# HIDA THEORY

NOTES TAKEN BY PAK-HIN LEE

Abstract. These are notes from the (ongoing) Student Number Theory Seminar on Hida theory at Columbia University in Fall 2017, which is organized by David Hansen and Samuel Mundy.

Contents



Last updated: September 19, 2017. Please send corrections and comments to phlee@math.columbia.edu. We thank Samuel Mundy for proofreading and editting these notes.

## 1. Lecture 1 (September 7, 2017): Samuel Mundy
## Ribet's Converse to Herbrand's Theorem

1.1. **Introduction.** Let $p$ be an odd prime, and $\omega : G_{\mathbf{Q}} \to \mu_{p-1} \subseteq \mathbf{Z}_p^\times$ be the Teichmüller character (so that $\sigma\zeta_p = \zeta_p^{\omega(\sigma)}$ for all $\sigma \in G_{\mathbf{Q}}$).

For any $\mathbf{Z}_p[G_{\mathbf{Q}}]$-module $M$ and $\varphi \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})^\wedge$, write $M^\varphi = \{m \in M \mid \sigma m = \varphi(\sigma)m\}$ to be the $\varphi$-eigenspace of $M$.

Let $B_n$ be the $n$-th Bernoulli number.

Today we are going to prove Ribet's converse to Herbrand's theorem:

**Theorem 1.1** (Ribet)**.** *Let $m$ be an odd integer with $3 \leq m \leq p-2$. If $p \mid B_{p-m}$, then $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p^\infty]^{\omega^m} \neq 0$.*

*Remark.* We have $v_p(B_{p-1}) = -1$ and $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p^\infty]^\omega = 0$.

The idea is to deduce properties of Galois representations attached to automorphic representations of $\mathrm{GL}_1$ using those for $\mathrm{GL}_2$.

1.2. **Modular forms.** Fix embeddings $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}_p} \hookrightarrow \mathbf{C}$. For $N \geq 1$ an integer, $\psi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ a Dirichlet character, and $A \subseteq \mathbf{C}$ a subring containing $\mathbf{Z}[\psi]$, write

$$S_k(N, \psi, A) = \left\{ \text{cusp forms } f = \sum_{n=1}^{\infty} a_n(f) q^n \text{ of weight } k, \text{ level } N, \text{ nebentypus } \psi \mid a_n(f) \in A \right\}$$

where $q = e^{2\pi i z}$. Denote by $\mathbb{T}_k(N, \psi, A)$ the sub-$A$-algebra of $\mathrm{End}_A(S_k(N, \psi, A))$ generated by the Hecke operators $T[n]$ for all $n$.

We define a pairing

$$\begin{aligned} S_k(N, \psi, A) \times \mathbb{T}_k(N, \psi, A) &\to A \\ \langle f, h \rangle &\mapsto a_1(f|h). \end{aligned}$$

In particular, $\langle f, T(n) \rangle = a_n(f)$.

**Theorem 1.2.** *This pairing is perfect.*

**Theorem 1.3.** *Let $B$ be an $A$-algebra with $\phi : A \to B$. Under the isomorphism*

$$\mathrm{Hom}_A(\mathbb{T}_k(N, \psi, A), B) \simeq S_k(N, \psi, A) \otimes_A B,$$

*the $A$-algebra homomorphisms $\mathrm{Hom}_{A\text{-alg}}(\mathbb{T}_k(N, \psi, A), B)$ correspond to the normalized eigenforms, i.e., $f = \sum a_n(f) q^n \in S_k(N, \psi, A) \otimes_A B \subset B[[q]]$ with $a_1(f) = 1$ such that for all $h \in \mathbb{T}_k(N, \psi, A)$, there exists $c \in B$ such that $\phi(f|h) = c\phi(f)$, where the corresponding homomorphism on the LHS sends an operator to its eigenvalue.*

**Theorem 1.4.** *Let $f = \sum_{n=1}^{\infty} a_n(f) q^n \in S_k(N, \psi, A)$ be a normalized eigenform. Then there exists a continuous Galois representation $\rho_f : G_{\mathbf{Q}} \to \mathrm{Aut}(V)$ with $\dim_{\overline{\mathbf{Q}_p}}(V) = 2$ such that*

