ELEMENTARY IWASAWA THEORY FOR CYCLOTOMIC FIELDS

HARUZO HIDA

In this topic course, assuming basic knowledge of algebraic number theory and commutative algebra, we pick topics from the theory of cyclotomic fields. Our treatment is elementary. We plan to discuss the following four topics:

(1) Class number formulas,
(2) Basics of cyclotomic fields and Iwasawa theory,
(3) Stickelberger's theorem,
(4) Cyclicity over the Iwasawa algebra of the cyclotomic Iwasawa module.

Since this is a topic course, for some of the topics, we just give the results without detailed proofs. Main reference is Chapters 4, 5, 6, 7 and 10 of the following book [ICF]:

[ICF] L. C. Washington, *Introduction to Cyclotomic fields*, Graduate Text in Mathematics **83**, 1997.

Here is a relevant book:

[LFE] H. Hida, *Elementary Theory of L–functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, 1993.

Here is an **Overview** of the goal of the lectures. We write $\overline{\mathbb{Q}}$ for the field of all algebraic numbers in $\mathbb{C}$. Any finite extension of $\mathbb{Q}$ inside $\overline{\mathbb{Q}}$ is called a number field. Write μ_N for the group of N-th roots of unity inside $\overline{\mathbb{Q}}^\times$ and $\mathbb{Q}(\mu_N)$ for the field generated by roots of unity in μ_N, which is called a cyclotomic field.

For any given number field K, the class group Cl_K defined by the quotient of the group of fractional ideals of K modulo principal ideals is a basic invariant of K. It is a desire of many algebraic number theorists to know the module structure of Cl_K. Or if $K/\mathbb{Q}$ is a Galois extension, $G_{K/\mathbb{Q}} := \mathrm{Gal}(K/\mathbb{Q})$ acts on Cl_K. Thus it might be easier to see the module structure of Cl_K over the group ring $\mathbb{Z}[G_{K/\mathbb{Q}}]$ larger than $\mathbb{Z}$.

The first step towards this goal of determining Cl_K for $K = \mathbb{Q}[\mu_N]$ was given in 1839 by Dirichlet as a formula of the order of the class group (his class number formula). The cyclotomic field K has its maximal real subfield K^+ and K/K^+ is a quadratic extension if N is odd with G_{K/K^+} generated by complex conjugation c. The norm map gives rise to a homomorphism $Cl_K \to Cl_K^+ := Cl_{K^+}$ whose kernel is written as Cl_K^- (the minus part of Cl_K). By the formula, if N is an odd prime p, the order of the Cl_K^- is given by

$$2p \prod_{\chi:(\mathbb{Z}/p\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times;\chi(-1)=-1} -\frac{1}{p}(\sum_{j=1}^{p-1} \chi^{-1}(a)a) \quad \text{(Dirichlet/Kummer).}$$

Date: April 14, 2018.

The author is partially supported by the NSF grant: DMS 1464106.

Since $G_{K/\mathbb{Q}} \cong (\mathbb{Z}/p\mathbb{Z})^\times$ sending $\sigma_a \in G_{K/\mathbb{Q}}$ with $\sigma_a(\zeta) = \zeta^a$ $(\zeta \in \mu_p)$ to $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have $\mathbb{Z}[G_{K/\mathbb{Q}}] \cong \mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^\times]$. Since each character χ of $G_{K/\mathbb{Q}}$ extends to an algebra homomorphism $\chi : \mathbb{Z}[G_{K/\mathbb{Q}}] \to \overline{\mathbb{Q}}$ sending σ_a to $\chi(a)$, Kummer–Stickelberger guessed that

$$\theta_0 := \sum_{a=1}^{p-1} \frac{a}{p}\sigma_a^{-1} \text{ annihilates } Cl_K^- \text{ as } \chi(\theta_0) = \frac{1}{p}(\sum_{j=1}^{p-1} \chi^{-1}(a)a).$$

This "symbolic" statement means that $\mathfrak{A}^{\beta\theta_0}$ (for any fractional ideal $\mathfrak{A}$ of K) is principal as long as $\beta\theta_0 \in \mathbb{Z}[G_{K/\mathbb{Q}}]$ for $\beta \in \mathbb{Z}[G_{K/\mathbb{Q}}]$. Writing $\mathfrak{a}$ for the $\mathbb{Z}[G_{K/\mathbb{Q}}]$-ideal generated by elements of the form $\beta\theta_0 \in \mathbb{Z}[G_{K/\mathbb{Q}}]$, we might expect:

$$Cl_K^- \cong \mathbb{Z}[G_{K/\mathbb{Q}}]/\mathfrak{a}? \quad (\text{Cyclicity over } \mathbb{Z}[G_{K/\mathbb{Q}}])$$

which is not generally true. After supplying basics of cyclotomic fields, we will prove in the course Stickelberger's theorem:

$$Cl_K^- \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}_p[G_{K/\mathbb{Q}}]^-/(\mathfrak{a} \otimes \mathbb{Z}_p)^- \quad (p\text{-Cyclicity})$$

assuming Kummer–Vandiever conjecture: $p \nmid |Cl_K^+|$ (see [BH] for numerical examples). Here $\mathfrak{A}^- = \{x \in \mathfrak{A} | cx = -x\}$ for complex conjugation c for an ideal $\mathfrak{A}$ of $\mathbb{Z}_p[G_{K/\mathbb{Q}}]$. Set $\Lambda = \mathbb{Z}_p[[T]]$ (one variable power series ring). Then we can easily prove that

$$\varprojlim_n \mathbb{Z}_p[G_{\mathbb{Q}[\mu_{p^n}]/\mathbb{Q}}] \cong \Lambda[\mu_{p-1}] \quad (\varprojlim_n \sigma_{1+p} \mapsto t = 1 + T),$$

where the limit is taken via restriction maps $G_{\mathbb{Q}[\mu_{p^{n+1}}]/\mathbb{Q}} \ni \sigma \mapsto \sigma|_{Q[\mu_{p^n}]} \in G_{\mathbb{Q}[\mu_{p^n}]/\mathbb{Q}}$. Then, assuming again Kummer–Vandiever conjecture, we further go on to show Iwasawa's way of proving his main conjecture and cyclicity of his Iwasawa module $X := \varprojlim_n (Cl^-_{\mathbb{Q}[\mu_{p^n}]} \otimes \mathbb{Z}_p)$:

$$X \cong \Lambda[\mu_{p-1}]^-/(L_p)$$

for the T-expansion L_p of the Kubota–Leopoldt p-adic L-function.

Contents

1. Cyclotomic fields

We recall basic structure theory of cyclotomic fields. We write $\overline{\mathbb{Q}}$ for the field of all algebraic numbers in $\mathbb{C}$. Any finite extension of $\mathbb{Q}$ inside $\overline{\mathbb{Q}}$ is called a number field. In algebraic number theory, the theory of cyclotomic fields occupies very peculiar place. It was the origin of the development of algebraic number theory and still inspires us with many miraculous special features.

Fix a prime $p > 2$ and consider a primitive root of unity $\zeta_{p^n} := \exp(\frac{2\pi i}{p^n})$. Then ζ_p satisfies the equation $\Phi_1(X) = \frac{X^p-1}{X-1} = 1+X+X^2+\cdots+X^{p-1} = \prod_{j=1}^{p-1}(X-\zeta_p^j)$. Note that $\Phi_1(X+1) = \frac{(X+1)^p-1}{X} = \sum_{j=1}^{p}\binom{p}{j}X^{j-1} = X^{p-1}+pX^{p-2}+\cdots+p$ which is an Eisenstein polynomial. Therefore $\Phi_1(X+1)$ is irreducible, and hence $\Phi_1(X)$ is irreducible. In the same manner, ζ_{p^n} is a root of $\Phi_n(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1} = \Phi_1(X^{p^{n-1}})$ is irreducible. Therefore $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ is a field extension of degree equal to $\deg(\Phi_n) = p^{n-1}(p-1)$. In particular, in $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$, p fully ramifies with $\zeta_{p^n}-1$ giving the unique prime ideal $(\zeta_{p^n}-1)$ over p; so, $(\zeta_{p^n}-1)^{p^{n-1}(p-1)} = (p)$ in $\mathbb{Q}[\zeta_{p^n}]$, and $\mathbb{Z}_p[\zeta_{p^n}-1]$ is the p-adic integer ring of $\mathbb{Q}_p[\zeta_{p^n}]$. For all other prime $l \neq p$, taking a prime $\mathfrak{l}$ of $\mathbb{Q}[\zeta_{p^n}]$ above l, $\overline{\zeta}_{p^n} := (\zeta_{p^n} \bmod \mathfrak{l})$ is a primitive p^n-th root in a finite field of characteristic l; so, $\overline{\zeta}_{p^n}^j$ are all distinct for $j = 1, \dots, p^{n-1}(p-1)$. Thus $\mathbb{Q}_l[\zeta_{p^n}]$ is unramified at l, and $\mathbb{Z}_l[\zeta_{p^n}]$ is an unramified valuation ring over $\mathbb{Z}_l$; so, it is the l-adic integer ring of $\mathbb{Q}_l[\zeta_{p^n}]$. This shows (cf. [CRT, §9])

Lemma 1.1. *The ring $\mathbb{Z}[\zeta_{p^n}]$ is the integer ring of $\mathbb{Q}[\zeta_{p^n}]$ and the roots of $\Phi_n(X)$ (i.e., all primitive p^n-th roots gives rise to a basis of $\mathbb{Z}[\zeta_{p^n}]$ over $\mathbb{Z}$, p fully ramifies in $\mathbb{Z}[\zeta_{p^n}]$, and $\zeta_{p^n}-1$ generates a unique prime ideal of $\mathbb{Z}[\zeta_{p^n}]$ over p.*

Since all Galois conjugate of ζ_{p^n} is again a root of $\Phi_n(X)$, $\mathbb{Q}[\zeta_{p^n}]$ is a Galois extension. Since $\sigma \in G_{\mathbb{Q}[\zeta_{p^n}]/\mathbb{Q}}$ is determined by $\zeta_{p^n}^\sigma = \zeta_{p^n}^{\nu_n(\sigma)}$ for $\nu_n(\sigma) \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, we have a character $G_{\mathbb{Q}[\zeta_{p^n}]/\mathbb{Q}} \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ which is injective. Since the LHS and RHS have the same order, ν_n is an isomorphism. Writing the residue field of $\mathfrak{l} \nmid p$ as $\mathbb{F} = \mathbb{Z}[\zeta_{p^n}]/\mathfrak{l}$, we have $\mathbb{F} = \mathbb{F}_l[\overline{\zeta}_{p^n}]$. Then the Frobenius element $\mathrm{Frob}_l \in G_{\mathbb{F}/\mathbb{F}_l} = D_l$ sends $\overline{\zeta}_{p^n}$ to $\overline{\zeta}_{p^n}^l$. Thus we get

Lemma 1.2. *For a prime $l \neq p$, we have $\nu_n(\mathrm{Frob}_l) = (l \bmod p^n)$.*

It is customary to write $\mu_{p^n} \subset \overline{\mathbb{Q}}^\times$ for the cyclic group generated by ζ_{p^n}. Since $\mathbb{Q}[\zeta_{p^n}]$ contains μ_{p^n}, we write hereafter $\mathbb{Q}[\mu_{p^n}]$ for $\mathbb{Q}[\zeta_{p^n}]$ freeing the notation from a choice of a generator of μ_{p^n}. Write $\mathbb{Q}[\mu_{p^\infty}] := \bigcup_n \mathbb{Q}[\mu_{p^n}]$. Then the restriction map $\mathrm{Res}_{m,n}(\sigma) = \sigma|_{\mathbb{Q}[\mu_{p^n}]}$ for $\sigma \in G_{\mathbb{Q}[\mu_{p^m}]/\mathbb{Q}}$ $(m > n)$ gives the following commutative diagram:

$$\begin{tikzcd}
G_{\mathbb{Q}[\mu_{p^m}]/\mathbb{Q}} \arrow[r, "\nu_m"] \arrow[d, "\mathrm{Res}"'] & (\mathbb{Z}/p^m\mathbb{Z})^\times \arrow[d, "\bmod p^n"] \\
G_{\mathbb{Q}[\mu_{p^n}]/\mathbb{Q}} \arrow[r, "\nu_n"] & (\mathbb{Z}/p^n\mathbb{Z})^\times.
\end{tikzcd}$$

Passing to the limit, we get

$$G_{\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q}} \xrightarrow[\sim]{\nu} \mathbb{Z}_p{}^\times \ \text{ with } \nu(\mathrm{Frob}_l) = l \text{ for } l \neq p. \tag{1.1}$$

Let $\Gamma := 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p{}^\times$. Then $\mathbb{Z}_p{}^\times/\Gamma \cong (\mathbb{Z}/p\mathbb{Z})^\times$ which has order $p-1$. Thus $z \mapsto z^p$ is the identity map on $(\mathbb{Z}/p\mathbb{Z})^\times$. On the other hand, for any $z \in \mathbb{Z}_p{}^\times$, $z^{p^n - p^{n-1}} \equiv 1 \mod p^n$ as $(\mathbb{Z}/p^n\mathbb{Z})^\times$ has order $p^n - p^{n-1}$. Thus $|z^{p^n} - z^{p^{n-1}}|_p \leq \frac{1}{p^n}$. We therefore have a limit $\omega(z) = \lim_{n\to\infty} z^{p^n}$ which satisfies plainly $\omega(z)^p = \omega(z)$; i.e, $\omega(z) \in \mu_{p-1}$ and $\omega(z) \equiv z \mod p$. Thus $\mu_{p-1} \subset \mathbb{Z}_p{}^\times$ is a cyclic subgroup of order $p-1$. We thus have $\mathbb{Z}_p{}^\times = \Gamma \times \mu_{p-1}$. Thus we get

Lemma 1.3. *Let D_l be the decomposition subgroup of $G_{\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q}}$ of a prime l. Then if $l \neq p$, D_l is the infinite cyclic subgroup topologically generated by* Frob_l *isomorphic to $\langle l\rangle^{\mathbb{Z}_p} \times \omega(l)^{\mathbb{Z}}$. If $l = p$, D_p is equal to the inertia subgroup I_p which is the entire group $G_{\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q}}$. In particular, for each prime, the number of prime ideals in $\mathbb{Z}_p[\mu_{p^\infty}]$ over l is finite and is equal to $[G_{\mathbb{Q}[\mu_{p^\infty}]/\mathbb{Q}} : D_l]$.*

Remark 1.4. More generally, for an integer N, making prime factorization $N = \prod_l l^{e(l)}$, $\mathbb{Q}[\mu_N]$ is the composite of $\mathbb{Q}[\mu_{l^{e(l)}}]$ with degree $|(\mathbb{Z}/l^{e(l)}/\mathbb{Z})^\times| = \varphi(l^{e(l)}) = l^{e(l)} - l^{e(l)-1}$. In the field $\mathbb{Q}[\mu_{l^{e(l)}}]$, the prime l ramifies fully and all other primes are unramified. Therefore the fields $\{\mathbb{Q}[\mu_{l^{e(l)}}]\}_{l|N}$ are linearly disjoint over $\mathbb{Q}$, and hence

$$G_{\mathbb{Q}[\mu_N]/\mathbb{Q}} \cong \prod_{l|N} G_{\mathbb{Q}[\mu_{l^{e(l)}}]/\mathbb{Q}} \cong \prod_{l|N} (\mathbb{Z}/l^{e(l)}\mathbb{Z})^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times.$$

This also tells us that the integer ring of $\mathbb{Q}[\mu_N]$ is given by $\mathbb{Z}[\mu_N] \cong \bigotimes_l \mathbb{Z}[\mu_{l^{e(l)}}]$. The decomposition subgroup of a prime $q \nmid N$ in $G_{\mathbb{Q}[\mu_N]/\mathbb{Q}}$ is isomorphic to the subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ generated by the class ($q \bmod N$). If $l|N$, I_l is isomorphic to $(\mathbb{Z}/l^{e(l)}\mathbb{Z})^\times$ and writing $N^{(l)} = N/l^{e(l)}$, D_l is isomorphic to the product of I_l and the subgroup of $(\mathbb{Z}/N^{(l)}\mathbb{Z})^\times$ generated by the class of l. Since the Galois group $G_{\mathbb{Q}[\mu_N]/\mathbb{Q}}$ is generated by inertia groups of primes $l|N$, for any intermediate extension $\mathbb{Q} \subset E \subset F \subset \mathbb{Q}[\mu_N]$, some prime ramifies. In other words, if F/E is unramified everywhere, we conclude $E = F$.

