=1}^{r_1}|x_i|+\sum_{j=1}^{r_2}2|y_j|\leq t\Big\},$$

then exists C_K such that for any $\mathfrak{a}$, if $t\geq C_K\mathrm{N}(\mathfrak{a})^{1/n}$ holds (equivalently, exists N_K such that for any $\mathfrak{a}$, if $\mathrm{Vol}(U_t)\geq N_K\mathrm{N}(\mathfrak{a})$ holds), then exists $0\neq\alpha\in\mathfrak{a}\cap U_t$. We thus have

$$\mathrm{N}(\alpha)\leq\left(\frac{C_K\mathrm{N}(\mathfrak{a})^{1/n}}{n}\right)^n.$$

(2) Consider the log map:

$$\ell : \mathcal{O}_K^\times \to \mathbb{R}^{r_1+r_2}, \quad u \mapsto (\log |\sigma(u)|_{\sigma_i})_{\sigma_i},$$

here σ_i runs over all infinite places and $|\cdot|_\sigma$ is the normalized valuation. Then $\ker \ell = \mu(K)$ and the image lies in the hyperplane $\mathbb{R}^{\Sigma=0}$. The image in discrete in $\mathbb{R}^{\Sigma=0}$, thus enough to show that $\mathrm{Im}\,\ell$ is a (full) lattice of $\mathbb{R}^{\Sigma=0}$.

Fact 1.2. *Let $n = r_1 + r_2$ and $A \in M_{n\times n}(\mathbb{R})$ such that every row lies in $\mathbb{R}^{\Sigma=0}$. If $a_{ii} > 0$ for all i and $a_{i,j} < 0$ for all $i \neq j$, then* $\mathrm{rank}\, A = n - 1$.

By the above fact enough to find for each infinite place σ_i an element $u_i \in \mathcal{O}_K^\times$ such that $|\sigma_j(u)| < 1$ for all $j \neq i$. Thus enough to show exists C_K large enough such that exists a sequence $\{a_n\}_n$ in $\mathcal{O}_K$ with norm bounded by C_K such that $\{|\sigma_j(a_n)|\}_n$ is strictly decreasing for any $j \neq i$. If this is down, choose $m > n$ such that $(a_m) = (a_n)$. Then a_m/a_n is what needed. We now show the existence of the sequence: Consider the following certrally symmetric convex connected region in $\mathbb{R}^{r_1+r_2}$:

$$V_{c,t} := \Big\{ x \in \mathbb{R}^{r_1+r_2} |\ |x_i|_{\sigma_i} < c_i \text{ and} \prod_i c_i = t \Big\}.$$

Then exists N_k such that for any $t \geq N_K$ and any $c = (c_1, \cdots, c_{r_1+r_2})$ with $\prod_i c_i = t$, exists $0 \neq \alpha \in V_{c,t} \cap \mathcal{O}_K$. By induction we can find the needed sequence.

□

1.2. **Variation.**

1.2.1. *Variation of ideal class group.* Recall a modulus $\mathfrak{m}$ of K is a formal product $\mathfrak{m}_f \cdot \mathfrak{m}_\infty$ of an integral ideal $\mathfrak{m}_f$ and a subset $\mathfrak{m}_\infty$ of real places of K. The ray class group modulo $\mathfrak{m}$ is defined by $\mathrm{Cl}(K)_\mathfrak{m} := I^{\mathfrak{m}_f}/P_{\mathfrak{m},1}$, here $I^{\mathfrak{m}_f}$ is the group of prime to $\mathfrak{m}_f$ fractional ideals and $P_{\mathfrak{m},1}$ is the subgroup of principal ideals which represented by elements $\alpha \in K^\times$ with $\alpha \equiv 1 \pmod{\mathfrak{m}_f}$ and $\sigma(\alpha) \geq 0$ for all $\sigma \in \mathfrak{m}_\infty$. If $\mathfrak{m} = 1$, we get the ideal class group. Denote $K_\mathfrak{m}$ the subgroup of K which is units at $\mathfrak{m}_f$ and $K_{\mathfrak{m},1}$ the subgroup of $K_\mathfrak{m}$ that congruent to 1 modulo $\mathfrak{m}_f$. Then we have the following exact sequence

$$0 \to \mathcal{O}_K^\times \cap K_\mathfrak{m}/\mathcal{O}_K^\times \cap K_{\mathfrak{m},1} \to K_\mathfrak{m}/K_{\mathfrak{m},1} \to \mathrm{Cl}(K)_\mathfrak{m} \to \mathrm{Cl}(K) \to 1.$$

In particular, $\#\mathrm{Cl}(K)_\mathfrak{m}$ is finite. We also have a canonical isomorphism

$$K_\mathfrak{m}/K_{\mathfrak{m},1} \simeq \prod_{\sigma\in\mathfrak{m}_\infty} \{\pm 1\} \times (\mathcal{O}_K/\mathfrak{m}_f)^\times.$$

1.2.2. *Variation of units.* Let S be a finite set of finite places of K, the group of S-units $\mathcal{O}_{K,S}$ of K is the subgroup of $K^\times$ consists of elements which are units outside S. Then we have the following exact sequence

$$1 \to \mathcal{O}_K^\times \to \mathcal{O}_{K,S}^\times \xrightarrow{(\mathrm{ord}_v(\cdot))_{v\in S}} \mathbb{Z}^S$$

and the cokernel of the last map is finite. Thus $\mathcal{O}_{K,S} \simeq \mathcal{O}_K^\times \oplus \mathbb{Z}^{\#S} \simeq \mathbb{Z}^{r_1+r_2+\#S-1}$.

1.3. **Class Number Formula.**

Theorem 1.3. *Let K be a number field. Then we have the class number formula*

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\#\mathrm{Cl}(K)\,\mathrm{Reg}(\mathcal{O}_K^\times)}{w_K\sqrt{|D_K|}}.$$

1.4. **Chebotarev density theorem.** Let L/K be a finite Galois extension of number fields. Let $\mathfrak{p}$ be a prime of K unramified in L and let $\mathfrak{P}$ be a prime of L above $\mathfrak{p}$. Define the Frobenius $\mathrm{Frob}_\mathfrak{P}(L/K)$ to be the element in $\mathrm{Gal}(L/K)$ such that $\mathrm{Frob}_\mathfrak{P}(L/K)$ stabilizes $\mathfrak{P}$ and is $x \mapsto x^{\#(\mathcal{O}_K/\mathfrak{p})}$ on $\mathcal{O}_L/\mathfrak{P}$. For $\sigma \in \mathrm{Gal}(L/K)$, we have $\mathrm{Frob}_{\mathfrak{P}^\sigma}(L/K) = \sigma\mathrm{Frob}_\mathfrak{P}(L/K)\sigma^{-1}$, therefore, we can define $\mathrm{Frob}_\mathfrak{p}(L/K) := [\mathrm{Frob}_\mathfrak{P}(L/K)]$ to be the conjugacy class of $\mathrm{Frob}_\mathfrak{P}(L/K)$ in $\mathrm{Gal}(L/K)$ for any $\mathfrak{P}$ above $\mathfrak{p}$. In particular, if L/K is abelian, then $\mathrm{Frob}_\mathfrak{p}(L/K)$ is indeed an element of $\mathrm{Gal}(L/K)$.

Theorem 1.4 (Chebotarev density theorem)**.** *Let $\sigma \in \mathrm{Gal}(L/K)$ be any fixed element. Then among all the primes of K unramified in L, the primes $\mathfrak{p}$ which satisfy* $\mathrm{Frob}_\mathfrak{p}(L/K) = [\sigma]$ *have density* $\#[\sigma]/[L:K]$.

In particular, there exists infinitely many prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathrm{Frob}_\mathfrak{p}(L/K) = [\sigma]$, as well as infinitely many prime $\mathfrak{P}$ of $\mathcal{O}_L$ such that $\mathrm{Frob}_\mathfrak{P}(L/K) = \sigma$.

1.5. **Class field theory.**

Theorem 1.5. *Let K be a number field. Let H_K be the maximal abelian extension over K unramified everywhere. Then there is a natural isomorphism (which is $\mathrm{Gal}(K/K_0)$-equivariant if K_0 is any subfield of K such that K/K_0 is Galois):*

$$\mathrm{Cl}(K) \xrightarrow{\sim} \mathrm{Gal}(H_K/K), \qquad [\mathfrak{p}] \mapsto \mathrm{Frob}_{\mathfrak{p}}(H_K/K).$$

Corollary 1.6. *For any $\mathcal{C} \in \mathrm{Cl}(K)$, the density of prime ideals $\mathfrak{p}$ such that $\mathfrak{p} \in \mathcal{C}$ is $1/\#\mathrm{Cl}(K)$.*

1.6. **The class number formula for cyclotomic fields.** If K is abelian over $\mathbb{Q}$, we have $\zeta_K(s) = \prod_\chi L(s,\chi)$, here χ runs over all primitive characters associated to characters of $\mathrm{Gal}(K/\mathbb{Q})$. Thus

$$\frac{2^{r_1}(2\pi)^{r_2}\#\mathrm{Cl}(K)\,\mathrm{Reg}(\mathcal{O}_K^\times)}{w_K\sqrt{|D_K|}} = \prod_{\chi\neq 1} L(s,\chi).$$

Now let K be the cyclotomic field $\mathbb{Q}(\zeta_p)$, p be an odd prime. Denote c the complex conjugation in $\mathrm{Gal}(K/\mathbb{Q})$ and $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be the fixed field of c, then the natural norm map $1 + c : \mathrm{Cl}(K) \to \mathrm{Cl}(K^+)$ is surjective. Define the minus part $\mathrm{Cl}(K)^-$ to be the kernel of this map.

If $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ is a non-trivial Dirichlet character, we have the special value formula of the Dirichlet L-function [7]

$$L(1,\chi) = \begin{cases} -\dfrac{G(\chi,\zeta_p)}{p} \displaystyle\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \overline{\chi}(a)\log|1-\zeta_p^a|, & \text{if } \chi \text{ is even and non-trivial,} \\ \pi i \dfrac{G(\chi,\zeta_p)}{p} B_{1,\overline{\chi}}, & \text{if } \chi \text{ is odd.} \end{cases}$$

Here $G(\chi,\zeta_p) := \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi(a)\zeta_p^a$ is the Gauss sum. Therefore we have

Proposition 1.7. [7]

$$\#\mathrm{Cl}(K^+) = \frac{1}{2^{(p-3)/2}R(\mathcal{O}_{K^+}^\times)} \prod_{\chi\neq 1 \text{ even}} \sum_{a \bmod p} -\chi(a)\log|1-\zeta_p^a|,$$

$$\#\mathrm{Cl}(K)^- = 2p \prod_{\chi \text{ odd}} -\frac{1}{2}B_{1,\chi}.$$

Denote $\mathcal{E}$ (resp. $\mathcal{E}^+$) the group of units of K (resp. K^+). Let $\mathcal{C}$ be the subgroup of $\mathcal{E}$ generated by $\frac{\zeta_p^b - 1}{\zeta_p - 1}$, $(b,p) = 1$ and roots of unity. Let $\mathcal{C}^+ = \mathcal{C} \cap K^+$.

Proposition 1.8. [7] *We have*

$$\#\mathrm{Cl}(K^+) = \#(\mathcal{E}/\mathcal{C}) = \#(\mathcal{E}^+/\mathcal{C}^+)$$

Let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ and $R = \mathbb{Z}[\Delta]$. For $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ let $\sigma_a \in \Delta$ be the element given by $\zeta_p \mapsto \zeta_p^a$. The following element

$$\theta := \frac{1}{p}\sum_{a=1}^{p-1} a\sigma_a^{-1} \in \mathbb{Q}[\Delta],$$

is called the *Stickelberger element*. The Stickelberger ideal is defined by $S = R \cap R\theta$.

Proposition 1.9. [7] *We have*

$$\#\mathrm{Cl}(K)^- = \#(R^-/S^-)$$

1.7. **A refinement of class number formula for cyclotomic fields.** Let K be the cyclotomic field $\mathbb{Q}(\zeta_p)$ where p is an odd prime and $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be the maximal real subfield of K.