1. *$\rho_f$ is irreducible;*
2. *for all $\ell \nmid pN$, $\rho_f$ is unramified at $\ell$;*
3. *for all $\ell \nmid pN$, $\mathrm{tr}\, \rho_f(\mathrm{Frob}_\ell) = a_\ell(f)$;*
4. *for all $\ell \nmid pN$, $\det \rho_f(\mathrm{Frob}_\ell) = \psi(\ell)\ell^{k-1}$.*

**Definition 1.5.** A normalized eigenform $f \in S_k(1, \overline{\mathbf{Q}_p})$ is *ordinary* if $|a_p(f)|_p = 1$.

**Theorem 1.6** (Mazur–Wiles)**.** *If $f$ is ordinary, then there exists a basis $v_1, v_2$ of $V$ such that*

$$\rho_f|_{G_{\mathbf{Q}_p}} = \begin{pmatrix} \alpha^{-1}\chi^{k-1} & * \\ & \alpha \end{pmatrix},$$

*where $\chi : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ is the cyclotomic character (i.e., $\sigma\zeta = \zeta^{\chi(\sigma)}$ for all $\zeta \in \mu_{p^\infty}$), and $\alpha : G_{\mathbf{Q}_p} \to \overline{\mathbf{Q}_p}^\times$ is the unramified character such that $\alpha(\mathrm{Frob}_p)$ is the unit root of $X^2 - a_p(f)X + p^{k-1}$.*

1.3. **Proof of Ribet's theorem.** The proof consists of the following steps.

**Step 0**: Let $\kappa$ by any finite field of characteristic $p$. Then

$$\begin{aligned} \mathrm{Cl}_{\mathbf{Q}(\zeta_p)}[p]^{\omega^m} \otimes_{\mathbf{F}_p} \kappa &\cong \mathrm{Hom}_{G_{\mathbf{Q}}}(G^{\mathrm{ab,unr}}_{\mathbf{Q}(\zeta_p)}, \kappa(\omega^m)) \\ &\cong H^1_{\mathrm{unr}}(G_{\mathbf{Q}(\zeta_p)}, \kappa(\omega^m))^{G_{\mathbf{Q}}} \\ &\overset{\mathrm{Res}^{-1}}{\cong} H^1_{\mathrm{unr}}(G_{\mathbf{Q}}, \kappa(\omega^m)) \\ &\cong \mathrm{Ext}^{\mathrm{unr}}_{\kappa[G_{\mathbf{Q}}]}(\kappa, \kappa(\omega^m)) \\ &\cong \mathrm{Ext}^{\mathrm{unr}}_{\kappa[G_{\mathbf{Q}}]}(\kappa(\omega^{p-1-m}), \kappa). \end{aligned}$$

**Step 1** (Construction of an eigenform): Let

$$E_k(z) = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \left( \sum_{d|n} d^{k-1} \right) q^n$$

be the Eisenstein series of weight $k$, where $k \geq 4$ is even. The following facts are classical:

(1) $\zeta(1-k) = -B_k/k$.
(2) $v_p(B_k) < 0 \Leftrightarrow p-1 \mid k \Leftrightarrow v_p(B_k) = -1$.
(3) $E_k \in M_k(1, \mathbf{C})$. If $p-1 \nmid k$, then $E_k \in M_k(1, \mathbf{Z}_p)$ by (2).
(4) If $m \equiv n \pmod{p-1}$, then $B_m \equiv B_n \pmod{p}$.

Note that

$$\begin{aligned} E_4(z) &= \frac{1}{240} + q + \cdots, \\ E_6(z) &= \frac{-1}{504} + q + \cdots. \end{aligned}$$

Let $k \geq 4$ and $k \equiv p - m \pmod{p-1}$. Write $k = 4a + 6b$ where $a, b \geq 0$. Then define

$$G_k = (240E_4)^a(-504E_6)^b = 1 + \sum_{n=1}^{\infty} a_n q^n$$

where $a_n \in \mathbf{Z}$. Let

$$F_k = E_k - \frac{\zeta(1-k)}{2} G_k = \sum_{n=1}^{\infty} b_n q^n$$

where $b_n = \frac{B_k}{2k} a_n + \sum_{d|n} d^{k-1}$.