Exercise 1.5. *Give a detailed proof of the fact: $\mathbb{Z}[\mu_N] \cong \bigotimes_l \mathbb{Z}[\mu_{l^{e(l)}}]$ and $\mathbb{Z}[\mu_N]$ is the integer ring of $\mathbb{Q}[\mu_N]$.*

Exercise 1.6. *Prove that for a finite set $S = \{l_1, \ldots, l_r\}$ of primes. prove that the number of prime ideals over any given prime l in $\mathbb{Z}[\mu_{l_1^\infty}, \ldots, \mu_{l_r^\infty}]$ is finite.*

2. An outline of class field theory

We give a brief outline of class field theory (a more detailed reference is, for example, [CFT] or [BNT]), which will be covered in Math 205c in Spring 2018. For a given number field F with integer ring O, pick an O-ideal $\mathfrak{n}$, let $I_{\mathfrak{n}}$ be the set of all fractional ideals prime to $\mathfrak{n}$. We put $O_{\mathfrak{n}} := \varprojlim_n O/\mathfrak{n}^n$ (the $\mathfrak{n}$-adic completion of O). Write the prime factorization of $\mathfrak{n} = \prod_{\mathfrak{l}|\mathfrak{n}} \mathfrak{l}^{e(\mathfrak{l})}$. Then by Chinese reminder theorem, we have $O_{\mathfrak{n}} \cong$

$\prod_{\mathfrak{l}} O/\mathfrak{l}^{e(\mathfrak{l})}O_{\mathfrak{l}}$. We write $O_{(\mathfrak{l})}$ for $O_{\mathfrak{l}} \cap F$ (which is the localization

$$O_{(\mathfrak{l})} = \left\{\frac{\beta}{\alpha} | \alpha, \beta \in O \text{ with } \alpha O + \mathfrak{l} = O\right\}.$$

Exercise 2.1. *Prove the above identity.*

For a principal ideal $(\alpha) \in I_{\mathfrak{n}}$, we write $\alpha \equiv 1(\text{mod } \mathfrak{n})^{\times}$ if $\alpha \in 1 + \mathfrak{l}^{e(\mathfrak{l})}O_{\mathfrak{l}}$ for all prime $\mathfrak{l}|\mathfrak{n}$. More generally, we write $\alpha \equiv \beta(\text{mod } \mathfrak{n})^{\times}$ for $(\alpha), (\beta) \in I_{\mathfrak{n}}$ if $\alpha/\beta \equiv 1(\text{mod } \mathfrak{n})^{\times}$.

Exercise 2.2. *Prove that $\alpha \equiv 1(mod\ \mathfrak{n})^{\times}$ if and only if $\alpha \in 1 + \mathfrak{l}^{e(\mathfrak{l})}O_{(\mathfrak{l})}$ for all prime $\mathfrak{l}|\mathfrak{n}$.*

Define

$$\begin{aligned} P_{\mathfrak{n}} &:= \{(\alpha) \in I_{\mathfrak{n}} | \alpha \equiv 1(\text{mod } \mathfrak{n})^{\times}\} \\ P_{\mathfrak{n}}^{+} &:= \{(\alpha) \in P_{\mathfrak{n}} | \sigma(\alpha) > 0 \text{ for all field embeddings } \sigma : F \to \mathbb{R}\}. \end{aligned} \tag{2.1}$$

If F has no real embedding (i.e., F is totally imaginary, we have $P_{\mathfrak{n}} = P_{\mathfrak{n}}^{+}$.

Exercise 2.3. *Let $F = \mathbb{Q}[\sqrt{5}]$. Is $P_O = P_O^{+}$ true? How about $\mathbb{Q}[\sqrt{15}]$?*

Then $Cl_{\mathfrak{n}} := I_{\mathfrak{n}}/P_{\mathfrak{n}}$ (resp. $Cl_{\mathfrak{n}}^{+} = I_{\mathfrak{n}}/P_{\mathfrak{n}}^{+}$) are called the (resp. strict) ray class group modulo $\mathfrak{n}$ of F. They are finite groups. We have written Cl_F for Cl_O. The order $|Cl_O|$ is called the class number of F. Here is a main theorem of class field theory:

Theorem 2.4. *For each $\mathfrak{n}$ as above, there is a unique abelian extension $H_{\mathfrak{n}}/F$ (resp. $H_{\mathfrak{n}}^{+}/F$) such that*

1. *Prime ideals prime to $\mathfrak{n}$ is unramified in $H_{\mathfrak{n}}/F$ and $H_{\mathfrak{n}}^{+}/F$, and every real embedding of F extends to a real embedding of $H_{\mathfrak{n}}$; in particular, if all Galois conjugates of F are in $\mathbb{R}$ (i.e., F is totally real), $H_{\mathfrak{n}}$ is totally real;*
2. *$Cl_{\mathfrak{n}} \cong G_{H_{\mathfrak{n}}/F}$ and $Cl_{\mathfrak{n}}^{+} \cong G_{H_{\mathfrak{n}}^{+}/F}$ by an isomorphism sending the class of prime ideal $\mathfrak{l}$ prime to $\mathfrak{n}$ in $Cl_{\mathfrak{n}}$ (resp. $Cl_{\mathfrak{n}}^{+}$) to the corresponding* $\text{Frob}_{\mathfrak{l}} \in G_{H_{\mathfrak{n}}/F}$ *(resp. $G_{H_{\mathfrak{n}}^{+}/F}$), where $Frob_{\mathfrak{l}}$ is a unique element in $G_{K/F}$ for $K = H_{\mathfrak{n}}, H_{\mathfrak{n}}^{+}$ such that* $\text{Frob}_{\mathfrak{l}}(\mathfrak{l}) = \mathfrak{l}$ *and* $\text{Frob}_{\mathfrak{l}}(x) \equiv x^{N(\mathfrak{l})} \mod \mathfrak{l}$ *for $N(\mathfrak{l}) := |O/\mathfrak{l}|$;*
3. *For any finite abelian extension K/F, there exists an O-ideal $\mathfrak{n}$ such that $K \subset H_{\mathfrak{n}}^{+}$ (the ideal maximal among $\mathfrak{n}$ with $K \subset H_{\mathfrak{n}}^{+}$ is called the "conductor" of K);*
4. *For a finite extension $F'_{/F}$ with integer ring O', we write $H_{\mathfrak{n}}/F$ and $H'_{\mathfrak{n}}/F'$ (resp. $Cl_{\mathfrak{n}}^{+}$ and $Cl'^{+}_{\mathfrak{n}}$ for the corresponding class fields (resp. the corresponding class groups). Then we have $H'_{\mathfrak{n}} \supset H_{\mathfrak{n}}$ and the following commutative diagram*

$$\begin{tikzcd} G_{H'^{+}_{\mathfrak{n}}/F'} \arrow[r, "\text{Res}"] & G_{H_{\mathfrak{n}}^{+}/F} \\ Cl'^{+}_{\mathfrak{n}} \arrow[u, "\wr"] \arrow[r, "N_{F'/F}"] & Cl_{\mathfrak{n}}^{+}. \arrow[u, "\wr"] \end{tikzcd}$$

Here $N_{F'/F}$ is induced by the norm map sending a O'-prime ideal $\mathfrak{L}$ prime to $\mathfrak{n}$ to $\mathfrak{l}^{f}$ ($\mathfrak{l} = \mathfrak{L} \cap O$) with $f = [O'/\mathfrak{L} : O/\mathfrak{l}]$ (note $N_{F'/F}\mathfrak{L} = \prod_{\sigma \in G_{F'/F}} \mathfrak{L}^{\sigma} \cap O$ if F'/F is a Galois extension).

Example 2.1. Suppose $F = \mathbb{Q}$. Consider the map $\{n \in \mathbb{Z} | n\mathbb{Z} + \mathfrak{n} = \mathbb{Z}\} \ni n \mapsto (n) \in Cl^+_{(N)}$ for each integer $n > 0$ prime to N. This induces an injective homomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \to Cl^+_N$. For each $(\alpha) \in I_N$, take an integer n prime to N with $\alpha \equiv n (\text{mod } N)^\times$ and $\alpha/n > 0$. Then the class of (α) and (n) in Cl^+_N coincide by definition. Therefore, we get $Cl^+_N \cong (\mathbb{Z}/N\mathbb{Z})^\times$, and hence $H^+_N = \mathbb{Q}[\mu_N]$.

Exercise 2.5. *What is $H_N \subset H^+_N = \mathbb{Q}[\mu_N]$? Determine $G_{H_N/\mathbb{Q}}$ as a quotient of $(\mathbb{Z}/N\mathbb{Z})^\times$.*

Corollary 2.6 (Kronecker–Weber–Hilbert)**.** *Any finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}[\mu_N]$ for some positive integer N.*

3. Relative class number formula and Stickelberger's theorem

Let $F_n := \mathbb{Q}[\mu_{p^{n+1}}]$. Complex conjugation c acts non-trivially on F_n as $\nu_n(c) = -1$. Let F^+_n be the fixed field of c; so, $[F^+_n : \mathbb{Q}] = \frac{p^n(p-1)}{2}$. We have the following field diagram

$$\begin{tikzcd}
F_n \arrow[r, "\hookrightarrow"] & H_n \\
F^+_n \arrow[u, "\cup"] \arrow[r, "\hookrightarrow"] & H^+_n \arrow[u, "\cup"']
\end{tikzcd}$$

for the Hilbert class fields H_n/F_n and H^+_n/F^+_n. Write the class group of F_n (resp. F^+_n) as Cl_n and Cl^+_n. Define then $Cl^-_n := \mathrm{Ker}(N_{F_n/F^+_n} : Cl_n \to Cl^+_n)$. Since H^+_n is real, $H^+_n \cap F_n = F^+_n$; so, $G_{H^+_n F_n/F_n} \cong G_{F_n/F^+_n} \times G_{H^+_n/F^+_n}$. Thus the restriction map $\mathrm{Res} : G_{H_n/F_n} \to G_{H^+_n/F^+_n}$ is onto. Therefore $N_{F_n/F^+_n} : Cl_n \to Cl^+_n$ is onto. Recall Dirichlet's L-function of a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ defined by an absolutely and locally uniformly converging sum for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$:

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s},$$

where we use the convention that $\chi(n) = 0$ if n and N are not co-prime. The function $L(s, \chi)$ extends to a meromorphic function on the whole complex plane $\mathbb{C}$ with only possible pole at $s = 1$, and if χ is non-trivial, it is holomorphic everywhere. Here is a formula of $|Cl^-_n|$ (e.g. [ICF, Theorem 4.17]):

Theorem 3.1. *Let $m = n + 1$. Then we have*

$$|Cl^-_n| = 2p^m \prod_{\chi:(\mathbb{Z}/p^m\mathbb{Z})^\times \to \mathbb{C}^\times; \chi(-1)=-1} \frac{1}{2} L(0, \chi^{-1})$$

with $L(0, \chi^{-1}) = -\frac{1}{p^f} \sum_{a=1}^{p^f} \chi^{-1}(a) a$, where χ is a primitive character modulo p^f with $0 < f \le m$.

By functional equation for primitive character modulo N (see [ICF, Chapter 4] or [LFE, §2.3]):

$$L(s,\chi)=\begin{cases}\frac{\tau(\chi)(2\pi/N)^sL(1-s,\chi^{-1})}{2\Gamma(s)\cos(\pi s/2)} & \text{if } \chi(-1)=1,\\ \frac{\tau(\chi)(2\pi/N)^sL(1-s,\chi^{-1})}{2\sqrt{-1}\Gamma(s)\sin(\pi s/2)} & \text{if } \chi(-1)=-1\end{cases}$$

with the Gauss sum $\tau(\chi)=\sum_{a=1}^{N}\chi(a)\exp(2\pi\sqrt{-1}a/N)$, $L(0,\chi^{-1})$ is almost $L(1,\chi)/2\pi i$ which is directly related to the class number. Because of this, we put χ^{-1} in the formula, though we can replace them by χ for an obvious reason.

We would like to study the group structure of $Cl_n = Cl_{F_n}$ and the module structure of Cl_n over $\mathbb{Z}[G_{F_n/\mathbb{Q}}]\cong\mathbb{Z}[(\mathbb{Z}/p^m\mathbb{Z})^\times]$ $(m=n+1)$. We first describe Kummer-Stickelberger theory to determine the annihilator of Cl_n^- in $\mathbb{Z}[(\mathbb{Z}/p^n\mathbb{Z})^\times]$. Writing $\sigma_a\in G_{F_n/\mathbb{Q}}$ for the element with $\zeta^{\sigma_a}=\zeta^a$ $(\zeta\in\mu_{p^m})$ for $a\in(\mathbb{Z}/p^m\mathbb{Z})^\times$, from the above class number formula, Kummer/Stickelberger guessed that $\theta=\theta_n:=\sum_{a=1}^{p^m}\frac{a}{p^m}\sigma_a^{-1}\in\mathbb{Z}[(\mathbb{Z}/p^m\mathbb{Z})^\times]$ would kill Cl_n as $\chi(\theta_n)\doteqdot L(0,\chi^{-1})$. More generally, let $F/\mathbb{Q}$ be an abelian extension with $F\subset\mathbb{Q}[\mu_N]$ for a minimal $N>0$. Define $\theta_F:=\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\left\{\frac{a}{N}\right\}\sigma_a^{-1}|_F\in\mathbb{Q}[G]$ for $G=G_{F/\mathbb{Q}}$, where $0\le\{x\}<1$ is the fractional part of a real number x (i.e., $x-\{x\}\in\mathbb{Z}$) and $\sigma_a\in G_{\mathbb{Q}[\mu_N]/\mathbb{Q}}$ sends every N-th root of unity ζ to ζ^a for $a\in(\mathbb{Z}/N\mathbb{Z})^\times$.

Theorem 3.2 (Stickelberger). *Pick $\beta\in\mathbb{Z}[G]$ such that $\beta\theta_F\in\mathbb{Z}[G]$. Then for any fractional ideal $\mathfrak{a}$ of F, $\mathfrak{a}^{\beta\theta_F}$ is principal.*

4. Basic properties of Gauss sum

The idea of proving this to compute prime factorization of the Gauss sum $G(\chi)$ of a finite field $\mathbb{F}$ of characteristic p and to show roughly $(G(\chi))=\mathfrak{a}^{\theta_F}$. Write $\mathrm{Tr}:\mathbb{F}\to\mathbb{F}_p$ for the trace map. Then for any character $\chi:\mathbb{F}^\times\to\overline{\mathbb{Q}}^\times$, the Gauss sum is defined to be

$$G(\chi):=-\sum_{a\in\mathbb{F}}\chi(a)\zeta_p^{\mathrm{Tr}(a)}\quad\text{for }\zeta_p:=\exp(\frac{2\pi i}{p}),$$

where we put $\chi(0)=0$ as before. Note that $G(\chi)=-\tau(\chi)$ if χ is a character of $\mathbb{F}_p^\times=(\mathbb{Z}/p\mathbb{Z})^\times$. The character $\psi:\mathbb{F}\to\mathbb{C}^\times$ given by $\psi(a)=\exp(\frac{2\pi i}{p})^{\mathrm{Tr}(a)}$ is non-trivial as $\mathbb{F}$ is generated by primitive N-th root of unity for $N=(|\mathbb{F}|-1)$ whose minimal polynomial is a factor of $X^N+X^{N-1}+\cdots+1$ (i.e., $\mathrm{Tr}(a)\neq 0$ for some $a\in\mathbb{F}$).

Exercise 4.1. *Give a detailed proof of the fact:* $\mathrm{Tr}(a)\neq 0$ *for some $a\in\mathbb{F}$; so,* $\mathrm{Tr}:\mathbb{F}\to\mathbb{F}_p$ *is onto.*

Lemma 4.2. *We have*

(1) $-\sum_{a\in\mathbb{F}}\chi(a)\zeta_p^{\mathrm{Tr}(ab)}=\overline{\chi}(b)G(\chi)$ *for* $b\in\mathbb{F}^\times$,
(2) $\overline{G(\chi)}=\chi(-1)G(\overline{\chi})$,
(3) *If* $\chi\neq\mathbf{1}$ *for the identity character* $\mathbf{1}$, $G(\chi)G(\overline{\chi})=\chi(-1)|\mathbb{F}|$,
(4) *If* $\chi\neq\mathbf{1}$, $|G(\chi)|^2=|\mathbb{F}|$.

Since $\tau(\chi)=-G(\chi)$ if $\mathbb{F}=\mathbb{F}_p$, we get the corresponding formula for $\tau(\chi)$.

Proof. The assertion (1) holds by the variable change $ab \mapsto a$ combined with $\overline{\chi(b)} = \chi^{-1}(b)$. Then we have

$$\overline{G(\chi)} = -\sum_{a\in\mathbb{F}} \overline{\chi}(a)\zeta_p^{-\mathrm{Tr}(a)} = -\sum_{a\in\mathbb{F}} \overline{\chi}(a)\zeta_p^{\mathrm{Tr}(a(-1))} \overset{(1)}{=} \chi(-1)G(\overline{\chi})$$

proving (2). Note that for $c \neq 1$,

$$\sum_{b\in\mathbb{F}^\times} \zeta_p^{\mathrm{Tr}(b(c-1))} = -1$$

as $1 + \sum_{b\in\mathbb{F}^\times} \zeta_p^{\mathrm{Tr}(b(c-1))} = 0$ (character sum). We then have

$$\begin{aligned} G(\chi)\overline{G(\chi)} &= \sum_{a,b\in\mathbb{F}^\times} \chi(ab^{-1})\zeta_p^{\mathrm{Tr}(a-b)} \\ &\overset{c=ab^{-1}}{=} \sum_{b,c\in\mathbb{F}^\times} \chi(c)\zeta_p^{\mathrm{Tr}(bc-b)} = \sum_{b\in\mathbb{F}^\times}\chi(1) + \sum_{c\neq 0,1}\chi(c)\sum_{b\in\mathbb{F}^\times}\zeta_p^{\mathrm{Tr}(b(c-1))} \\ &= (|\mathbb{F}|-1) + \sum_{c\neq 0,1}\chi(c)(-1) = |\mathbb{F}|. \end{aligned}$$

This finishes the proof (3), and (4) follows from (2) and (3). □

For two characters $\varphi, \phi : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$, we define the Jacobi sum as

$$J(\varphi,\phi) := -\sum_{a\in\mathbb{F}} \varphi(a)\phi(1-a).$$

See [We1] and [We2] for amazing properties of Gauss sum and Jacob sum which was the origin of Weil's conjecture (Riemann hypothesis for zeta function of algebraic varieties over finite fields), which was solved by P. Deligne. Here are some such properties:

Lemma 4.3. (1) $J(\mathbf{1},\mathbf{1}) = 2 - |\mathbb{F}|$,
(2) $J(\mathbf{1},\chi) = J(\chi,\mathbf{1}) = 1$ *if* $\chi \neq \mathbf{1}$,
(3) $J(\chi,\overline{\chi}) = \chi(-1)$ *if* $\chi \neq \mathbf{1}$,
(4) $J(\varphi,\phi) = \frac{G(\varphi)G(\phi)}{G(\varphi\phi)}$ *if* $\varphi \neq \mathbf{1}, \phi \neq \mathbf{1}, \varphi\phi \neq \mathbf{1}$.