Theorem 1.10. *Let q be a prime such that $q \nmid p(p-1)$. Let L be a finite extension of $\mathbb{Q}_q$ and $\chi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathcal{O}_L^\times$ be an odd character. Then*

$$\#\left(\mathrm{Cl}(K) \otimes_{\mathbb{Z}} \mathcal{O}_L\right)_\chi = |B_{1,\overline{\chi}}|_q^{-[L:\mathbb{Q}_q]}.$$

Equivalently, $\mathrm{Cl}(K)^- \otimes \mathbb{Z}_q$ and $(R^-/S^-) \otimes \mathbb{Z}_q$ have the same Jordan-Hölder series as $\mathbb{Z}_q[\Delta]$-modules, which is a refinement of the minus class number formula (Prop. 1.9).

Theorem 1.11. *Let q be a prime such that $q \nmid \frac{p(p-1)}{2}$. Let L be a finite extension of $\mathbb{Q}_q$ and $\chi : \mathrm{Gal}(K^+/\mathbb{Q}) \to \mathcal{O}_L^\times$ be a character. Then*

$$\#\left(\mathrm{Cl}(K^+) \otimes_{\mathbb{Z}} \mathcal{O}_L\right)_\chi = \#\left((\mathcal{E}^+/\mathcal{C}^+) \otimes_{\mathbb{Z}} \mathcal{O}_L\right)_\chi .$$

Equivalently, $\mathrm{Cl}(K^+) \otimes \mathbb{Z}_q$ and $(\mathcal{E}^+/\mathcal{C}^+) \otimes \mathbb{Z}_q$ have the same Jordan-Hölder series as $\mathbb{Z}_q[\Delta^+]$-modules, here $\Delta^+ = \mathrm{Gal}(K^+/\mathbb{Q})$. This is a refinement of the plus class number formula (Prop. 1.8).

Note that R^-/S^- and $\mathcal{E}^+/\mathcal{C}^+$ are cyclic **(??????)** hence we obtain the following two results as corollaries:

Proposition 1.12. *Let q be a prime such that $q \nmid p(p-1)$. Then $S \otimes_{\mathbb{Z}} \mathbb{Z}_q$ annihilates $\mathrm{Cl}(K) \otimes_{\mathbb{Z}} \mathbb{Z}_q$.*

Theorem 1.13 (Thaine's Theorem)**.** *Let q be a prime such that $q \nmid \frac{p(p-1)}{2}$. Let $R^+ = \mathbb{Z}_q[\Delta^+]$. Then*

$$2 \cdot \mathrm{Ann}_{R^+}\left((\mathcal{E}^+/\mathcal{C}^+) \otimes_{\mathbb{Z}} \mathbb{Z}_q\right) \subseteq \mathrm{Ann}_{R^+}\left(\mathrm{Cl}(K^+) \otimes_{\mathbb{Z}} \mathbb{Z}_q\right).$$

In fact, we have the Stickelberger's Theorem which is slightly stronger than Proposition 1.12:

Theorem 1.14 (Stickelberger's Theorem)**.** *The Stickelberger ideal S annihilates $\mathrm{Cl}(K)$.*

We present a proof of Stickelberger's Theorem in §2, and a proof of the following weak version of Thaine's Theorem in §3, without using the refinement of class number formula.

Theorem 1.15. *Let q be a prime such that $q \nmid p(p-1)$. Let $R^+ = \mathbb{F}_q[\Delta^+]$. Then*

$$\mathrm{Ann}_{R^+}\left((\mathcal{E}^+/\mathcal{C}^+) \otimes_{\mathbb{Z}} \mathbb{F}_q\right) \subseteq \mathrm{Ann}_{R^+}\left(\mathrm{Cl}(K^+) \otimes_{\mathbb{Z}} \mathbb{F}_q\right).$$

2. Stickelberger's Theorem

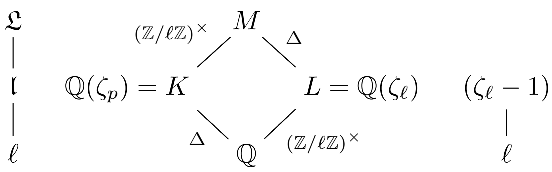
Recall that $K = \mathbb{Q}(\zeta_p)$, $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ and $R = \mathbb{Z}[\Delta]$. We are going to prove the Stickelberger's Theorem (Thm. 1.14), namely, the Stickelberger ideal $S := R \cap R\theta$ annihilates $\mathrm{Cl}(K)$.

Lemma 2.1. *Let $\mathfrak{C} \in \mathrm{Cl}(K)$ be an ideal class. Then there exists infinitely many prime $\ell \equiv 1 \pmod p$ such that there exists a prime $\mathfrak{l}$ of K above ℓ satisfying $\mathfrak{l} \in \mathfrak{C}$.*

Proof. Consider the Hilbert class field H_K of K. Then $H_K/\mathbb{Q}$ is Galois. Consider the element $\sigma_{\mathfrak{C}} \in \mathrm{Gal}(H_K/K) \subset \mathrm{Gal}(H_K/\mathbb{Q})$ corresponding to $\mathfrak{C}$. By Chebotarev density theorem, there exists infinitely many prime $\mathfrak{L}$ of H_K such that $\mathrm{Frob}_{\mathfrak{L}}(H_K/\mathbb{Q}) = \sigma_{\mathfrak{C}}$. Take $\ell = \mathfrak{L} \cap \mathbb{Z}$ and $\mathfrak{l} = \mathfrak{L} \cap \mathcal{O}_K$ then they satisfy the desired condition. □

Therefore we only need to prove that for any such $\mathfrak{l}$ and any $\beta \in R$ such that $\beta\theta \in R$, $\mathfrak{l}^{\beta\theta}$ is principal.

Let $L = \mathbb{Q}(\zeta_\ell)$, then K and L are linearly disjoint over $\mathbb{Q}$. Let $M = KL$:



Since ℓ is unramified in K and is totally ramified in L, the $\mathfrak{l}$ is totally ramified in M. Let $\mathfrak{L}$ be the unique prime ideal of M over $\mathfrak{l}$, then $\mathfrak{l}\mathcal{O}_M = \mathfrak{L}^{\ell-1}$. The $(\zeta_\ell - 1)\mathcal{O}_L$ is the unique prime ideal of L above ℓ, and $\ell\mathcal{O}_L = (\zeta_\ell - 1)^{\ell-1}\mathcal{O}_L$. Any prime of K above ℓ is of form $\mathfrak{l}^\sigma$ for a unique $\sigma \in \Delta$, and we have $\ell\mathcal{O}_K = \prod_{\sigma\in\Delta} \mathfrak{l}^\sigma$. Similarly, any prime of M above ℓ is of form $\mathfrak{L}^\sigma$ for a unique $\sigma \in \mathrm{Gal}(M/L) \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q}) = \Delta$, and we have $(\zeta_\ell - 1)\mathcal{O}_M = \prod_{\sigma\in\mathrm{Gal}(M/L)} \mathfrak{L}^\sigma$ as well as $\ell\mathcal{O}_M = \prod_{\sigma\in\mathrm{Gal}(M/L)} (\mathfrak{L}^\sigma)^{\ell-1}$.

Let s be a generator of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ and define a surjective group homomorphism $\chi : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \mu_p$ by $s \mapsto \zeta_p$. Consider the Gauss sum $G(\chi, \zeta_\ell) \in \mathcal{O}_M$. We have $G(\chi, \zeta_\ell) \cdot \overline{G(\chi, \zeta_\ell)} = \ell$, therefore we may write

$$G(\chi, \zeta_\ell)\mathcal{O}_M = \prod_{\sigma\in\mathrm{Gal}(M/L)} (\mathfrak{L}^\sigma)^{r(\sigma)},$$

where for each σ, $r(\sigma)$ is an integer satisfying $0 \le r(\sigma) \le \ell - 1$. If $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, denote by $r(a) := r(\sigma_a^{-1})$.

Lemma 2.2. *There exists an element $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ we have $r(a) = (\ell - 1)\left\{\frac{ac}{p}\right\}$, here $\left\{\frac{ac}{p}\right\}$ is the fractional part of $\frac{ac}{p}$. In particular, we have $0 < r(a) < \ell - 1$.*

Proof. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ be an element and denote $\sigma := \sigma_a^{-1}$. Consider the quantity $G(\chi,\zeta_\ell)/(\zeta_\ell - 1)^{r(a)} \in M$, then by definition it is a $\mathfrak{L}^\sigma$-unit. Since any prime above ℓ is totally ramified over M/K, for any $\tau \in \mathrm{Gal}(M/K)$, any $\sigma \in \mathrm{Gal}(M/L)$ and any $x \in \mathcal{O}_M$, we have $x^\tau \equiv x \pmod{\mathfrak{L}^\sigma}$. Now we take τ to be $\zeta_\ell \mapsto \zeta_\ell^s$, then we have

$$0 \not\equiv \frac{G(\chi,\zeta_\ell)}{(\zeta_\ell-1)^{r(a)}} \equiv \left(\frac{G(\chi,\zeta_\ell)}{(\zeta_\ell-1)^{r(a)}}\right)^\tau \pmod{\mathfrak{L}^\sigma}.$$

On the other hand, we have $G(\chi,\zeta_\ell)^\tau = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi(a)\zeta_\ell^{sa} = \chi(s^{-1})\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times}\chi(a)\zeta_\ell^a = \zeta_p^{-1}G(\chi,\zeta_\ell)$ as well as $(\zeta_\ell-1)^\tau = \zeta_\ell^s - 1 = (\zeta_\ell-1)(\zeta_\ell^{s-1}+\cdots+\zeta_\ell+1)$, hence

$$\left(\frac{G(\chi,\zeta_\ell)}{(\zeta_\ell-1)^{r(a)}}\right)^\tau = \frac{\zeta_p^{-1}}{(\zeta_\ell^{s-1}+\cdots+\zeta_\ell+1)^{r(a)}}\cdot\frac{G(\chi,\zeta_\ell)}{(\zeta_\ell-1)^{r(a)}} \equiv \frac{\zeta_p^{-1}}{s^{r(a)}}\cdot\frac{G(\chi,\zeta_\ell)}{(\zeta_\ell-1)^{r(a)}} \pmod{\mathfrak{L}^\sigma},$$

therefore $s^{r(a)} \equiv \zeta_p^{-1} \pmod{\mathfrak{L}^\sigma}$, taking σ^{-1} and note that both side are in $\mathcal{O}_K$, we obtain $s^{r(a)} \equiv (\zeta_p^{-1})^{\sigma^{-1}} = \zeta_p^{-a} \pmod{\mathfrak{l}}$. Note that $\mathcal{O}_K/\mathfrak{l} \cong \mathbb{Z}/\ell\mathbb{Z}$ and that ℓ is unramified in K, we have $\zeta_p^{-1} \in (\mathcal{O}_K/\mathfrak{l})^\times$ is of exact order p, hence there exists $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ (of course independent of a) such that $\zeta_p^{-1} \equiv s^{c\cdot(\ell-1)/p} \pmod{\mathfrak{l}}$. Therefore $s^{r(a)} \equiv s^{ac\cdot(\ell-1)/p} \pmod{\mathfrak{l}}$, which means $r(a) \equiv ac\cdot(\ell-1)/p \pmod{\ell-1}$, combined with $0 \le r(a) \le \ell-1$ we obtain the desired result. □

In the above proof we actually shows that for any $\tau \in \mathrm{Gal}(M/K)$, $G(\chi,\zeta_\ell)^\tau/G(\chi,\zeta_\ell) \in \mu_p \subset \mathcal{O}_K$. Therefore $G(\chi,\zeta_\ell)^{\ell-1} \in \mathcal{O}_K$. Note that for any $\sigma \in \mathrm{Gal}(M/L)$, we have $\mathfrak{l}^\sigma\mathcal{O}_M = (\mathfrak{L}^\sigma)^{\ell-1}$, hence

$$G(\chi,\zeta_\ell)^{\ell-1}\mathcal{O}_K = \prod_{\sigma\in\mathrm{Gal}(M/L)} (\mathfrak{l}^\sigma)^{r(\sigma)} = \left(\sum_{a=1}^{p-1} r(a)\sigma_a^{-1}\right)\mathfrak{l} = \big((\ell-1)\sigma_c\theta\big)\mathfrak{l}$$

is a principal ideal; here we note that $\sum_{a=1}^{p-1} r(a)\sigma_a^{-1} = \sum_{a=1}^{p-1}(\ell-1)\left\{\frac{ac}{p}\right\}\sigma_a^{-1} = (\ell-1)\sigma_c\theta$.

