IWASAWA THEORY

Romyar Sharifi

Contents

Introduction

The class group Cl_F of a number field F is an object of central importance in number theory. It is a finite abelian group, and its order h_F is known as the class number. In general, the explicit determination of h_F, let alone the structure of Cl_F as a finite abelian group, can be a difficult and computationally intensive task.

In the late 1950's, Iwasawa initiated a study of the growth of class groups in certain towers of number fields. Given a tower $F = F_0 \subset F_1 \subset F_2 \subset \cdots$ of Galois extensions of F, one asks if there is any regularity to the growth of h_{F_n}. The knowledge of this growth, in turn, can be used to say something about the structure of Cl_{F_n} as a finite abelian group. Iwasawa was concerned with towers such that $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$ for some prime p, where $F_\infty = \bigcup_n F_n$, known as $\mathbb{Z}_p$-extensions. He set $\Gamma = \mathrm{Gal}(F_\infty/F)$ and $\Gamma_n = \mathrm{Gal}(F_n/F)$, and let us suppose that F_n is chosen to be (cyclic) of degree p^n over F. For example, for odd p, the cyclotomic $\mathbb{Z}_p$-extension F_∞ of F is the largest subextension of $F(\mu_{p^\infty})/F$ with pro-p Galois group.

The question of how h_{F_n} grows in the tower defined by a $\mathbb{Z}_p$-extension is quite difficult, in particular as the order away from p of Cl_{F_n} has little to do with the order away from p of $\mathrm{Cl}_{F_{n+1}}$, other than the fact that the latter order is a multiple of the former. On the other hand, if we concentrate on the order $h_{F_n}^{(p)}$ of the Sylow p-sugroup A_n of F_n, we have the following theorem of Iwasawa.

THEOREM (Iwasawa). *There exist nonnegative integers λ and μ and an integer ν such that*

$$h_{F_n}^{(p)} = p^{n\lambda + p^n\mu + \nu}$$

for all sufficiently large n.

In the case that F_∞ is the cyclotomic $\mathbb{Z}_p$-extension, Iwasawa conjectured that the invariant μ in the theorem is 0. Ferrero and Washington later proved this result for abelian extensions of $\mathbb{Q}$.

We have maps between the p-parts of class group in the tower in both directions $j_n \colon A_n \to A_{n+1}$, which takes the class of an ideal $\mathfrak{a}$ to the class of the ideal it generates, and $N_n \colon A_{n+1} \to A_n$, which takes the class of an ideal to the class of its norm. Iwasawa considered the direct and inverse limits

$$A_\infty = \varinjlim_n A_n \quad \text{and} \quad X_\infty = \varprojlim_n A_n$$

under the j_n and N_n, respectively. As each A_n has the structure of a finite $\mathbb{Z}_p[\Gamma_n]$-module through the standard action of Γ_n on ideal classes, both X_∞ and the Pontryagin dual $A_\infty^\vee = \mathrm{Hom}_{\mathrm{cts}}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ of A_∞ are finitely generated torsion modules over the competed $\mathbb{Z}_p$-group ring of Γ:

$$\mathbb{Z}_p[\![\Gamma]\!] = \varprojlim_n \mathbb{Z}_p[\Gamma_n].$$

The ring $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ is known as the Iwasawa algebra, and it has a very simple structure. In fact, a choice of a topological generator γ of Γ gives rise to an isomorphism

$$\mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \Lambda, \qquad T \mapsto \gamma - 1.$$

The following result on the structure of Λ-modules allowed Serre to rephrase the theorem of Iwasawa.

THEOREM (Serre). *For any finitely generated torsion Λ-module M, there exists a homomorphism of Λ-modules*

$$M \to \bigoplus_{i=1}^{s} \Lambda/f_i(T)^{k_i}\Lambda \oplus \bigoplus_{j=1}^{t} \Lambda/p^{\ell_j}\Lambda,$$

with finite kernel and cokernel, for some nonnegative integers s and t, irreducible $f_i(T) \in \mathbb{Z}_p[T]$ with $f_i(T) \equiv T^{\deg f_i} \bmod p$, and positive integers k_i and ℓ_j.

From Serre's theorem, we are able to deduce several important invariants of a finitely generated Λ-module M. For instance, in the notation of the theorem, let us set

$$\lambda(M) = \sum_{i=1}^{s} k_i \deg f_i \quad \text{and} \quad \mu(M) = \sum_{j=1}^{t} \ell_j.$$

These are known as the λ and μ-invariants of M. Serre showed that these invariants for X_∞ and $A_\infty^\vee$ agree with the λ and μ of Iwasawa's theorem. An even more interesting invariant of M is its characteristic ideal, given by

$$\mathrm{char}_\Lambda M = \left(p^{\mu(M)} \prod_{i=1}^{s} f_i(T)^{k_i} \right) \Lambda,$$

which we shall consider in a specific case shortly.

It is worth remarking here that one usually thinks of X_∞ as a Galois group. Recall that the Artin reciprocity map provides an isomorphism between A_n and the Galois group of the Hilbert p-class field L_n of F_n, which is to say the maximal unramified abelian p-extension of F_n. Setting $L_\infty = \bigcup_n L_n$, we have a canonical isomorphism $X_\infty \cong \mathrm{Gal}(L_\infty/F_\infty)$. The resulting action on Γ on $\mathrm{Gal}(L_\infty/F_\infty)$ is a conjugation action, given by a lift of Γ to a subsgroup of $\mathrm{Gal}(L_\infty/F)$.

Let us focus now on the specific case that $F = \mathbb{Q}(\mu_p)$, and let us take F_∞ to be the cyclotomic $\mathbb{Z}_p$-extension of F for an odd prime p. In this setting, Iwasawa proved that his $\mu = \mu(X_\infty)$ is zero.

We define the Teichmüller character $\omega\colon \Delta \to \mathbb{Z}_p^\times$ by setting $\omega(\delta)$ for $\delta \in \Delta$ to be the unique $(p-1)$st root of unity in $\mathbb{Z}_p$ such that

$$\delta(\zeta_p) = \zeta_p^{\omega(\delta)}$$

for any primitive pth root of unity ζ_p.

As with Γ, the Galois group $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ will act on X_∞. For any i, we may consider the eigenspace $X_\infty^{(i)}$ of X_∞ on which every $\delta \in \Delta$ acts through multiplication by $\omega^i(\delta)$. We have the following theorem of Herbrand and Ribet.

THEOREM (Herbrand-Ribet). *Let k be an even with $2 \leq k \leq p-3$. Then $X_\infty^{(1-k)} \neq 0$ if and only if p divides the Bernoulli number B_k.*

The interesting fact is that Bernoulli numbers and their generalizations appear as values of L-functions. Kubota and Leopoldt showed how that the L-values of certain characters at negative integers can be interpolated, in essence, by a function of $\mathbb{Z}_p$, denoted $L_p(\chi, s)$ and known as a p-adic L-function.

Let us fix the particular generator γ of Γ such that $\gamma(\zeta) = \zeta^{1+p}$ for every p-power root of unity ζ, and in particular the isomorphism of Λ with $\mathbb{Z}_p[\![T]\!]$. Iwasawa made the following conjecture on the characteristic ideal of an eigenspace of X, which was later proven by Mazur and Wiles.

THEOREM (Main conjecture of Iwasawa theory, Mazur-Wiles). *Let k be an even integer. Then*

$$\mathrm{char}_\Lambda X_\infty^{(1-k)} = (f_k),$$

where $f_k((1+p)^s - 1) = L_p(\omega^k, s)$ for all $s \in \mathbb{Z}_p$.

In fact, Mazur and Wiles proved a generalization of this to abelian extensions F of $\mathbb{Q}$, and Wiles proved a further generalization to abelian extensions of totally real fields. This line of proof was primarily geometric in nature, and came by studying the action of the absolute Galois group of F on the cohomology groups of modular curves. Rubin gave a proof of a rather different nature of a main conjecture for abelian extensions of imaginary quadratic fields, following work of Kolyvagin and Thaine, using a Galois cohomological tool known as an Euler system.

Let us end this introduction by mentioning the two of the major directions in which Iwasawa theory has expanded over the years. As a first and obvious course of action, one can replace our limits of class groups with more general objects. Via class field theory, we note that the Pontryagin dual $X_\infty^\vee$ may be identified with the kernel of the map

$$\ker\Big(H^1(G_{F_\infty,S}, \mathbb{Q}_p/\mathbb{Z}_p) \to \bigoplus_{v\in S} H^1(I_v, \mathbb{Q}_p/\mathbb{Z}_p)\Big),$$

where $G_{F_\infty,S}$ denotes the Galois group of the maximal extension of F_∞ unramified outside S and S in this case is the set of primes of F_∞ lying over p, and where I_v is the inertia group at $v \in S$ in the absolute

Galois group of F_∞. That is, we have realized $X_\infty^\vee$ as what is known as a Selmer group. This generalizes nicely.

By way of the most interesting example, let E be an elliptic curve over F with ordinary reduction at p, and let $E[p^\infty]$ denote its p-power torsion (over $\overline{\mathbb{Q}}$). The Selmer group of E over F_∞ is exactly

$$\mathrm{Sel}(E/F_\infty) = \ker\left(H^1(G_{F_\infty,S}, E[p^\infty]) \to \bigoplus_{v\in S} H^1(I_v, E[p^\infty])\right),$$

where S is now the set of primes of F_∞ over p or any primes of bad reduction of E. In the case that $F = \mathbb{Q}$, there is a corresponding main conjecture for the structure of $\mathrm{Sel}(E/F_\infty)^\vee$ in terms of a p-adic L-function of E. Great progress has been made on this particular main conjecture, due to successively more recent work of Rubin (for CM curves), Kato, and Skinner and Urban.

In the second generalization, one allows the Galois group Γ of the tower to take a more general form than $\mathbb{Z}_p$. The case that Γ is a p-adic Lie group, which is to say isomorphic to an open subgroup of $\mathrm{GL}_m(\mathbb{Z}_p)$ for some $m \geq 1$, has come under the greatest consideration. In this case, main conjectures become more difficult to formulate, as the structure theory of $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$-modules is no longer simple. Still, in the past decade, such main conjectures have been formulated using K-theory as one of several tools. In the classical setting of limits of class groups, the corresponding main conjecture has been proven by Kakde and Ritter-Weiss.[1]

[1]The reader should be aware that parts of these notes were hurriedly written and, at present, have not been proofread or checked. Also, references and attributions of results have not been properly made. We hope to rectify these issues in later versions. Comments pointing out errors are welcome.