Proof. Since there are $|\mathbb{F}| - 2$ elements in $\mathbb{F} - \{0,1\}$, we get (1). When one character is $\mathbf{1}$ and the other not, the Jacobi sum is the sum over $\mathbb{F} - \{0,1\}$, and hence the result (2) follows.

To show (4), we set $\varphi(0) = \phi(0) = 1$ and we compute $G(\varphi)G(\phi)$:

$$\begin{aligned} G(\varphi)G(\phi) &= \sum_{a,b\in\mathbb{F}} \varphi(a)\phi(b)\zeta_p^{\mathrm{Tr}(a+b)} \\ &\overset{a+b\mapsto c}{=} \sum_{a,c\in\mathbb{F}} \varphi(a)\phi(c-a)\zeta_p^{\mathrm{Tr}(c)} = \sum_{a\in\mathbb{F},c\in\mathbb{F}^\times} \varphi(a)\phi(c-a)\zeta_p^{\mathrm{Tr}(c)} + \sum_{a\in\mathbb{F}}\varphi(a)\phi(-a). \end{aligned}$$

If $\varphi\phi \neq \mathbf{1}$, we have

$$\sum_{a\in\mathbb{F}} \varphi(a)\phi(-a) = \phi(-1)\sum_{a\in\mathbb{F}^\times} \varphi\phi(a) = 0.$$

As for the first sum, without assuming $\varphi\phi \neq \mathbf{1}$, we have

$$\sum_{a\in\mathbb{F},c\in\mathbb{F}^\times} \varphi(a)\phi(c-a)\zeta_p^{\mathrm{Tr}(c)} \overset{a=bc}{=} \sum_{b\in\mathbb{F},c\in\mathbb{F}^\times} \varphi(c)\phi(c)\varphi(b)\phi(1-b)\zeta_p^{\mathrm{Tr}(c)} = G(\varphi\phi)J(\varphi,\phi).$$

Therefore we get

$$G(\varphi)G(\phi) = G(\varphi\phi)J(\varphi,\phi)$$

as desired if $\varphi\phi \neq \mathbf{1}$.

Suppose now $\varphi\phi = \mathbf{1}$. Then we have

$$\sum_{a\in\mathbb{F}}\varphi(a)\phi(-a) = \phi(-1)\sum_{a\in\mathbb{F}}\mathbf{1}(a) = \phi(-1)(|\mathbb{F}|-1).$$

Thus

$$\varphi(-1)|\mathbb{F}| = G(\varphi)G(\varphi^{-1}) = \varphi(-1)(|\mathbb{F}|-1) + G(\mathbf{1})J(\varphi,\overline{\varphi})$$

with $G(\mathbf{1}) = -\sum_{a\in\mathbb{F}^\times}\zeta_p^{\mathrm{Tr}(a)} = -(\sum_{a\in\mathbb{F}}\zeta_p^{\mathrm{Tr}(a)} - 1) = 1$. This shows (3). □

Corollary 4.4. *Suppose that $\varphi^N = \phi^N = 1$ for $0 < N \in \mathbb{Z}$. Then $\frac{G(\varphi)G(\phi)}{G(\varphi\phi)}$ is an algebraic integer in $\mathbb{Q}(\mu_N)$.*

Let $0 < N \in \mathbb{Z}$, and suppose $p \nmid N$. Then $\mathbb{Q}(\mu_N)$ and $\mathbb{Q}(\mu_p)$ is linearly disjoint as p is unramified in $\mathbb{Q}(\mu_N)$ while p fully ramify in $\mathbb{Q}(\mu_p)$. Thus

$$G_{\mathbb{Q}(\mu_{pN})/\mathbb{Q}} \cong G_{\mathbb{Q}(\mu_N)/\mathbb{Q}} \times G_{\mathbb{Q}(\mu_p)/\mathbb{Q}} \cong (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times.$$

Let $\sigma_a \in G_{\mathbb{Q}(\mu_{pN})/\mathbb{Q}}$ be the automorphism of $\mathbb{Q}(\mu_{pN})$ corresponding to $(a,1) \in (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Lemma 4.5. *If $\chi^N = 1$ and a is an integer prime to Np, then $\frac{G(\chi)^a}{G(\chi)^{\sigma_a}} = G(\chi)^{a-\sigma_a} \in \mathbb{Q}(\mu_N)$ and $G(\chi)^N \in \mathbb{Q}(\mu_N)$.*

Proof. Since $\zeta^{\sigma_a} = \zeta^a$ for $\zeta \in \mu_N$ and $\zeta_p^{\sigma_a} = \zeta_p$, we have

$$G(\chi)^{\sigma_a} = (-\sum_{x\in\mathbb{F}}\chi(x)\zeta_p^{\mathrm{Tr}(x)})^{\sigma_a} = -\sum_{x\in\mathbb{F}}\chi^a(x)\zeta_p^{\mathrm{Tr}(x)} = G(\chi^a).$$

Similarly, for $\sigma \in G_{\mathbb{Q}[\mu_{pN}]/\mathbb{Q}[\mu_N]}$, we have some $0 < b \in \mathbb{Z}$ prime to p such that $\zeta_p^\sigma = \zeta_p^b$. Then we have

$$G(\chi)^\sigma = (-\sum_{x\in\mathbb{F}}\chi(x)\zeta_p^{\mathrm{Tr}(x)})^\sigma = -\sum_{x\in\mathbb{F}}\chi(x)\zeta_p^{\mathrm{Tr}(bx)} \overset{bx\mapsto b}{=} \chi^{-1}(b)G(\chi).$$

Replacing χ by χ^a, we get

$$G(\chi^a)^\sigma = \chi^{-a}(b)G(\chi^a).$$

Thus σ fixes $\frac{G(\chi)^a}{G(\chi)^{\sigma_a}}$, and hence we get $G(\chi)^{a-\sigma_a} \in \mathbb{Q}(\mu_N)$. Taking $a := 1+N$, we get the last assertion. □

Here is the last lemma in this section:

Lemma 4.6. *We have $G(\chi^p) = G(\chi)$.*

Proof. The Frobenius automorphism Frob_p of $\mathbb{F}$ acts $\mathrm{Frob}_p(a) = a^p$. Thus $\mathrm{Tr}(a^p) = \mathrm{Tr}(\mathrm{Frob}_p(a)) = \mathrm{Tr}(a)$. Then we have

$$G(\chi^p) = -\sum_{a\in\mathbb{F}} \chi^p(a)\zeta_p^{\mathrm{Tr}(a)} = -\sum_{a\in\mathbb{F}} \chi(a^p)\zeta_p^{\mathrm{Tr}(a^p)} = -\sum_{a\in\mathbb{F}} \chi(\mathrm{Frob}_p(a))\zeta_p^{\mathrm{Tr}(\mathrm{Frob}_p(a))}$$
$$\overset{\mathrm{Frob}_p(a)\mapsto a}{=} -\sum_{a\in\mathbb{F}} \chi(a)\zeta_p^{\mathrm{Tr}(a)} = G(\chi).$$

as desired. □

5. Prime factorization of Gauss sum

Let $I' = I'_F := \{\beta \in \mathbb{Z}[G] | \beta\theta_F \in \mathbb{Z}[G]\}$ for $G = G_{F/\mathbb{Q}}$ for an abelian extension $F/\mathbb{Q}$. We put $\mathfrak{s}_F := I'\theta_F = (\theta_F) \cap \mathbb{Z}[G]$ which is called the Stickerberger ideal of F. We start with the following lemma.

Lemma 5.1. *Suppose $F = \mathbb{Q}[\mu_N]$ and put $G := G_{F/\mathbb{Q}}$. Then the ideal I' is generated by $c - \sigma_c$ for $c \in \mathbb{Z}$ prime to N.*

Proof. We first show that $I' \supset I'' := (c - \sigma_c)_c$ in $\mathbb{Z}[G]$. We have plainly

$$(c - \sigma_c)\theta = \sum_a \left(c\left\{\frac{a}{N}\right\} - \left\{\frac{ac}{N}\right\}\right)\sigma_a^{-1} \in \mathbb{Z}[G]$$

which shows the result.

Now we show the converse. Suppose that $x = \sum_a x_a\sigma_a \in I'$. Then

$$x\theta = \sum_c \left(\sum_a x_c \left\{\frac{a}{N}\right\}\right)\sigma_{ac^{-1}}^{-1} \overset{ac^{-1}\mapsto b, c\mapsto a}{=} \sum_b \left(\sum_a x_a \left\{\frac{ab}{N}\right\}\right)\sigma_b^{-1}.$$

The coefficient of σ_1^{-1} is given by

$$\sum_a x_a \left\{\frac{a}{N}\right\} \equiv \sum_a \left\{\frac{x_a a}{N}\right\} \equiv \left\{\frac{\sum_a x_a a}{N}\right\} \mod 1.$$

Thus $\sum_a x_a \equiv 0 \mod N$. Since $N = (1+N) - \sigma_{1+N} \in I''$, we find

$$\sum_a x_a\sigma_a = \sum_a x_a(\sigma_a - a) + \sum_a x_a \in I''.$$

Thus $I' \subset I''$. □

Theorem 5.2 (Stickelberger)**.** *Let $F = \mathbb{Q}[\mu_N]$. Then $\mathfrak{s}_F$ annihilates Cl_F; i.e., for any $\beta \in I'$ and a fractional ideal $\mathfrak{A}$ of F, $\mathfrak{A}^{\beta\theta}$ for $\theta := \theta_F$ is principal.*

Here for $x = \sum_a x_a\sigma_a$, $\mathfrak{A}^x = \prod_a \mathfrak{A}^{x_a\sigma_a}$.

We prepare several lemmas before going into the final phase of the proof. The idea is to make prime factorizatioin of Gauss sums which gives a canonical generator of $\mathfrak{p}^{\beta\theta}$ for a prime $\mathfrak{p}$.

Let p be a prime and $\mathbb{F}$ be a finite extension of $\mathbb{F}_p$; so, $|\mathbb{F}| = p^f =: q$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\mu_{q-1}]$ above p. Since $\mathbb{F}^\times$ is a cyclic group of order $q-1$, we have an isomorphism $\omega = \omega_{\mathfrak{p}} : \mathbb{F}^\times \cong \mu_{q-1} \subset \mathbb{Z}[\mu_{q-1}]^\times$. Since all $q-1$-th roots of unity are distinct modulo $\mathfrak{p}$, we may assume that $\omega(a) \mod \mathfrak{p} = a \in \mathbb{F}^\times$.

Step 1: *We analyze the exponent of* $\mathfrak{P}$ *appearing in the Gauss sum.* Pick a prime $\mathfrak{P}|\mathfrak{p}$ in $\mathbb{Z}[\mu_{(q-1)p}]$. Write prime factorization of an ideal $\mathfrak{A}$ of $\prod_{\mathfrak{L}} \mathfrak{L}^{v_{\mathfrak{L}}(\mathfrak{A})}$. If $\mathfrak{A} = (\alpha)$ is principal, we simply write $v_{\mathfrak{L}}(\alpha)$ for $v_{\mathfrak{L}}(\mathfrak{A})$. Simply write $v(i)$ for $v_{\mathfrak{P}}(G(\omega^{-i}))$. Here is a lemma on the behavior of the exponent v.

Lemma 5.3. (1) $v(0) = 0$;
(2) $0 \le v(i+j) \le v(i) + v(j)$;
(3) $v(i+j) \equiv v(i) + v(j)$ *mod* $(p-1)$;
(4) $v(pi) = v(i)$;
(5) $\sum_{i=1}^{q-2} v(i) = (q-2)f(p-1)/2$ *if* $q = p^f$;
(6) $v(i) > 0$ *if* $i \not\equiv 0 \mod (q-1)$;
(7) $v(1) = 1$, *in particular,* $G(\omega^{-1}) \equiv \pi \mod \mathfrak{P}^2$.

Proof. Since $G(\mathbf{1}) = 1$ as $\sum_{a \in \mathbb{F}} \zeta_p^{\mathrm{Tr}(a)} = 0$ (character sum), we get (1). Since $\frac{G(\varphi)G(\phi)}{G(\varphi\phi)}$ is an algebraic integer (Corollary 4.4), (2) follows. Moreover, again by Corollary 4.4, $\frac{G(\varphi)G(\phi)}{G(\varphi\phi)}$ is an algebraic integer in the smaller field $\mathbb{Q}[\mu_N]$ in which $\mathfrak{p}$ does not ramify, the difference $v(i+j) - (v(i) + v(j))$ is divisible by the ramification index $p-1$ of $\mathfrak{P}/\mathfrak{p}$. Therefore, we get (3). By the existence of Frobenius automorphism on $\mathbb{F}$, we have $G(\chi^p) = G(\chi)$ (Lemma 4.6), which shows (4). Since $G(\omega^{-i})G(\omega^i) = G(\overline{\omega}^i)G(\omega^i) = \pm q = \pm p^f$ as long as $\omega^i \neq \mathbf{1}$ (i.e., $1 \le i \le p^f - 2$), $v(-i) + v(i) = f(p-1)$ as $p-1$ is the ramification index of $\mathfrak{P}/(p)$, summing these up, we get (5). To show (6), we put $\pi := \zeta_p - 1$ which is a generator of the unique prime in $\mathbb{Z}[\mu_p]$ (Lemma 1.1); so, $\pi \in \mathfrak{P}$. Then we see

$$G(\omega^{-i}) = -\sum_a \omega^{-i}(a)\zeta_p^{\mathrm{Tr}(a)} \equiv -\sum_a \omega^{-i}(a) \equiv 0 \mod \mathfrak{P},$$

which shows $v(i) > 0$. Now we prove (7) by showing $G(\omega^{-1}) \equiv \pi \mod \mathfrak{P}^2$. By a computation similar to the case of (6), we see

$$\begin{aligned} G(\omega^{-1}) &= -\sum_a \omega^{-1}(a)\zeta_p^{\mathrm{Tr}(a)} = -\sum_a \omega^{-1}(a)(1+\pi)^{\mathrm{Tr}(a)} \\ &\equiv -\sum_a \omega^{-1}(a)(1+\pi\mathrm{Tr}(a)) \mod \mathfrak{P}^2 \equiv -\pi \sum_a \omega^{-1}(a)\mathrm{Tr}(a) \mod \mathfrak{P}^2. \end{aligned}$$

Note that $G_{\mathbb{F}/\mathbb{F}_p} = \langle \mathrm{Frob}_p \rangle = \{1, \mathrm{Frob}_p, \mathrm{Frob}_p^2, \dots, \mathrm{Frob}_p^{f-1}\}$. Thus we have $\mathrm{Tr}(a) = a + a^p + \cdots + a^{p^{f-1}}$. Therefore, we get

$$\sum_a \omega^{-1}(a)\mathrm{Tr}(a) \equiv \sum_{0 \neq a \in \mathbb{Z}[\mu_N]/\mathfrak{p}} a^{-1}(a + a^p + \cdots + a^{p^{f-1}}) \mod \mathfrak{p}.$$

Since $a \mapsto a^{p^b - 1}$ is a non-trivial character of $\mathbb{F}^\times$ if $0 < b \le f$, the sum $\sum_{0 \neq a \in \mathbb{Z}[\mu_N]/\mathfrak{p}} a^{p^b-1}$ vanishes modulo $\mathfrak{p}$, and hence the sum reduces to $\sum_{0 \neq a \in \mathbb{Z}[\mu_N]/\mathfrak{p}} 1 = q - 1 \equiv -1 \mod \mathfrak{p}$; therefore, we conclude $G(\omega^{-1}) \equiv \pi \mod \mathfrak{P}^2$ as desired. □

Step 2: *Prime factorization of* $G(\chi)$*:* To clarify the notation, fix a positive integer N, and choose a prime $p \nmid N$. Write f for the order of the class of p in $(\mathbb{Z}/N\mathbb{Z})^\times$. Thus $N|p^f-1$ (exactly). Let $\chi := \omega^{-d}$ for $d = (q-1)/N$; so, χ has values in μ_N and therefore $\chi^N = \mathbf{1}$. Let R be a complete representative set for $(\mathbb{Z}/N\mathbb{Z})^\times/\langle p\rangle$. Let $\mathfrak{p}$ be a prime over p of $\mathbb{Z}[\mu_{q-1}]$ such that $\omega(a) \mod \mathfrak{p} = a \in \mathbb{F}^\times$, and put $\mathfrak{p}_0 = \mathfrak{p} \cap \mathbb{Z}[\mu_N]$ (which is the base prime for the prime factorization of $G(\chi)$). Then by Remark 1.4, $\{\mathfrak{p}_0^{\sigma_a^{-1}} | a \in R\}$ is the set of all distinct primes above (p) in $\mathbb{Z}[\mu_N]$. Let $\mathfrak{P}_0$ be the unique prime above $\mathfrak{p}_0$ in $\mathbb{Z}[\mu_{pN}]$ as any prime above p fully ramifies in $\mathbb{Z}[\mu_{pN}]/\mathbb{Z}[\mu_N]$. Let $\mathcal{P}_0$ (resp. $\widetilde{\mathcal{P}}_0$) be a prime in $\mathbb{Z}[\mu_{q-1}]$ (resp. $\mathbb{Z}[\mu_{(q-1)p}]$) over $\mathfrak{p}_0$ (resp. $\mathfrak{P}_0$).