Let $\gamma := (\sigma_c^{-1}\beta)G(\chi,\zeta_\ell) \in M$, then $\gamma^{\ell-1} = (\sigma_c^{-1}\beta)G(\chi,\zeta_\ell)^{\ell-1} \in K$ and $\gamma^{\ell-1}\mathcal{O}_K = \big((\ell-1)\beta\theta\big)\mathfrak{l}$ is the $(\ell-1)$-th power of the fractional ideal $(\beta\theta)\mathfrak{l}$ of K. Hence the extension $K(\gamma)/K$ is unramified outside $\ell-1$ (exercise 2). However, $K(\gamma) \subset M$ and M/K is is totaly ramified at ℓ, so we must have $K(\gamma) = K$, $\gamma \in K$ and $\gamma\mathcal{O}_K = (\beta\theta)\mathfrak{l}$ is principal. This completes the proof of Stickelberger's Theorem.

3. Thaine's Theorem

In this section we prove Theorem 1.15.

Recall that $K^+ = \mathbb{Q}(\zeta_p+\zeta_p^{-1})$, $\Delta^+ = \mathrm{Gal}(K^+/\mathbb{Q})$, q is a prime not dividing $p(p-1)$, and $R^+ = \mathbb{F}_q[\Delta^+]$. Recall that $\mathcal{E} := \mathcal{O}_K^\times$, $\mathcal{E}^+ := \mathcal{O}_{K^+}^\times$, $\mathcal{C} := \left\langle \frac{\zeta_p^b-1}{\zeta_p-1} \mid b \in (\mathbb{Z}/p\mathbb{Z})^\times \right\rangle \cdot \mu(K) \subset \mathcal{E}$, and $\mathcal{C}^+ := \mathcal{C}\cap\mathcal{E}^+$. Obviously we have $(\mathcal{E}^+/\mathcal{C}^+)\otimes\mathbb{F}_q = \mathcal{E}^+/(\mathcal{E}^+)^q\mathcal{C}^+$. Note that $\frac{\zeta_p^{-b}-1}{\zeta_p-1} = -\zeta_p^{-b}\frac{\zeta_p^b-1}{\zeta_p-1}$, so we also have $\mathcal{C} = \left\langle \frac{\zeta_p^b-1}{\zeta_p-1} \mid 2 \le b \le \frac{p-1}{2}\right\rangle \cdot \mu(K)$.

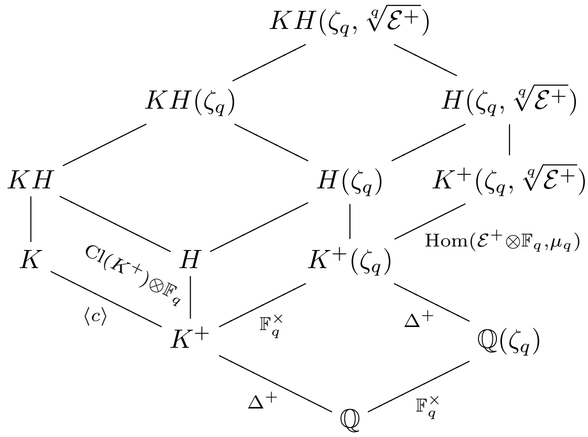
Fact 3.1. *The $\mathcal{E}^+\otimes\mathbb{F}_q$ is a cyclic $\mathbb{F}_q[\Delta^+]$-module.*

Lemma 3.2. *Let $\mathfrak{C} \in \mathrm{Cl}(K^+)\otimes\mathbb{F}_q$ be a class. Then there exists infinity many prime $\ell \equiv 1 \pmod{pq}$ such that there exists a prime $\mathfrak{l}$ of K^+ above ℓ satisfying $\mathfrak{l}\in\mathfrak{C}$ and such that the natural map*

$$\mathcal{E}^+\otimes\mathbb{F}_q \to (\mathcal{O}_{K^+}/\ell\mathcal{O}_{K^+})^\times\otimes\mathbb{F}_q \cong \prod_{\sigma\in\Delta^+}(\mathcal{O}_{K^+}/\mathfrak{l}^\sigma)^\times\otimes\mathbb{F}_q \cong \prod_{\sigma\in\Delta^+}(\mathbb{Z}/\ell\mathbb{Z})^\times\otimes\mathbb{F}_q \tag{3.1}$$

is injective.

Proof. Let H be the maximal unramified abelian extension of K^+ such that $\mathrm{Gal}(H/K^+)$ is killed by q. Then $\mathrm{Gal}(H/K^+) \cong \mathrm{Cl}(K^+) \otimes \mathbb{F}_q$ and $H/\mathbb{Q}$ is Galois. Consider the following field extension diagram:



Here by Kummer theory, we have the isomorphism of $\mathrm{Gal}(K^+(\zeta_q)/\mathbb{Q})$-modules

$$\begin{aligned} \mathrm{Gal}(K^+(\zeta_q, \sqrt[q]{\mathcal{E}^+})/K^+(\zeta_q)) &\xrightarrow{\sim} \mathrm{Hom}(\mathcal{E}^+ \otimes \mathbb{F}_q, \mu_q), \\ \sigma &\mapsto \left(u \mapsto \frac{(\sqrt[q]{u})^\sigma}{\sqrt[q]{u}} \right). \end{aligned}$$

We note that the K, H and $K^+(\zeta_q, \sqrt[q]{\mathcal{E}^+})$ are pairwise linearly disjoint over K^+:

- the K and $H(\zeta_q, \sqrt[q]{\mathcal{E}^+})$ are linearly disjoint over K^+ since p is totally ramified over K/K^+ and is unramified over $H(\zeta_q, \sqrt[q]{\mathcal{E}^+})/K^+$;
- the H and $K^+(\zeta_q)$ are linearly disjoint over K^+ since q is unramified over H/K^+ and is totally ramified over $K^+(\zeta_q)/K^+$;
- the $H(\zeta_q)$ and $K^+(\zeta_q, \sqrt[q]{\mathcal{E}^+})$ are linearly disjoint over $K^+(\zeta_q)$, since $\mathrm{Gal}(K^+(\zeta_q)/K^+)$ acts on $\mathrm{Gal}(H(\zeta_q)/K^+(\zeta_q))$ by trivial character, and acts on $\mathrm{Gal}(K^+(\zeta_q, \sqrt[q]{\mathcal{E}^+})/K^+(\zeta_q)) \cong \mathrm{Hom}(\mathcal{E}^+ \otimes \mathbb{F}_q, \mu_q)$ by mod q cyclotomic character.

Hence we have $\mathrm{Gal}(KH(\zeta_q, \sqrt[q]{\mathcal{E}^+})/K^+) \cong \mathrm{Gal}(K/K^+) \times \mathrm{Gal}(H/K^+) \times \mathrm{Gal}(K^+(\zeta_q, \sqrt[q]{\mathcal{E}^+})/K^+)$, and $KH(\zeta_q, \sqrt[q]{\mathcal{E}^+})/\mathbb{Q}$ is Galois.

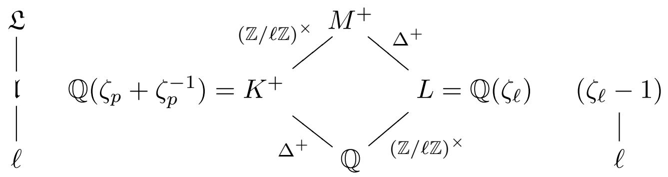
Since $\mathcal{E}^+ \otimes \mathbb{F}_q$ is a cyclic $\mathbb{F}_q[\Delta^+]$-module, the $\mathrm{Gal}(K^+(\zeta_q, \sqrt[q]{\mathcal{E}^+})/K^+(\zeta_q)) \cong \mathrm{Hom}(\mathcal{E}^+ \otimes \mathbb{F}_q, \mu_q)$ is also a cyclic $\mathbb{F}_q[\Delta^+]$-module. Let τ be a generator of it. Let $\sigma_{\mathfrak{C}} \in \mathrm{Gal}(H/K^+)$ be the element corresponding to $\mathfrak{C}$. Then by Chebotarev density theorem, there exists infinitely many prime $\mathfrak{L}$ of $KH(\zeta_q, \sqrt[q]{\mathcal{E}^+})$ such that $\mathrm{Frob}_{\mathfrak{L}}(KH(\zeta_q, \sqrt[q]{\mathcal{E}^+})/\mathbb{Q})$ is equal to

$$\begin{aligned} (1, \sigma_{\mathfrak{C}}, \tau) &\in \mathrm{Gal}(K/K^+) \times \mathrm{Gal}(H/K^+) \times \mathrm{Gal}(K^+(\zeta_q, \sqrt[q]{\mathcal{E}^+})/K^+(\zeta_q)) \\ &\subset \mathrm{Gal}(K/K^+) \times \mathrm{Gal}(H/K^+) \times \mathrm{Gal}(K^+(\zeta_q, \sqrt[q]{\mathcal{E}^+})/K^+) \\ &= \mathrm{Gal}(KH(\zeta_q, \sqrt[q]{\mathcal{E}^+})/K^+) \subset \mathrm{Gal}(KH(\zeta_q, \sqrt[q]{\mathcal{E}^+})/\mathbb{Q}). \end{aligned}$$

Take $\ell = \mathfrak{L} \cap \mathbb{Z}$ and $\mathfrak{l} = \mathfrak{L} \cap \mathcal{O}_{K^+}$, we claim that they satisfy the desired condition. In fact we only need to check that the map (3.1) is injective. Suppose $u \in \mathcal{E}^+$ is in the kernel of (3.1), then we have $(u \bmod \mathfrak{l}^\sigma) \in ((\mathcal{O}_{K^+}^\times/\mathfrak{l}^\sigma)^\times)^q \cong (\mathbb{F}_\ell^\times)^q$ for any $\sigma \in \Delta^+$, i.e. $u^{(\ell-1)/q} \equiv 1 \pmod{\mathfrak{l}^\sigma}$ for any $\sigma \in \Delta^+$. Since the τ is equal to the restriction of $\mathrm{Frob}_{\mathfrak{L}}$ to $K^+(\zeta_q, \sqrt[q]{\mathcal{E}^+})$, we have $(\sqrt[q]{u})^\tau \equiv (\sqrt[q]{u})^\ell \pmod{\mathfrak{L}}$, therefore $(\sqrt[q]{u})^\tau/\sqrt[q]{u} \equiv (\sqrt[q]{u})^{\ell-1} = u^{(\ell-1)/q} \equiv 1 \pmod{\mathfrak{L}}$. On the other hand, $(\sqrt[q]{u})^\tau/\sqrt[q]{u} \in \mu_q \subset \mathbb{F}_\ell^\times$, hence we must have $(\sqrt[q]{u})^\tau = \sqrt[q]{u}$ and $\sqrt[q]{u} \in K^+(\zeta_q)$ since τ is a generator. This implies that $u \in (K^\times)^q$ (let σ_a be a generator of $\mathrm{Gal}(K^+(\zeta_q)/K^+) \cong \mathbb{F}_q^\times$, then $1 \neq a \in \mathbb{F}_q^\times$ hence $1 - a \in \mathbb{F}_q^\times$; we have $(\sqrt[q]{u})^{\sigma_a} = \zeta \cdot \sqrt[q]{u}$ for some $\zeta \in \mu_q$, let $b = (1-a)^{-1} \in \mathbb{F}_q^\times$ then it's easy to see that $\zeta^b \cdot \sqrt[q]{u}$ is fixed by σ_a), hence $u \in (\mathcal{E}^+)^q$. □

Therefore we only need to prove that for any such $\mathfrak{l}$, if $\beta \in \mathrm{Ann}_{R^+}((\mathcal{E}^+/\mathcal{C}^+) \otimes_{\mathbb{Z}} \mathbb{F}_q)$, i.e. if $u^\beta \in (\mathcal{E}^+)^q \mathcal{C}^+$ for all $u \in \mathcal{E}^+$, then $\mathfrak{l}^\beta \in \mathrm{Cl}(K^+)^q$.