CHAPTER 1

Class groups and units

1.1. Notation and background

Throughout, we will let F be a number field. We recall a number of objects attached to F and finite Galois extensions thereof and results regarding them.

NOTATION 1.1.1. To a number field, we attach the following objects:

- the ring of integers $\mathscr{O}_F$ of F,
- the unit group $\mathscr{O}_F^\times$ of F, which is to say the unit group of $\mathscr{O}_F$,
- the ideal group I_F of F, i.e., the group of nonzero finitely generated $\mathscr{O}_F$-submodules of F,
- the prinicipal ideal group P_F of F, i.e., those $\mathscr{O}_F$-submodules (α) of F generated by a single element $\alpha \in F^\times$, and
- the class group $\mathrm{Cl}_F = I_F/P_F$ of F.

REMARK 1.1.2. The class group Cl_F is a finite abelian group.

These objects fit into the following nice commutative diagram

$$\begin{array}{ccccccccc} & & & & P_F & & & & \\ & & & \nearrow & & \searrow & & & \\ 1 & \longrightarrow & \mathscr{O}_F^\times & \longrightarrow & F^\times & \longrightarrow & I_F & \longrightarrow & \mathrm{Cl}_F \longrightarrow 0 \end{array}$$

in which the lower row is exact.

DEFINITION 1.1.3. The *absolute norm* $N\mathfrak{a}$ of a nonzero ideal $\mathfrak{a}$ of $\mathscr{O}_F$ is the index $N\mathfrak{a} = [\mathscr{O}_F : \mathfrak{a}]$.

NOTATION 1.1.4. The number of real places of F is denoted $r_1(F)$, and the number of complex places of F is denoted $r_2(F)$.

REMARK 1.1.5. Since each complex places consists of a pair of complex conjugate embeddings of F, the degree formula tells us that $r_1(F) + 2r_2(F) = [F : \mathbb{Q}]$.

THEOREM 1.1.6 (Dirichlet's unit theorem). *The unit group $\mathscr{O}_F^\times$ is a finitely generated abelian group of rank $r_1(F) + r_2(F) - 1$ with torsion subgroup the group $\mu(F)$ of roots of unity in F.*

Next, we turn quickly to the zeta function of a number field.

DEFINITION 1.1.7. The *Dedekind ζ-series* ζ_F of a number field F is

$$\zeta_F(s) = \sum_{\mathfrak{a} \subseteq \mathscr{O}_F} \frac{1}{(N\mathfrak{a})^s},$$

for $s \in \mathbb{C}$ with real part $\operatorname{Re} s > 1$, where the sum is taken over nonzero ideals of $\mathscr{O}_F$.

THEOREM 1.1.8. *The Dedekind ζ-series of F converges absolutely on s with* $\operatorname{Re} s > 1$. *It has a unique mermomorphic continuation to* $\mathbb{C}$ *which is holomorphic outside* 1 *and has a simple pole at* $s = 1$.

With this in hand, we define the Dedekind zeta function to be the meromorphic continuation of ζ_F to $\mathbb{C}$.

DEFINITION 1.1.9. The *Dedekind zeta function* ζ_F of a number field F is the meromorphic continuation to $\mathbb{C}$ of the Dedekind ζ-series ζ_F.

The Dedekind zeta function has the following functional equation relating its values at s and $1-s$.

THEOREM 1.1.10. *Let*

$$\Lambda_F(s) = (2^{-r_2(F)}\pi^{-[F:\mathbb{Q}]}|d_F|^{1/2})^s \Gamma(s/2)^{r_1(F)}\Gamma(s)^{r_2(F)}\zeta_F(s),$$

where Γ *is the gamma function and* d_F *denotes the discriminant of* F. *Then* $\Lambda_F(s)$ *is analytic on* $\mathbb{C}$ *and satisfies*

$$\Lambda_F(s) = \Lambda_F(1-s).$$

For any Galois extension E/F and prime $\mathfrak{p}$ of F, let $\varphi_{\mathfrak{P}}$ denote a Frobenius at a prime $\mathfrak{P}$ over $\mathfrak{p}$. We have

$$\varphi_{\mathfrak{P}}(\alpha) \equiv \alpha^{N\mathfrak{p}} \bmod \mathfrak{P}$$

for $\alpha \in \mathscr{O}_E$. If E/F is unramified, its conjugacy class in $\operatorname{Gal}(E/F)$ depends only on $\mathfrak{p}$, and let us denote it by $[\varphi_{\mathfrak{p}}]$. If E/F is abelian and unramified, we denote the unique Frobenius more simply by $\varphi_{\mathfrak{p}}$.

THEOREM 1.1.11 (Čebotarev density theorem). *Let E/F be a finite Galois extension of number fields with group G. Let X be the set of unramified primes in E/F. Let C be a conjugacy class in G. Then*

$$\lim_{N\to\infty} \frac{\{\mathfrak{p} \in X \mid [\varphi_{\mathfrak{p}}] \in C \text{ and } N\mathfrak{p} \le N\}}{\{\mathfrak{p} \in X \mid N\mathfrak{p} \le N\}} = \frac{|C|}{|G|}.$$

We will denote the class of a fractional ideal $\mathfrak{a} \in I_F$ by $[\mathfrak{a}] \in \operatorname{Cl}_F$. The class group has an other description in terms of the Hilbert class field H_F of F, which is to say the maximal unramified abelian extension of F. We recall the following classical result of class field theory.

THEOREM 1.1.12. *The Artin map*

$$\phi_F\colon \mathrm{Cl}_F \to \mathrm{Gal}(H_F/F),$$

defined by $\phi_F([\mathfrak{p}]) = \varphi_{\mathfrak{p}}$ *for all primes* $\mathfrak{p}$ *of* F*, is an isomorphism.*

1.2. Regulators

Let F be a number field. We will shorten our notation for units slightly as follows.

NOTATION 1.2.1. We set $E_F = \mathscr{O}_F^\times$.

DEFINITION 1.2.2. We say that a set of r units of F is *independent* if it generates a subgroup of E_F isomorphic to $\mathbb{Z}^r$.

We will use the following notation.

NOTATION 1.2.3. Set $r = r_1(F) + r_2(F) - 1$. Let $\sigma_1, \dots, \sigma_{r_1(F)}\colon F \hookrightarrow \mathbb{R}$ be the real embeddings of F and $\sigma_{r_1(F)+1}, \dots, \sigma_{r+1}\colon F \hookrightarrow \mathbb{C}$ be representatives of the distinct complex conjugacy classes of complex embeddings of F. Let $V = \bigoplus_{i=1}^{r_1(F)+r_2(F)} \mathbb{R}\sigma_i$ and

$$V_0 = \left\{ \sum_{i=1}^{r+1} a_i\sigma_i \in V \mid \sum_{i=1}^{r+1} a_i = 0 \right\}.$$

We define an $\mathbb{R}$-linear homomorphism $\kappa\colon F^\times \otimes_{\mathbb{Q}} \mathbb{R} \to V_0$ by

$$\kappa(\alpha) = \sum_{i=1}^{r+1} c_i \log|\sigma_i(\alpha)|\sigma_i,$$

where

$$c_i = \begin{cases} 1 & \text{if } \sigma_i \text{ real} \\ 2 & \text{if } \sigma_i \text{ complex.} \end{cases}$$

The following is typically proven in the course of a proof of *Dirichlet's unit theorem*. Let κ_0 denote the restriction of κ to a map $\kappa_0\colon E_F \otimes_{\mathbb{Q}} \mathbb{R} \to V_0$, the image landing in V_0 by the product formula.

PROPOSITION 1.2.4. *The map* $\kappa_0\colon E_F \otimes_{\mathbb{Q}} R \to V_0$ *is an isomorphism.*

DEFINITION 1.2.5. The *regulator* $R_F(\alpha_1, \alpha_2, \dots, \alpha_r)$ of a set $\{\alpha_1, \alpha_2, \dots, \alpha_r\}$ of r independent units is $|\det \mathfrak{R}|$, where $\mathfrak{R} = \mathfrak{R}(\alpha_1, \alpha_2, \dots, \alpha_r)$ is the r-by-r matrix with (i,j)-entry $c_i \log|\sigma_i(\alpha_j)|$.

REMARK 1.2.6. Exactly one archimedean place is omitted in the definition of the regulator. For any $\alpha \in E_F$, one has

$$\sum_{i=1}^{r+1} c_i \log|\sigma_i(\alpha)| = \log \prod_{i=1}^{r+1} |\sigma_i(\alpha)|^{c_i} = 0$$

by the product formula, so the rows of the matrix determining the regulator sum to the what would have been the row corresponding to the embedding that is omitted. The choice of σ_i and their ordering are then seen by the usual rules for the effect of row operations on determinants to not affect the absolute value of the determinant of the matrix in question.

In particular, we have the following.

LEMMA 1.2.7. *For a set $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ of $r = \operatorname{rank}_{\mathbb{Z}} E_F$ independent units, $R_F(\alpha_1, \alpha_2, \ldots, \alpha_r)$ is the absolute value of the determinant of the linear transformation $\kappa_0 \colon E_F \otimes_{\mathbb{Z}} \mathbb{R} \to V_0$ relative to the basis of $E_F \otimes_{\mathbb{Z}} \mathbb{R}$ given by the α_i and the basis of V_0 given by $\sigma_j - \frac{1}{r+1}\sum_{k=1}^{r+1} \sigma_k$ for $1 \leq j \leq r$.*

DEFINITION 1.2.8. Let A and B be subgroups of an abelian group.

a. We say that A and B are *commensurable* if A and B are of finite index in $A + B$.

b. If A and B are commensurable, then we define the *relative index* of A in B by

$$(B : A) = [A + B : A] \cdot [A + B : B]^{-1}.$$

The following is easily verified.