Lemma 5.4. *Let the notation be as above. Then we have*

$$(G(\chi)) = \mathfrak{P}_0^{\sum_{a\in R} v(ad)\sigma_a^{-1}} = \prod_{a\in R} \mathfrak{P}_0^{\sigma_a^{-1} v(ad)}.$$

Proof. Note that $\mathfrak{P}_0^{\sigma_a^{-1}}$ is the unique prime above $\mathfrak{p}_0^{\sigma_a^{-1}}$. Write $\mathfrak{P} := \mathfrak{P}_0^{\sigma_a^{-1}}$. Then we have

$$v_{\mathfrak{P}}(G(\chi)) = v_{\mathfrak{P}_0}(G(\chi)^{\sigma_a}) = v_{\mathfrak{P}_0}(G(\chi^a)) = v_{\widetilde{\mathcal{P}}_0}(G(\chi^a)) = v(ad).$$

This shows that the exponent of $\mathfrak{P} = \mathfrak{P}_0^{\sigma_a^{-1}}$ in $G(\chi)$ is given by $v(ad)$. □

Step 3: *Determination of* $v(i)$ *via* p*-adic expansion:*

Lemma 5.5. *Let* $0 \le i < q-1$ *and expand* i *into a standard* p*-adic expansion* $i = a_0(i)+a_1(i)p+\cdots+a_{f-1}(i)p^{f-1}$ *with* $0 \le a_j(i) \le p-1$*. Then* $v(i) = a_0(i)+a_1(i)+\cdots+a_{f-1}(i)$*.*

Proof. Since $v(i) = v(\overbrace{1+1+\cdots+1}^{i}) \le i\cdot v(1) = i$ as $v(i+j) \le v(i)+v(j)$ and and $v(1) = 1$ by Lemma 5.3 (2) and (7). Since $v \mod (p-1)$ is linear by Lemma 5.3 (3), we find $v(i) \equiv i \mod (p-1)$. Thus if $0 \le i < p-1$, we get $v(i) = i$. Now assume that $i \ge p$. Since $v(pi) = v(i)$ by Lemma 5.3 (3), we can sharpen $v(i) \le i$ to $v(i) \le a_0(i)+a_1(i)+\cdots+a_{f-1}(i)$. Then we have

$$\sum_{i=0}^{q-1}(a_0(i)+a_1(i)+\cdots+a_{f-1}(i)) = (1+2+\cdots+p-1)fp^{f-1} = \frac{p(p-1)}{2}fp^{f-1} = \frac{p-1}{2}fq$$

as each $a_j(i)$ takes value 0 to $p-1$ exactly p^{f-1} times when i varies from 0 to p^{f-1}. Removing $i = q-1 = (p-1)+(p-1)p+\cdots+(p-1)p^{f-1}$, we get

$$\sum_{i=0}^{q-2} v(i) \le \sum_{i=0}^{q-2}(a_0(i)+a_1(i)+\cdots+a_{f-1}(i)) = \frac{p-1}{2}fq - (p-1)f \overset{\text{Lemma 5.3 (5)}}{=} \sum_{i=0}^{q-2} v(i),$$

which shows that each term $v(i)$ must be equal to $a_0(i)+a_1(i)+\cdots+a_{f-1}(i)$. □

We now make more explicit the value $v(i)$:

Lemma 5.6. *If* $0 \le a < q-1$*, then*

$$v(a) = (p-1)\sum_{j=0}^{f-1}\left\{\frac{p^j a}{q-1}\right\} \quad \textit{and} \quad v(ad) = (p-1)\sum_{j=0}^{f-1}\left\{\frac{p^j a}{N}\right\}.$$

Proof. Expand $a = a_0(a) + a_1(a)p + \cdots + a_{f-1}(a)p^{f-1}$. Then we have

$$p^j a = a_0(a)p^j + a_1(a)p^{j+1} + \cdots + a_{f-1}(a)p^{j+f-1}.$$

Since $p^f \equiv 1 \mod (q-1)$, once the exponent $j+k$ of p in $a_k(a)p^{j+k}$ exceeds f, we can remove p^f modulo $q-1$. Thus we have

$$p^j a \equiv \sum_{k=j}^{f-1} a_{k-j}(a)p^k + \sum_{\ell=0}^{j-1} a_{f+\ell-j}(a)p^\ell \mod (q-1).$$

Here p^k, p^ℓ runs through $\{1, p, \dots, p^{f-1}\}$ once for each, and $a_j(a)$ for $j = 0, 1 \dots, f-1$ appears once for each.

Since the right-hand-side is less than $q-1$, we have

$$\left\{\frac{p^j a}{q-1}\right\} = \frac{\sum_{k=j}^{f-1} a_{k-j}(a)p^k + \sum_{\ell=0}^{j-1} a_{f+\ell-j}(a)p^\ell \mod (q-1)}{q-1}.$$

Now we sum up over j. By moving j from 0 to $f-1$, modulo $q-1$, for each p^k, the term $a_i(a)p^k$ shows up once for each i with $0 \le i \le f-1$. Then each term involving $a_k(a)$ is given by

$$a_k(a)(1 + p + \cdots + p^{f-1}) = a_k(a)\frac{p^f - 1}{p-1} = a_k(a)\frac{q-1}{p-1}.$$

Thus we conclude

$$\sum_{j=0}^{f-1}\left\{\frac{p^j a}{q-1}\right\} = \frac{1}{q-1}\frac{q-1}{p-1}\sum_k a_k(a) = \frac{1}{p-1}\sum_k a_k(a) = \frac{v(a)}{p-1}.$$

Then we see for $d = \frac{q-1}{N}$,

$$v(ad) = (p-1)\sum_{j=0}^{f-1}\left\{\frac{p^j ad}{q-1}\right\} = (p-1)\sum_{j=0}^{f-1}\left\{\frac{p^j a}{N}\right\}$$

as desired. □

Corollary 5.7. *We have $(G(\chi)^N) = \mathfrak{p}_0^{N\theta_F}$ in $\mathbb{Z}[\mu_N]$.*

Proof. Since $G(\chi)^\tau = \overline{\chi}(a)G(\chi)$ for $G_{\mathbb{Q}[\mu_{pN}]/F}$ with $\zeta_p^\tau = \zeta_p^a$ (Lemma 4.2 (1)), we have $G(\chi)^N \in \mathbb{Z}[\mu_N]$. Since $\mathbb{Q}[\mu_{pN}]/F$ fully ramifies at $\mathfrak{p}_0$ with ramification index $p-1$, we find $\mathfrak{P}_0^{(p-1)} = \mathfrak{p}_0$. We have

$$\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times/\langle p\rangle} v(ad)\sigma_a^{-1} = (p-1)\sum_{j=0}^{f-1}\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times/\langle p\rangle}\left\{\frac{p^j a}{N}\right\}\sigma_a^{-1}.$$

Note that $\mathfrak{p}_0^{\sigma_p} = \mathfrak{p}_0$ as σ_p is the generator of the decomposition group of p; so, the effect of σ_{ap^j} on $\mathfrak{p}_0$ is the same as the effect of σ_a on $\mathfrak{p}_0$. Thus we conclude

$$\mathfrak{p}_0^{\sum_{j=0}^{f-1}\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times/\langle p\rangle}\{\frac{p^j a}{N}\}\sigma_a^{-1}} = \mathfrak{p}_0^{\sum_{j=0}^{f-1}\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times/\langle p\rangle}\{\frac{p^j a}{N}\}\sigma_{ap^j}^{-1}} \underset{(*)}{=} \mathfrak{p}_0^{\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\{\frac{a}{N}\}\sigma_a^{-1}}.$$

The last equality $(*)$ follows from the bijection $(\mathbb{Z}/N\mathbb{Z})^\times \leftrightarrow \langle p\rangle \times (\mathbb{Z}/N\mathbb{Z})^\times/\langle p\rangle$ Then by Lemma 5.6,

$$(G(\chi)^N) = \mathfrak{P}_0^{N(p-1)\theta_F} = \mathfrak{p}_0^{N\theta_F}$$

as desired. □

Step 4: *Proof of Stickelberger's theorem:* Let $\mathfrak{A}$ be an ideal of $\mathbb{Q}[\mu_N]$ prime to (N). Write the prime factorization of $\mathfrak{A}$ as $\prod_i \mathfrak{p}_i$ (here $\mathfrak{p}_i' s$ may overlap). Let χ_i be the character of $(\mathbb{Z}[\mu_N]/\mathfrak{p}_i)^\times = \mathbb{F}^\times$ given by $\omega_{\mathfrak{p}_i}^d$ for $d = \frac{q-1}{N}$ for $q = N(\mathfrak{p}_i) = |\mathbb{F}|$. By Corollary 5.7 applied to each $\mathfrak{p}_i$, we have

$$\mathfrak{A}^{N\theta_F} = \prod_i \mathfrak{p}_i^{N\theta_F} = (\prod_i G(\chi_i)^N).$$

Write $\gamma := \prod_i G(\chi_i) \in \mathbb{Q}[\mu_{PN}]$ for $P = \prod_i p_i$. If $\beta\theta_F \in \mathbb{Z}[G]$ $(G = G_{F/\mathbb{Q}})$, then

$$\mathfrak{A}^{N\beta\theta_F} = (\gamma^{\beta N}).$$

Since $\gamma^\beta \in F$ by Proposition 5.1 and $G(\chi)^{b-\sigma_b} \in F$ (Lemma 4.5), we have $F[\gamma^\beta]/F$ is a Kummer extension adding N-th root γ^β of $\gamma^{N\beta} \in F$. Now we claim that

(Ur) *$F(\gamma^\beta)/F$ can ramify only at prime factors of N.*

Here is the proof of (Ur): By adding N-th root, only ramified primes in the extension are factors of N and prime factors of $\gamma^{N\beta}$. Since $(\gamma^{N\beta})$ is N-th power of ideal $\mathfrak{A}$, for a prime factor $\mathfrak{l}$ of $\gamma^{\beta N}$, $F_{\mathfrak{l}}[\gamma^\beta] = F_{\mathfrak{l}}[\sqrt[N]{u}]$ for a unit u of the $\mathfrak{l}$-adic completion $F_{\mathfrak{l}}$. Since $\mathfrak{l} \nmid N$, $F_{\mathfrak{l}}[\sqrt[N]{u}]/F_{\mathfrak{l}}$ is unramified.

By definition,

$$F \subset F[\gamma^\beta] \subset \mathbb{Q}[\mu_{NP}] = F[\mu_P].$$

The only primes ramifying in $F[\mu_P]/F$ is factors of P which is prime to N. Therefore by (Ur), $F[\gamma^\beta]$ is unramified everywhere over F and is abelian over $\mathbb{Q}$, which is impossible by Remark 1.4 unless $F = F[\gamma^\beta]$. Therefore, $\mathfrak{A}^{\beta\theta} = (\gamma^\beta)$ with $\gamma^\beta \in F$. □

6. A consequence of the Kummer–Vandiver conjecture

Recall $F_n = \mathbb{Q}[\mu_{p^{n+1}}]$ with $m = n+1$. Let $h_n^+ = |Cl_{F_n^+}| = |Cl_n^+|$. The following conjecture is well known but we do not have a theoretical eveidence except for the conjecture numerically verified to be true valid for primes up to 163 million [BH]:

Conjecture 6.1 (Kummer–Vandiver). *$p \nmid h_0^+$ (so, $Cl_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p = 0$).*

Suppose hereafter Conjecture 6.1. Let $A_n^\pm := Cl_n^\pm \otimes_{\mathbb{Z}} \mathbb{Z}_p$ (the p-Sylow part of $Cl_n^\pm$, and put $R_n := \mathbb{Z}_p[G_{F_n/\mathbb{Q}}]$. Then $A_n^\pm$ is a module over R_n. Define $\mathfrak{s}_n := R_n \cap \theta_{F_n} R_n$. Since $R_n = \mathbb{Z}[G_{F_n/\mathbb{Q}}] \otimes_{\mathbb{Z}} \mathbb{Z}_p$, we have $\mathfrak{s}_n = \mathfrak{s}_{F_n} \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and hence by Stickelberger's theorem (Theorem 3.2), we have $\mathfrak{s}_n A_n^- = 0$ without assuming Conjecture 6.1. Here Iwasawa's cyclicity theorem which is a goal of this course:

Theorem 6.2 (Iwasawa). *Suppose $p \nmid h_0^+$. Then we have an isomorphism $A_n^- \cong R_n^-/\mathfrak{s}_n^-$ as R_n-modules, where $X^- = (1-c)X$ (the "$-$" eigenspace of complex conjugation c).*

We start preparing several facts necessary for the proof of the theorem. We first compute the index $[R_n^- : \mathfrak{s}_n^-]$.

Lemma 6.3. *We have* $[R_n^- : \mathfrak{s}_n^-] = |A_n^-|$.

Proof. Let $G = G_{F_n/\mathbb{Q}}$ and $\theta = \theta_{F_n}$. Let $\mathrm{Tr} := \sum_{\sigma \in G} \sigma \in R_n$. Since $\{z\} + \{-z\} = 1$ and $c\sigma_a = \sigma_{-a}$, $(1+c)\theta$ is equal to

$$\sum_{a \in (\mathbb{Z}/p^m\mathbb{Z})^\times} \left\{\frac{a}{p^m}\right\} \sigma_a^{-1} + \sum_{a \in (\mathbb{Z}/p^m\mathbb{Z})^\times} \left\{\frac{a}{p^m}\right\} \sigma_{-a}^{-1} = \sum_{a \in (\mathbb{Z}/p^m\mathbb{Z})^\times} \left(\left\{\frac{a}{p^m}\right\} + \left\{\frac{-a}{p^m}\right\}\right) \sigma_a^{-1} = \mathrm{Tr}.$$

Let $\theta^\pm := \frac{1 \pm c}{2}\theta = \theta - \frac{1+c}{2}\theta = \theta - \frac{\mathrm{Tr}}{2} \in \frac{1-c}{2}R_n = R_n^-$. Thus we have

$$\theta^+ := \frac{1+c}{2}\theta = \frac{1}{2}\mathrm{Tr}. \tag{6.1}$$

Since $\mathfrak{s}_n = R_n \cap \theta R_n$, we have $\mathfrak{s}_n^- = \frac{1-c}{2}R_n \cap \frac{1-c}{2}\theta R_n = R_n^- \cap \theta^- R_n$.

We first compute the index $[R_n\theta^- : \mathfrak{s}_n^-] = [R_n\theta^- : R_n^- \cap \theta^- R_n]$. Take $x = \sum_{b \in (\mathbb{Z}/p^m\mathbb{Z})^\times} x_b\sigma_b \in R_n$. Since $\theta^+ = \frac{1}{2}\mathrm{Tr} \in R_n$, we have $x\theta^- \in R_n^- \Leftrightarrow x\theta \in R_n$. Then

$$x\theta = \frac{1}{p^m}\sum_b\sum_a a x_b \sigma_a^{-1}\sigma_b = \frac{1}{p^m}\sum_b\sum_a a x_b \sigma_{ba^{-1}} \overset{a^{-1}b \mapsto b}{=} \frac{1}{p^m}\sum_b\sum_a a x_{ab}\sigma_b.$$

This shows $x\theta^- \in R_n^- \Leftrightarrow x\theta \in R_n \Leftrightarrow \sum_a a x_{ab} \equiv 0 \mod p^m$ for all b prime to p. But

$$\sum_a a x_{ab} \equiv b^{-1}\sum_a (ab) x_{ab} \equiv b^{-1}\sum_a a x_a \mod p^m.$$

Therefore

$$x\theta^- \in R_n^- \Leftrightarrow x\theta \in R_n \Leftrightarrow \sum_a a x_a \equiv 0 \mod p^m.$$

Thus $R_n\theta^- \cap R_n^- = \{x\theta^- \in R_n | \sum_a a x_a \equiv 0 \mod p^m\}$. Then $R_n\theta^-/(R_n\theta^- \cap R_n^-) \hookrightarrow \mathbb{Z}/p^m\mathbb{Z}$ by sending $x\theta^-$ to $\sum_s x_a a \mod p^m$. This map is surjective taking $x := \sigma_1$ as $\sum_s x_a a = 1$. Therefore we conclude $[R_n\theta^- : R_n\theta^- \cap R_n^-] = p^m$.