Let $L = \mathbb{Q}(\zeta_\ell)$, then K^+ and L are linearly disjoint over $\mathbb{Q}$. Let $M^+ = K^+L$:



Since ℓ is unramified in K^+ and is totally ramified in L, the $\mathfrak{l}$ is totally ramified in M^+. Let $\mathfrak{L}$ be the unique prime ideal of M^+ over $\mathfrak{l}$, then $\mathfrak{l}\mathcal{O}_{M^+} = \mathfrak{L}^{\ell-1}$. The $(\zeta_\ell - 1)\mathcal{O}_L$ is the unique prime ideal of L above ℓ, and $\ell\mathcal{O}_L = (\zeta_\ell - 1)^{\ell-1}\mathcal{O}_L$. Any prime of K^+ above ℓ is of form $\mathfrak{l}^\sigma$ for a unique $\sigma \in \Delta^+$, and we have $\ell\mathcal{O}_{K^+} = \prod_{\sigma\in\Delta^+}\mathfrak{l}^\sigma$. Similarly, any prime of M^+ above ℓ is of form $\mathfrak{L}^\sigma$ for a unique $\sigma \in \mathrm{Gal}(M^+/L) \xrightarrow{\sim} \mathrm{Gal}(K^+/\mathbb{Q}) = \Delta^+$, and we have $(\zeta_\ell - 1)\mathcal{O}_{M^+} = \prod_{\sigma\in\mathrm{Gal}(M^+/L)}\mathfrak{L}^\sigma$ as well as $\ell\mathcal{O}_{M^+} = \prod_{\sigma\in\mathrm{Gal}(M^+/L)}(\mathfrak{L}^\sigma)^{\ell-1}$.

Note that $\prod_{\sigma\in\Delta^+}(\mathbb{Z}/\ell\mathbb{Z})^\times \otimes \mathbb{F}_q$ is (non-canonically) isomorphic to $\mathbb{F}_q[\Delta^+]$ as a $\mathbb{F}_q[\Delta^+]$-module, given by $(s^{n(\sigma)})_{\sigma\in\Delta^+} \mapsto \sum_{\sigma\in\Delta^+} n(\sigma)\sigma$, where s is a fixed generator of $(\mathbb{Z}/\ell\mathbb{Z})^\times$. We can conclude that under this isomorphism and (3.1), $\mathcal{E}^+ \otimes \mathbb{F}_q$ is isomorphic to $\mathbb{F}_q[\Delta^+]^{\mathrm{sum}=0}$ as a $\mathbb{F}_q[\Delta^+]$-module, where $\mathrm{sum} : \mathbb{F}_q[\Delta^+] \to \mathbb{F}_q$, $\sum_{\sigma\in\Delta^+} n(\sigma)\sigma \mapsto \sum_{\sigma\in\Delta^+} n(\sigma)$. This is by counting dimension and note that for any $u \in \mathcal{E}^+$ we have $[u] = [u^{q+1}] \in \mathcal{E}^+/(\mathcal{E}^+)^q$ and $\mathrm{N}_{K^+/\mathbb{Q}}(u^{q+1}) = 1$, it's easy to see that the image of u^{q+1} in $\mathbb{F}_q[\Delta^+]$ is contained in $\mathbb{F}_q[\Delta^+]^{\mathrm{sum}=0}$.

Lemma 3.3. *Let $\delta \in (\mathcal{C}^+)^2$ be an element. Then there exists an element $\varepsilon \in \mathcal{O}_{M^+}^\times$ such that $\mathrm{N}_{M^+/K^+}(\varepsilon) = 1$ and $\varepsilon \equiv \delta \pmod{\mathfrak{L}^\sigma}$ for all $\sigma \in \mathrm{Gal}(M^+/L)$ (or equivalently, $\varepsilon \equiv \delta \pmod{\zeta_\ell - 1}$).*

Proof. Let c be the unique non-trivial element of $\mathrm{Gal}(M/M^+)$, which is also the unique non-trivial element of $\mathrm{Gal}(K/K^+)$, here the field $M = KL$ is defined in §2. First we claim that $(\mathcal{C}^+)^2 = \mathrm{N}_{K/K^+}(\mathcal{C})$: in fact, for $b \in (\mathbb{Z}/p\mathbb{Z})^\times$ we have $\left(\frac{\zeta_p^b-1}{\zeta_p-1}\right)^c = \frac{\zeta_p^{-b}-1}{\zeta_p^{-1}-1} = \zeta_p^{1-b}\frac{\zeta_p^b-1}{\zeta_p-1}$, therefore

$$\mathrm{N}_{K/K^+}(\mathcal{C}) = \left\{ \prod_{b=2}^{(p-1)/2} (\zeta_p^{1-b})^{m(b)} \prod_{b=2}^{(p-1)/2} \left(\frac{\zeta_p^b - 1}{\zeta_p - 1}\right)^{2m(b)} \;\middle|\; m(b) \in \mathbb{Z} \right\},$$

as well as

$$\mathcal{C}^+ = \left\{ \gamma \prod_{b=2}^{(p-1)/2} \left(\frac{\zeta_p^b - 1}{\zeta_p - 1}\right)^{m(b)} \;\middle|\; \begin{array}{l} m(b) \in \mathbb{Z},\ \gamma \in \mu(K) = \mu_{2p} \text{ such that} \\ \gamma^2 = \prod_{b=2}^{(p-1)/2} (\zeta_p^{1-b})^{m(b)} \in \mu_p \end{array} \right\},$$

here we note that once $m(b)$ is given, there are always two γ satisfy the condition.

Therefore if $\delta \in (\mathcal{C}^+)^2 = \mathrm{N}_{K/K^+}(\mathcal{C})$, we may write

$$\delta = \mathrm{N}_{K/K^+}\left(\prod_{b\in(\mathbb{Z}/p\mathbb{Z})^\times} (\zeta_p^b - 1)^{m(b)} \right) = \prod_{b\in(\mathbb{Z}/p\mathbb{Z})^\times} \left((\zeta_p^b - 1)(\zeta_p^{-b} - 1)\right)^{m(b)}$$

where $m(b)$ satisfies $\sum_{b\in(\mathbb{Z}/p\mathbb{Z})^\times} m(b) = 0$. We take ε to be

$$\varepsilon := \mathrm{N}_{M/M^+}\left(\prod_{b\in(\mathbb{Z}/p\mathbb{Z})^\times} (\zeta_p^b - \zeta_\ell)^{m(b)} \right) = \prod_{b\in(\mathbb{Z}/p\mathbb{Z})^\times} \left((\zeta_p^b - \zeta_\ell)(\zeta_p^{-b} - \zeta_\ell)\right)^{m(b)},$$

then it is easy to check that ε satisfies all the desired properties. □

Now let $u_0 \in \mathcal{E}^+$ be an element which maps to a generator of $\mathcal{E}^+ \otimes \mathbb{F}_q$ as a $\mathbb{F}_q[\Delta^+]$-module (note that $\mathcal{E}^+ \otimes \mathbb{F}_q \cong \mathbb{F}_q[\Delta^+]^{\mathrm{sum}=0} \xrightarrow{\sim} \mathbb{F}_q[\Delta^+]/\sum_{\sigma\in\Delta^+}\sigma$ which is a cyclic $\mathbb{F}_q[\Delta^+]$-module), and let $u = u_0^{q+1} \in \mathcal{E}^+$, then obviously u and u_0 map to the same element of $\mathcal{E}^+ \otimes \mathbb{F}_q$ (by abuse of notation, we denote its image in $\mathbb{F}_q[\Delta^+]$ by u). Since $u_0^\beta \in (\mathcal{E}^+)^q\mathcal{C}^+$, we may write $u_0^\beta = v_0^q\delta_0$ for some $v_0 \in \mathcal{E}^+$ and $\delta_0 \in \mathcal{C}^+$, and write $u^\beta = v^q\delta$ with $v = v_0^{q+1} \in \mathcal{E}^+$ and $\delta = \delta_0^{q+1} \in (\mathcal{C}^+)^{q+1} \subset (\mathcal{C}^+)^2$ since q is odd. Let ε be the element corresponding to δ in the above lemma.

The generator s of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ gives a generator τ of $\mathrm{Gal}(M^+/K^+)$ by $\zeta_\ell \mapsto \zeta_\ell^s$. The $\tau \mapsto \varepsilon$ extends to a cocycle $\mathrm{Gal}(M^+/K^+) \to (M^+)^\times$ by the condition $\mathrm{N}_{M^+/K^+}(\varepsilon) = 1$. Hence by Hilbert's Theorem 90,

$H^1(M^+/K^+, (M^+)^\times) = 0$, the above cocycle is a coboundary, which means that there exists $\alpha \in (M^+)^\times$ such that $\alpha^\tau/\alpha = \varepsilon$.

The fractional ideal $\alpha\mathcal{O}_{M^+}$ is stable by $\mathrm{Gal}(M^+/K^+)$-action, hence by considering prime ideal decomposition, $\alpha\mathcal{O}_{M^+} = (\mathfrak{a}\mathcal{O}_{M^+})\mathfrak{b}$ for some fractional ideal $\mathfrak{a}$ of K^+ whose prime ideal decomposition only contains unramified primes over M^+/K^+, and $\mathfrak{b}$ is a fractional ideal of M^+ whose prime ideal decomposition only contains ramified primes over M^+/K^+, namely, $\{\mathfrak{L}^\sigma\}_{\sigma\in\mathrm{Gal}(M^+/L)}$. This means that

$$\alpha\mathcal{O}_{M^+} = (\mathfrak{a}\mathcal{O}_{M^+}) \prod_{\sigma\in\mathrm{Gal}(M^+/L)} (\mathfrak{L}^\sigma)^{r(\sigma)}, \tag{3.2}$$

where for each σ, $r(\sigma)$ is an integer.

Similar to the proof of Lemma 2.2, for any $\sigma \in \mathrm{Gal}(M^+/L)$, the $\alpha/(\zeta_\ell - 1)^{r(\sigma)} \in M^+$ is a $\mathfrak{L}^\sigma$-unit, and

$$0 \not\equiv \frac{\alpha}{(\zeta_\ell-1)^{r(\sigma)}} \equiv \left(\frac{\alpha}{(\zeta_\ell-1)^{r(\sigma)}}\right)^\tau = \frac{\varepsilon\alpha}{(\zeta_\ell^s-1)^{r(\sigma)}} \equiv \frac{\varepsilon}{s^{r(\sigma)}}\cdot\frac{\alpha}{(\zeta_\ell-1)^{r(\sigma)}} \pmod{\mathfrak{L}^\sigma},$$

therefore $s^{r(\sigma)} \equiv \varepsilon \equiv \delta \pmod{\mathfrak{L}^\sigma}$ for any σ. Note that $s^{r(\sigma)}$ and δ are in $\mathcal{O}_{K^+}$, we obtain $s^{r(\sigma)} \equiv \delta \pmod{\mathfrak{l}^\sigma}$ for any σ, hence the image of δ (also equals the image of u^β) under the map

$$\mathcal{E}^+ \otimes \mathbb{F}_q \hookrightarrow (\mathcal{O}_{K^+}/\ell\mathcal{O}_{K^+})^\times \otimes \mathbb{F}_q \cong \mathbb{F}_q[\Delta^+]$$

is $\sum_{\sigma\in\Delta^+} r(\sigma)\sigma$. Since $\mathbb{F}_q[\Delta^+] = \mathbb{F}_q[\Delta^+]^{\mathrm{sum}=0} \oplus \mathbb{F}_q \cdot \sum_{\sigma\in\Delta^+}\sigma = \mathbb{F}_q[\Delta^+]\cdot u \oplus \mathbb{F}_q\cdot\sum_{\sigma\in\Delta^+}\sigma$, this implies that $\beta \in R^+$ can be written as $\beta = \beta_1\sum_{\sigma\in\Delta^+} r(\sigma)\sigma + \beta_2\sum_{\sigma\in\Delta^+}\sigma$ for some $\beta_1 \in \mathbb{F}_q[\Delta^+]$ and $\beta_2 \in \mathbb{F}_q$.