Now assume $p \mid B_{p-m}$. Then by (4), $p \mid B_k$ and so $b_n \equiv \sum_{d|n} d^{k-1} \pmod{p}$. Thus the map

$$\mathbb{T}_k(1, \mathbf{Z}_p) \to \mathbf{F}_p$$

$$T(n) \mapsto \sum_{d|n} d^{k-1} \pmod{p}$$

is a $\mathbf{Z}_p$-algebra homomorphism, corresponding to $F_k \pmod{p}$.

Let $\mathfrak{m} \subseteq \mathbb{T}_k(1, \mathbf{Z}_p)$ be the kernel, and $\mathfrak{p} \subseteq \mathfrak{m}$ be a minimal prime. Let $f$ be the eigenform corresponding to the homomorphism

$$\mathbb{T}_k(1, \mathbf{Z}_p) \to A := \mathbb{T}_k(1, \mathbf{Z}_p)/\mathfrak{p} \hookrightarrow \mathcal{O}_L,$$

where $L := \operatorname{Frac} A$. Then $f \in S_k(1, \mathcal{O}_L)$ and $f \equiv F_k \pmod{\lambda}$, where $\lambda \in \mathcal{O}_L$ is a uniformizer.

**Step 2** (Analysis of $\rho_f$): Write $f = \sum_{n=1}^{\infty} c_n q^n$. Then

$$c_p \equiv \sum_{d|p} d^{k-1} \equiv 1 + p^{k-1} \equiv 1 \pmod{\lambda},$$

so $f$ is ordinary. Let $v_1, v_2 \in V_{\rho_f}$ such that

$$\rho_f|_{G_{\mathbf{Q}_p}} = \begin{pmatrix} \alpha^{-1}\chi^{k-1} & * \\ & \alpha \end{pmatrix}.$$

Let $\sigma_0 \in G_{\mathbf{Q}_p}$ be an element such that $\chi^{k-1}(\sigma_0) \not\equiv 1 \pmod{\lambda}$ (possible since $k-1$ is odd, so $p - 1 \nmid k - 1$). Write $\beta := \chi^{k-1}(\sigma_0)$. Replacing $v_1$ by $\alpha(\sigma_0)v_1$ and $v_2$ by $\alpha^{-1}(\sigma_0)v_2 + (\text{something}) \cdot v_1$, we may assume

$$\rho_f(\sigma_0) = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}.$$

For $\sigma \in \mathcal{O}_L[G_{\mathbf{Q}}]$, let $\rho_f(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$.

**Lemma 1.7.**

(1) *For all $\sigma, \tau \in \mathcal{O}_L[G_{\mathbf{Q}}]$, we have $a_\sigma, d_\sigma, b_\sigma c_\tau \in \mathcal{O}_L$ and*

$$a_\sigma \equiv \omega^{k-1}(\sigma), \quad d_\sigma \equiv \mathbb{1}(\sigma), \quad b_\sigma c_\tau \equiv 0 \pmod{\lambda},$$

*where $\mathbb{1}$ is the trivial $G_{\mathbf{Q}}$-character, and $\omega^{k-1}, \mathbb{1}$ are extended by linearity to $\mathcal{O}_L[G_{\mathbf{Q}}]$.*

(2) *$C = \{c_\sigma \mid \sigma \in \mathcal{O}_L[G_{\mathbf{Q}}]\}$ is a nonzero fractional ideal.*

(3) *$c_\sigma = 0$ for all $\sigma \in I_\ell$ and primes $\ell$.*

*Proof.* Omitted; play with matrix coefficients using information about the trace. □

**Step 3** (Construction of the lattice): Let $M_1 = \mathcal{O}_L v_1$, $M_2 = Cv_2$ and $M = M_1 \oplus M_2 \subseteq V_{\rho_f}$. This is $G_{\mathbf{Q}}$-stable, generated over $\mathcal{O}_L[G_{\mathbf{Q}}]$ by $v_1$.

Let $\kappa = \mathcal{O}_L/\lambda$ and $\overline{M} = M/\lambda M$.

*Claim.* $\overline{M_2} := M_2/\lambda M_2 \subseteq \overline{M}$ is a $G_{\mathbf{Q}}$-stable line with trivial action.