LEMMA 1.2.9. *Let A and B be finitely generated subgroups of a vector space V over a subfield E of $\mathbb{C}$. If A and B are commensurable, then there exists an E-linear automorphism T of V such that $T(A) = B$, and for any such T, we have $(B : A) = |\det(T)|$.*

LEMMA 1.2.10. *Suppose that $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ and $\{\beta_1, \beta_2, \ldots, \beta_r\}$ are independent sets of r units in F, where $r = \operatorname{rank}_{\mathbb{Z}} E_F$. Let*

$$A = \mu(F) \cdot \langle \alpha_1, \alpha_2, \ldots, \alpha_r \rangle \quad \text{and} \quad B = \mu(F) \cdot \langle \beta_1, \beta_2, \ldots, \beta_r \rangle.$$

Then

$$\frac{R_F(\beta_1, \beta_2, \ldots, \beta_r)}{R_F(\alpha_1, \alpha_2, \ldots, \alpha_r)} = (B : A).$$

PROOF. Let $V = E_F \otimes_{\mathbb{Z}} \mathbb{R}$. There exists an automorphism T of V carrying the image of A in V to the image of B. Since both A and B contain $\mu(F)$, we have $(B : A) = |\det T|$. On the other hand, κ_0 is an $\mathbb{R}$-linear isomorphism, so

$$\frac{R_F(\beta_1, \beta_2, \ldots, \beta_r)}{R_F(\alpha_1, \alpha_2, \ldots, \alpha_r)} = \frac{|\det(\kappa_0 \circ T)|}{|\det \kappa_0|} = |\det T|,$$

with the determinant taken relative to the bases of Lemma 1.2.7. □

COROLLARY 1.2.11. *If $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ and $\{\beta_1, \beta_2, \ldots, \beta_r\}$ are independent sets in E_F with images generating the same subgroup of $E_F/\mu(F)$, then*

$$R_F(\alpha_1, \alpha_2, \ldots, \alpha_r) = R_F(\beta_1, \beta_2, \ldots, \beta_r).$$

We may then make the following definitions.

DEFINITION 1.2.12. A *fundamental set of units* of a number field F is a set $\{\alpha_1, \ldots, \alpha_r\}$ of r units in E_F such that

$$E_F = \mu(F) \cdot \langle \alpha_1, \alpha_2, \ldots, \alpha_r \rangle.$$

DEFINITION 1.2.13. The *regulator* R_F of a number field F is $R_F(\alpha_1, \alpha_2, \ldots, \alpha_r)$ for any fundamental set of units $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ of F.

We also need the following notation.

NOTATION 1.2.14. Let w_F denote the number of roots of unity in a number field F.

Now that we have defined the regulator, we can describe the residue at $s = 1$ of the Dedekind zeta function.

THEOREM 1.2.15 (Analytic class number formula). *For a number field F, one has*

$$\lim_{s \to 1} (s-1)\zeta_F(s) = \frac{2^{r_1(F)}(2\pi)^{r_2(F)} h_F R_F}{w_F |d_F|^{1/2}}.$$

1.3. Finite Galois extensions

Suppose that E/F is a finite Galois extension, and let $G = \mathrm{Gal}(E/F)$. Then Cl_E becomes a G-module via the action $\sigma([\mathfrak{a}]) = [\sigma\mathfrak{a}]$ for $\sigma \in G$ and $\mathfrak{a} \in I_E$, where

$$\sigma\mathfrak{a} = \{\sigma(a) \mid a \in \mathfrak{a}\} \in I_E.$$

The Galois group $\mathrm{Gal}(H_E/E)$ is a G-module too, but to see this requires a little bit of work.

PROPOSITION 1.3.1. *Let E be a finite Galois extension of F. Then H_E/F is Galois.*

PROOF. Let $\widetilde{H_E}$ denote the Galois closure of H_E as an extension of F. Let $G = \mathrm{Gal}(E/F)$. For $\sigma \in G$, let $\tilde{\sigma}$ denote a lift of σ to $\mathrm{Gal}\left(\widetilde{H_E}/F\right)$. Note that the field $\tilde{\sigma}(H_E)$ is independent of the choice of lift $\tilde{\sigma}$ of σ, as any element in $\mathrm{Gal}\left(\widetilde{H_E}/E\right)$ necessarily preserves the subfield H_E of $\widetilde{H_E}$, as H_E/E is Galois.

Next, we claim that

$$\widetilde{H_E} = \prod_{\sigma \in G} \tilde{\sigma}(H_E).$$

It suffices to show that $\prod_{\sigma \in G} \tilde{\sigma}(H_E)/F$ is Galois by the minimality of $\widetilde{H_E}$ as a Galois extension of F. For this, note that for any $\delta \in \mathrm{Gal}\left(\widetilde{H_E}/F\right)$, one has

$$\delta\tilde{\sigma}(H_E) = \tilde{\sigma'}(H_E),$$

where $\sigma' = \delta|_E \sigma \in G$, by the independence of conjugates of H_E from the choice of lift. This proves the claim. It then follows that $\tilde{H_E}/E$ is abelian, since each $\tilde{\sigma}(H_E)/E$ is. That is, any $\tau \in \mathrm{Gal}(\tilde{\sigma}(H_E)/E)$ has the property that $\tilde{\sigma}|_{H_E}^{-1} \tau \tilde{\sigma}|_{H_E} \in \mathrm{Gal}(H_E/E)$, and the latter group is abelian.

Now, let I_v be the inertia group at a prime v of E in the abelian extension $\mathrm{Gal}\left(\widetilde{H_E}/E\right)$. If I_v is nontrivial, then its image in some $\mathrm{Gal}(\tilde{\sigma}(H_E)/E)$ must be as well. Then $\tilde{\sigma}^{-1} I_v \tilde{\sigma}$ has nontrivial image in $\mathrm{Gal}(H_E/E)$. Since the former group equals the inertia group $I_{\sigma^{-1}v}$ and H_E/E is unramified, this image must be trivial. Therefore $I_v = 0$, and so $\widetilde{H_E}/E$ is an unramified abelian extension of E containing H_E. By the maximality of H_E, we have $\widetilde{H_E} = H_E$, as desired. □

Consequently, if E/F is finite Galois with group G, then $\mathrm{Gal}(H_E/E)$ becomes a G-module for the conjugation action: $\sigma \in G$ acts on $\tau \in \mathrm{Gal}(H_E/E)$ by sending it to $\sigma\tau\sigma^{-1}$. The following is then a consequence of class field theory.

PROPOSITION 1.3.2. *For E/F finite Galois with Galois group G, then Artin map ϕ_E is G-equivariant (i.e., a G-module homomorphism), which is to say that*

$$\phi_E([\sigma\mathfrak{a}]) = \sigma\phi_E([\mathfrak{a}])\sigma^{-1}$$

for all $\sigma \in G$ and $\mathfrak{a} \in I_E$.

DEFINITION 1.3.3. For E/F finite Galois, we define a map

$$j_{E/F} \colon \mathrm{Cl}_F \to \mathrm{Cl}_E, \qquad j_{E/F}([\mathfrak{a}]) = [\mathfrak{a}\mathscr{O}_E]$$

and the norm map

$$N_{E/F} \colon \mathrm{Cl}_E \to \mathrm{Cl}_F, \qquad N_{E/F}([\mathfrak{a}]) = \left[\left(\prod_{\sigma \in G} \sigma(\mathfrak{a})\right) \cap \mathscr{O}_F\right].$$

Our goal in this section will be to study these maps.

LEMMA 1.3.4. *Let p be a prime, and let A_K denote the p-part of the class group of any number field K. If the order of G is prime to p , then the maps*

$$A_F \to A_E^G \quad \text{and} \quad (A_E)_G \to A_F$$

defined by $j_{E/F}$ and $N_{E/F}$, respectively, are isomorphisms.

PROOF. Note that $N_{E/F} \circ j_{E/F} = |G|$, so $j_{E/F}$ is injective on A_F and the image of $N_{E/F}$ contains A_F. Let $\mathbb{Z}' = \mathbb{Z}[|G|^{-1}]$, and note that A_E is a $\mathbb{Z}'[G]$-module. Define an idempotent

$$\varepsilon_G = \frac{1}{|G|} N_G \in \mathbb{Z}'[G].$$

Since $\varepsilon_G A_E = A_E^G$, the group A_E^G is both a submodule and a quotient of A_E. Note that $|G|\varepsilon_G = j_{E/F} \circ N_{E/F}$, which forces $j_{E/F}$ to have image A_E^G on A_F. The map $A_F \to A_E^G$ induced by $j_{E/F}$ is therefore an isomorphism. As A_E is finite, both A_E^G and $(A_E)_G$ have the same order, so therefore now the same order as A_F. Since $N_{E/F}$ induces a surjective map $(A_E)_G \to A_F$, that map must also be an isomorphism. □

For instance, we have that $A^{\Delta}_{\mathbb{Q}(\mu_p)} = 0$ for any prime p, as p is prime to $[\mathbb{Q}(\mu_p) : \mathbb{Q}] = p-1$.

PROPOSITION 1.3.5. *Let E/F be a finite Galois extension of number fields with Galois group G. There is a canonical exact sequence*

$$0 \to \ker j_{E/F} \to H^1(G, \mathscr{O}_E^\times) \to I_E^G/I_F \to \mathrm{Cl}_E^G/j_{E/F}(\mathrm{Cl}_F) \to H^1(G, P_E).$$

PROOF. By Hilbert's Theorem 90, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathscr{O}_F^\times & \longrightarrow & F^\times & \longrightarrow & P_F & \longrightarrow & 0 \\ & & \| & & \| & & \downarrow & & \\ 0 & \longrightarrow & \mathscr{O}_F^\times & \longrightarrow & F^\times & \longrightarrow & P_E^G & \to H^1(G, \mathscr{O}_E^\times) & \longrightarrow 0, \end{array}$$

and it provides an isomorphism $H^1(G, \mathscr{O}_E^\times) \cong P_E^G/P_F$. Noting this and applying the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_F & \longrightarrow & I_F & \longrightarrow & \mathrm{Cl}_F & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & P_E^G & \longrightarrow & I_E^G & \longrightarrow & \mathrm{Cl}_E^G & \to H^1(G, P_E), & \end{array}$$

we obtain the desired exact sequence. □

Note that the map $\ker j_{E/F} \to H^1(G, \mathscr{O}_E^\times)$ is given explicitly by taking $[\mathfrak{a}]$ to a cocycle $\sigma \mapsto \alpha^{\sigma-1}$, where $\alpha \in E^\times$ satisfies $(\alpha) = \mathfrak{a}\mathscr{O}_E$. The map $H^1(G, \mathscr{O}_E^\times) \to I_E^G/I_F$ is given by taking a cocycle f to the image of an element $(\alpha) \in I_E^G$ with $f(\sigma) = \alpha^{\sigma-1}$ for all $\sigma \in G$.

DEFINITION 1.3.6. An ideal in I_F with class in the kernel of $j_{E/F}$ is said to capitulate in the extension E/F. The kernel of $j_{E/F}$ is known as the capitulation kernel.