The N_{M^+/K^+} of (3.2) reads

$$\mathrm{N}_{M^+/K^+}(\alpha)\mathcal{O}_{K^+} = \mathfrak{a}^{\ell-1}\prod_{\sigma\in\Delta^+}(\mathfrak{l}^\sigma)^{r(\sigma)} = \mathfrak{a}^{\ell-1}\cdot\left(\sum_{\sigma\in\Delta^+} r(\sigma)\sigma\right)\mathfrak{l}$$

which is a principal ideal, hence $\left(\sum_{\sigma\in\Delta^+} r(\sigma)\sigma\right)\mathfrak{l} \in \mathrm{Cl}(K^+)^q$. On the other hand $\left(\sum_{\sigma\in\Delta^+}\sigma\right)\mathfrak{l} = \prod_{\sigma\in\Delta^+}\mathfrak{l}^\sigma = \ell\mathcal{O}_{K^+}$ is principal, so $\mathfrak{l}^\beta \in \mathrm{Cl}(K^+)^q$. This completes the proof of Theorem 1.15.

4. Catalan Equation

Theorem 4.1 (Catalan Conjecture)**.** *Let $p, q \geq 2$ be two integers, then the equation*

$$x^p - y^q = 1$$

has no solutions (x, y) in positive integers other that $(x, y, p, q) = (3, 2, 2, 3)$.

The cases of $q = 2$ and $p = 2$ are proved by Lebesgue and Chao Ko, respectively. Then to prove the conjecture, it reduces to the following

Main Theorem [Mihailescu]. *Let $p \neq q$ be two odd primes. Then the equation*

$$\begin{cases} x^p - y^q = 1, \\ x, y \in \mathbb{Z}\setminus\{0\} \end{cases}$$

has no solutions. (We call the above Diophantine equation $(*)$ the Catalan equation.)

We give some elementary remarks. First, $x^p - y^q = 1$ is equivalent to $(-y)^q - (-x)^p = 1$.

Lemma 4.2. *For any integer $x \neq 1$,*

$$\left(x-1, \frac{x^p-1}{x-1}\right) = 1 \text{ or } p.$$

Moreover, $p|x-1$ if and only if $p\left|\frac{x^p-1}{x-1}\right.$, and in this case $p^2 \nmid \frac{x^p-1}{x-1}$.

Proof. Note that $\frac{(z+1)^p-1}{z} - p \equiv 0 \mod z$ for any integer $z \neq 0$. ∎

Lemma 4.3. *If (x, y) is a solution to the Catalan equation. Then*

$$\left(x-1, \frac{x^p-1}{x-1}\right) = p \iff p|y, \qquad \left(y+1, \frac{y^q+1}{y+1}\right) = q \iff q|x.$$

Lemma 4.4. *Assume that $q|x$, then*

(i) *$y \equiv -1 \pmod{q^{p-1}}$ and $|y| \geq q^{p-1} - 1$.*
(ii) *Moreover, if $(p, q-1) = 1$, then $|x| \geq q^{p-1} + q$.*

Proof. By Lemma 4.3, we may write

$$y+1=q^{p-1}a^p, \qquad \frac{y^q+1}{y+1}=qb^p; \qquad x=qab.$$

Thus (i) follows and moreover, we have

$$q^{p-1}\big|\ (y+1)\ \Big|\ \frac{y^q+1}{y+1}-q=q(b^p-1),$$

and therefore $b^p\equiv 1 \mod q^{p-2}$. Note that $(\mathbb{Z}/q^{p-2}\mathbb{Z})^\times \cong \mathbb{F}_q^\times \times \mathbb{Z}/q^{p-3}\mathbb{Z}$, and by assumption $(p,q(q-1))=1$, we have that $b\equiv 1 \mod q^{p-2}$. It is easy to see that $b>1$, thus

$$|x|\ge qb\ge q(q^{p-2}+1)=q^{p-1}+q.$$

□

Proposition 4.5 (Cassels)**.** *Assume that (x,y) is a solution to the Catalan equation. Then we have*

(1) *$q|x$ and $p|y$;*
(2) *$x\equiv 1 \pmod{p^{q-1}}$ and $y\equiv -1 \pmod{q^{p-1}}$;*
(3) *$|x|\ge \max(p^{q-1}(q-1)^q-1,\ q^{p-1}+q)$ and $|y|\ge \max(q^{p-1}(p-1)^p-1,\ p^{q-1}+p)$.*

Proof. It is easy to see that parts (2) and (3) follow from (1) by Lemma 4.4. Assume that $q\nmid x$. Then $\left(y+1,\dfrac{y^q+1}{y+1}\right)=1$ and $y+1=b^p$ for some integer $b\neq 0,1$. Thus $x^p-(b^p-1)^q=1$. Consider the increasing function $f(x)=x^p-(b^p-1)^q$ with $b\neq 0,1$ constant and x variable. It is easy to see that $f(b^q)>1$ and if $p>q$, then

$$\begin{cases}(b^q-1)^{1/q}<(b^p-1)^{1/p}, & \text{if } b>1;\\ (1+(-b)^q)^{1/q}>(1+(-b)^p)^{1/p}, & \text{if } b<0,\end{cases}$$

and therefore $f(b^q-1)<0$. Thus we have shown that if $p>q$ then $q|x$, and by symmetric if $q>p$ then $p|y$.

We now assume $p>q$ and want to show that $p|y$. Suppose that $p\nmid y$, then $x-1=a^q$ for some integer $a\neq 0$, and therefore $y=a^pF(a^{-q})$, where F is the function

$$F(t)=((1+t)^p-t^p)^{1/q}.$$

An observation is that the Taylor series around $t=0$ of $F(t)$ and that of $(1+t)^{p/q}$ have the same terms of degree $i<p$ (which is $\binom{p/q}{i}t^i$), since near $t=0$ we have that

$$F(t)=\sum_{i=0}^{\infty}\binom{1/q}{i}((1+t)^p-t^p-1)^i, \qquad (1+t)^{p/q}=\sum_{i=0}^{\infty}\binom{1/q}{i}((1+t)^p-1)^i.$$

Now for integer k, $p/q<k<p$, consider the q-integer

$$\beta=\beta_k:=a^{qk}\left(F(t)-F_k(t)\right)\big|_{t=a^{-q}}\in\mathbb{Z}[q^{-1}], \qquad F_k(t)=\sum_{i=0}^{k}\binom{p/q}{i}t^i$$

whose q-adic valuation is $\operatorname{ord}_q\binom{p/q}{k}=-k-\operatorname{ord}_q k!$. Thus we have a lower bound of $|\beta|$:

$$|\beta|\ge q^{\operatorname{ord}_q\beta}=q^{-k-\operatorname{ord}_q k!}.$$

On the other hand, since $q|x$ and $(p,q-1)=1$, by Lemma 4.4, $|a^q+1|=|x|\ge q^{p-1}+q$. This produces a contradictory upper bound of $|\beta|$ by applying the below lemma to $t=a^{-q}$ and $k=[p/q]+1$:

$$|\beta|\le\frac{|a|^q}{(|a|^q-1)^2}\le\frac{1}{|a|^q-2}\le q^{1-p}<q^{-k-\operatorname{ord}_q k!}.$$

□

Lemma 4.6. *For $k=[p/q]+1$, we have*

$$|F(t)-F_k(t)|\le\frac{|t|^{k+1}}{(1-|t|)^2}, \qquad \forall t\in\mathbb{R}, |t|<1.$$

Proof of Lemma 4.6. For $|t|<1$, we have

$$|F(t)-F_k(t)| \le \left|F(t)-(1+t)^{p/q}\right| + \left|(1+t)^{p/q}-F_k(t)\right|.$$

Now the first term can be estimated by the mean value theorem for the function $x \mapsto x^{1/q}$:

$$|F(t)-(1+t)^{p/q}| \le q^{-1}|t|^p|t'|^{q^{-1}-1} \le q^{-1}|t|^p(1-|t|)^{p(q^{-1}-1)} \le q^{-1}|t|^p(1-|t|)^{-2}.$$

Here $t' \in \mathbb{R}$ is between $(1+t)^p$ and $(1+t)^p - t^p$ so that $|t'| \ge (1-|t|)^p$. To estimate the second term, by the remainder term of Taylor series expansion of $G(t) := (1+t)^{p/q}$ (note that $G_k = F_k$ for $k<p$), we have

$$\left|(1+t)^{p/q}-F_k(t)\right| = \left|\frac{t^{k+1}}{(k+1)!}G^{k+1}(t')\right| \le \left|\binom{p/q}{k+1}\right||t|^{k+1}(1-|t|)^{-k-1+p/q} \le \frac{1}{k+1}|t|^{k+1}(1-|t|)^{-2}.$$

Here $t' \in \mathbb{R}$ is between 0 and t so that $|1+t'| \le 1-|t|$.

Now combining two terms and noting that $p>k+1, k, q \ge 2$, we have

$$|F(t)-F_k(t)| \le \left(\frac{|t|^p}{q} + \frac{|t|^{k+1}}{k+1}\right)(1-|t|)^{-2} \le |t|^{k+1}(1-|t|)^{-2}.$$

□

4.1. **Selmer group and Mihailescu element.** Let $K = \mathbb{Q}(\mu_p)$ and $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. Denote I_K the group of fractional ideals of K. Consider the selmer group

$$\mathrm{Sel}(K,\mu_q) := \ker\left(K^\times/K^{\times,q} \to I_K/qI_K, \quad [\xi] \mapsto (\xi)\right).$$

Let E be the group of global units of K and $\mathrm{Cl}(K)$ the ideal class group of K. We have a exact sequence of $\mathbb{F}_q[\Delta]$-modules:

$$0 \to E/E^q \to \mathrm{Sel}(K,\mu_q) \to \mathrm{Cl}(K)[q] \to 0.$$

Here the first map is embedding and the second is given by $[\xi] \mapsto (\xi)^{1/q}$.

Proposition 4.7. *Let (x,y) be a solution of Catalan's equation in $\mathbb{Z}^2_{\neq 0}$, then:*

$$\xi := \left[\frac{x-\zeta}{1-\zeta}\right] \in \mathrm{Sel}(K,\mu_q),$$

here ζ is a fixed primitive p-th root of unity.

Remark 4.8. For any $\theta \in \mathbb{F}_q[\Delta]^{\deg=0}$, $\left[\frac{x-\zeta}{1-\zeta}\right]^\theta = [(x-\zeta)^\theta] \in \mathrm{Sel}(K,\mu_q)$. In particular, $\left[\frac{x-\zeta}{1-\zeta}\right]^- = [(x-\zeta)^-] \in \mathrm{Sel}(K,\mu_q)^-$.

4.2. **Stickelberger's theorem and** $[(x-\zeta)^-]$**.** The Stickelberger element in $\mathbb{Q}[\Delta]$ is defined by $\Theta = \sum_{i=1}^{p-1}\left\{\frac{i}{p}\right\}\sigma_i^{-1}$. The Stickelberger ideal is defined by $I = \mathbb{Z}[\Delta] \cap \Theta\mathbb{Z}[|\Delta]$.

Remark 4.9.

(1) The Stickelberger ideal is generated by $\theta_a = (a-\sigma_a)\Theta = \sum_{i=1}^{p-1}\left[\frac{ai}{p}\right]\sigma_i^{-1}$ for $(a,p)=1$.

(2) $(1-\tau)I$ is generated by $(1-\iota)(\theta_{a+1}-\theta_a)$, for $1 \le a \le (p-1)/2$.

Theorem 4.10 (Stickelberger)**.** [6]*$I \subset \mathrm{Ann}_{\mathbb{Z}[\Delta]}(\mathrm{Cl}(K))$. In particular,$(I \otimes \mathbb{F}_q)^- \subset \mathrm{Ann}_{\mathbb{F}_q[\Delta]}\mathrm{Sel}(K,\mu_q)^-$.*

Theorem 4.11. [8]*[A] Suppose $(x,y) \in \mathbb{Z}^2_{\neq 0}$ is a solution of Catalan's equation, then*

(0) *$p|h_q^-$ and $q|h_p^-$. In particular, $p,q \ge 41$.*
(1) *$q^2|x$ and $p^2|y$.*
(2) *$(q,p-1)=1$ and $(p,q-1)=1$.*

Remark 4.12. Idea of the proof:

(0) The element $[(x-\zeta)^-]$ is nontrivial in $\mathrm{Sel}(K,\mu_q)^- \simeq \mathrm{Cl}(K)[q]^-$.
(1) Using Stickelberger element, we can show that $\mathrm{Ann}_{\mathbb{F}_q[\Delta]}([(x-\zeta)^-]) \neq 0$. And we thus have $(1-\zeta x)^\theta = b^q$ for some $\theta \in (1-\tau)\mathbb{Z}[\Delta]$ (For example, $\theta = (1-\tau)\theta_2$.) such that $q \nmid \theta$ and $b \in K^\times$. As $q|x$, we know that $(1-\zeta x)^\theta = b^q \equiv 1 \pmod q$. Thus $(1-\zeta x)^\theta \equiv 1 \pmod{q^2}$, thus $q^2|x$.