Consider the linear map $T : R_n^- \to R_n^-$ given by the multiplication by $p^m\theta^-$. Then

$$\begin{aligned}
[R_n^- : p^m R_n^- \theta] &= |\det(T)|_p^{-1} \\
&= |p^{m[F_n^+:\mathbb{Q}]}\prod_\chi L(0,\chi)|_p^{-1} = p^{m|G|/2-m}|A_n^-| = [R_n^-\theta^- : p^m R_n^-\theta^-]p^{-m}|A_n^-|.
\end{aligned}$$

by the class number formula (Theorem 3.1). Thus

$$|A_n^-| = \frac{[R_n^- : p^m R_n^- \theta][R_n\theta^- : R_n\theta^- \cap R_n^-]}{[R_n^-\theta^- : p^m R_n^-\theta^-]}.$$

Since $R_n^- \supset \mathfrak{s}_n^- \supset p^m R_n^- \theta$ and $R_n^-\theta \supset \mathfrak{s}_n^- \supset p^m R_n^- \theta$, we have

$$\frac{[R_n^- : p^m R_n^- \theta]}{[R_n^-\theta^- : p^m R_n^-\theta^-]} = \frac{[R_n^- : \mathfrak{s}_n^-]}{[R_n^-\theta^- : \mathfrak{s}_n^-]}.$$

From this we see

$$|A_n^-| = \frac{[R_n^- : \mathfrak{s}_n^-]][R_n\theta^- : R_n\theta^- \cap R_n^-]}{[R_n^-\theta^- : \mathfrak{s}_n^-]} = \frac{[R_n^- : \mathfrak{s}_n^-][R_n^-\theta^- : \mathfrak{s}_n^-]}{[R_n^-\theta^- : \mathfrak{s}_n^-]} = [R_n^- : \mathfrak{s}_n^-].$$

This shows the desired index formula. □

7. Kummer theory

Let F/F_0 be a finite extension inside $\overline{\mathbb{Q}}$. If $\alpha \in F^\times$ is not a p-power in $F^\times$, $F[\sqrt[p]{\alpha}]/F$ is a Galois extension of degree p, as a complete set of conjugates of $\sqrt[p]{\alpha}$ over F is given by $\{\zeta\sqrt[p]{\alpha}|\zeta \in \mu_p\}$. Thus $G_{F[\sqrt[p]{\alpha}]/F} \cong \mathbb{Z}/p\mathbb{Z}$ by sending $\sigma_a \in G_{F[\sqrt[p]{\alpha}]/F}$ with $\sigma_a(\sqrt[p]{\alpha}) = \zeta_p^a\sqrt[p]{\alpha}$ to $a \in \mathrm{Aut}(\mu_p) = \mathbb{Z}/p\mathbb{Z}$. The extension $F[\sqrt[p]{\alpha}]_{/F}$ only depends on $\alpha \bmod (F^\times)^p$. Thus we simply write $F[\sqrt[p]{\alpha}]$ for the extension corresponding to $\alpha \in F^\times/(F^\times)^p$. For a subset B of $F^\times/(F^\times)^p$, we put $F[\sqrt[p]{B}] := F[\sqrt[p]{\alpha}]_{\alpha\in B}$, which is a $(p, p, \dots, p)$-Galois extension of F.

Conversely, we take a p-cyclic extension K/F with a fixed isomorphism $G_{K/F} \cong \mathbb{Z}/p\mathbb{Z}$ with $\sigma \in G_{K/F}$ corresponding to $1 \in \mathbb{Z}/p\mathbb{Z}$. By the normal basis theorem in Galois theory, K is free of rank 1 over the group algebra $F[G_{K/F}]$. Thus for any character $\xi : \mathbb{Z}/p\mathbb{Z} \to \mu_p$, the ξ-eigenspace $F[\xi] = \{x \in K|\sigma(x) = \xi(\sigma)x \text{ for all } \sigma \in G_{K/F}\}$ is one dimensional over F. Suppose that $\xi(\sigma_a) = \zeta_p^a$. Pick $\beta \in F[\xi]$. then $\alpha := \beta^p \in F$ as it is invariant under $G_{K/F}$. Since $K \supset F[\sqrt[p]{\alpha}]$ and $F[\sqrt[p]{\alpha}]$ has degree p over F, we conclude $K = F[\sqrt[p]{\alpha}]$. Thus every $(p, p, \dots, p)$-extension of F is of the form $F[\sqrt[p]{B}]$. Since $F[\sqrt[p]{\alpha}^a] \subset F[\sqrt[p]{\alpha}]$ for any $a \in \mathbb{F}_p$, replacing B by the span of B in $F^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$, we may assume that B is an $\mathbb{F}_p$-vector subspace of $F^\times \otimes_{\mathbb{Z}} \mathbb{F}_p = F^\times/(F^\times)^p$.

Lemma 7.1. *Let the notation be as above. Suppose* $\dim_{\mathbb{F}_p} B < \infty$*. We have a non-degenerate pairing* $\langle\cdot,\cdot\rangle : G_{F[\sqrt[p]{B}]/F} \times B \to \mu_p$ *given by* $\langle\tau, \beta\rangle := \tau(\sqrt[p]{\beta})/\sqrt[p]{\beta}$*.*

Proof. If $\langle\tau, \beta\rangle = 1$ for all $\tau \in G_{F[\sqrt[p]{B}]/F}$, plainly $\sqrt[p]{\beta} \in F^\times$; so, $\beta = 0$ in $F^\times/(F^\times)^p$. Thus the pairing is non-degenerate on the B side. Thus $\dim_{\mathbb{F}_p} G_{F[\sqrt[p]{B}]/F} \geq \dim_{\mathbb{F}_p} B$.

Since $F[\sqrt[p]{\beta}] \supset F[\sqrt[p]{\beta}^a]$ for $a \in \mathbb{F}_p$ and $F[\sqrt[p]{\alpha\beta}] \subset F[\sqrt[p]{\alpha}, \sqrt[p]{\beta}]$, we find that $F[\sqrt[p]{B}] = F[\sqrt[p]{\beta_1}, \dots, \sqrt[p]{\beta_d}]$ for a basis $\{\beta_1, \dots, \beta_d\}$ of B over $\mathbb{F}_p$; so, $p^{\dim_{\mathbb{F}_p} B} = p^d \geq [F[\sqrt[p]{B}] : F] = |G_{F[\sqrt[p]{\alpha}]/F}|$, which shows $\dim_{\mathbb{F}_p} G_{F[\sqrt[p]{B}]/F} = d$, and this finishes the proof. □

Lemma 7.2. *Suppose* $F \supset F_0 = \mathbb{Q}[\mu_p]$*. Let* K/F *be the maximal* $(p, p, \dots, p)$*-extension unramified outside* p*. Then for* $B := O[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$*, we have* $K = F[\sqrt[p]{B}]$ *and* $\dim_{\mathbb{F}_p} B < \infty$*.*

Proof. Let $L := F[\sqrt[p]{\alpha}]$. By multiplying p-power of a non-zero integer, we may assume that $\alpha \in O - \{0\}$. Write prime factorization of $(\alpha) = \prod_{\mathfrak{l}} \mathfrak{l}^{e(l)}$. Plainly if $\mathfrak{l} \nmid p$ and $p \nmid e(\mathfrak{l})$, $\mathfrak{l}$ ramifies in $L_{/F}$. As for p, residually, any p-th root does not give any non-trivial extension as Frob_p just raises p-power. Thus p can ramify independent of $e(\mathfrak{l})$ for $\mathfrak{l}|p$. This shows the result. By Dirichlet's unit theorem, $\mathrm{rank}_{\mathbb{Z}} O[\frac{1}{p}]^\times \leq [F : \mathbb{Q}] +$ the number of prime factors of $p = r$. Thus $\dim_{\mathbb{F}_p} B \leq r$. □

Exercise 7.3. *Compute* $\dim_{\mathbb{F}_p} B$ *in* Lemma 7.2*.*

Corollary 7.4. *Let the notation be as in* Lemma 7.2*. Assume* $F = F_n$*. Then* $K = F[\sqrt[p]{B}]$ *for* B *generated by* $O^\times$ *and* $1 - \zeta_{p^m}$ $(m = n + 1)$*.*

This is because the unique prime ideal $\mathfrak{p}$ over p in F_n is principal generated by $1-\zeta_{p^{n+1}}$ by Lemma 1.1.

8. Cyclicity theorem for $F_0 = \mathbb{Q}[\mu_p]$

Let $F = F_n$ and $L = L_{n/F_n}$ be the maximal p-elementary abelian extension unramified everywhere. Here elementary means that $\mathrm{Gal}(L_n/F_n)$ is killed by p. Write A_n for the maximal p-abelian quotient $Cl_n \otimes_{\mathbb{Z}} \mathbb{Z}_p$ of Cl_n. Since L/F is elementary p-abelian, $\mathrm{Gal}(L/F)$ is an $\mathbb{F}_p$-vector space. By class field theory (and Galois theory), $\mathrm{Gal}(L/F) \cong Cl_n/pCl_n = A_n/pA_n$. By Kummer theory, $L = F[\sqrt[p]{B}]$ for an $\mathbb{F}_p$-vector subspace B of $F^\times \otimes_{\mathbb{Z}} \mathbb{F}_p = F^\times/(F^\times)^p$. Since $F[\sqrt[p]{b}]_{/F}$ is everywhere unramified for $b \in F^\times$ with $\overline{b} = (b \bmod (F^\times)^p) \in B$, the principal ideal (b) is a p-power $\mathfrak{a}^p$ for an O-ideal $\mathfrak{a}$. The class of $\mathfrak{a}$ in A_n only depends on the class of b modulo $(F^\times)^p$ as $F[\sqrt[p]{a^p b}] = F[\sqrt[p]{b}]$. Thus sending $\overline{b} := b \bmod (F^\times)^p$ to the class of $\mathfrak{a}$, we get a homomorphism $\phi : B \to A_n[p] = \{x \in A_n | px = 0\}$, which is obviously $\mathbb{Z}_p[G]$-linear for $G := G_{F/\mathbb{Q}}$. Assume $\overline{b} \in \mathrm{Ker}(\phi)$. Then $(b) = (a)^p$; so, $b = a^p\varepsilon$ with $\varepsilon \in O^\times$. In other words, $F[\sqrt[p]{b}] = F[\sqrt[p]{\varepsilon}]$. Thus we conclude that $\mathrm{Ker}(\phi) \subset O^\times/(O^\times)^p = O^\times \otimes_{\mathbb{Z}} \mathbb{F}_p$ as $\mathbb{Z}_p[G]$-modules.

Now we assume that $F = F_0$. Then $\widehat{G} = \mathrm{Hom}(G, {\mathbb{Z}_p}^\times)$ is generated by Teichmüller character ω of order $p-1$. Then $\mathbb{Z}_p[G] = \bigoplus_{i \bmod p-1} \mathbb{Z}_p e_i$ for the idempotent $e_i = \frac{1}{|G|}\sum_\sigma \omega^{-i}(\sigma)\sigma$. For a finite p-abelian group H, we define $p\text{-rank}(H) = \dim_{\mathbb{F}_p} H \otimes_{\mathbb{Z}} \mathbb{F}_p = \dim_{\mathbb{F}_p} H[p]$ for $H[p] = \{x \in H | px = 0\}$ (which is the minimal number of generators of H by the fundamental theorem of finite abelian groups); thus, H is cyclic if and only if $p\text{-rank}(H) = 1$. We first prove

Theorem 8.1. *Let A be the p-Sylow subgroup of Cl_0 and put $A = \bigoplus_i e_i A$. If i is even and j is odd with $i + j \equiv 1 \mod (p-1)$, then we have*

$$p\text{-rank}(e_iA) \le p\text{-rank}(e_jA) \le 1 + p\text{-rank}(e_iA).$$

This implies a famous result of Kummer (when he proved FLT for regular primes): $p\big||Cl_0^+| \Rightarrow p\big||Cl_0^-|$.

Proof. By class field theory, $A/pA \cong \mathrm{Gal}(L/F)$ for the maximal p-abelian elementary extension unramified everywhere. Then we have perfect Kummer pairing as in Lemma 7.1 $\langle \cdot, \cdot \rangle : A/pA \times B \to \mu_p$. Note that $\sigma_a \mathfrak{a} = \omega^i(a)\mathfrak{a}$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ if $\mathfrak{a} \in A_i := e_iA$. Since $\langle \mathfrak{a}, b\rangle^{\omega(a)} = \langle \mathfrak{a}, b\rangle^{\sigma_a} = \langle \mathfrak{a}^{\sigma_a}, b^{\sigma_a}\rangle = \langle \omega^i(a)\mathfrak{a}, \omega^k(a)b\rangle = \langle \mathfrak{a}, b\rangle^{\omega^{i+k}(a)}$ for $b \in B_k = e_kB$, $\langle \mathfrak{a}, b\rangle = 1$ unless $i + k \equiv 1 \mod (p-1)$. This shows that $\langle \cdot, \cdot \rangle$ indices a perfect pairing on $A_i \times B_j$. Thus $\dim_{\mathbb{F}_p} A_i = \dim_{\mathbb{F}_p} B_j$.

Now $\phi : B_j \to A_i[p] = e_i(A[p])$ is $\mathbb{Z}_p[G]$-linear. Since $\mathrm{Ker}(\phi) \cap B_j \subset e_j(O^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)$ and

$$E_k := e_k(O^\times \otimes_{\mathbb{Z}} \mathbb{F}_p) \cong \begin{cases} \mathbb{F}_p & \text{if } k \text{ is even, } k \not\equiv 0 \mod (p-1)\text{; or } k \equiv 1 \mod (p-1), \\ 0 & \text{otherwise} \end{cases}$$

by Dirichlet's unit theorem, we have

$$(8.1) \qquad p\text{-rank}(A_l) = \dim B_k \le \dim E_k + \dim A_k[p] \text{ if } l + k \equiv 1 \mod (p-1).$$

If i is even (and j is odd), taking $k = i$ (and $l = j$), we have

$$p\text{-rank}(A_j) = \dim B_i \le \dim E_i + \dim A_i[p] = 1 + p\text{-rank}(A_i).$$

If j is odd and $j \not\equiv 1 \mod (p-1)$, we have

$$p\text{-rank}(A_i) \leq \dim A_j[p] = p\text{-rank}(A_j).$$

Thus if $j \not\equiv 1 \mod (p-1)$, the result follows.

Suppose that $j \equiv 1 \mod (p-1)$. Then $i = 0$. Let L_0 be the subfield of L with $G_{L_0/F} = A_0$. From the exact sequence:

$$1 \to G_{L_0/F} \to G_{L_0/\mathbb{Q}} \to G \to 1$$

with G acting on the normal subgroup $G_{L_0/F}$ by conjugation, $G_{L_0/\mathbb{Q}}$ is abelian. Then for the inertia subgroup I at p in $G_{L_0/\mathbb{Q}}$ is isomorphic to $G_{F/\mathbb{Q}}$; so, L_0^I is everywhere unramified extension of $\mathbb{Q}$; so, $A_0 \cong G_{L_0^I/\mathbb{Q}}$ is trivial.

Consider $c = 1 + p$. Then $\omega(c - \sigma_c) = 1 + p - 1 = p$. For the Stickelberger element $\theta = \frac{1}{p}\sum_{a=1}^{p-1} \sigma_a^{-1} a$, $\omega((c - \sigma_c)\theta_F) = \sum_a a\omega^{-1}(a) \equiv 1(p-1) \mod p$ kills A_1; so, $A_1 = 0$. This shows the result when $j \equiv 1 \mod (p-1)$. □

Corollary 8.2. *Assume the Kummer–Vandiver conjecture. Then we have $A_0^- \cong R_0^-/\mathfrak{s}_0^-$ as R_0-modules for $R_0 := \mathbb{Z}_p[G_{F_0/\mathbb{Q}}]$.*

Proof. By Kummer–Vandiver, p-rank$(e_iA) = 0$ for i even. Then by the above theorem (Theorem 8.1), p-rank$(A_j) \leq 1$; so, A_j is cyclic. Thus we have a surjective module homomorphism $e_jR_0 \twoheadrightarrow A_j$. We write the image of e_j in A_j as $\overline{e}_j$. $A_0^- = \bigoplus_{j:odd} e_jA = \sum_{j:odd} R_0\overline{e}_j = R_0(\sum_{j:odd} \overline{e}_j)$; so, A_0^- is cyclic. Since $\mathfrak{s}_0$ kills A_0^- and $|A_0^-| = [R_0^- : \mathfrak{s}_0^-]$ by Lemma 6.3, we conclude $A_0^- \cong R_0^-/\mathfrak{s}_0^-$. □

9. Proof of the cyclicity theorem

We first recall Nakayama's lemma: Let R be a local ring with a unique maximal ideal $\mathfrak{m}_R$ and M be finitely generated R-module.

Lemma 9.1 (NAK). *If $M = \mathfrak{m}_R M$, then $M = 0$.*

See [CRT, p.8] for a proof of this lemma This can be used as follows to determine the number of generators: Take a basis $\overline{m}_1, \ldots, \overline{m}_r$ of $M/\mathfrak{m}_R M$ over $R/\mathfrak{m}_R$ and lift it to $m_j \in M$ so that $(m_j \mod \mathfrak{m}_R) = \overline{m}_j$.