LEMMA 1.3.7. *Let E/F be a Galois extension of number fields with Galois group G. The cokernel of $N_{E/F}$ is canonically isomorphic to the Galois group of the maximal unramified abelian subextension of F inside E.*

PROOF. The norm map on ideal classes factors the the G-coinvariant group $(\mathrm{Cl}_E)_G$ of Cl_F. We consider the complex

$$(\mathrm{Cl}_E)_G \xrightarrow{N_{E/F}} \mathrm{Cl}_F \to \mathrm{coker}\, N_{E/F} \to 0.$$

Using the Artin map, we may write the latter complex as

$$\mathrm{Gal}(H_E/E)_G \to \mathrm{Gal}(H_F/F) \to \mathrm{coker} N_{E/F} \to 0,$$

where the first map is restriction, and therefore has image $\mathrm{Gal}(H_F/E \cap H_F)$. It follows that

$$\mathrm{coker} N_{E/F} \cong \mathrm{Gal}(H_F \cap E/F),$$

as desired. □

Lemma 1.3.7 has the following immediate corollary.

COROLLARY 1.3.8. *If E/F is totally ramified at any prime, then $N_{E/F}$ is surjective.*

Now suppose that E/F is abelian. Let I_v denote the inertia group in $G = \mathrm{Gal}(E/F)$ at a prime v of F, and let

$$\Sigma_{E/F} : \bigoplus_v I_v \to G$$

denote the map that is the product of the natural inclusions.

PROPOSITION 1.3.9. *Let E/F be an abelian extension of number fields with Galois group G. Then there is an exact sequence*

$$\ker \Sigma_{E/F} \to Q_{E/F} \xrightarrow{N_{E/F}} \mathrm{Cl}_F \to \mathrm{coker} \Sigma_{E/F} \to 0,$$

where $Q_{E/F}$ is the quotient of Cl_E by its subgroup that is taken to the commutator subgroup of $\mathrm{Gal}(H_E/F)$ under the Artin map.

PROOF. The exactness outside of $(\mathrm{Cl}_E)'$ follows from Lemma 1.3.7, since $\mathrm{coker} \Sigma_{E/F} \cong \mathrm{Gal}(H_F \cap E/F)$ by definiton.

We define

$$\ker \Sigma_{E/F} \to Q_{E/F}$$

as follows. Employing the Artin map, we have canonical isomorphisms

$$Q_{E/F} \cong \mathrm{Gal}(H_E/E)/[\mathrm{Gal}(H_E/F), \mathrm{Gal}(H_E/F)] \cong \mathrm{Gal}(L/E),$$

where L is the maximal unramified extension of E that is abelian over F. Let J_v denote the inertia group at a prime w over v in $\mathrm{Gal}(L/F)$. As L/E is unramified, J_v maps isomorphically to I_v under restriction. We have a map

$$\bigoplus_v J_v \to \mathrm{Gal}(L/F)$$

given by the product of the canonial inclusions, and the map from $\bigoplus_v I_v$ is then given by the identifications $I_v \cong J_v$. Since $\ker \Sigma_{E/F}$ lands in $\mathrm{Gal}(L/E)$ under this map, we have the desired map.

It remains to check exactness at $Q_{E/F}$. Again, we use the Artin isomorphism to see that the kernel of the map to Cl_F is precisely $\mathrm{Gal}(L/E \cdot H_F)$. On the other hand, the image of $\ker \Sigma_{E/F}$ in $\mathrm{Gal}(L/E)$ is the intersection with $\mathrm{Gal}(L/E)$ of the subgroup of $\mathrm{Gal}(L/F)$ generated by its inertia groups. As L/F is abelian and H_F is the Hilbert class field of F, this is precisely $\mathrm{Gal}(L/E \cdot H_F)$. □

We have the following interesting corollary.

COROLLARY 1.3.10. *Let E/F be a cyclic p-extension, and suppose that there is at most one prime of F that ramifies in it. Then the map $(\mathrm{Cl}_E)_G \to \mathrm{Cl}_F$ induced by $N_{E/F}$ is injective.*

PROOF. Since E/F is cyclic, the quotient $Q_{E/F}$ of Proposition 1.3.9 equals $(\mathrm{Cl}_E)_G$. Since $\bigoplus_{v \in S} I_v$ is either I_v at the unique ramified prime, or 0 if there is no ramified prime, the map $\Sigma_{E/F}$ is injective. □

In the case that $|G|$ divides the order of p, we can give another nice consequence. First, we require the following lemma.

LEMMA 1.3.11. *Suppose that E/F is a finite Galois p-extension ramified at no more than one prime of F. If E/F is nonabelian, suppose further that, if there is such a prime, that it is nonsplit in the extension. Then if $A_F = 0$, we have $A_E = 0$ as well.*

PROOF. We begin with the case that $G = \mathrm{Gal}(E/F)$ is abelian. By Corollary 1.3.10, the map $(A_E)_G \to A_F$ is injective, and therefore $(A_E)_G = 0$. Thus, we have

$$A_E/\mathfrak{m}_G A_E = (A_E)_G/p(A_E)_G = 0.$$

Noting Proposition 2.3.7, Nakayama's lemma then tells us that $A_E = 0$.

Since any finite p-group has a finite filtration with abelian (or even cyclic) graded quotients, the result in general follows from the abelian case by recursion, noting that by assumption there is at most one prime that ramifies in each intermediate extension. □

We illustrate the use of this with the following interesting example.

EXAMPLE 1.3.12. Let $F = \mathbb{Q}(\mu_p)$ and $E = F(p^{1/p})$. Then this extension is totally ramified of degree p at the unique prime above p in F, which is $(1 - \zeta_p)$ for a primitive pth root of unity ζ_p. Therefore, we have that $(A_E)_G \cong A_F$ via the norm map. For a prime p such that $A_F = 0$, which is known as a regular prime (e.g., all primes less than 37), Lemma 1.3.11 implies that $A_E = 0$. When $p = 37$, it turns out that $A_F = \mathrm{Cl}_F \cong \mathbb{Z}/37\mathbb{Z}$, and in fact we have that A_E is isomorphic to $\mathbb{Z}/37\mathbb{Z}$ as well.

To go even further, it is useful to restrict to the case of a cyclic extension. We begin with the following useful result.

PROPOSITION 1.3.13. *Let E/F be a cyclic extension of number fields. Then*

$$N_{E/F}E^\times = F^\times \cap \bigcap_v N_{E_w/F_v}E_w^\times,$$

where v runs over all primes of F and w is some prime of E above v.

PROOF. Let G_v denote the decomposition group in G at any w over v. Choose a set S of representatives of $G_v\backslash G$. For $a \in E^\times$, we have

$$N_{E/F}(a) = N_{E_w/F_v}\left(\prod_{\sigma\in S}\sigma a\right),$$

so every global norm is a local norm everywhere.

Recall the following exact sequence for the Brauer group of E/F:

$$0 \to H^2(G,E^\times) \to \bigoplus_v H^2(G_v,E_w^\times) \to \frac{1}{|G|}\mathbb{Z}/\mathbb{Z},$$

where G_v denotes the decomposition group in G at any w over v. By the periodicity of Tate cohomology of a cyclic group, this becomes

$$0 \to \hat{H}^0(G,E^\times) \to \bigoplus_v \hat{H}^0(G_v,E_w^\times) \to \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}.$$

In particular, we have an injection

$$F^\times/N_{E/F}E^\times \hookrightarrow \bigoplus_v F_v^\times/N_{E_w/F_v}E_w^\times.$$

Therefore, if $a \in F^\times$ is a local norm everywhere, it is a global norm, as desired. □

Note that an element $a \in F^\times$ is automatically a local norm at any prime where E/F is unramified and the valuation of a at that prime is trivial. Hence, there are actually only finitely many places to check that a is a local norm to see that it is a global one.

We now derive a nine-term exact sequence that gives us information on the behavior of class groups in cyclic extensions. A proof is possible by making use of Tate cohomology, as found in the appendix to [**HS**], but we give a more explicit proof.

THEOREM 1.3.14. *Let E/F be a cyclic extension of number fields, and let G be its Galois group. Let I_v denote the inertia group in G at a prime v of F, and let*

$$\Sigma_{E/F}\colon \bigoplus_v I_v \to G$$

denote the map that is the product of the natural inclusions. Then we have an exact sequence

$$0 \to \ker j_{E/F} \to H^1(G, \mathscr{O}_E^\times) \to I_E^G/I_F \to \mathrm{Cl}_E^G/j_{E/F}(\mathrm{Cl}_F)$$
$$\to \mathscr{O}_F^\times/N_{E/F}\mathscr{O}_E^\times \to \ker\Sigma_{E/F} \to (\mathrm{Cl}_E)_G \xrightarrow{N_{E/F}} \mathrm{Cl}_F \to \mathrm{coker}\,\Sigma_{E/F} \to 0.$$

Moreover, the group I_E^G/I_F is noncanonically isomorphic to $\bigoplus_v I_v$.

PROOF. By Proposition 1.3.5, we have an exact sequence

$$0 \to \ker j_{E/F} \to H^1(G, \mathscr{O}_E^\times) \to I_E^G/I_F \to \mathrm{Cl}_E^G/j_{E/F}(\mathrm{Cl}_F) \to H^1(G, P_E)$$

including the first row. By Proposition 1.3.9, the final part of the sequence beginning with $\ker\Sigma_{E/F}$ is exact.

Let σ be a generator of G. Define

$$\mathrm{Cl}_E^G/j_{E/F}(\mathrm{Cl}_F) \xrightarrow{\partial} \mathscr{O}_F^\times/N_{E/F}\mathscr{O}_E^\times$$

as the map that takes image of an ideal class $[\mathfrak{a}] \in \mathrm{Cl}_E^G$ to the image of $N_{E/F}\alpha$, where α is any generator of $\mathfrak{a}^{\sigma-1}$. To see that this is well-defined, note that if α is replaced by another generator α', then $\alpha' = \alpha u$ with $u \in \mathscr{O}_E^\times$, and

$$N_{E/F}\alpha' \cdot (N_{E/F}\alpha)^{-1} \in N_{E/F}\mathscr{O}_E^\times.$$

Moreover, if $\mathfrak{a}$ is replaced by an ideal $\mathfrak{a}'$ with the same class, then $\mathfrak{a}' = \mathfrak{a} \cdot b$ for some $b \in E^\times$. We then have

$$(\mathfrak{a}b)^{\sigma-1} = \mathfrak{a}^{\sigma-1}b^{\sigma-1} = (\alpha b^{\sigma-1}).$$

It follows that

$$N_{E/F}(\alpha b^{\sigma-1}) = N_{E/F}(\alpha).$$

Finally, if $\mathfrak{b} \in j_{E/F}(\mathrm{Cl}_F)$, then $\mathfrak{b}^{\sigma-1} = (1)$, so ∂ takes $[\mathfrak{b}]$ to 1.