Let $m_2 \in M_2$, so $m_2 = c_\tau v_2$ for some $c_\tau \in C$. If $\sigma \in G_{\mathbf{Q}}$, then

$$\rho_f(\sigma)m_2 = c_\tau b_\sigma v_1 + c_\tau d_\sigma v_2 \equiv d_\sigma m_2 = \mathbb{1}(\sigma)m_2 = m_2 \pmod{\lambda}$$

which proves the claim.

Let $\overline{M_1} = M_1/\lambda M_1$. Then $\overline{M_1} \cong \kappa(\omega^{k-1})$ by a similar argument, and there is a short exact sequence

$$0 \to \kappa \to \overline{M} \to \kappa(\omega^{k-1}) \to 0$$

which is:

- nonsplit over $G_{\mathbf{Q}}$ because, if it were, $\overline{M_2} \cong \kappa$ would be a quotient and hence the image of $v_1$ would belong to the kernel by this quotient. This is because $\sigma_0$ acts as $\beta \not\equiv 1 \pmod{\lambda}$ on $v_1$, but $v_1$ generates $\overline{M}$ over $G_{\mathbf{Q}}$. Hence the kernel is all of $\overline{M}$, a contradiction.
- split over $I_\ell$ for all $\ell$ because $\mathcal{O}_L v_1 \pmod{\lambda}$ is a stable line under $I_\ell$, since

$$\rho(\sigma)v_1 = a_\sigma v_1 + c_\sigma v_2 \equiv a_\sigma v_1 \pmod{\lambda}.$$

Since $\omega^{k-1} = \omega^{p-1-m}$, this extension gives a nontrivial class in $\mathrm{Ext}^{\mathrm{unr}}_{\kappa[G_{\mathbf{Q}}]}(\kappa(\omega^{p-1-m}), \kappa)$. This finishes the proof of Theorem 1.1.

## 2. Lecture 2 (September 14, 2017): Samuel Mundy
## Basic Iwasawa Theory

2.1. **$\mathbf{Z}_p$-extensions and Iwasawa's theorem.** Last time we understood better the structure of $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}$ as a $G_{\mathbf{Q}}$-module. A natural question is: What about $\mathrm{Cl}_{\mathbf{Q}(\zeta_{p^n})}$?

**Theorem 2.1** (Iwasawa)**.** *There exist integers $n_0$ and $\mu$, $\lambda$, $\kappa$ such that for all $n > n_0$,*

$$\#\mathrm{Cl}_{\mathbf{Q}(\zeta_{p^n})}[p^\infty] = p^{\mu p^n + \lambda n + \kappa}.$$

This statement *a priori* does not have anything to do with the Galois structure of class groups, but the proof relies heavily on that.

Recall that $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times$. Let $\mathbf{Q}(\zeta_{p^\infty}) = \bigcup_{n\geq 0} \mathbf{Q}(\zeta_{p^n})$. Then

$$\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}) \simeq \mathbf{Z}_p^\times,$$
$$\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}(\zeta_p)) \simeq \mathbf{Z}_p.$$

The element $1 - \zeta_{p^n} \in \mathcal{O}_{\mathbf{Q}(\zeta_{p^n})} = \mathbf{Z}[\zeta_{p^n}]$ generates the (totally ramified) prime above $p \in \mathbf{Z}$. With these facts we are ready to study basic Iwasawa theory.

**Definition 2.2.** Let $K_0$ be a number field. A $\mathbf{Z}_p$*-extension* of $K_0$ is an algebraic extension $K_\infty/K_0$ such that $\mathrm{Gal}(K_\infty/K_0) \simeq \mathbf{Z}_p$ topologically; equivalently, it is a tower of finite extensions

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup_{n\geq 0} K_n$$

such that $\mathrm{Gal}(K_n/K_0) \simeq \mathbf{Z}/p^n\mathbf{Z}$.