Corollary 9.2. *The elements $m_1, \ldots, m_j$ generate M over R, and r is the minimal number of generators.*

Proof. For the R-linear map $\pi : A^r \to M$ given by $(a_1, \ldots, ar) \mapsto \sum_j a_j m_j$, $\text{Coker}(\pi) \otimes_R R/\mathfrak{m}_R = 0$ as $\overline{m}_j$ generate $M \otimes_R R/\mathfrak{m}_R$. Thus $\text{Coker}(\pi) = 0$ by NAK; so, $m_1, \ldots, m_r$ generate M. □

We recall the cyclicity theorem:

Theorem 9.3 (Iwasawa). *Suppose $p \nmid h_0^+$. Then we have an isomorphism $A_n^- \cong R_n^-/\mathfrak{s}_n^-$ as R_n-modules and $A_n^+ = 0$.*

Proof. We have already proven the result when $n = 0$. Note that $R_0 = \prod_{i=0}^{p-1} e_i R_0$ and $e_i R_0 \cong \mathbb{Z}_p$ as a ring. Note that the restriction map $G_{F_{n'}/\mathbb{Q}} \ni \sigma \mapsto \sigma|_{F_n} \in G_{F_n/\mathbb{Q}}$ induces a surjective ring homomorphism $\pi^n_{n'} : R_{n'} \to R_n$ for $n' > n$. Take $\epsilon_i \in R_n$ projecting down to e_i. Since $e_i^2 = e_i$ (so, $e_i^j = e_i$), $\epsilon_i^2 \equiv \epsilon_i$. Since $(\pi^0_n)^{-1}(e_i R_0)$ is a p-profinite ring, $\lim_{j \to \infty} \epsilon_j^{p^j}$ converges to an idempotent, lifting e_j. We again wrote this lift as e_j; so, $R_n^- = \prod_{j=0,j:odd}^{p-1} e_j R_n$ as a ring direct product. Note that $G_{F_n/\mathbb{Q}} \cong (\mathbb{Z}/p^m\mathbb{Z})^\times = \mu_{p-1} \times \Gamma/\Gamma^{p^n}$ for $\Gamma = 1 + p\mathbb{Z}_p$ as $\mathbb{Z}_p{}^\times = \mu_{p-1} \times \Gamma$. Thus $R_n^- = R_0^- \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Gamma/\Gamma^{p^n}] = \prod_{j=0,j:odd}^{p-1} e_j R_0 \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$; so, $e_j R_n \cong \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$. Since Γ/Γ^{p^n} is a p-group, $\mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$ is a local ring with $\mathbb{Z}_p[\Gamma/\Gamma^{p^n}]/(\gamma - 1) \cong \mathbb{Z}_p$ as rings for the generator $\gamma = 1 + p$ of Γ.

To show cyclicity, we need to show that $M := e_i A_n^-$ is generated by one element over $\Lambda_n := \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$. This is equivalent to $M/\mathfrak{m}_n M \cong \mathbb{F}_p$ for the maximal ideal $\mathfrak{m}_n = (p, \gamma - 1) \subset \Lambda_n$ by Nakayama's lemma. Let L_n/F_n be the maximal p-abelian extension unramified everywhere. Let $X_n = G_{L_n/F_n}$. We have a following field diagram

$$\begin{tikzcd}
F_n \arrow[r] & L_0 F_n \arrow[r] & L_n \\
F_0 \arrow[r] \arrow[u] & L_0. \arrow[u] &
\end{tikzcd}$$

Since F_n/F_0 is fully ramified at p, F_n and L_0 is linearly disjoint. Thus

$$G_{L_n/F_0} = G_{F_n/F_0} \ltimes X_n$$

identifying G_{F_n/F_0} with the inertia subgroup at p of G_{L_n/F_0}. Therefore, $G_{L_0F_n/F_n} \cong G_{L_0/F_0}$, and we have an exact sequence

$$1 \to G_{L_n/L_0F_n} \to X_n \to X_0 \to 1.$$

Since X_0 is the maximal abelian quotient of G_{L_n/F_0}, G_{L_n/L_0F_0} is the commutator subgroup of G_{L_n/F_0}. Since $G_{L_n/F_0} = G_{F_n/F_0} \ltimes X_n$ and G_{F_n/F_0} is generated by γ, any element in G_{L_n/F_0} is of the form $\gamma^j x$ for $x \in X_n$ uniquely. Then the commutator subgroup is generated by $(\gamma, x) = x^{\gamma - 1} = (\gamma - 1)x$ for $x \in X_n$ since X_n is abelian. In other words, $G_{L_n/F_0} = (\gamma - 1)X_n$ written additively as Λ_n-module. This implies $e_i X_n/(\gamma - 1)e_i X_n \cong e_i X_0$ and hence $e_i X_n/\mathfrak{m}_n e_i X_n = e_i X_0/\mathfrak{m}_0 e_i X_0 \cong \mathbb{F}_p$. Thus by Nakayama's lemma, $e_i X_n$ is cyclic over Λ_n, and hence X_n is cyclic over R_n. In particular, if i is even, by Kummer–Vandiver, $e_i X_0 = 0$, and hence $e_i X_n = 0$. This implies $A_n^+ = 0$. Therefore $A_n^- \cong X_n = R_n^-/\mathfrak{a}_n$ for an ideal $\mathfrak{a}_n \supset \mathfrak{s}_n^-$.

We now prove $\mathfrak{a}_n = \mathfrak{s}_n$. By the lemma following this theorem Lemma 6.3, we have $[R_n^- : \mathfrak{s}_n^-] = |A_n^-| = |X_n| = [R_n : \mathfrak{a}_n]$, we conclude $\mathfrak{a}_n = \mathfrak{s}_n$. □

Remark 9.4. There is another proof of this theorem via the class number formula of F_n^+ we describe Section 13 with more input from Kummer theory. For the proof, see [ICF, §10.3].

10. Iwasawa theory

Let $R_\infty = \varprojlim_n R_n = \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mu_{p-1}]$ for $\Lambda = \varprojlim_n \Lambda_n = \varprojlim_n [\Gamma/\Gamma^{p^n}]$. Since Λ_n is a local ring with maximal ideal $\mathfrak{m}_{\Lambda_n} = (p, \gamma - 1)$, Λ is a local ring with unique maximal ideal $\mathfrak{m}_\Lambda = (p, \gamma - 1)$. Set $X = \varprojlim_n X_n$ for $X_n := G_{L_n/F_n} \cong A_n$, which is a R_∞-module.

Lemma 10.1. *Under the projection $G_{F_{n'}/\mathbb{Q}} \to G_{F_n/\mathbb{Q}}$ sending $\sigma \in G_{F_{n'}/\mathbb{Q}}$ to $\sigma|_{G_{F_n/\mathbb{Q}}}$, $\theta^-_{n'} \in \mathbb{Q}[G_{F_{n'}/\mathbb{Q}}]$ for $n' > n$ projects down to $\theta^-_n \in \mathbb{Q}[G_{F_n/\mathbb{Q}}]$.*

Proof. Define Hurwitz zeta function by

$$\zeta(s, x) = \sum_{n=0}^{\infty} \frac{1}{(x+n)^s} \ (\mathrm{Re}(s) > 1, 0 < x \leq 1).$$

This function can be analytically continued to $s \in \mathbb{C}$ and holomorphic outside $s = 1$ and known that $\zeta(1-n, x) = -\frac{B_n(x)}{n}$ $(0 < n \in \mathbb{Z})$ for the Bernoulli polynomial $B_n(x)$ (cf. [LFE, §2.3]). By definition,

$$f^{-s}\zeta(s, \frac{a}{f}) = \sum_{n \equiv a \mod f, n>0}^{\infty} \frac{1}{n^s}.$$

Thus

$$\mathbb{C}[(\mathbb{Z}/p^{m'}\mathbb{Z})^\times] \ni \sum_{a \in (\mathbb{Z}/p^{m'}\mathbb{Z})^\times} p^{-m's}\zeta(s, \frac{a}{p^{m'}})\sigma_a^{-1} \mapsto \sum_{a \in (\mathbb{Z}/p^{m}\mathbb{Z})^\times} p^{-ms}\zeta(s, \frac{a}{p^{m}})\sigma_a^{-1} \in \mathbb{C}[(\mathbb{Z}/p^m\mathbb{Z})^\times]$$

under the reduction map modulo p^m (here $m = n + 1$ and $m' = n' + 1$). Note that $B_1(x) = x - \frac{1}{2}$, and hence, taking $s = 0$, $\sum_{a=1,(a,p)=1}^{p^m} B_1(a/p^m)\sigma_a^{-1} = \theta^-_n$ by (6.1). □

Since $a - \sigma_a \in \mathbb{Z}_p[G_{F_n/\mathbb{Q}}] = R_n$ for $a \in \mathbb{Z}_p{}^\times$ also gives compatible system with respect to the projective system $R_\infty = \varprojlim_n R_n$, we have $(a - \sigma_a)\theta^-_\infty := \varprojlim_n (a - \sigma_a)\theta^-_n$. Then we get an idempotent $e_j \in \mathbb{Z}_p[\mu_{p-1}] \subset R_\infty$. Since we can choose a as above such that $a - \omega^j(a) \in \mathbb{Z}_p{}^\times$ if $j \neq 1$ $(0 < j < p - 1)$, $e_j(a - \sigma_a) \in (e_j R_\infty)^\times$. Thus we have $L_j := e_j\theta^-_\infty \in \Lambda$ for odd j, and hence $e_j\mathfrak{s}^-_n$ is generated by $e_j\theta^-_n$ for all odd $1 < j < p-1$, and hence $\mathfrak{s}^{(j)}_\infty = e_j\mathfrak{s}^-_\infty = \varprojlim_n e_j\mathfrak{s}^-_n = (L_j) \subset \Lambda$. Put $X^{(j)} = e_jX$. Since we know that $e_1A^-_n = 0$ for all n, we find $X^{(1)} = 0$. The following is the consequence of the cyclicity theorem (see [I69]).

Theorem 10.2 (Iwasawa). *Suppose $3 \leq j < p - 1$ be an odd integer. If $p \nmid |Cl^+_n|$, then*

$$X^{(j)} \cong \Lambda/\mathfrak{s}^{(j)}_\infty = \Lambda/(L_j)$$

as Λ-modules. In particular $X^{(j)}_n = e_jX_n = X^{(j)}/(\gamma^{p^n} - 1)X^{(j)} \cong \Lambda/(L_j, \gamma^{p^n} - 1)$.

Recall $\gamma := \sigma_{1+p} \in G_{F_\infty/F_0}$. Since $\mathbb{Z}_p$-module Γ satisfies $\Gamma/\Gamma^p \cong \mathbb{F}_p$, by Nakayama's lemma, Γ is generated by γ over $\mathbb{Z}_p$. Thus $\Gamma = \{(1+p)^s = \sum_{n=0}^{\infty} \binom{n}{s} X^n | s \in \mathbb{Z}_p\}$, and γ is a topological generator of the group Γ.

Lemma 10.3. *We have $\Lambda \cong \mathbb{Z}_p[[T]]$ by sending γ to $t := 1 + T$, where $\mathbb{Z}_p[[T]]$ is the one variable power series ring.*

Proof. We have $\Lambda = \varprojlim_n \mathbb{Z}_p[G_{F_n/F_0}] \cong \varprojlim_n \mathbb{Z}_p[t]/(t^{p^n}-1)$ as $G_{F_n/F_0} = \Gamma/\Gamma^{p^n}$ is a cyclic group of order p^n generated by $\gamma = \sigma_{1+p}$.

Inside $\mathbb{Z}_p[[T]]$, $t^{p^n}-1 = \prod_j \Phi_j(t)$ for the minimal polynomial $\Phi_j(t)$ of p^j-th roots of unity. Since $|\alpha_n|_p < 1$ for $\alpha_n := \zeta_{p^n}-1$, any power series $f(T) \in \mathbb{Z}_p[[T]]$ converges at α_n; so, $f(t) \mapsto f(\alpha_n)$ gives a onto algebra homomorphism $\mathbb{Z}_p[[T]] \to \mathbb{Z}_p[\mu_{p^n}]$ whose kernel is generated by $\Phi_n(t)$.

Thus $(\Phi_n(t)) \subset \mathfrak{m}_\Lambda$; so,

$$\bigcap_n (t^{p^n}-1) = \bigcap_n (\Phi_1 \cdots \Phi_n) \subset \bigcap_n \mathfrak{m}_\Lambda^n = (0).$$

This shows the desired result. □

For each character $\chi : G_{F_\infty/\mathbb{Q}} \cong \mathbb{Z}_p{}^\times \to \overline{\mathbb{Q}}_p^\times$ with $\chi|_{\mu_{p-1}} = \omega^{-j}$ for $\mu_{p-1} \subset \mathbb{Z}_p{}^\times$ factoring through $G_{F_n/\mathbb{Q}}$, we have $\chi(L_j) = \chi(e_j\theta_n) = L(0,\chi)$. Since $\chi(T) = \chi(t)-1 = \chi(\gamma)-1$ with $|\chi(\gamma)-1|_p < 1$ as $\chi(\gamma) \in \mu_{p^\infty} = \bigcup_j \mu_{p^j}$, we find $\chi(L_j) = L_j(\chi(\gamma)-1)$ regarding L_j as a power series $L_j(T) \in \mathbb{Z}_p[[T]]$. Actually we can show that $L_j((1+p)^k-1) = (1-p^{k-1})\zeta(1-k)$ for all integers $k \equiv j+1 \mod (p-1)$ (see [ICF, Theorem 5.11] or [LFE, §3.5 and §4.4]). The p-adic analytic function $\mathbb{Z}_p \ni s \mapsto L_j((1+p)^s-1) \in \mathbb{Z}_p$ is called the Kubota–Leopoldt p-adic L-function.

Here is a general theory of Λ-modules (see [ICF, §13.2]). If M is finitely generated torsion Λ-module, then there exists finitely many non-zero elements $f_j \in \Lambda$ $(j = 1, 2, \dots, r)$ and a Λ-linear map $i : M \to \bigoplus_{j=1}^r \Lambda/(f_j)$ such that $|\ker(i)| < \infty$ and $|\operatorname{Coker}(i)| < \infty$ (i.e., i is a pseudo isomorphism). Moreover the set of ideals $(f_1), \dots, (f_r)$ is independent of the choice of i, and the ideal $\operatorname{char}(M) := (\prod_j f_j))$ is called the characteristic ideal of M. It is easy to see that $X^{(j)}$ is a torsion Λ-module of finite type as $X_1^{(j)} = X^{(j)}/(\gamma-1)X^{(j)} \subset Cl_1^-$ is finite. Iwasawa conjectured that $\operatorname{char}(X^{(j)}) = (L_j)$ in general for odd j, and it was first proven by Mazur–Wiles in 1984 [MW] and there is another more elementary proof by Rubin (see [ICF, §15.7]). But the above theorem tells more that $X^{(j)}$ for odd j is cyclic over Λ, and Iwasawa conjectured also that $r \le 1$ (pseudo-cyclicity conjecture), which is not known yet. Iwasawa himself seems to have had a belief not just $r = 1$ but the cyclicity without finite error (see [U3, C.1]).

11. An asymptotic formula of $|A_n^-|$

We would like to prove the following theorem of Iwasawa:

Theorem 11.1. *There exist integer constants λ, μ, ν such that*

$$|A_n^-| = p^{\lambda n + \mu p^n + \nu}$$

for all n sufficiently large.

There is another theorem by Ferrero–Washington [FW] (see also [S]) which was conjectured by Iwasawa when he proved the above theorem:

Theorem 11.2. *We have $\mu = 0$.*

In this section, we prove Theorem 11.1 under the Kummer–Vandiver conjecture. A polynomial $P(T)$ in $\mathbb{Z}_p[T]$ is called *distinguished* if $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ with $p|a_i$ for all i. We first quote Weierstrass' preparation theorem in our p-adic setting:

Theorem 11.3 (Weierstrass preparation theorem)**.** *Let $f(T) = \sum_{i=0}^{\infty} a_i T^i \in \mathbb{Z}_p[[T]]$, and suppose $(f(T) \mod p\mathbb{Z}_p[[T]]) = \sum_{i\geq n} \overline{a}_i T^i \in \mathbb{F}_p[[T]]$ with $\overline{a}_n \neq 0$. Then there exists a distinguished polynomial $P(T)$ of degree n and a unit $U(T) \in \mathbb{Z}_p[[T]]$ such that $f(T) = P(T)U(T)$. More generally, for any non-zero $f(T) \in \mathbb{Z}_p[[T]]$, we can find an integer $\mu \geq 0$ and a distinguished polynomial $P(T)$ and a unit such that $f(T) = p^{\mu}P(T)U(T)$. The triple $P(T), \mu, U(T)$ is uniquely determined by $f(T)$.*

Once the first assertion is proven, $P(T) = \prod_{\alpha}(T-\alpha)$ for zeros $\alpha \in \overline{\mathbb{Q}}_p$ with $|\alpha|_p < 0$; so, the decomposition is unique. In other words, $\mathrm{Spec}(\lambda)(\overline{\mathbb{Q}}_p) \cong \{\alpha \in \overline{\mathbb{Q}}_p : |\alpha|_p < 1\}$ (the open unit disk) which contains a "natural" $\mathbb{Z}_p$-line $p\mathbb{Z}_p$. Before proving this theorem, we state a division algorithm for Λ:

Proposition 11.4 (Euclidean algorithm)**.** *Let $f(T) = \sum_{i=0}^{\infty} a_i T^i \in \mathbb{Z}_p[[T]]$, and suppose $(f(T) \mod p\mathbb{Z}_p[[T]]) = \sum_{i\geq n} \overline{a}_i T^i \in \mathbb{F}_p[[T]]$ with $\overline{a}_n \neq 0$. Suppose that the index n is the minimal with $\overline{a}_n \neq 0$. For each $g(T) \in \Lambda$, there exists a pair $(q(T), r(T))$ with $q(T) \in \Lambda$ and $r(T) \in \mathbb{Z}_p[T]$ (a polynomial) such that* $\deg(r(T)) < n$ *and* $g(T) = q(T)f(T) + r(T)$.