We check exactness at $\mathrm{Cl}_E^G/j_{E/F}(\mathrm{Cl}_F)$. If $\mathfrak{b} \in I_E^G$, then again $\mathfrak{b}^{\sigma-1} = (1)$, so ∂ maps $[\mathfrak{b}]$ to 1. On the other hand, if ∂ takes the image of $[\mathfrak{a}]$ to $N_{E/F}\alpha = 1$, and therefore $\alpha = \beta^{\sigma-1}$ with $\sigma \in G$. We then have

$$(\mathfrak{a}\beta^{-1})^{\sigma-1} = (1),$$

which means $\mathfrak{a}\beta^{-1} \in I_E^G$. As $[\mathfrak{a}\beta^{-1}] = [\mathfrak{a}]$, we have that the image of $[\mathfrak{a}]$ is in the image of the map from I_E^G/I_F.

Next, we define

$$\mathscr{O}_F^\times/N_{E/F}\mathscr{O}_E^\times \to \ker\Big(\bigoplus_v I_v \to G\Big)$$

by the direct sum of the local reciprocity maps ρ_{E_w/F_v}. (We remark that $I_v = 0$ for all but finitely many v, so the map $\Sigma_{E/F}$ makes sense.) Since the product of the reciprocity maps at all places on a global

element is trivial, the image of this map is indeed contained in $\ker\Sigma_{E/F}$ Also, the map is well-defined since every global norm is a local norm. Note that the image of ∂ is the set of $N_{E/F}\alpha \in \mathscr{O}_F^\times$ with $\alpha \in E^\times$. Again, such elements are local norms, and map to zero under each ρ_{E_w/F_v}. Conversely, if $c \in \mathscr{O}_F^\times$ satisfies $\rho_{E_w/F_v}(c) = 1$ for every v, then $c \in N_{E_w/F_v}E_w^\times$ for all v, since c is a unit. By Theorem 1.3.13, we have that $c = N_{E/F}\alpha$ for some $\alpha \in F^\times$ with $(\alpha) = \mathfrak{a}^{\sigma-1}$ for some $\mathfrak{a} \in I_E$ and $\sigma \in G$. In other words, c is the image of the image of the class of $[\mathfrak{a}]$ under ∂.

We check exactness at $\ker\Sigma_{E/F}$. Let L denote the maximal abelian extension of E that is abelian over F. For $c \in \mathscr{O}_F^\times$, we have

$$\prod_v \rho_{L_{w'}/F_v}(c) = 1,$$

with w' lying over w. Since $\rho_{L_{w'}/F_v}(c)|_E = \rho_{E_w/F_v}(c)$, the image of c in J_v is $\rho_{L_{w'}/F_v}(c)$, and the resulting product in $\mathrm{Gal}(L/E)$ is trivial. On the other hand, suppose that $\widetilde{\sigma}_v \in J_v$ lifts some $\sigma_v \in I_v$ and

$$\prod_v \widetilde{\sigma}_v = 1.$$

Then there exist local units $c_v \in \mathscr{O}_{F_v}^\times$ for each v with $\rho_{L_{w'}/F_v}(c_v) = \widetilde{\sigma}_v$. We take $c_v = 1$ if $\widetilde{\sigma}_v = 1$. By global class field theory, the idele $\mathbf{c}$ with $\mathbf{c}_v = c_v$ for each v is the product of the norm of an idele $\mathbf{b}$ of L with an element $c \in F^\times$. Recall that

$$\mathbb{C}_F/N_{H_F/F}\mathbb{C}_{H_F} \cong \mathrm{Cl}_F,$$

so we have that

$$F^\times N_{H_F/F}\mathbb{I}_{H_F} = F^\times \prod_v \mathscr{O}_{F_v}^\times,$$

where we take $\mathscr{O}_{F_v} = F_v$ if v is archimedean. Since L contains H_F, the idele $\mathbf{b}$ may be taken to be a unit at all places. But, as each c_v is a local unit at all v and

$$(N_{L/F}\mathbf{b} \cdot c)_v = \mathbf{c}_v = c_v$$

for all v, this means that c must be a unit at all places as well. That is, $c \in \mathscr{O}_F^\times$. As $N_{L/F}\mathbf{b}$ is a local norm from E everywhere, we have

$$\rho_{E_w/F_v}(c) = \rho_{E_w/F_v}(c_v) = \sigma_v$$

for every v, as desired.

Finally, recall that I_E is the free abelian group generated by the prime ideals of $\mathscr{O}_E$. For an element of I_E to be fixed under G, every prime in its decomposition must appear with the same exponent as its conjugates. That is, I_E^G is generated by the $\prod_{i=1}^g \mathfrak{P}_i$, where $\mathfrak{P}_1, \ldots \mathfrak{P}_g$ are the primes of E lying

over a prime $\mathfrak{p}$ of F. Of course, $(\prod_{i=1}^{g}\mathfrak{P}_i)^{e_v} = \mathfrak{p}\mathscr{O}_E$, where e_v is the ramification index of the place v corresponding to $\mathfrak{p}$, so we have

$$I_E^G/I_F \cong \bigoplus_v \mathbb{Z}/e_v\mathbb{Z} \cong \bigoplus_{v\in S} I_v.$$

□

REMARK 1.3.15. Every map but the map between the two rows is canonical in the exact sequence of Theorem 1.3.14. The remaining map depends only upon a choice of generator of G. It can be made canonical by considering instead the map

$$\mathrm{Cl}_E^G / j_{E/F}(\mathrm{Cl}_F) \otimes_{\mathbb{Z}} G \to \mathscr{O}_F^\times / N_{E/F}\mathscr{O}_E^\times$$

given on the image of a tensor of $[\mathfrak{a}] \in \mathrm{Cl}_E^G$ and $\sigma \in G$ by writing $\mathfrak{a}^{\sigma-1} = \alpha\mathscr{O}_E^\times$ and taking the image of $N_{E/F}\alpha \in \mathscr{O}_F^\times$ in the quotient.

Next, we generalize the situation slightly.

NOTATION 1.3.16. For a set S of places in a number field F, we let S_f denote its subset of finite places and S_∞ its subset of infinite places.

DEFINITION 1.3.17. Let S denote a set of places of F.

a. The *S-class group* $\mathrm{Cl}_{F,S}$ of F is the quotient of the class group by the subgroup generated by the classes of the finite primes in S.

b. The *Hilbert S-class field* $H_{F,S}$ of F is the maximal unramified abelian extension of F in which all primes in S split completely.

c. The *ring of S-integers* $\mathscr{O}_{F,S}$ of F is

$$\mathscr{O}_{F,S} = \{a \in F \mid v_\mathfrak{p}(a) \geq 0 \text{ for all } \mathfrak{p} \notin S_f\},$$

where $\mathfrak{p}$ is used to denote a finite prime of F and $v_\mathfrak{p}$ its additive valuation.

d. The *S-ideal group* $I_{F,S}$ is the group of nonzero fractional ideals in $\mathscr{O}_{F,S}$, and the S-principal ideal group $P_{F,S}$ is the subgroup of principal fractional ideals.

e. The *S-unit group* in F is $\mathscr{O}_{F,S}^\times$.

NOTATION 1.3.18. If S is a set of primes of F and let E/F is a finite extension, then we let S_E denote the set of places of E lying over those in S. For brevity, we denote $\mathscr{O}_{E,S_E}$, Cl_{F,S_E}, and so on more succinctly by $\mathscr{O}_{E,S}$, $\mathrm{Cl}_{E,S}$, and so on similarly. That is, we use S in the subscript to denote S_E. If E/F is algebraic, we may still speak of its S-integers $\mathscr{O}_{E,S}$ as the union of S-integers in the finite subextensions of F in E.

Let us fix a set of places of S for the rest of this section.

REMARK 1.3.19. The Artin isomorphism ϕ_F induces an isomorphism

$$\phi_{F,S}\colon \mathrm{Cl}_{F,S} \to \mathrm{Gal}(H_{F,S}/F).$$

We have an analogue of the exact sequence of Theorem 1.3.14 for S-class groups and S-units. The proof is much as before, and is therefore omitted.

THEOREM 1.3.20. *Let E/F be a cyclic extension of number fields, and let G be its Galois group. Let I_v (resp., G_v) denote the inertia group (resp., decomposition group) in G at a prime v of F, and let*

$$\Sigma^S_{E/F}\colon \bigoplus_{v\notin S} I_v \oplus \bigoplus_{v\in S} G_v \to G$$

denote the map that is the product of the natural inclusions. Then we have an exact sequence

$$\begin{aligned} 0 \to \ker(\mathrm{Cl}_{F,S} \xrightarrow{j_{E/F}} \mathrm{Cl}_{E,S}) \to H^1(G, \mathscr{O}^\times_{E,S}) \to I^G_{E,S}/I_{F,S} \to \mathrm{Cl}^G_{E,S}/j_{E/F}(\mathrm{Cl}_{F,S}) \\ \to \mathscr{O}^\times_{F,S}/N_{E/F}\mathscr{O}^\times_{E,S} \to \ker\Sigma^S_{E/F} \to (\mathrm{Cl}_{E,S})_G \xrightarrow{N_{E/F}} \mathrm{Cl}_{F,S} \to \mathrm{coker}\,\Sigma^S_{E/F} \to 0. \end{aligned}$$

1.4. Kummer theory

For a set of S primes of F, we let S_f denote the set of finite places of F in S, we let S_∞ denote the set of archimedean places, and for any $n \geq 1$, we let S_n denote the set of primes of S above p for any prime p dividing n. If E is an extension of F, we generally also use the symbol S to denote the set of primes S_E of E above those in S. We will let V denote the set of all primes of F, so we may speak of V_∞ and so forth. For brevity, let us set $V_{n\infty} = V_n \cup V_\infty$.

DEFINITION 1.4.1. We say that an extension E of F is *S-ramified* if it is unramified outside of the places in S.