**Proposition 2.3.** *Let $K_\infty/K_0$ be a $\mathbf{Z}_p$-extension. Then:*

1. *Some prime is ramified in $K_\infty$.*
2. *For any ramified prime $\mathfrak{p} \subseteq \mathcal{O}_{K_0}$, there exists $n_0$ such that if $\mathfrak{q} \subseteq \mathcal{O}_{K_{n_0}}$ is such that $\mathfrak{q} \mid \mathfrak{p}$, then $\mathfrak{q}$ is totally ramified in $K_\infty/K_{n_0}$.*
3. *Every ramified prime lies over $p \in \mathbf{Z}$.*

*Proof.*

1. The maximal unramified abelian extension of $K_0$ is finite over $K_0$.
2. Let $\mathfrak{p}$ be ramified in $K_\infty/K_0$, and $I_\mathfrak{p} \subseteq \mathrm{Gal}(K_\infty/K_0) \simeq \mathbf{Z}_p$ be the inertia group at $\mathfrak{p}$. This is nontrivial and closed. Thus $I_\mathfrak{p} \simeq p^{n_0}\mathbf{Z}_p$ for some $n_0$, so $I_\mathfrak{p} = \mathrm{Gal}(K_\infty/K_0)$.

(3) Let $\mathfrak{p} \subseteq \mathcal{O}_{K_0}$ be ramified in $K_\infty$. By local class field theory,

$$\mathrm{Gal}(K_{0,\mathfrak{p}}^{\mathrm{ab}}/K_{0,\mathfrak{p}}) \cong \widehat{K_{0,\mathfrak{p}}^\times} \simeq \pi^{\hat{\mathbf{Z}}} \times \mathcal{O}_{K_{0,\mathfrak{p}}}^\times$$

corresponding to the unramified and ramified parts respectively, so by (2) we get an infinite subgroup of $\mathcal{O}_{K_{0,\mathfrak{p}}}^\times$ isomorphic to $\mathbf{Z}_p$, forcing $K_{0,\mathfrak{p}}$ to have residue characteristic $p$. □

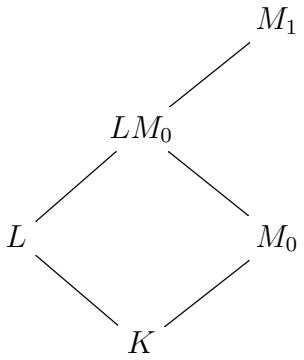
**Proposition 2.4.** *Let $L/K$ be an extension of number fields such that some prime in $K$ is totally ramified in $L$. Then the norm map*

$$\mathrm{Nm} : \mathrm{Cl}_L[p^\infty] \to \mathrm{Cl}_K[p^\infty]$$

*is surjective.*

*Remark.* This is true without taking $p$-primary parts and essentially the same proof will work. It is also true if the ramified prime is at infinity.

*Proof.* Let $M_0/K$ be the maximal unramified abelian $p$-extension of $K$, and $M_1$ that for $L$. Then $M_0$ and $L$ are linearly disjoint over $K$ (i.e., $M_0 \cap L = K$ in any $\overline{K}$).




Since $LM_0/L$ is an unramified abelian $p$-extension, it is contained in $M_1$. Then by class field theory, the diagram

$$\begin{array}{ccc} \mathrm{Cl}_L[p^\infty] & \xrightarrow[\mathrm{Art}]{\sim} & \mathrm{Gal}(M_1/L) \\ {\scriptstyle \mathrm{Nm}}\downarrow & & \downarrow{\scriptstyle \text{restriction to } M_0} \\ \mathrm{Cl}_K[p^\infty] & \xrightarrow[\mathrm{Art}]{\sim} & \mathrm{Gal}(M_0/K) \end{array}$$

commutes. □

This suggests that we should look at

$$C := \varprojlim_{n \geq 0} \mathrm{Cl}_{K_n}[p^\infty],$$

where the inverse limit is taken with respect to Nm. Write $\Gamma_n = \mathrm{Gal}(K_n/K_0)$. Since $\mathrm{Cl}_{K_n}[p^\infty]$ is a $\mathbf{Z}_p[\Gamma_n]$-module, $C$ is a module over

$$\Lambda := \varprojlim_{n \geq 0} \mathbf{Z}_p[\Gamma_n],$$

where the inverse limit is taken with respect to restriction maps $\Gamma_m \twoheadrightarrow \Gamma_n$ if $m \geq n$.