(2) To show $(p, q-1) = 1$, reduce to show $q < 4p^2$. Note that for $\theta \in I(1-\tau)$, let $\alpha_\theta \in K^\times$ be such that $(x-\zeta)^\theta = \alpha_\theta^q$, then α_θ is very close to some ζ_q under a fixed embedding $K \to \mathbb{C}$. When $q \geq 4p^2$, We will find a θ such that α_θ and $\overline{\alpha_\theta}$ are very close to 1 and $||\theta||$ is very small such that the upper bound of $N(\alpha_\theta - 1)$ will small than the lower bound of $N(\alpha_\theta - 1) \geq (1+|x|)^{-||\theta||(p-1)/2q}$.

Proof.
(0)

Fact 4.13. *Let $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha - \beta \in \mathcal{O}_K^\times$ and $\alpha/\beta \in K^{\times, q}$, then we can produce a unit*

$$\gamma := (\alpha^{1/q} - \beta^{1/q})^q \in \mathcal{O}_K^\times,$$

where $\alpha^{1/q}, \beta^{1/q}$ are chosen such that $(\alpha^{1/q})^q = \alpha$, $(\beta^{1/q})^q = \beta$ and $\alpha^{1/q}/\beta^{1/q} \in K$.

If $\left[\frac{x-\zeta}{x-\overline{\zeta}}\right] \in \mathrm{Sel}(K, \mu_q)$ is trival, then $\frac{x-\zeta}{z-\overline{\zeta}} \in K^{\times, q}$. Let $\alpha = \frac{x-\zeta}{1-\zeta}$ and $\beta = \frac{x-\overline{\zeta}}{1-\zeta}$, then $\alpha, \beta \in \mathcal{O}_K$ and $\alpha - \beta = \frac{\overline{\zeta}-\zeta}{1-\zeta} \in \mathcal{O}_K^\times$. Then we have a unit $\gamma \in \mathcal{O}_K^\times$ as in the above fact. As K has no real embedding, $N(\gamma) = 1$. Note that γ does not depend on the choice of $\alpha^{1/q}$ and $\beta^{1/q}$, because $\zeta_q \notin K$. Let π be the unique prime ideal of K above p. We will study π-adic properties of the equation $N(\gamma) = 1$.

Write $\alpha = 1 + \mu$ here $\mu = \frac{x-1}{1-\zeta}$ with $p^{q-1}\pi^{-1} | \mu$. And we have $\beta = -\overline{\zeta}(1 + \overline{\mu})$ with $p^{q-1}\pi^{-1} | \overline{\mu}$. We may choose

$$w := (1+\mu)^{1/q} := \sum_{i=0}^{\infty} \binom{1/q}{i} \mu^i \in \overline{K} \cap K_\pi, \quad \text{and } w' := (-\overline{\zeta}(1+\overline{\mu}))^{1/q} := -\zeta^{-1/q} \sum_{i=0}^{\infty} \binom{1/q}{i} \overline{\mu}^i \in \overline{K} \cap K_\pi.$$

We have $w/w' \in K$ follows from $w \equiv 1 \pmod{\pi}$, $w' \equiv -1 \pmod{\pi}$ and the following fact:

Fact 4.14. *Let $\delta \in K$ be the unique element such that $\delta^q = \frac{x-\zeta}{x-\overline{\zeta}}$, then $\delta \equiv -1 \pmod{\pi}$.*

Proof. This is because $1 \equiv \delta\overline{\delta} \equiv \delta^2 \pmod{\pi}$ and $\delta^q \equiv -1 \pmod{\pi}$. ☐

$N(w - w')^q \equiv 1 \left(\operatorname{mod} \mu^2\right)$ implies $w - w' \equiv 1 + \overline{\zeta} \left(\operatorname{mod} \mu^2\right)$: By computation we have:

$$N(w - w')^q \equiv 1 + \frac{(x-1)(1-q)}{2q} \pmod{\pi(x-1)},$$

Thus $p | 1 - q$ and

$$w - w' \equiv (1 + \mu/q) + \zeta^{-1/q}(1 + \overline{\mu}/q) \equiv 1 + \overline{\zeta} \left(\operatorname{mod} \mu^2\right).$$

By the above analysis, we may consider expansion of $N(w - w')^q$ modulo μ^3. It turns out that

$$N(w - w')^q \equiv 1 + \frac{(1-q)(x-1)^2}{2q} \frac{1-p^2}{12} \left(\operatorname{mod} \mu^3\right),$$

thus $p^{q-1} | \frac{\pi^3(q-1)}{3}$, contradiction.

(2) We first reduce to show $q < 4p^2$: Write $y + 1 = q^{p-1}a^p$, then $1 \equiv q^{p-1}a^p \equiv a^p \pmod{p}$ and hence $a^p \equiv 1 \left(\operatorname{mod} p^2\right)$. As $p^2 | y$, we have $q^{p-1} \equiv 1 \left(\operatorname{mod} p^2\right)$. If $p | q-1$ then $q^p \equiv 1 \left(\operatorname{mod} p^2\right)$, thus $p^2 | q-1$. Fix an embedding $K \to \mathbb{C}$. Suppose that $q \geq 4p^2$, by the following lemma and the facts $|x| > q^{p-1}$ and $q > 5$ we get the contradiction.

Lemma 4.15. *If $q \geq 4p^2$, then there exists $\theta \in I^-$ with $||\theta|| \leq \frac{3q}{p-1}$ such that $N(\alpha_\theta - 1) \leq \frac{2^{p-1}}{(|x|+1)^2}$, here $\alpha_\theta \in K^\times$ is such that $(x-\zeta)^\theta = \alpha_\theta^q$.*

Proof.
- We have an injective homomorphism:

$$(1-\tau)\mathrm{Ann}_{\mathbb{Z}[\Delta]}([(x-\zeta)^-]) \to \{\alpha \in K^\times | \; \exists \zeta_q \in \mu_q \text{ such that } |\phi(\alpha) - \zeta_q| \leq \frac{||\theta||}{q(|x|-1)}\}$$

$$\theta \mapsto \alpha_\theta \text{ (such that } (x-\zeta)^\theta = \alpha_\theta^q).$$

  - Existence of ζ_q: Exists ζ_q such that $q \arg(\alpha_\theta \zeta_q^{-1}) = \arg(\alpha_\theta^q)$. Note that $|\alpha_\theta| = 1$, thus

$$|\alpha - \zeta_q| < |\arg(\alpha_\theta \zeta_q^{-1})| \leq 1/q |\log(1 - \zeta/x)^\theta| \leq \frac{||\theta||}{q(|x|-1)}.$$

  Here the last inequality follows from for $|z| < 1$, $|\log(1+z)| \leq \frac{|z|}{1-|z|}$, here the log is the principle branch of the logarithm.

  - Injectivity:(i) $\frac{x-\sigma(\zeta)}{1-\zeta}$ are co-prime to each other; (ii) The lower bound of $|x|$ implies $\frac{x-\sigma(\zeta)}{1-\zeta}$ is not unit.
- If $p, q \geq 5$ and $q \geq 4p^2$, then exists at least $q+1$ element in $I^- \subset (\mathrm{Ann}_{\mathbb{Z}[\Delta]}[(x-\zeta)^-])$ with size $||\theta|| \leq \frac{3}{2}\frac{q}{p-1}$.

  Thus by box principle, exists θ', θ'' such that corresponding to same ζ_q, thus can get upper bound of $|\alpha_{\theta'-\theta''}-1|$: $|\alpha_{\theta'-\theta''}-1| \leq |\alpha_{\theta'}-\zeta_q| + |\alpha_{\theta''}-\zeta_q| \leq \frac{3}{(p-1)(|x|-1)}$. Thus

$$N(\alpha_{\theta'-\theta}) \leq \frac{2^{p-1}}{(|x|+1))^2}.$$

  - Consider the stickelberger element $\theta_a = \sum_{i=1}^{p-1}\left[\frac{ai}{p}\right]\sigma_i^{-1}$, $1 \leq i \leq (p-1)/2$. Then $e_i := (1-\tau)(\theta_{i+1}-\theta_i)$ is a $\mathbb{Z}$-basis of I^- and has the property that half of coefficients equals to 1 and half of coefficients equals to -1. By using this fact, under the restriction $q \geq 4p^2$, exists at least $q+1$ element in I^- with $||\cdot|| \leq \frac{3q}{p-1}$.

□

□

Remark 4.16. Let E be the group of global units of K, C the subgroup of E generated by cyclic units i.e. the subgroup generated by roots of unity and $\frac{\zeta^{\frac{a}{2}}-\zeta^{-\frac{a}{2}}}{\zeta^{\frac{1}{2}}-\zeta^{-\frac{1}{2}}}$, $a = 2, \cdots, (p-1)/2$. Let C_q the subgroup of C generated by root of unity and elements which congruent to 1 modulo q^2.

(1) Let $\mathrm{Sel}_{\text{q-str,p-rel}}(K, \mu_q)$ be the subgroup of $K^\times/K^{\times,q}$ consists of ξ such that the prime decomposition of (ξ) is a q-th power outside primes above p and ξ is a q-th power at every prime divides q. $q^2|x$ implies that $[x-\zeta] \in \mathrm{Sel}_{\text{q-str,p-rel}}(K, \mu_q)$. As $q^2|x$, thus for any $\theta \in \mathbb{F}_q[\Delta]^+$, if $(x-\zeta)^\theta \in CK^{\times,q}/K^{\times,q}$, then $(x-\zeta)^\theta \in C_qK^{\times,q}/K^{\times,q}$.

(2) $(q, p-1) = 1$ implies that $R = \mathbb{F}_q[\Delta]$ is a semisimple algebra. Note that E/E^q is a cyclic R-module. Consider the filtration of E/E^q,

$$C_qE^q/E^q \subset CE^q/E^q \subset E/CE^q \subset EE^q,$$

we have

$$\mathrm{Ann}_R(C_qE^q/E^q)\cdot\mathrm{Ann}_R(CE^q/E^q)\cdot\mathrm{Ann}_R(E/C\mathcal{E}^q) = \mathrm{Ann}_R(E/E^q) = NR$$

4.3. **Rigidity of $[x-\zeta]^+$.** Let (x, y) be a solution to the Catalan equation and $\zeta \in \mu_p$ be a primitive p-th root of unity (will viewed as an element in $\mathbb{C}$). The algebraic number

$$x-\zeta \in K := \mathbb{Q}(\mu_p) \subset \mathbb{C}$$

will play a key role in the story. The following rigidity property of $x-\zeta$ is important to the proof of Catalan conjecture. Let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, $\sigma : (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} \Delta$ the isomorphism such that $\sigma_a(\zeta) = \zeta^a$. Denote by

$$\mathbb{Z}[\Delta]^+ = \{\sum_a n_a\sigma_a \in \mathbb{Z}[\Delta] \mid n_a = n_{p-a}\} = (1+\sigma_{-1})\mathbb{Z}[\Delta],$$

denote by $\deg : \mathbb{Z}[\Delta] \to \mathbb{Z}$ be the degree map $\deg(\sum n_a\sigma_a) = \sum_a n_\sigma$. Then we have

Theorem 4.17 (Mihailescu)**.** [2] *If $\theta \in (1+\tau)\mathbb{Z}[\Delta]$ with $q|\deg\theta$ such that $(x-\zeta)^\theta \in K^{\times,q}$, then $\theta \in q\mathbb{Z}[\Delta]$.*