Proof. If $g = 0$, we have $qf + r = 0$. Since $\overline{f}$ has leading term $\overline{a}_n T^n$, we find $\overline{r} = 0$. Thus $\overline{q}\overline{f} = 0$; so, $\overline{q} = 0$. Dividing by p and repeating this argument, we find $q \equiv r \equiv 0 \mod p^j$ for all $j > 0$; so, $q = r = 0$. This shows the uniqueness of (q, r) for $g \neq 0$.

Define $R : \Lambda \to \Lambda$ removing first n terms and dividing by T^n; so, $R(\sum_{j=0}^{\infty} a_j T^j) = \sum_{j=n}^{\infty} a_j T^{j-n}$. We put $A := \mathrm{Id} - T^n R$; so, A projects a power series to the first n-term up to degree $n-1$. Thus we have

(1) $R(T^n h(T)) = h(T)$;
(2) $R(h) = 0 \Leftrightarrow h$ is a polynomial of degree $< n$.

Since $R(f)^{-1} = a_n^{-1}(1 + T\phi(T))^{-1} = a_n^{-1}\sum_{j=0}^{\infty}(-1)^j T^j \phi(T)^j \in \Lambda$ for $\phi(T) \in \mathbb{Z}_p[[T]]$, we have $R(f) \in \Lambda^{\times}$.

We like to solve $g = qf + r$. This is to solve $R(g) = R(qf)$ by (2) above. Note that $f = A(f) + T^n R(f)$; so, we need to solve

$$R(g) = R(qA(f)) + R(qT^n R(f)) = R(qA(f)) + qR(f)$$

by (1) above. Write $X = qR(f)$. Then the above equation becomes

$$R(g) = R(X\frac{A(f)}{R(f)}) + X = (\mathrm{id} + R \circ \frac{A(f)}{R(f)})(X).$$

We need to solve this equation of X. As a linear map, $R \circ \frac{A(f)}{R(f)}$ has values in $\mathfrak{m}_\Lambda$ as $A(f)$ is divisible by p. Thus the map $\mathrm{id} + R \circ \frac{A(f)}{R(f)} : X \mapsto X + R(X\frac{A(f)}{R(f)})$ is invertible with inverse given by

$$(\mathrm{id} + R \circ \frac{A(f)}{R(f)})^{-1} = \sum_{j=0}^{\infty}(-R \circ \frac{A(f)}{R(f)})^j.$$

In particular, $X = (\mathrm{id} + R \circ \frac{A(f)}{R(f)})^{-1}(R(g))$, and hence $q = XR(f)^{-1}$ and $r = g - qf$. □

Once an Euclidean algorithm is known, it is a standard to have a unique factorization theorem from the time of Euclid:

Corollary 11.5. *The ring Λ is a unique factorization domain.*

Proof of Weierstrass theorem: Dividing $f(T)$ by p^μ for $\mu = \min_j v(a_j)$ for the p-adic valuation v, we may assume that $\overline{a}_n \neq 0$ for n as above. Therefore we only prove the first part. Apply Euclidean algorithm above to $g = T^n$, we get $T^n = qf + r$ with a polynomial r of degree $< n$. Writing $q(T) = \sum_{j=0}^{\infty} c_n T^n$ and comparing the coefficient of T^n, we get $1 \equiv c_0 a_n \mod \mathfrak{m}_\Lambda$; so, $c_0 \in \mathbb{Z}_p{}^\times$; so, $f = q^{-1}(T^n - r)$. Thus $U(T) := q^{-1}$ and $P(T) := T^n - r$ satisfies the property of the preparation theorem. □

Lemma 11.6. *If $E = \Lambda/p^\mu\Lambda$, then $|E/(\gamma^{p^n} - 1)E| = p^{\mu p^n}$.*

Proof. Since $E = \Lambda/p^\mu\Lambda = (\mathbb{Z}/p^\mu\mathbb{Z})[[T]]$, from $(\mathbb{Z}/p^\mu\mathbb{Z})[[T]]/(\gamma^{p^n} - 1)(\mathbb{Z}/p^\mu\mathbb{Z})[[T]] \cong (\mathbb{Z}/p^\mu\mathbb{Z})[[T]][\Gamma/\Gamma^{p^n}]$, we conclude the desired assertion. □

Lemma 11.7. *If $E = \Lambda/g(T)\Lambda$ for a distinguished polynomial of degree λ with $g(\zeta - 1) \neq 0$ for all $\zeta \in \mu_{p^\infty}$, then there exists an integer $n_0 > 0$ and a constaint $\nu \in \mathbb{Z}$ such that $|E/(\gamma^{p^n} - 1)E| = p^{\lambda n + \nu}$ for all $n > n_0$.*

Proof. A monic polynomial $f(T) \in \mathbb{Z}_p[T]$ is distinguished if and only if $f(T) \equiv T^\lambda \mathrm{mod}\ p$; so, a product and a factor of distinguished polynomials are distinguished.

We put $N_{n,n'} := \frac{\gamma^{p^n} - 1}{\gamma^{p^{n'}} - 1} = \sum_{j=0}^{p^n - p^{n'}} \gamma^{jp^{n'}}$ for $n > n'$. Writing $g(T) = T^\lambda - pQ(T)$ with $Q(T) \in \mathbb{Z}_p[T]$, we have $T^\lambda \equiv pQ(T) \mod g$; so, $T^k \equiv pQ_k(T) \mod g$ for all $k \geq \lambda$ with some polynomial $Q_k(T) \in \mathbb{Z}_p[T]$. Therefore if $p^n > \lambda$,

$$\gamma^{p^n} = (1+T)^{p^n} = 1 + pR(T) + T^{p^n} \equiv 1 + pS_n(T) \mod g(T)$$

for $R(T), S_n(T) \in \mathbb{Z}_p[T]$. Thus

$$(1+T)^{p^{n+1}} \equiv (1 + pS_n(T))^p \equiv 1 + p^2 S'_n(T) \mod g(T).$$

Thus we find

$$\gamma^{p^{n+2}} - 1 = (\gamma^{p^{n+1}})^p - 1 = (\gamma^{p^{n+1}} - 1)(1 + \gamma^{p^{n+1}} + \cdots + \gamma^{(p-1)p^{n+1}})$$
$$\equiv (\overbrace{1 + \cdots + 1}^{p} + p^2 P(T))(\gamma^{p^{n+1}} - 1) \mod g(T) = p(1 + pP(T))(\gamma^{p^{n+1}} - 1),$$

where $P(T) \in \mathbb{Z}_p[T]$. Since $(1 + pP(T))^{-1} = \sum_{j=0}^{\infty}(-pP(T))^j \in \Lambda$, $1 + pP(T)$ is a unit in Λ. Therefore multiplication by $N_{n+2,n+1} = \frac{\gamma^{p^{n+2}} - 1}{\gamma^{p^{n+1}} - 1}$ is equal to multiplication by p on E as long as E is $\mathbb{Z}_p$-free of rank λ; so, we find $|E/pE| = p^\lambda$. Thus if $p^{n_0} > \lambda$ and $n \geq n_0$, we get the desired formula. □

Since $X^{(j)} = \Lambda/(L_j)$ for j odd with $j > 1$, by the above two lemmas, we get Theorem 11.1 for $\lambda = \sum_{1<j<p-1,odd} \lambda_j$ and $\mu = \sum_{1<j<p-1,j:odd} \mu_j$, where $L_j = p^{\mu_j} D_j(T) U_j(T)$ with distinguished polynomial D_j of degree λ_j and units $U_j(T)$.

Remark 11.8. Actually for any $\mathbb{Z}_p$-extension $K_{\infty/K} = \bigcup_n K_{n/K}$ (i.e., $G_{K_\infty/K} \cong \mathbb{Z}_p$ and $G_{K_\infty/K_n} \cong p^n\mathbb{Z}_p$) for a number field K, writing the p-primary part of the class number of $K_n = K_\infty^{p^n\mathbb{Z}_p}$ as p^{e_n}, it is known that $e_n = ln + mp^n + c$ for constants l, m, c if n is sufficiently large (see [ICF, Theorem 13.3]).

If $\mathcal{X}$ is a smooth projective curve over the finite field $\mathbb{F}_p$, we can think of the extension $\overline{\mathbb{F}}_p(\mathcal{X})/\mathbb{F}_p(\mathcal{X})$ of the function fields, where $\overline{\mathbb{F}}_p$ is a fixed algebraic closure of $\mathbb{F}_p$. Then $\mathrm{Gal}(\overline{\mathbb{F}}_p(\mathcal{X})/\mathbb{F}_p(\mathcal{X})) \cong \widehat{\mathbb{Z}} = \mathrm{Frob}_p^{\widehat{\mathbb{Z}}}$. Put $X = \mathrm{Gal}(L/\overline{\mathbb{F}}_p(\mathcal{X}))$ for the maximal abelian extension unramified everywhere $L/\overline{\mathbb{F}}_p(\mathcal{X})$. Then $\mathrm{Gal}(\overline{\mathbb{F}}_p(\mathcal{X})/\mathbb{F}_p(\mathcal{X}))$ acts on X by conjugation. Let $\mathcal{J}_{/\mathbb{F}_p}$ be the Jacobian variety of $\mathcal{X}$ (i.e., degree 0 divisors modulo principal divisors). Then $X = \prod_l T_l\mathcal{J}$ for the Tate module $T_l\mathcal{J} = \varprojlim_n \mathcal{J}[l^n]$ for primes l. In particular, $T_l\mathcal{J} \cong \mathbb{Z}_l^{2g}$ for the genus g of $\mathcal{X}$ if $l \neq p$. If $l = p$, then $T_p\mathcal{J} \cong \mathbb{Z}_p{}^r$ for $0 \leq r \leq g$ called the p-rank of $\mathcal{X}$. The Frobenius has reciprocal characteristic polynomial $\det(1_{2g} - \mathrm{Frob}_p|_{T_l\mathcal{J}}x) = \phi(x) \in \mathbb{Z}[x]$ independent of $l \neq p$. Then (the main part of) the zeta function of $\mathcal{X}$ is given by $L(s, \mathcal{X}) = \phi(p^{-s})$. For an eigenvalue α of Frob_p on $T_l\mathcal{J}$, Weil proved that $|\alpha| = \sqrt{p}$. Thus by definition, $L(s, \mathcal{X}) = 0 \Leftrightarrow p^{-s} = \alpha$ for an eigenvalue α. This implies $\mathrm{Re}(s) = \frac{1}{2}$ (Riemann hypothesis for $\mathcal{X}$).

In Iwasawa's case, for the maximal p-abelian extension L/F_∞ unramified everywhere, $X := \mathrm{Gal}(L/F_\infty)$ is a module over $\Gamma := \mathrm{Gal}(F_\infty/F_0) = \gamma^{\mathbb{Z}_p}$. By $\mu = 0$, X is $\mathbb{Z}_p$-free (under the Kummer–Vandiver conjecture). We have an isomorphism of Λ-modules $X \cong \bigoplus_{0<j<p-1, j\neq 1, j:odd} \Lambda/(L_j)$. Write $X_j := e_jX = \Lambda/(L_j)$ and $L_j(T) = P_j(T)U_j(T)$ for $U_j \in \Lambda^\times$ and a distinguished polynomial $P_j(T)$. Regard $P_j(T)$ as a polynomial of $t = 1+T$ and write $P_j(t)$. Since $X_j \cong \Lambda/(P_j(t))$, the action of γ on X_j satisfies $P_j(\gamma) = 0$; so, $P_j(t) = \det(t - \gamma|_{X_j})$. Perhaps an analogue of the Riemann hypothesis is to believe that $P_j(t)$ factors into a product of linear polynomials in $\mathbb{Z}_p[T]$ as $\{z \in \mathbb{Z}_{p_p} : |z|_p < 1\}$ is a line in $D = \{z \in \overline{\mathbb{Q}}_p : |z|_p < 1\}$. This is something which Iwasawa seems to have believed to be true (see [U3, C.6]).

12. Cyclotomic units

We now prepare some facts for determining $|Cl_n^+|$ as an index of the cyclotomic units in the entire units in O_n^+. This is a base of the proof of the cyclicity theorem in [ICF, §10.3] a bit different from our proof in Section 9. For a number field, if $F \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$, we know $\mathrm{rank}_{\mathbb{Z}}\, O^\times = \dim_{\mathbb{Q}} O^\times \otimes_{\mathbb{Z}} \mathbb{Q} = r + s - 1$. Since $F_n \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{C}^{(p^{n+1}-p^n)/2}$, we find $\mathrm{rank}\, O_n^\times = (p^{n+1} - p^n)/2 - 1$ for the integer ring O_n of F_n. Let V_n be the multiplicative group generated by $\mu_{p^{n+1}} \cup \{1 - \zeta_{p^{n+1}}^a | 1 < a \leq p^{n+1} - 1\}$. Put $C_n := O_n^\times \cap V_n$. A unit in C_n is called a *cyclotomic unit.*

Lemma 12.1. (1) *$C_n^+ := C_n \cap F_n^+$ is generated by -1 and the units*

$$\xi_a := \zeta_{p^{n+1}}^{(1-a)/2} \frac{1 - \zeta_{p^{n+1}}^a}{1 - \zeta_{p^{n+1}}} \quad \textit{with} \quad 1 < a < p^{n+1}/2 \textit{ and } (a, p) = 1;$$

(2) *we have $C_n = C_n^+ \mu_{p^{n+1}}$.*

Proof. Let $m = n + 1$, and write $\zeta := \zeta_{p^m}$. Note that

$$\xi_a = \zeta^{(1-a)/2}\frac{1-\zeta^a}{1-\zeta} = \frac{\zeta^{-a/2}-\zeta^{a/2}}{\zeta^{-1/2}-\zeta^{1/2}} = \pm\frac{\sin(\pi a/p^m)}{\sin(\pi/p^m)}.$$

Since $\zeta^{1/2} = -\zeta_{p^m}$ as p is odd, $\xi_a \in F_m^+$. Note that $(1-\zeta) = \mathfrak{p} = \mathfrak{p}^{\sigma_a} = (1-\zeta^a)$ for the unique prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\mu_{p^m}]$ above p, we find $(\xi_a) = O_m$, and hence $\xi_a \in (O_m^+)^\times$. Thus the assertion (2) implies (1).

We now prove (2). Note that $\zeta^{p^{m-k}}$ generates μ_{p^k}; so, we have for $0 \le k < m$

$$1 - X^{p^k} = \prod_{j=0}^{p^k-1}(1-\zeta^{jp^{m-k}}X).$$

Thus making $X = \zeta^b$ for $0 < b \in \mathbb{Z}$ prime to p, we have

$$1 - \zeta^{bp^k} = \prod_{j=0}^{p^k-1}(1-\zeta^{b+jp^{m-k}}).$$

Since $(1-\zeta^{-a}) = -\zeta^{-a}(1-\zeta^a)$, to show (2), we only need to consider $(1-\zeta^a)$ for $1 \le a < p^m/2$ prime to p.

Suppose that $\xi := \pm\zeta^d\prod_{1<a<p^m/2,(a,p)=1}(1-\zeta^a)^{e_a} \in O_m^\times$. Since $\mathfrak{p} = (1-\zeta) = \mathfrak{p}^{\sigma_a} = (1-\zeta^a)$, we have $(\xi) = \mathfrak{p}^{\sum_a e_a}$; therefore $\sum_a e_a = 0$, which implies $\prod_a(1-\zeta^a)^{e_a} = 1$, and hence

$$\xi = \pm\zeta^d\prod_a\frac{(1-\zeta^a)^{e_a}}{(1-\zeta)^{e_a}} = \pm\zeta^f\prod_a\xi_a$$

with $f = d + \sum_a e_a(a-1)/2$. This shows (2). □

13. Class number formula for F_n^+

Generally, take a number field F with integer ring O. Identify $F \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$ as semi-simple algebras, and write $\sigma_1, \ldots, \sigma_{r+s}$ be the projection of F into each simple factor of $F \otimes_{\mathbb{Q}} \mathbb{R}$ so that $\sigma_1, \ldots, \sigma_r$ having values in $\mathbb{R}$. We write the corresponding simple factor as F_{σ_i}. By Dirichlet's unit theorem, $O^\times$ has rank $R := r + s - 1$; so, it has $r + s - 1$ independent units $\varepsilon_1, \ldots, \varepsilon_R$. By the proof of Dirichlet's unit theorem, $R_F(\varepsilon_1, \ldots, \varepsilon_R) := \det(\log|\varepsilon_i^{\sigma_j}|^{d_i})_{1\le i,j\le R}$ is non-zero real number called the regulator of $\{\varepsilon_1, \ldots, \varepsilon_R\}$. Here $d_i = \dim_{\mathbb{R}} F_{\sigma_i}$ (so, $d_i = 1, 2$ according as F_{σ_i} is real or complex embedding). If $\{\varepsilon_1, \ldots, \varepsilon_R\}$ span the maximal free quotient of $O^\times$, $R_F(\varepsilon_1, \ldots, \varepsilon_R)$ is independent of the choice of the basis $R_F(\varepsilon_1, \ldots, \varepsilon_R)$ and is just written as R_F (and is called the *regulator* of F).