**Theorem 2.5** (Iwasawa)**.** *$C$ is a finitely generated torsion $\Lambda$-module.*

We will see how Theorem 2.1 follows from this.

2.2. **$\Lambda$-modules.** We need to first understand the structure of $\Lambda$. Let $\gamma \in \Gamma := \mathrm{Gal}(K_\infty/K_0) \subseteq \Lambda^\times$ be a topological generator. An observation due to Serre is that:

**Proposition 2.6** (Serre)**.** *There is an isomorphism*

$$\Lambda \simeq \mathbf{Z}_p[[T]]$$

*of topological rings, induced by $\gamma - 1 \mapsto T$.*

*Proof.* Omitted; see Lang's *Cyclotomic Fields I and II*, Chapter 5. □

**Corollary 2.7** (Nakayama's lemma)**.** *If $M$ is a compact $\Lambda$-module and $M/TM = M/(\gamma - 1)M$ is finitely generated over $\mathbf{Z}_p$, then any set of generators in $M/TM$ lifts to a set of generators in $M$. In particular, $M$ is finitely generated.*

**Definition 2.8.** A *quasi-isomorphism* of $\Lambda$-modules $M, N$ is a map $\varphi : M \to N$ such that there exists an exact sequence

$$0 \to A \to M \xrightarrow{\varphi} N \to B \to 0$$

with $A, B$ of finite cardinality.

Quasi-isomorphism is an equivalence relation.

**Theorem 2.9** (Weierstrass preparation)**.** *Let $f \in \mathbf{Z}_p[[T]]$ be a nonconstant power series. Then there exist a unique integer $n \geq 0$ and unique $g, u \in \mathbf{Z}_p[[T]]$ such that $g$ is* distinguished *and $u \in \mathbf{Z}_p[[T]]^\times$, and*

$$f = p^n u g.$$

*(A monic polynomial $g = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ is* distinguished *if $p \mid a_i$ for all $i = 0, \cdots, n-1$.)*

**Theorem 2.10.** *Let $M$ be a finitely generated $\Lambda$-module. Then there exist integers $r$, $n_i$ and distinguished $f_j$ (where $i \in I$ and $j \in J$ with $I$ and $J$ finite) such that*

$$M \overset{\text{q-iso}}{\simeq} \Lambda^r \oplus \bigoplus_{i \in I} \Lambda/(p^{n_i}) \oplus \bigoplus_{j \in J} \Lambda/(f_j).$$

2.3. **Proof of Iwasawa's theorem.** We will prove Theorem 2.1 and Theorem 2.5 in the case when there is only one ramified prime $\mathfrak{p} \subseteq \mathcal{O}_{K_0}$ above $p$.

*Proof of Theorem 2.5.* For simplicity, we further assume that $\mathfrak{p}$ is totally ramified in $K_\infty/K_0$. Then we make the main

*Claim.* $C/(\gamma - 1)C \simeq \mathrm{Cl}_{K_0}$.

Let $M_n/K_n$ be the maximal unramified abelian $p$-extension, and $M_\infty := \bigcup_{n \geq 0} M_n$, so $M_\infty/K_\infty$ is the maximal unramified pro-$p$ abelian extension. Let $G_C := \mathrm{Gal}(M_\infty/K_\infty) \cong C$, $G := \mathrm{Gal}(M_\infty/K_0)$ and $\Gamma = \mathrm{Gal}(K_\infty/K_0)$.

*Claim* (Subclaim 1). If $I \subset G$ is the inertia at $\mathfrak{p}$, then $G \simeq G_C \rtimes I$.

There is an exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(M_\infty/K_\infty) & \longrightarrow & \mathrm{Gal}(M_\infty/K_0) & \longrightarrow & \mathrm{Gal}(K_\infty/K_0) & \longrightarrow & 1. \\ & & \| & & \| & & \| & & \\ & & G_C & & G & & \Gamma & & \end{array}$$

Since $\mathfrak{p}$ is totally ramified in $K_\infty$, $I$ surjects onto $\Gamma$ and has empty intersection with $G_C$. This proves $\Gamma \simeq I$ and subclaim 1.