Proof. Note that if $\alpha \in K^{\times,q}$, then there exists a unique $\alpha^{1/q} \in K^\times$. Consider

$$(x-\zeta)^{\theta/q} = x^{\deg\theta/q}(1-\zeta x^{-1})^{\theta/q} = x^{\deg\theta/q}G(x^{-1}),$$

where $G(t)$ is the analytic function around $t = 0$ defined as follows. Write $\theta = \sum n_a\sigma_a$ and fix an embedding of $\zeta+\zeta^{-1} \in \mathbb{R}$, then

$$G(t) = (1-\zeta t)^{\theta/q} = \prod_a(1-\zeta^a t)^{n_a/q} = \prod_a\sum_{i=0}^{\infty}\binom{n_a/q}{i}(-\zeta^a)^i t^i$$
$$= \sum_{k=0}^{\infty}\left(\sum_{\sum i_a = k}\prod_a\binom{n_a/q}{i_a}(-\zeta^a)^{i_a}\right)t^k = \sum_{k=0}^{\infty}\frac{a_k}{k!\cdot q^k}t^k,$$

where the summation over a should be regarded as summation over $a \mod \pm 1$ using $\theta \in \mathbb{Z}[\Delta]^+$

$$\begin{aligned} a_k &= k! q^k \sum_{\sum_a i_a = k} \prod_a \binom{n_a/q}{i_a} (-\zeta^a)^{i_a} \\ &= \sum_{\sum_{\sum i_a = k}} \frac{k!}{\prod_a i_a!} \prod_a n_a(n_a - q) \cdots (n_a - (i_a - 1)q)(-\zeta^a)^{i_a} \in \mathcal{O}_K \\ &\equiv \left(-\sum_a n_a \zeta^a \right)^k \pmod q \end{aligned}$$

Note that q is unramified over K, it is enough to show that $q | a_i$ for some $i > 0$. We may assume that $\theta = \sum_a n_a \sigma_a$ with

$$n_a \geq 0, \ \forall a; \quad 0 < k := \deg \theta / q \leq \frac{p-1}{2},$$

and we will show that $q | a_k$. Consider

$$\beta := q^{k + \mathrm{ord}_q k!} x^k \left(G(x^{-1}) - G_k(x^{-1}) \right) \in \mathcal{O}_K, \quad \beta \equiv a_k \mod q.$$

Here we have $x^k G(x^{-1}) \in \mathcal{O}_K$ since $n_a \geq 0$ for all a. We will actually show that $\beta = 0$ so that $q | a_k$ and complete the proof. Comparing $G(t)$ and $H(t) := (1-t)^{-k}$, by Taylor's theorem

$$\begin{aligned} |\beta| &\leq q^{k + \mathrm{ord}_q k!} |x|^k \left(H(|x|^{-1}) - H_k(|x|^{-1}) \right) \\ &\leq q^{k + \mathrm{ord}_q k!} |x|^k \left| |x|^{-(k+1)} \binom{-k}{k+1} (1 - |x|^{-1})^{-k-(k+1)} \right| < 1 \end{aligned}$$

where the last inequality follows from $|x| \geq q^{p-1} + q$ by Proposition 4.5 and $0 < k \leq (p-1)/2$.

Note that $\theta \in \mathbb{Z}[\Delta]^+$. For any $\sigma \in \Delta$ and $t \in \mathbb{Q}$ with $|t| < 1$,

$$\left((1 - \zeta t)^{\theta/q} \right)^\sigma = (1 - \zeta t)^{\sigma \theta / q} \in \mathbb{R}.$$

(Since they are q-th root of $(1 - \zeta t)^\theta \in \mathbb{R}$.) Thus by the same argument, $|\beta^\sigma| < 1$ for all $\sigma \in \Delta$, and therefore $\beta = 0$ and $q | a_m$. □

4.4. **Thaine's theorem and $[x - \zeta]^+$.** As $(p-1, q) = 1$, we have natural isomorphism of $\mathbb{Z}_q[\Delta]$-algebras

$$\mathbb{Z}_q[\Delta] = \bigoplus_{[\chi]} \mathbb{Z}_q[\mathrm{Im}\, \chi],$$

here χ runs over all q-adic characters of Δ and $[\chi]$ is the $\mathrm{Gal}(\overline{\mathbb{Q}}_q / \mathbb{Q}_q)$-orbit of χ. For any $\mathbb{Z}_q[G]$-module M, denote $M_\chi = M \otimes_{\mathbb{Z}_q[G]} \mathbb{Z}_q[\mathrm{Im}\, \chi]$.

Theorem 4.18. [4][5] *Suppose $(q, p-1) = 1$, then for any $\chi : \Delta \to \overline{\mathbb{Q}}_q$ a even character, then $\#(E/C)[q^\infty]_\chi = \#\mathrm{Cl}(K)[q^\infty]_\chi$. In particular, two $\mathbb{Z}_q[\Delta]$-modules $(E/C)[q^\infty]_\chi$, $\mathrm{Cl}(K)[q^\infty]_\chi$ have same Jordan-Holder series.*

Corollary 4.19. *$E/CE^q \simeq \mathrm{Cl}(K)[q]^+$ as R-modules.*

Corollary 4.20.

$$(\mathrm{Sel}(K, \mu_q)^+)^{\mathrm{Ann}_R(E/CE^q)} \subset CE^q/E^q$$

here view CE^q/E^q as subgroup of $\mathrm{Sel}(K, \mu_q)$.

Remark 4.21. The proof of the corollary only use the property $\mathrm{Ann}_R(E/CE^q) \subset \mathrm{Ann}_R \mathrm{Cl}(K)[q]^+$. And this property can be prove only using a result of Thaine: $\mathrm{Ann}_{\mathbb{Z}_q[\Delta]}((E/C)[q^\infty]) \subset \mathrm{Ann}_{\mathbb{Z}_q[\Delta]}(\mathrm{Cl}(K)[q^\infty]^+)$.

Corollary 4.22. *Assume the Catalan's equation has a solution in $\mathbb{Z}^2_{\neq 0}$, then*

$$\mathrm{Ann}_R(C_q E^q / E^q) \mathrm{Ann}_R(E/CE^q) \subset \mathrm{Ann}_R(E/E^q).$$

Proof. Consider $[(x - \zeta)^+] = \left[\frac{x-\zeta}{1-\zeta}^+ \right] [(1-\zeta)^{-1}]^+ \in K^\times / K^{\times, q}$. Note that $\left[\frac{x-\zeta}{1-\zeta} \right]^+ \in \mathrm{Sel}(K, \mathbb{Q})$ and $[1-\zeta]^\theta$ is represented by cyclotomic unit for any θ with $\deg \theta = 0$. By Corollary 4.20, for any $\theta \in \mathrm{Ann}_R((E/CE^q)) \cap R^{\deg = 0}$, we have $[(x-\zeta)^+]^\theta \in CK^\times / K^{\times, q}$, and thus in $C_q K^\times / K^{\times, q}$ by first remark of Remark 4.16. By rigidity of Mihailescu element

$$0 = \mathrm{Ann}_R(C_q E^q / E^q)(\mathrm{Ann}_R((E/CE^q)) \cap R^{\deg = 0}).$$

As the norm element N kill E/E^q and $\mathbb{F}_q \cdot N + R^{\deg=0} = R$, thus

$$\mathrm{Ann}_R(C_qE^q/E^q)\mathrm{Ann}_R(E/CE^q) \subset \mathrm{Ann}_R(C_qE^q/E^q)(\mathrm{Ann}_R(E/CE^q) \cap R^{\deg=0} + \mathbb{F}_qN) \subset \mathrm{Ann}_R(E/E^q)$$

□

4.5. Proof of the main theorem.

Theorem 4.23. [1][3] *Assume $q < p$ are two odd primes, then the following equation*

$$x^p - y^q = 1$$

has no solution in nonzero integers.

Proof. If (x, y) is a solution, by Corollary 4.22 and the second remark of Remark 4.16, we have

$$\mathrm{Ann}_R(CE^q/C_qE^q) = 0,$$

contradict with the following proposition

Proposition 4.24. *If $q < p$, then $C_qE^q \neq CE^q$.*

Proof. Let ζ be a primitive p-th root of unity, consider the cyclotomic unit $1+\zeta^q = \frac{1-\zeta^{2q}}{1-\zeta^q}$. If $1+\zeta^q \in C_q$, then $1 + \zeta^q \equiv u^q \pmod{q^2}$ for some $u \in E$. We have $(1 + \zeta)^q \equiv u^q \pmod q$, as q is unramified in K, $1 + \zeta \equiv u \pmod q$, thus $(1 + \zeta)^q \equiv u^q \pmod{q^2}$. This implies that $(1 + \zeta)^q \equiv 1 + \zeta^q \pmod{q^2}$. Consider the polynimial $1/q((1 + T)^q - T^q - 1) \in \mathbb{Z}[T]$, it has $p - 1$ distinct solution in $\mathbb{Z}[\mu_p]/(q^2)$, we must have $p \leq q$, contradiction. □

□

5. Femart Equation

Let $K = \mathbb{Q}(\mu_p)$.

Theorem 5.1. [6] *Let p be a odd prime that does not divides $\#\mathrm{Cl}(K)$, then the equation*

$$x^p + y^p = z^p$$

has no solution in nonzero integers.

Proof. Let (x, y, x) be a solution of Femart equation in $(\mathbb{Z}\backslash\{0\})^3$.

- If $p \nmid xyz$, then for any primitive p-th root of unity, $x + \zeta^{\pm}y \in \mathrm{Sel}(K, \mu_p)$ and $x + \zeta^{\pm}y$ is a unit at p. Let E (resp. $\mathcal{O}$) be the group of units (resp. integers)of K and $\mathrm{Cl}(K)$ the ideal class group of K. Consider the exact sequence:

  $$0 \to E/E^p \to \mathrm{Sel}(K, \mu_p) \to \mathrm{Cl}(K)[p] \to 0.$$

  By assumption, $\mathrm{Cl}(K)[p] = 0$. And we have a natural map

  $$\alpha : E/E^p \to E_v/E_v^p \simeq 1 + \pi E_v/(1 + \pi E_v)^p \twoheadrightarrow 1 + \pi\mathcal{O}/1 + p\mathcal{O},$$

  here v is the prime of K above p and $\pi = 1 - \zeta$. The image of $x + \zeta^{\pm}y$ in $1 + \pi\mathcal{O}/1 + p\mathcal{O}$ is $\frac{x+\zeta^{\pm}y}{x+y}$. As every element x in $\mathbb{Z}[\zeta]$ has the property $x^p \equiv a \pmod p$ for some $a \in \mathbb{Z}$. Write $\frac{x+\zeta^{\pm}y}{x+y} = \zeta^{\pm r}u^+a \in 1+\pi\mathcal{O}/1+p\mathcal{O}$ for $u^+ \in \mathcal{O}_E^{\times,+}$ and $a \in \mathbb{Z}$, then we have $\frac{x+\zeta y}{x+y} = \zeta^{2r}\frac{x+\zeta^{-1}y}{x+y}$ in $1 + \pi\mathcal{O}/1 + p\mathcal{O}$. Thus $x + \zeta y = \zeta^{2r}(x + \zeta^{-1}y) \pmod p$. This will contradicts with the following fact.

  Fact 5.2. *ζ^i, $i = 1, \cdots, p - 1$ is an integral basis of $\mathcal{O}$.*

- If $p|xyz$, may assume $p|z$ and $(p, xy) = 1$. Let ζ be a primitive p-th root of unity. We may prove a stronger statement: There is no solution of equation $x^p+y^p = u(1-\zeta)^{kp}z_0^p$ with $x, y, z \in \mathcal{O}\cap\mathcal{O}_{(p)}^{\times}$ co-prime, $u \in \mathcal{E}$, $k \in \mathbb{Z}_{>0}$. Suppose we have a solution, then
  (*i*) $\xi := \frac{x+\zeta y}{1-\zeta}$ and $\overline{\xi}$ are in $\mathrm{Sel}(K, \mu_p)$ and they are in $\mathcal{O} \cap \mathcal{O}_{(p)}^{\times}$.
  (*ii*) $\frac{x+y}{1-\zeta} = u'(1 - \zeta)^{(k-1)p}\gamma^p$ with $u' \in \mathcal{E}$ and $\gamma \in \mathcal{O} \cap \mathcal{O}_{(p)}^{\times}$.
  (*iii*) $\xi, \overline{\xi}$ and $\frac{x+y}{1-\zeta}$ are coprime.