LEMMA 1.4.2. *There exists a maximal S-ramified extension F_S of F, and it is Galois over F.*

PROOF. A union of S-ramified extensions is S-ramified, so the existence of F_S is clear. If E is an S-ramified finite degree extension of F, then so is any conjugate of E over F in an algebraic closure $\overline{F}$ of F containing E, as the inertia degrees at conjugate primes above p in E and $\sigma(E)$ are the same (and similarly for real places). The product

$$\prod_{\sigma\colon E\hookrightarrow\overline{F}} \sigma(E)$$

is Galois (in fact, it is the Galois closure of E in $\overline{F}$) and also S-ramified as a compositum of S-ramified extensions. Therefore, F_S is a union of finite Galois subextensions, hence itself Galois. □

DEFINITION 1.4.3. We use $G_{F,S}$ to denote the Galois group $\mathrm{Gal}(F_S/F)$, i.e., the Galois group of the maximal S-ramified extension F_S of F.

Kummer theory in S-ramified extensions has as its basis the following proposition.

PROPOSITION 1.4.4. *Let S be a set of primes of F. We have a canonical isomorphism*

$$\mathrm{Cl}_{F,S} \xrightarrow{\sim} H^1(G_{F,S}, \mathscr{O}_{F_S,S}^{\times}),$$

given by taking an ideal class $[\mathfrak{a}]$ to the cocycle that takes $\sigma \in G_{F,S}$ to $\alpha^{\sigma-1}$, where α is a generator of $\mathfrak{a}\mathscr{O}_{F_S,S}$.

PROOF. To reduce clutter in the notation, let us set $\mathscr{G} = G_{F,S}$ and $\Omega = F_S$. A similar argument to that of the proof of Proposition 1.3.5 produces an isomorphism

$$P_{\Omega,S}^{\mathscr{G}}/P_{F,S} \xrightarrow{\sim} H^1(\mathscr{G}, \mathscr{O}_{E,S}^{\times})$$

that takes (α) to $\sigma \mapsto \alpha^{\sigma-1}$. Again similarly to before, we have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_{F,S} & \longrightarrow & I_{F,S} & \longrightarrow & \mathrm{Cl}_{F,S} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & P_{\Omega,S}^{\mathscr{G}} & \longrightarrow & I_{\Omega,S}^{\mathscr{G}} & \longrightarrow & \mathrm{Cl}_{\Omega,S}^{\mathscr{G}} & & \end{array} \tag{1.4.1}$$

The lower row arises as a direct limit of like sequences for intermediate finite extensions E of F in Ω. However, since S contains the finite primes that are ramified in any such extension E/F, the map $I_{F,S} \to I_{E,S}^{\mathscr{G}}$ is not merely an injection, but an isomorphism. Moreover, $j_{\Omega/F}$ is the zero map, since Ω contains H_F by definition, and every ideal in I_F becomes principal in H_F. Hence, the snake lemma provides an isomorphism

$$\mathrm{Cl}_{F,S} \to P_{\Omega,S}^{\mathscr{G}}/P_{F,S}$$

taking $[\mathfrak{a}]$ to (α) where $(\alpha) = \mathfrak{a}\mathscr{O}_{\Omega,S}$. □

PROPOSITION 1.4.5. *Suppose that S contains $V_{n\infty}$. Then there is a canonical exact sequence*

$$1 \to \mathscr{O}_{F,S}^{\times}/\mathscr{O}_{F,S}^{\times n} \to H^1(G_{F,S}, \mu_n) \to \mathrm{Cl}_{F,S}[n] \to 0.$$

PROOF. For any $\alpha \in \mathscr{O}_{F_S,S}^{\times}$, the extension $F_S(\alpha^{1/n})/F_S$ is unramified outside of S and therefore trivial, as the only primes that can ramify in such a Kummer extension are the real places, those $\mathfrak{p}$ with $v_{\mathfrak{p}}(\alpha) \neq 0$, and those primes dividing n, all of which are contained in S. We then have that

$$1 \to \mu_n \to \mathscr{O}_{F_S,S}^{\times} \xrightarrow{n} \mathscr{O}_{F_S,S}^{\times} \to 1$$

is exact, and the result follows immediately from the exact sequence

$$H^0(G_{F,S},\mathscr{O}_{F_S,S}^\times)\xrightarrow{n}H^0(G_{F,S},\mathscr{O}_{F_S,S}^\times)\to H^1(G_{F,S},\mu_n)\to H^1(G_{F,S},\mathscr{O}_{F_S,S}^\times)\xrightarrow{n}H^1(G_{F,S},\mathscr{O}_{F_S,S}^\times).$$

□

In the case that $S=\varnothing$, we have the following.

LEMMA 1.4.6. *Fix $n\geq 1$ such that F contains μ_n, and let $B_n\leq\mathscr{O}_F^\times$ be the subgroup*

$$B_n=\{a\in\mathscr{O}_F^\times \mid F(a^{1/n})/F \text{ is unramified}\}.$$

There is a canonical exact sequence

$$1\to B_n/\mathscr{O}_F^{\times n}\to H^1(G_{F,\varnothing},\mu_n)\to \mathrm{Cl}_F[n].$$

PROOF. From the short exact sequence

$$1\to\mu_n\to\mathscr{O}_{F_\varnothing}^\times\xrightarrow{n}\mathscr{O}_{F_\varnothing}^{\times n}\to 1,$$

we obtain an exact sequence

$$\mathscr{O}_F^\times\xrightarrow{n}\mathscr{O}_{F_\varnothing}^{\times n}\cap\mathscr{O}_F^\times\to H^1(G_{F,\varnothing},\mu_n)\to H^1(G_{F,\varnothing},\mathscr{O}_{F_\varnothing}^\times)\xrightarrow{n}H^1(G_{F,\varnothing},\mathscr{O}_{F_\varnothing}^{\times n}). \tag{1.4.2}$$

As the nth power map $\mathscr{O}_{F_\varnothing}^\times\xrightarrow{n}\mathscr{O}_{F_\varnothing}^\times$ takes values in $\mathscr{O}_{F_\varnothing}^{\times n}$, the kernel of the rightmost map in (1.4.2) is contained in the kernel of

$$H^1(G_{F,\varnothing},\mathscr{O}_{F_\varnothing}^\times)\xrightarrow{n}H^1(G_{F,\varnothing},\mathscr{O}_{F_\varnothing}^\times),$$

which is isomorphic to $\mathrm{Cl}_F[n]$ by Proposition 1.4.4. Noting that

$$B_n=F_\varnothing^{\times n}\cap\mathscr{O}_F^\times=\mathscr{O}_{F_\varnothing}^{\times n}\cap\mathscr{O}_F^\times,$$

equation (1.4.2) yields the result. □

DEFINITION 1.4.7. A number field F is said to be *abelian* if it is an abelian extension of $\mathbb{Q}$.

DEFINITION 1.4.8. A number field F is said to be *totally real* if it has no complex places.

REMARK 1.4.9. There exits a maximal totally real subfield F^+ of any number field F, as the compositum of any two totally real fields is totally real.

DEFINITION 1.4.10. A number field F is *CM* if it has no real places and is a degree 2 extension of F^+.

EXAMPLE 1.4.11. Let $n \geq 3$. Then the cyclotomic field $\mathbb{Q}(\mu_n)$ is CM, and

$$\mathbb{Q}(\mu_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1}),$$

where ζ_n is a primitive nth root of unity. As a consequence of this and the Kronecker-Weber theorem, every abelian field is either totally real or CM.

Fix a CM field F, and let τ be the nontrivial element of $\mathrm{Gal}(F/F^+)$. Given a $\mathbb{Z}[\mathrm{Gal}(F/F^+)]$-module A, we have submodules

$$A^{\pm} = \{a \in A \mid \tau(a) = \pm a\}.$$

Note that

$$A^+ \cap A^- = A[2].$$

and $A/(A^+ + A^-)$ is 2-torsion. If multiplication by 2 is invertible on A, then

$$A \cong A^+ \oplus A^-, \qquad a \mapsto \frac{a+\tau(a)}{2} + \frac{a-\tau(a)}{2}.$$

LEMMA 1.4.12. *The groups $\mathscr{O}_F^\times$ and $(\mathscr{O}_F^\times)^+$ have the same $\mathbb{Z}$-rank, and $(\mathscr{O}_F^\times)^-$ is the group $\mu(F)$ of roots of unity in F.*

PROOF. The first statement is an immediate consequence of Dirichlet's unit theorem. Since it holds, $(\mathscr{O}_F^\times)^-$ consists only of elements of finite order, which is to say, roots of unity. Since every root of unity ξ satisfies $\tau(\xi) = \xi^{-1}$, we have the result. □

We note that for an odd prime p, the map j_{F/F^+} provides a canonical identification of A_{F^+} with A_F^+ by Lemma 1.3.4.

LEMMA 1.4.13. *The map $\mathrm{Cl}_{F^+} \to \mathrm{Cl}_F^+$ induced by j_{F/F^+} has kernel of order dividing 2.*

PROOF. Note that if $\tau(x)x = 1$ for $x \in \mathscr{O}_F^\times$, then x must be a root of unity. On the other hand, the group of $\tau(y)y^{-1}$ with $y \in \mathscr{O}_F^\times$ contains $\mu(F)^2 = \mu(F)^{\tau-1}$. Thus $H^1(G, \mathscr{O}_F^\times) \cong \hat{H}^{-1}(G, \mathscr{O}_F^\times)$ is isomorphic to a quotient of $\mu(F)/\mu(F)^2$. The result then follows from Proposition 1.3.5. □

REMARK 1.4.14. If L and M are Galois extensions of a field K with L contained in M, then $\mathrm{Gal}(L/K)$ acts on $H^i(\mathrm{Gal}(M/L), A)$ for any $\mathbb{Z}_p[\mathrm{Gal}(M/K)]$-module A. The action is induced by the following action of $\tau \in \mathrm{Gal}(M/K)$ on a cochain $f \in C^i(\mathrm{Gal}(M/L), A)$:

$$(\tau \cdot f)(\sigma_1, \ldots, \sigma_i) = \tau \cdot f(\tau^{-1}\sigma_1\tau, \ldots, \tau^{-1}\sigma_i\tau).$$

On cohomology, this action factors through an action on $\mathrm{Gal}(L/K)$ since, on $\mathrm{Gal}(M/L)$, this action is the conjugation action on cohomology, which is trivial.

For a finitely generated abelian group A, let us use $r(A)$ to denote its rank and

$$r_p(A) = \dim_{\mathbb{F}_p} A[p]$$

to denote its p-rank for a prime p.

THEOREM 1.4.15. *Let F be a CM field such that $\mu_p \subset F$ for an odd prime p. We then have*

$$r_p(\mathrm{Cl}_F^+) - \delta \leq r_p(\mathrm{Cl}_F^-) \leq r_p(\mathrm{Cl}_F^+) + r(\mathscr{O}_F^\times),$$

where $\delta = 0$ if $F(\mu(F)^{1/p})/F$ is ramified at p and 1 otherwise.