Let $\zeta_F(s) := \sum_{\mathfrak{n}} N(\mathfrak{n})^{-s} = \prod_{\mathfrak{l}}(1 - N(\mathfrak{l})^{-s})^{-1}$ be the Dedekind zeta function of F, where $\mathfrak{n}$ (resp. $\mathfrak{l}$) runs over all non-zero (resp. prime) O-ideals and $N(\mathfrak{n}) = |O/\mathfrak{n}|$. The sum converges absolutely and locally uniformly if $\mathrm{Re}(s) > 1$. By Hecke, this zeta function is continued meromorphically to the whole complex plane having an only simple pole at $s = 1$ (e.g., [LFE, §2.7] and [CFT, V.2]). So $\lim_{s\to+1}(s-1)\zeta_F(s)$ exists which was proven by Dedekind earlier than Hecke. Here is his limit formula (e.g., [CFT, V.2.2]):

Theorem 13.1 (R. Dedekind). *We have*

$$\mathrm{Res}_{s=1}\zeta_F(s) = \lim_{s\to+1}(s-1)\zeta_F(s) = \frac{2^r(2\pi)^s|Cl_F|R_F}{w\sqrt{|D_F|}},$$

where w is the number of roots of unity in F and D_F is the discriminant of F.

Theorem 13.2 (Dirichlet/Hecke). *The L-functions $L(s,\chi)$ and $\zeta_F(s)$ can be continued analytically to $\mathbb{C}-\{1\}$ and satisfies*

$$\Lambda_F(s)\zeta_F(s) = \Lambda_F(1-s)\zeta_F(s) \quad \textit{and}\ \Lambda_\chi(s)L(s,\chi) = \varepsilon_\chi\Lambda_\chi(1-s)L(1-s,\chi^{-1}),$$

where $\Lambda_F(s) = A^s\Gamma(\frac{s}{2})^r\Gamma(s)^s$ with $A = 2^{-s}\pi^{-[F:\mathbb{Q}]/2}\sqrt{|D_F|}$, $\varepsilon_\chi = \frac{-G(\chi)}{\sqrt{\chi(-1)f}}$ for the conductor f of χ and $\Lambda_\chi(s) = (f/\pi)^{s/2}\Gamma(\frac{s+\delta}{2})$ with $\delta = \frac{1-\chi(-1)}{2}$. If $\chi \neq \mathbf{1}$, $L(s,\chi)$ is holomorphic everywhere on $\mathbb{C}$.

Since $\mathrm{Res}_{s=1}\zeta(s) = 1$, we get

Corollary 13.3. *We have*

$$\lim_{s\to+1}\frac{\zeta_F(s)}{\zeta(s)} = \frac{2^r(2\pi)^s|Cl_F|R_F}{w\sqrt{|D_F|}}.$$

Lemma 13.4. *Let $\{\eta_1,\dots,\eta_R\}$ be a basis of a subgroup E of $O^\times$ modulo torsion. Then we have*

$$\frac{R_F}{R_F(\eta_1,\dots,\eta_R)} = [O^\times/\mathit{torsion} : E].$$

This is because $R_F(\eta_1,\dots,\eta_R)$ is the volume of the lattice spanned by $\mathrm{Log}(\eta) = (\log|\eta^{\sigma_j}|^{d_i})_i$ in the subspace $\{x \in F | \mathrm{Tr}_{F/\mathbb{Q}}(x) = 0\} \otimes_{\mathbb{Q}} \mathbb{R}$ of the real vector space $F \otimes_{\mathbb{Q}} \mathbb{R}$. See [ICF, Lemma 4.15] for more details.

Suppose now that $F = F_n^+$ with $m = n+1$ for $n \geq 0$. We now quote from [ICF, Theorem 4.9]:

Theorem 13.5 (Dirichlet–Kummer). *For a primitive character $\chi : (\mathbb{Z}/p^m\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$ with $\chi(-1) = 1$, we have*

$$L(1,\chi) = -\frac{\tau(\chi)}{p^m}\sum_{a=1}^{p^m}\overline{\chi}(a)\log|1-\zeta_{p^m}^a|.$$

The Galois group $G_{F/\mathbb{Q}} \cong (\mathbb{Z}/p^m\mathbb{Z})^\times/\{\pm1\}$ acts on F, and hence $F = \mathbb{Q} \oplus \mathrm{Ker}(\mathrm{Tr}_{F/\mathbb{Q}})$ as a Galois module. Let ρ be the representation of $G_{F/\mathbb{Q}}$ on $\mathrm{Ker}(\mathrm{Tr}_{F/\mathbb{Q}})$. By a normal basis theorem of Galois theory, we have $F \cong \mathbb{Q}[G_{F/\mathbb{Q}}] \cong \mathbb{Q}[(\mathbb{Z}/p^m\mathbb{Z})^\times]$ as Galois modules; so, $F \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong \bigoplus_\chi \chi$, where χ runs over all characters of $(\mathbb{Z}/p^m\mathbb{Z})^\times$ with $\chi(-1) = 1$. Thus shows $\rho \cong \bigoplus_{\chi\neq\mathbf{1}}\chi$. Then we have

Lemma 13.6. *We have $\zeta_{F_n^+}(s) = \zeta(s)L(s,\rho) = \zeta(s)\prod_{\chi\neq\mathbf{1},\chi(-1)=1}L(s,\chi)$, where χ runs over all characters of $(\mathbb{Z}/p^m\mathbb{Z})^\times/\{\pm1\}$ and $L(s,\chi)$ is the Dirichlet L-function of a character $\chi : (\mathbb{Z}/p^m\mathbb{Z})^\times/\{\pm1\} \to \overline{\mathbb{Q}}^\times$.*

Proof. Let $0 < l \neq p$ be a prime. Then $(l) = \prod_{j=1}^{g} \mathfrak{l}_j$ for primes $\mathfrak{l}_j$ in F, where g is the index of the subgroup D_l of $(\mathbb{Z}/p^m\mathbb{Z})^\times$ generated by l (see Lemma 1.1). Then writing $f = |D_l|$, we have $gf = [F:\mathbb{Q}]$. Note that

$$(1 - N(\mathfrak{l}_j)^{-s}) = (1 - l^{-fs}) = \prod_{\zeta \in \mu_f} (1 - \zeta l^{-s}) = \prod_{\chi} (1 - \chi(l) l^{-s}),$$

where χ runs over all characters of D_l. The restriction map $\mathrm{Hom}((\mathbb{Z}/p^m\mathbb{Z})^\times, \overline{\mathbb{Q}}^\times) \to \mathrm{Hom}(D_l, \overline{\mathbb{Q}}^\times)$ has fiber containing g elements, we get the desired formula by Euler factorization of ζ_F. □

Corollary 13.7. *For $F = F_n^+$, we have*

$$\prod_{\chi \neq \mathbf{1}} L(1,\chi) = \frac{2^{[F:\mathbb{Q}]} |Cl_F| R_F}{w\sqrt{|D_F|}},$$

where χ runs over all non-trivial characters of $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ with $\chi(-1) = 1$. In addition, we have

$$\prod_{\chi \neq \mathbf{1}} \varepsilon_\chi = 1 \quad \text{and} \quad \prod_{\chi \neq \mathbf{1}} (-G(\chi)) = \sqrt{|D_F|}. \tag{13.1}$$

This follows from Lemma 13.6 and the functional equation of Theorem 13.2 via the formula $\Gamma(\frac{s}{2})\Gamma(\frac{s+1}{2}) = 2^{1-s}\sqrt{\pi}\Gamma(s)$.

Exercise 13.8. *For a general field F not necessarily abelian over $\mathbb{Q}$, we write the Galois representation on $V := \mathrm{Ker}(\mathrm{Tr}_{F/\mathbb{Q}}) \subset F$ as ρ and define*

$$L(s,\rho) = \prod_{l} \det(1 - \rho|_{V^{I_l}}(\mathrm{Frob}_l) l^{-s})^{-1} \text{ (Artin L-finction of } \rho).$$

Prove that $\zeta_F(s) = \zeta(s) L(s,\rho)$.

Lemma 13.9. *Let G be a finite abelian group, and let $f : G \to \mathbb{C}$ be a function. Then*

1. $\det(f(\tau\sigma^{-1}))_{\sigma,\tau \in G} = \det(f(\sigma\tau))_{\sigma,\tau \in G} = \prod_{\chi \in \mathrm{Hom}(G,\mathbb{C}^\times)} \sum_{\sigma \in G} \chi(\sigma) f(\sigma)$*;*
2. $\det(f(\tau\sigma^{-1}) - f(\tau))_{\sigma,\tau \neq 1} = \det(f(\sigma\tau) - f(\tau))_{\sigma,\tau \neq 1} = \prod_{\chi \neq \mathbf{1}} \sum_{\sigma \in G} \chi(\sigma) f(\sigma)$.

A proof of this lemma will be given after proving the following theorem:

Theorem 13.10. *Let $F = F_n^+$. Then we have $|Cl^+_{F_n}| = [(O_n^+)^\times : C_n^+]$, and $\{\xi_a\}_{1 \le a < p^m/2, p \nmid a}$ is a set of independent units giving a basis of $(O_n^+)^\times \otimes_{\mathbb{Z}} \mathbb{Q}$.*

Iwasawa seemes to have believed $A_0^+ \cong ((O_0^+)^\times / C_0^+) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ as Galois modules (this follows from $A_0^+ \cong R_0^- / \mathfrak{s}_0^-$; see the statement below [U3, C.1]).

Proof. Let $\{\xi_a\}_{1 < a < p^m/2, (a,p)=1}$ be the generators of C_n^+ in Lemma 12.1. Note that

$$\xi_a = \frac{(\zeta^{-1/2}(1-\zeta))^{\sigma_a}}{\zeta^{-1/2}(1-\zeta)}.$$

Note that $|\{\xi_a\}| = [F : \mathbb{Q}] - 1$ for $F = F_n^+$. Thus we can think of the regulator $R_C := R_F(\{\xi_a\})$. Write $\zeta = \zeta_{p^m}$ $(m = n+1)$ and $l(\sigma) = \log|(\zeta^{-1/2}(1-\zeta))^\sigma| = \log|1-\zeta^\sigma|$ for $\sigma \in G = G_{F/\mathbb{Q}}$. We have for $G = G_{F/\mathbb{Q}}$

$$\begin{aligned}
R_C &= \pm\det(\log|\xi_a^\tau|)_{a,\tau\in G-\{\mathbf{1}\}} \\
&= \pm\det(l(\sigma\tau) - l(\tau))_{\sigma,\tau\neq 1} \\
&\overset{\text{Lemma 13.9 (2)}}{=} \pm\prod_{\chi\neq\mathbf{1}}\sum_{\sigma\in G}\chi(\sigma)l(\sigma) \\
&= \pm\prod_{\chi\neq\mathbf{1}}\sum_{1\le a<p^m/2}\chi(a)\log|(1-\zeta)^{\sigma_a}| \\
&= \pm\prod_{\chi\neq\mathbf{1}}\sum_{1\le a<p^m/2}\chi(a)\log|1-\zeta^a| \\
&= \pm\prod_{\chi\neq\mathbf{1}}\frac{1}{2}\sum_{a=1}^{p^m}\chi(\sigma)\log|1-\zeta^a| \ \text{ as } |1-\zeta^a| = |-\zeta^a(1-\zeta^{-a})| = |1-\zeta^{-a}|.
\end{aligned}$$

Since $\prod_{1<a<p^m, a\equiv b \mod p^k}(1-\zeta^a) = 1-\zeta_{p^k}^b$ for $1 \le k \le m$, we get for χ primitive modulo p^k

$$\sum_{a=1}^{p^m}\chi(\sigma)\log|1-\zeta^a| = \sum_{b=1}^{p^k}\chi(\sigma)\log|1-\zeta^b| = -\frac{p^k}{\tau(\chi^{-1})}L(1,\chi^{-1}) = -\tau(\chi)L(1,\chi^{-1}).$$

Therefore we conclude from the formula (13.1)

$$R_C = \pm\prod_{\chi\neq\mathbf{1}} -\frac{1}{2}L(1,\chi) = |Cl_F|R_F.$$

Since $R_C/R_F = [(O_n^+)^\times : C_n^+]$ by Lemma 13.4, we conclude the theorem. □

Proof of Lemma 13.9: The proof is representation theoretic, and left regular representation and right regular representation of G is isomorphic, we get $\det(f(\tau\sigma^{-1}))_{\sigma,\tau\in G} = \det(f(\sigma\tau))_{\sigma,\tau\in G}$ and $\det(f(\tau\sigma^{-1}) - f(\tau))_{\sigma,\tau\neq 1} = \det(f(\sigma\tau) - f(\tau))_{\sigma,\tau\neq 1}$. Thus we prove

(1) $\det(f(\tau\sigma^{-1}))_{\sigma,\tau\in G} = \prod_{\chi\in\mathrm{Hom}(G,\mathbb{C}^\times)}\sum_{\sigma\in G}\chi(\sigma)f(\sigma)$;

(2) $\det(f(\tau\sigma^{-1}) - f(\tau))_{\sigma,\tau\neq 1} = \prod_{\chi\neq\mathbf{1}}\sum_{\sigma\in G}\chi(\sigma)f(\sigma)$.

Let V be the complex vector space of $\mathbb{C}$-valued functions on G, and let $\sigma \in G$ act on V by inner left multiplication. Consider the linear transformation $T : V \to V$ given by $\phi \mapsto \sum_\sigma f(\sigma)\phi(\sigma x)$. Let ϕ_τ be the characteristic function of $\{\tau\}$; i.e, $\phi_\tau(\sigma) = \delta_{\sigma,\tau}$ for the Kronecker symbol δ. Then $\beta := \{\phi_\tau\}_\tau$ is a basis of V. Since

$$\phi_\tau(\sigma x) = 1 \Leftrightarrow \sigma x = \tau \Leftrightarrow x = \sigma^{-1}\tau \Leftrightarrow \phi_{\sigma^{-1}\tau}(x) = 1,$$

we have

$$T\phi_\tau(x) = \sum_\sigma f(\sigma)\phi_\tau(\sigma x) = \sum_\sigma f(\sigma)\phi_{\sigma^{-1}\tau}(x) \overset{\sigma^{-1}\tau\mapsto\sigma}{=} \sum_\sigma f(\tau\sigma^{-1})\phi_\sigma(x).$$

Thus the matrix expression of T with respect to the basis β is given by $(f(\tau\sigma^{-1}))_{\sigma,\tau\in G}$. Since $\{\chi\}_{\chi\in\mathrm{Hom}(G,\mathbb{C}^\times)}$ also form an T-eigen basis of V with eigenvalue $\sum_\sigma \chi(\sigma)f(\sigma)$. This shows (1).

To show (2), let $V_0 = \{h \in V | \sum_s h(\sigma) = 0\}$ which is stable under the action of G. Set $\psi_\sigma = \phi_\sigma - \frac{1}{|G|}$ which is in V_0, and $\beta_0 := \{\psi_\sigma\}_{\sigma\neq 1}$ forms a basis of V_0. Since $\psi_1 + \sum_{\sigma\neq 1}\psi_\sigma = 0$, we have $\psi_1 = -\sum_{\tau\neq 1}\psi_\tau$. Since

$$\psi_\tau(\sigma x) = 1 - (1/|G|) \Leftrightarrow \tau x = \tau \Leftrightarrow x = \sigma^{-1}\tau \Leftrightarrow \phi_{\sigma^{-1}\tau}(x),$$

we have

$$T\psi_\tau(x) = \sum_{\sigma\in G} f(\tau\sigma^{-1})\phi_\sigma(x) = \sum_{\sigma\neq 1}(f(\tau\sigma^{-1}) - f(\tau))\phi_\sigma(x).$$

Then $T|_{V_0}$ has the matrix expression $(f(\tau\sigma^{-1}) - f(\tau))_{\sigma,\tau\neq 1}$. This shows (2). □

References

Books

[BNT] A. Weil, *Basic Number Theory*, Springer, New York, 1974.

[CFT] J. Neukirch, *Class Field Theory*, Springer, 1986.

[CRT] H. Matsumura, *Commutative Ring Theory*, Cambridge studies in advanced mathematics **8**, Cambridge Univ. Press, 1986

[ICF] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Text in Mathematics, **83**, Springer, 1980

[LFE] H. Hida, *Elementary Theory of L–functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, 1993

Articles

[BH] J. Buhler and D. Harvey, Irregular primes to 163 million, Math. Comp. **80** (2011), 2435-2444

[FW] B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. **109** (1979), 377–395.

[I69] K. Iwasawa, On p-adic L-functions, Ann. of Math. **89** (1969), 198–205.

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of **Q**. Inventiones Math. **76** (1984), 179–330.

[S] W. Sinnott, On the μ–invariant of the Γ–transform of a rational function, Inventiones Math. **75** (1984), 273–282.

[U3] K. Iwasawa, Some problems on cyclotomic fields and $\mathbb{Z}_p$-extensions, U3 (unpublished work no.3) in his collected papers in Volume II 853–861.

[We1] A. Weil, Numbers of solutions of equations in finite fields, Bull. AMS **55** (1949), 497–508.

[We2] A. Weil, Jacobi Sums as "Grössencharaktere" Transactions of the American Mathematical Society, **73** (1952), 487–495.