Let $\Gamma \simeq I$ act on $G_C$ by conjugation. Then this action is the same as that on $C$: $\mathrm{Frob}_{\sigma\mathfrak{q}} = \sigma \,\mathrm{Frob}_{\mathfrak{q}}\, \sigma^{-1}$.

*Claim* (Subclaim 2). Let $G'$ be the commutator subgroup of $G$. Then $G' = (\gamma - 1)G$.

Let $g \in G$. Then $(\gamma - 1)g = \tilde{\gamma} g \tilde{\gamma}^{-1} g^{-1} \in G'$, where $\tilde{\gamma}$ is a lift of $\gamma$ to $I$. Conversely, $G/(\gamma - 1)G$ is the largest quotient where $\Gamma$ acts trivially. So conjugation by elements in $I$ is trivial, and since $G_C$ is abelian and $G = G_C \rtimes I$, we have that $G/(\gamma - 1)G$ is abelian and hence $(\gamma - 1)G \subseteq G'$. This proves subclaim 2.

To prove the main claim that $C/(\gamma - 1)C \simeq \mathrm{Cl}_{K_0}[p^\infty]$, it is the same to prove

$$G_C/(\gamma - 1)G_C \cong \mathrm{Gal}(M_0/K_0).$$

Note $(\gamma - 1)G_C = (\gamma - 1)G$ (because if $g \in G_C$, $\iota \in I$ and $\gamma \in \Gamma$, then picking a lift $\tilde{\gamma} \in I$, we have $(\gamma - 1)g\iota = \tilde{\gamma} g \iota \tilde{\gamma}^{-1} \iota^{-1} g^{-1} = \tilde{\gamma} g \iota \iota^{-1} \tilde{\gamma}^{-1} g^{-1} = (\gamma - 1)g$; the reverse inclusion is trivial). Then

$$\begin{aligned} G_C/(\gamma - 1)G_C &= G_C/(\gamma - 1)G \\ &\cong G/I \cdot (\gamma - 1)G \\ &= G/I \cdot G' \\ &= \mathrm{Gal}(M_0/K_0). \end{aligned}$$

This proves the main claim.

Since $\mathrm{Cl}_{K_0}[p^\infty] = C/(\gamma - 1)C$ is finite, by Nakayama's lemma $C$ is finitely generated. Write

$$C \overset{\text{q-iso}}{\simeq} \Lambda^r \oplus \bigoplus \Lambda/(p^{n_i}) \oplus \bigoplus \Lambda/(f_j).$$

Then since $\Lambda^r/(\gamma - 1)\Lambda^r \simeq \mathbf{Z}_p^r$, we have $r = 0$. This proves Theorem 2.5. □

*Remark.* Since $C/(\gamma^{p^n} - 1)C$ is finite, we see that $f_j$ is coprime to $(1 + T)^{p^n} - 1$ for all $j, n$.

Finally, let us prove Theorem 2.1: There exist $n_0$ and $\mu, \lambda, \kappa$ such that for all $n > n_0$,

$$\#\mathrm{Cl}_{K_n}[p^\infty] = p^{\mu p^n + \lambda n + \kappa}.$$

*Exercise.*

(1) $\#\Lambda/(p^m, \gamma^{p^n} - 1) = p^{mp^n}$.
(2) Let $f$ be a distinguished polynomial coprime to $(1 + T)^{p^n} - 1$ for all $n$. Then there exists $n_0$ such that if $n > n_0$, then $\#\Lambda/(f, \gamma^{p^n} - 1) = p^{\deg(f)n + c}$ for some $c = c(f)$.

*Proof of Theorem 2.1.* Replacing $K_0$ by $K_n$ where $n \gg 0$, we may assume the ramified prime is totally ramified. Then setting $\mu = \sum_i n_i$ and $\lambda = \sum_j \deg f_j$, we get (by the previous exercise and remark) $\kappa$ such that

$$\#\mathrm{Cl}_{K_n}[p^\infty] = \#C/(\gamma^{p^n} - 1)C = p^{\mu p^n + \lambda n + \kappa}$$

for sufficiently large $n$. $\square$

*Remark.* For the cyclotomic extension $\mathbf{Q}(\zeta_{p^\infty})$, it is known that $\mu = 0$; this is the Ferrero–Washington theorem.