PROOF. Note that

$$H^1(G_{F,\varnothing}, \mu_p) \cong \mathrm{Hom}(\mathrm{Gal}(H_F/F), \mu_p),$$

and

$$\mathrm{Hom}(\mathrm{Gal}(H_F/F), \mu_p)^\pm \cong \mathrm{Hom}(\mathrm{Cl}_F, \mu_p)^\pm \cong \mathrm{Hom}(\mathrm{Cl}_F^\mp, \mu_p),$$

as τ acts on μ_p by inversion. Combining this with Lemma 1.4.6, with $B = B_p$ as in said lemma, we have

$$r_p(\mathrm{Cl}_F^\mp) = r_p(H^1(G_{F,\varnothing}, \mu_p)^\pm) \leq r_p(\mathrm{Cl}_F^\pm) + r_p((B/\mathscr{O}_F^{\times p})^\pm).$$

By Lemma 1.4.12, we have that $\mathscr{O}_F^\times = \mathscr{O}_F^+ \cdot \mu(F)$ and

$$r_p((B/\mathscr{O}_F^{\times p})^-) = r_p(B \cap \mu(F)) = \delta,$$

while

$$r_p((B/\mathscr{O}_F^{\times p})^+) \leq r_p((\mathscr{O}_F^\times/\mathscr{O}_F^{\times p})^+) = r((\mathscr{O}_F^\times)^+) = r(\mathscr{O}_F^\times).$$

The result follows. □

1.5. Leopoldt's conjecture

For each place v of F, Let

$$\widehat{F_v^\times} = \varprojlim_n F_v^\times/F_v^{\times p^n},$$

and consider its subgroup

$$\mathscr{U}_v = \varprojlim_n \mathscr{O}_{F_v}^\times/\mathscr{O}_{F_v}^{\times p^n}.$$

If v is finite, then $\widehat{F_v^\times} \cong \mathbb{Z}_p \oplus \mathscr{U}_v$, and $\mathscr{U}_v$ is the group of p-power roots of unity in F_v if v does not lie over p while $\mathscr{U}_v$ is the group of 1-units if v lies over p. If v is infinite, then $\mathscr{U}_v = \widehat{F_v^\times}$, and both groups are trivial unless v is real and $p = 2$, in which case they are $\mathbb{Z}/2\mathbb{Z}$.

Let us set

$$\mathscr{E}_F = \mathscr{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \varprojlim_n \mathscr{O}_F^\times/\mathscr{O}_F^{\times p^n}.$$

We may consider the natural map

$$\iota_F = (\iota_v)_{v\in V_p}\colon \mathscr{E}_F \to \bigoplus_{v\in V_p} \mathscr{U}_v.$$

Clearly, the kernel of $\mathscr{O}_F^\times \to \mathscr{O}_{F_v}^\times$ is trivial for $v \in V_p$. Yet, the problem may arise that there exist, for instance, two units $x, y \in \mathscr{O}_F^\times$ generating a rank two subgroup and $a, b \in \mathbb{Z}_p$ such that $\iota_v(x)^a \iota_v(y)^b = 1$. So, in theory, ι_F could have a kernel. This brings us to Leopoldt's conjecture.

CONJECTURE 1.5.1 (Leopoldt). *The map $\iota_F\colon \mathscr{E}_F \to \bigoplus_{v\in V_p} \mathscr{U}_v$ is injective.*

REMARK 1.5.2. We could, equivalently, consider the map

$$\iota'_F\colon \mathscr{E}_F \to \bigoplus_{v\in V_{p\infty}} \mathscr{U}_v,$$

that includes the archimdean places, setting $\mathscr{U}_v = \widehat{F_v^\times}$ for such v. The point is that $\mathscr{U}_v = 1$ for archimedean v unless $p = 2$ and v is real, in which case $\mathscr{U}_v \cong \mathbb{R}^\times/\mathbb{R}^{\times 2}$.

We have that $\ker \iota'_F \subseteq \ker \iota_F$ by definition. On the other hand, we have $(\ker \iota_F)^2 \subseteq \ker \iota'_F$. In particular, the two kernels have the same $\mathbb{Z}_p$-rank. Moreover, the 2-torsion in $\mathscr{E}_F$ is μ_2, and -1 is not in the kernel of ι_v for any v, so $\ker \iota_F = 0$ if and only if $\ker \iota'_F = 0$.

EXAMPLE 1.5.3. For $F = \mathbb{Q}$, Leopoldt's conjecture holds as $\mathscr{E}_\mathbb{Q} = 1$ for $p \neq 2$ and $\mathscr{E}_\mathbb{Q} = \mu_2$ for $p = 2$.

Let S denote a finite set of primes of F containing $V_{p\infty}$. We wish to state several equivalent forms of this conjecture. For this, we set

$$\mathscr{E}_{F,S} = \mathscr{O}_{F,S}^\times \otimes_\mathbb{Z} \mathbb{Z}_p,$$

and extend ι_F to a map

$$\iota_{F,S} = (\iota_v)_{v\in S}\colon \mathscr{E}_{F,S} \to \bigoplus_{v\in S} \widehat{F_v^\times}.$$

Let $\mathfrak{X}_{F,S}$ denote the Galois group of the maximal abelian pro-p unramified outside S extension of F. Let $\widehat{G_v^{\mathrm{ab}}}$ denote the Galois group of the maximal abelian pro-p extension of F_v for each v. The following exact sequences will be useful.

THEOREM 1.5.4. *There are two exact sequences fitting into a commutative diagram*

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \ker \iota_F & \longrightarrow & \mathscr{E}_F & \longrightarrow & \bigoplus_{v\in S} \mathscr{U}_v & \longrightarrow & \mathfrak{X}_{F,S} & \longrightarrow & A_F \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \| & & \downarrow \\
0 & \longrightarrow & \ker \iota_{F,S} & \longrightarrow & \mathscr{E}_{F,S} & \xrightarrow{\iota_{F,S}} & \bigoplus_{v\in S} \widehat{F_v^\times} & \xrightarrow{\rho_{F,S}} & \mathfrak{X}_{F,S} & \longrightarrow & A_{F,S} \longrightarrow 0,
\end{array} \tag{1.5.1}$$

where $\rho_{F,S}$ is the product over $v \in S$ of the composition of the p-completion of the local reciprocity map $\rho_v \colon \widehat{F_v^\times} \to \widehat{G_v^{\mathrm{ab}}}$ with the natural map j_v from $\widehat{G_v^{\mathrm{ab}}}$ onto the decomposition group at v in $\mathfrak{X}_{F,S}$, and where the maps $\mathfrak{X}_{F,S} \to A_F \to A_{F,S}$ are the natural quotient maps (under the indentifications given by the Artin map).

PROOF. In the horizontal sequences in the diagram (1.5.1), we note that $\operatorname{im}\rho_{F,S}$ (resp., the corresponding map in the upper sequence) is the compositum of the decomposition groups (resp., inertia groups) at all $v \in S$ in $\mathfrak{X}_{F,S}$. Being that $\mathfrak{X}_{F,S}$ already has trivial inertia groups at $v \notin S$, the quotient $\operatorname{coker}\rho_{F,S}$ is therefore the Galois group of the maximal unramified abelian p-extension of F in which all primes in S split completely (resp., maximal unramified abelian p-extension of F), and is therefore canonically isomorphic to $A_{F,S}$ (resp., A_F) via Artin reciprocity.

For the upper horizontal sequence, the exactness at $\bigoplus_{v\in S}\mathscr{U}_v$ will follow from the exactness at $\bigoplus_{v\in S}\widehat{F_v^\times}$ in the lower horizontal sequence by noting that $\mathscr{E}_F$ consists exactly of the elements of $\mathscr{E}_{F,S}$ that have image under $\iota_{F,S}$ lying in $\bigoplus_{v\in S}\mathscr{U}_v$. We are therefore reduced to proving the latter exactness.

Recall that $H^1(G_{F,S}, \mu_{p^n})$ is identified via Kummer theory with the quotient $\mathscr{B}_n/F^{\times p^n}$, where $\mathscr{B}_n$ is the subgroup of $x \in F^\times$ such that $x\mathscr{O}_{F,S} = \mathfrak{a}^{p^n}$ for some fractional ideal $\mathfrak{a}$ of $\mathscr{O}_{F,S}$. In other words, we have an exact sequence

$$1 \to \mathscr{O}_{F,S}^\times/\mathscr{O}_{F,S}^{\times p^n} \to \mathscr{B}_n/F^{\times p^n} \to A_{F,S}[p^n] \to 0.$$

It then follows from the finiteness of $A_{F,S}$ that

$$\varprojlim_n \mathscr{B}_n/F^{\times p^n} \cong \mathscr{E}_{F,S},$$

We claim that there is an exact sequence

$$\mathscr{B}_n/F^{\times p^n} \to \bigoplus_{v\in S} F_v^\times/F_v^{\times p^n} \to \mathfrak{X}_{F,S}/p^n\mathfrak{X}_{F,S},$$

where the first map is induced by the localization maps and the second map is $\rho_{F,S}$ taken modulo p^n. In that all of the terms of this sequence are finite, we can take the inverse limit as we vary n to obtain an exact sequence

$$\mathscr{E}_{F,S} \xrightarrow{\iota_{F,S}} \bigoplus_{v\in S} \widehat{F_v^\times} \xrightarrow{\rho_{F,S}} \mathfrak{X}_{F,S}, \tag{1.5.2}$$

finishing the verification of the exactness of the lower sequence.

Let us use $\rho_{n,v}$ and $j_{n,v}$ to denote the modulo p^n reductions of ρ_v and j_v for any v. Any $a \in \mathscr{B}_n$ has valuation a multiple of p^n at $v \notin S$, so $\rho_v(a)$ lies in the compositum of the inertia group and the subgroup of p^nth powers in $\widehat{G_v^{\mathrm{ab}}}$. In particular, we have that $j_{n,v}(\rho_{n,v}(a)) = 1$ for such v. Global class

field theory then tells us that

$$\prod_{v\in S} j_v(\rho_v(a)) = \prod_v j_v(\rho_v(a)) = 1,$$

which tells us that (1.5.2) is a complex.