  Proposition 5.3. *ξ and $\overline{\xi}$ are in the same class of* $\mathrm{Sel}(K, \mu_p)$.

Once they are in the same class, we can write $\xi = v\alpha^p$ and $\overline{\xi} = v\beta^p$ for some $v \in \mathcal{E}$ and $\alpha, \beta \in \mathcal{O} \cap \mathcal{O}_{(p)}^\times$. We have $\alpha^p + (-\beta)^p = v^{-1}u'(1+\zeta)(1-\zeta)^{(k-1)p}\gamma^p$. By descent, we prove the theorem.

Proof of proposition. As p is regular, $\xi, \overline{\xi}$ represented by element in $\mathcal{E}$.

Lemma 5.4 (Kummer's lemma)**.** *If p is regular, then $x \in \mathcal{E}/\mathcal{E}^p$ is trivial if and only if x congruent to an integer modulo p in $\mathcal{O}$.*

The Kummer lemma is equivalent to the map α is injective. As ξ and $\overline{\xi}$ are p-adic units, $\alpha(\xi), \alpha(\overline{\xi})$ equivalent to the image of $\xi, \overline{\xi}$ as element in $\mathcal{E}_v$ under the map

$E_v/E_v^p \simeq \mu_{p-1} \times (1+\pi\mathcal{O}_v)/\mu_{p-1} \times (1+\pi\mathcal{O}_v)^p \twoheadrightarrow 1+\pi\mathcal{O}_v/1+p\mathcal{O}_v \simeq 1+\pi\mathcal{O}/1+p\mathcal{O}$.

As $p | \frac{x+y}{1-\zeta^{\pm}}$, we have $\alpha(\xi) = \alpha(\overline{\xi})$, thus they are in the same class in $\mathrm{Sel}(K, \mu_p)$. □

Algebraic proof of Kummer's lemma. Sufficient to prove if $u \in \mathcal{E}$ is congruent to an integer modulo p, then $K(u^{1/p})$ is unramified. Let v be a finite place of K. If v does not divides p, then $\mathrm{Disc}(u^{1/p}, , \zeta u^{1/p} \cdots, \zeta^{p-1}u^{1/p}) \in D_{K(u^{1/p})/K}$ is a v-adic unit. When v divides p, As u congruent to a nonzero integer modulo p, replace u by u^{p-1} may assume $u \equiv 1 \pmod p$. Consider the norm of u, we must have $u \equiv 1 \mod \pi p$, where $\pi = 1-\zeta$. Now Consider the polynomial $\pi^{-p}((\pi x-1)^p + u) \in \mathcal{O}[x]$, its discriminant is a p-adic unit. Thus $K(u^{1/p})$ is unramified everywhere. □

□

6. Exercises and Projects

6.1. Exercises.

Exercise 1. Let Δ be a finite abelian group, p be a prime such that $p \nmid \#\Delta$. Let L be a finite extension of $\mathbb{Q}_p$ which contains all the values of all the characters od Δ. Let M be a finite $\mathbb{Z}_p[\Delta]$-module, for any character $\chi : \Delta \to \mathcal{O}_L^\times$, define $M^\chi := \{a \in M \otimes \mathcal{O}_L \mid a^\sigma = \chi(\sigma)a \text{ for all } \sigma \in \Delta\}$ and $M_\chi := (M \otimes \mathcal{O}_L)/\langle a^\sigma - \chi(\sigma)a \mid a \in M \otimes \mathcal{O}_L, \sigma \in \Delta\rangle$.

(i) Prove that the natural map $M^\chi \to M_\chi$ is an isomorphism.
(ii) Let M and N be finite $\mathbb{Z}_p[\Delta]$-modules. Prove that the followings are equivalent:
  (a) M and N have the same Jordan-Hölder series;
  (b) $\#M_\chi = \#N_\chi$ for all character $\chi : \Delta \to \mathcal{O}_L^\times$.

Exercise 2. Let K be a number field, $\alpha \in K^\times$, $n \geq 1$ be an integer, $L = K(\sqrt[n]{\alpha})$. Let $\mathfrak{p} \nmid n$ be a prime ideal of $\mathcal{O}_K$. Prove that L/K is unramified at $\mathfrak{p}$ if and only if $n \mid \mathrm{ord}_\mathfrak{p}(\alpha)$.

Exercise 3. Let K be a totally real field which is Galois over $\mathbb{Q}$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Prove that there is a unit $u \in \mathcal{O}_K^\times$ such that $\mathbb{Z}[G]u$ is finite index in $\mathcal{O}_K^\times$. Show that $\mathcal{O}_K^\times \otimes \mathbb{Q} \cong \mathbb{Q}[G]/N_G$ as $\mathbb{Q}[G]$-modules in particular. (Hint: read the proof of Drichlet's unit theorem.)

Exercise 4. Let G be a finite abelian group. Let p be a prime number such that $p \nmid |G|$. For a character $\chi : G \to \overline{\mathbb{Q}_p}^\times$, let $\mathbb{Z}_p[\chi]$ denote the ring generated by the values of χ over $\mathbb{Z}_p$. Then $\mathbb{Z}_p[\chi]$ is a $\mathbb{Z}_p[G]$ module by $g(a) = \chi(g)a$.

(1) Prove that $\mathbb{Z}_p[\chi] \cong \mathbb{Z}_p[\chi^\sigma]$ as $\mathbb{Z}_p[G]$-modules. Here $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ and $\chi^\sigma = \sigma \circ \chi$ is also a character of G (we call such two characters are $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ conjugate).
(2) Prove that
$$\mathbb{Z}_p[G] \cong \prod_{\chi/\sim} \mathbb{Z}_p[\chi],$$
where $\chi_1 \sim \chi_2$ means they are $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ conjugate. Prove that for any $\mathbb{Z}_p[G]$-module M,
$$M \cong \prod_{\chi/\sim} M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\chi].$$
(3) Let M and N be two finite generated free $\mathbb{Z}_p$-modules with an action of G. Prove that if $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong N \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ as $\mathbb{Q}_p[G]$-modules, then $M \cong N$ as $\mathbb{Z}_p[G]$-modules.

6.2. Projects. ??? Read Euler system argument ???

Appendix A. Thaine's Theorem (Work in progress)

Recall that $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $\Delta^+ = \mathrm{Gal}(K^+/\mathbb{Q})$, q is a prime not dividing $\frac{p(p-1)}{2}$, and $R^+ = \mathbb{Z}_q[\Delta^+]$. Recall that $\mathcal{E} := \mathcal{O}_K^\times$, $\mathcal{E}^+ := \mathcal{O}_{K^+}^\times$, $\mathcal{C} := \left\langle \frac{\zeta_p^b - 1}{\zeta_p - 1} \mid b \in (\mathbb{Z}/p\mathbb{Z})^\times \right\rangle \cdot \mu(K) \subset \mathcal{E}$, and $\mathcal{C}^+ := \mathcal{C} \cap \mathcal{E}^+$. Let $n \geq 1$ be a sufficiently large integer such that q^n annihilates $(\mathcal{E}^+/\mathcal{C}^+) \otimes_{\mathbb{Z}} \mathbb{Z}_q$ and $\mathrm{Cl}(K^+) \otimes_{\mathbb{Z}} \mathbb{Z}_q$. Then $(\mathcal{E}^+/\mathcal{C}^+) \otimes_{\mathbb{Z}} \mathbb{Z}_q = (\mathcal{E}^+/\mathcal{C}^+) \otimes_{\mathbb{Z}} (\mathbb{Z}/q^n\mathbb{Z}) = \mathcal{E}^+/(\mathcal{E}^+)^{q^n}\mathcal{C}^+$ and $\mathrm{Cl}(K^+) \otimes_{\mathbb{Z}} \mathbb{Z}_q = \mathrm{Cl}(K^+) \otimes_{\mathbb{Z}} (\mathbb{Z}/q^n\mathbb{Z}) = \mathrm{Cl}(K^+)/\mathrm{Cl}(K^+)^{q^n}$. Let ℓ be a prime $\equiv 1 \pmod{p^n}$. Then ℓ splits completely in K^+. Let $\mathfrak{l}$ be a prime of K^+ above ℓ.

Let $L = \mathbb{Q}(\zeta_\ell)$, then K^+ and L are linearly disjoint over $\mathbb{Q}$. Let $M = K^+L$:

$$\begin{array}{ccccccc}
\mathfrak{L} & & & M & & & \\
| & & {\scriptstyle(\mathbb{Z}/\ell\mathbb{Z})^\times} \swarrow & & \searrow {\scriptstyle\Delta^+} & & \\
\mathfrak{l} & \mathbb{Q}(\zeta_p + \zeta_p^{-1}) = K^+ & & & & L = \mathbb{Q}(\zeta_\ell) & (\zeta_\ell - 1) \\
| & & {\scriptstyle\Delta^+} \searrow & & \swarrow {\scriptstyle(\mathbb{Z}/\ell\mathbb{Z})^\times} & & | \\
\ell & & & \mathbb{Q} & & & \ell
\end{array}$$

Since ℓ is unramified in K^+ and is totally ramified in L, the $\mathfrak{l}$ is totally ramified in M. Let $\mathfrak{L}$ be the unique prime ideal of M over $\mathfrak{l}$, then $\mathfrak{l}\mathcal{O}_M = \mathfrak{L}^{\ell-1}$. The $(\zeta_\ell - 1)\mathcal{O}_L$ is the unique prime ideal of L above ℓ, and $\ell\mathcal{O}_L = (\zeta_\ell - 1)^{\ell-1}\mathcal{O}_L$. Any prime of K^+ above ℓ is of form $\mathfrak{l}^\sigma$ for a unique $\sigma \in \Delta^+$, and we have $\ell\mathcal{O}_{K^+} = \prod_{\sigma \in \Delta^+} \mathfrak{l}^\sigma$. Similarly, any prime of M above ℓ is of form $\mathfrak{L}^\sigma$ for a unique $\sigma \in \mathrm{Gal}(M/L) \xrightarrow{\sim} \mathrm{Gal}(K^+/\mathbb{Q}) = \Delta^+$, and we have $(\zeta_\ell - 1)\mathcal{O}_M = \prod_{\sigma \in \mathrm{Gal}(M/L)} \mathfrak{L}^\sigma$ as well as $\ell\mathcal{O}_M = \prod_{\sigma \in \mathrm{Gal}(M/L)} (\mathfrak{L}^\sigma)^{\ell-1}$.

Lemma A.1. *Let $\delta \in \mathcal{C}^+$ be an element. Then there exists an element $\varepsilon \in \mathcal{O}_M^\times$ such that $\mathrm{N}_{M/K^+}(\varepsilon) = 1$ and $\varepsilon \equiv \delta \pmod{\mathfrak{L}^\sigma}$ for all $\sigma \in \Delta^+$ (or equivalently, $\varepsilon \equiv \delta \pmod{\zeta_\ell - 1}$).*

Proof. To be added □

Fix a generator s of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ which gives a generator τ of $\mathrm{Gal}(M/K^+)$ by $\zeta_\ell \mapsto \zeta_\ell^s$. The $\tau \mapsto \varepsilon$ extends to a cocycle $\mathrm{Gal}(M/K^+) \to M^\times$ by the condition $\mathrm{N}_{M/K^+}(\varepsilon) = 1$. Hence by Hilbert's Theorem 90, $H^1(M/K^+, M^\times) = 0$, the above cocycle is a coboundary, which means that there exists $\alpha \in M^\times$ such that $\alpha^\tau/\alpha = \varepsilon$.

To be added...

References

[1] Mihailescu, *Primary cyclotomic units and a proof of Catalan's conjecture.*
[2] Bilu, *Catalan's conjecture.*
[3] Metsankyl, *Catalan's conjecture: Another old Diophantine problem solved.*
[4] Greenberg, *On p-adic L-functions and cyclotomic fields.II.*
[5] Rubin, *The Main conjecture.* (Appendix in Serge lang's Cyclotomtic fields I and II)
[6] Washington, *Introduction to cyclotomtic fields.*
[7] Serge Lang, *Cyclotomtic fields I and II.*
[8] Schoof, *Catalan's conjecture.*