Let M_n be the maximal S-ramified abelian extension of F of exponent p^n. Its Galois group $\mathrm{Gal}(M_n/F) \cong \mathfrak{X}_{F,S}/p^n\mathfrak{X}_{F,S}$ is the quotient of $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ by the composition of all inertia groups at primes $v \notin S$ and the p^nth powers of all of the decomposition groups. By global class field theory, we therefore have an isomorphism

$$\frac{\mathbb{I}_F}{F^\times \cdot \mathbb{I}_F^{p^n} \cdot \prod_{v\notin S} \mathscr{O}_v^\times} \xrightarrow{\sim} \mathrm{Gal}(M_n/F).$$

where for simplicity of notation, we have set $\mathscr{O}_v = \mathscr{O}_{F_v}$. Similarly, if we let L_n' be the maximal unramified abelian extension of F of exponent p^n in which every prime in S splits completely, so that $\mathrm{Gal}(L_n'/F) \cong A_{F,S}/p^nA_{F,S}$, class field theory again provides an isomorphism

$$\frac{\mathbb{I}_F}{F^\times \cdot \mathbb{I}_F^{p^n} \cdot (\prod_{v\in S} F_v^\times \times \prod_{v\notin S} \mathscr{O}_v^\times)} \xrightarrow{\sim} \mathrm{Gal}(L_n'/F).$$

We see, then, that we have isomorphisms

$$\frac{\mathbb{I}_F^{p^n} \cdot (\prod_{v\in S} F_v^\times \times \prod_{v\notin S} \mathscr{O}_v^\times)}{(F^\times \cap \mathbb{I}_F^{p^n}(\prod_{v\in S} F_v^\times \times \prod_{v\notin S} \mathscr{O}_v^\times)) \cdot \mathbb{I}_F^{p^n} \prod_{v\in S} \mathscr{O}_v^\times} \cong \frac{F^\times \cdot \mathbb{I}_F^{p^n} \cdot (\prod_{v\in S} F_v^\times \times \prod_{v\notin S} \mathscr{O}_v^\times)}{F^\times \cdot \mathbb{I}_F^{p^n} \cdot \prod_{v\notin S} \mathscr{O}_v^\times} \cong \mathrm{Gal}(M_n/L_n'),$$

where in the first step, we have used the second isomorphism theorem. Since

$$\bigoplus_{v\in S} F_v^\times/F_v^{\times p^n} \cong \frac{\mathbb{I}_F^{p^n} \cdot (\prod_{v\in S} F_v^\times \times \prod_{v\notin S} \mathscr{O}_v^\times)}{\mathbb{I}_F^{p^n} \prod_{v\in S} \mathscr{O}_v^\times}$$

and

$$\mathscr{B}_n = F^\times \cap \mathbb{I}_F^{p^n} \left(\prod_{v\in S} F_v^\times \times \prod_{v\notin S} \mathscr{O}_v^\times \right),$$

we have an exact sequence

$$\mathscr{B}_n \to \bigoplus_{v\in S} F^\times/F^{\times p^n} \to \mathrm{Gal}(M_n/L_n'),$$

where the maps agree with the maps in question, hence the result. □

REMARK 1.5.5. Theorem 1.5.4 can also be derived using Poitou-Tate duality and Kummer theory.

PROPOSITION 1.5.6. *The kernel of $\iota_{F,S}$ is contained in $\mathscr{E}_F$. In particular, Leopoldt's conjecture is equivalent to the injectivity of $\iota_{F,S}$.*

PROOF. Let $\alpha \in \ker \iota_{F,S}$. Then α may be written as

$$\alpha = \sum_{i=1}^{m} a_i \otimes c_i,$$

were $a_i \in \mathscr{O}_{F,S}^{\times}$ and $c_i \in \mathbb{Z}_p$ for each $1 \leq i \leq m$, for some $m \geq 0$. For each $v \in S_f$, we then have

$$\sum_{i=1}^{m} v(a_i)c_i = 0,$$

which means that the $c_i \in \mathbb{Z}_p$ are $\mathbb{Z}$-linearly dependent if some $v(a_i) \neq 0$. If $v(a_m) \neq 0$, without loss of generality, then $\alpha^{v(a_m)}$ may be written as a sum of $m-1$ tensors. Continuing in this way, we obtain that some nonzero integer power of α is a $\mathbb{Z}_p$-linear combination of units at v. Since there are only finitely many $v \in S$, we have $\alpha^c \in \mathscr{E}_F$ for some $c \in \mathbb{Z}$, which forces $\alpha \in \mathscr{E}_F$. □

The following theorem is also a corollary of Theorem 1.5.4 and Proposition 1.5.6, which gives in particular equivalent conditions for Leopoldt's conjecture to hold (noting that $\mathscr{E}_F$ is p-torsion free). Let $\operatorname{rank}_{\mathbb{Z}_p} A$ denote the $\mathbb{Z}_p$-rank of a finitely generated $\mathbb{Z}_p$-module A.

THEOREM 1.5.7. *The following are equivalent for a given $\delta \geq 0$:*

i. $\operatorname{rank}_{\mathbb{Z}_p} \ker \iota_F = \delta$,

ii. $\operatorname{rank}_{\mathbb{Z}_p} \operatorname{im} \iota_F = r_1(F) + r_2(F) - 1 - \delta$,

iii. $\operatorname{rank}_{\mathbb{Z}_p} \ker \iota_{F,S} = \delta$, *and*

iv. $\operatorname{rank}_{\mathbb{Z}_p} \mathfrak{X}_{F,S} = r_2(F) + 1 + \delta$.

PROOF. For $v \in S$, we have that

$$\operatorname{rank}_{\mathbb{Z}_p} \widehat{\mathscr{U}_v} = \begin{cases} [F_v : \mathbb{Q}_p] & \text{if } v \in V_p, \\ 0 & \text{if } v \in S - V_p. \end{cases}$$

We also have

$$\operatorname{rank}_{\mathbb{Z}_p} \mathscr{E}_F = r_1(F) + r_2(F) - 1$$

by Dirichlet's unit theorem, and A_F is finite. Note that

$$r_1(F) + 2r_2(F) = [F : \mathbb{Q}] = \sum_{v \in V_p} [F_v : \mathbb{Q}_p].$$

Hence, Proposition 1.5.6 and the exactness of the upper exact sequence in (1.5.1) yield the result. □

COROLLARY 1.5.8. *The $\mathbb{Z}_p$-module $\mathfrak{X}_{F,S}$ is finitely generated of $\mathbb{Z}_p$-rank independent of S containing $V_{p\infty}$.*

The δ in Theorem 1.5.7 is known as the Leopoldt defect of F

DEFINITION 1.5.9. The *Leopoldt defect* $\delta(F)$ is the $\mathbb{Z}_p$-rank of $\ker \iota_F$.

Leopoldt's conjecture for F is equivalent to the statement that the Leopoldt defect $\delta(F)$ is 0. We may also phrase Leopoldt's conjecture for F in terms of the nonvanishing of a p-adic regulator of F, which replaces the always nonzero complex regulator.

DEFINITION 1.5.10. For a p-adic field E, the *p-adic logarithm* of E is the unique homomorphism $\log_p \colon E^\times \to E$ such that $\log_p(p) = 0$ and such that for any x in the maximal ideal of $\mathscr{O}_E$, one has

$$\log_p(1+x) = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{x^k}{k}.$$

REMARK 1.5.11. The kernel of $\log_p$ on a p-adic field E is $\mu(E)$.

NOTATION 1.5.12. We use $\mathbb{C}_p$ to denote the completion of the algebraic closure of $\mathbb{Q}_p$ with respect to the unique extension of the p-adic absolute value on $\mathbb{Q}_p$. We have a *p-adic absolute value*

$$|\cdot|_p \colon \mathbb{C}_p \to \mathbb{R}_{\geq 0}$$

with $|p|_p = p^{-1}$.

REMARK 1.5.13. The p-adic logarithm extends to a continuous homomorphism $\log_p \colon \mathbb{C}_p^\times \to \mathbb{C}_p$.

It turns out that $\mathbb{C}$ and $\mathbb{C}_p$ are abstractly isomorphic (being algebraically closed of characteristic 0 and having the same cardinality), and we can fix an embedding $\iota \colon \mathbb{C} \to \mathbb{C}_p$. Let $d = [F : \mathbb{Q}]$, and let $\tau_i \colon F \hookrightarrow \mathbb{C}_p$ for $1 \leq i \leq r+1$ be the compositions $\tau = \iota \circ \sigma_i$ of the real and complex embeddings σ_i of F previously chosen in Section 1.2.

DEFINITION 1.5.14. Let $\alpha_1, \ldots, \alpha_r$ be r independent units in E_F. The *p-adic regulator* $R_p(F)$ of E_F is the determinant of the r-by-r matrix $\mathscr{R}_p(\alpha_1, \ldots, \alpha_r) = (c_i \log_p \tau_i(\alpha_j))_{i,j}$, where c_i is 1 if σ_i is real and 2 if σ_i is complex.

REMARK 1.5.15. The p-adic regulator is well-defined up to sign, so as an element of $\mathbb{C}_p^\times / \langle -1 \rangle$.

The following is immediate.

PROPOSITION 1.5.16. *Leopoldt's conjecture for a number field F is equivalent to the statement the nonvanishing of the p-adic regulator $R_p(F)$.*

Baker proved that if $\alpha_1, \ldots \alpha_n \in \overline{\mathbb{Q}}^\times$ are such that $2\pi i, \log \alpha_1, \ldots, \log \alpha_n$ are $\mathbb{Q}$-linearly independent, then they are $\overline{\mathbb{Q}}$-linearly independent. Via Baker's method, Brumer proved a p-adic analogue.

THEOREM 1.5.17 (Brumer). *Let $\beta_1, \ldots, \beta_n$ be algebraic numbers that are also p-adic units, and suppose that the p-adic logarithms $\log_p \beta_1, \ldots, \log_p \beta_n$ are $\mathbb{Q}$-linearly independent. Then these logarithms are also $\overline{\mathbb{Q}}$-linearly independent.*

Using this result, Brumer was able to prove Leopoldt's conjecture for an abelian extensions of number fields with $r = 0$. Note that the only fields with $r = 0$ are $\mathbb{Q}$ and the imaginary quadratic fields. We need several preliminary results. We begin with the following result, only the first part of which is needed at the moment.

PROPOSITION 1.5.18. *Let G be a finite abelian group and $f\colon G \to \mathbb{C}$ be a function. Let $\hat{G}$ denote the group of characters $G \to \mathbb{C}^\times$.*

a. We have

$$\prod_{\chi\in\hat{G}} \left(\sum_{\sigma\in G} \chi(\sigma) f(\sigma) \right) = \det(f(\sigma\tau^{-1}))_{\sigma,\tau\in G}.$$

In fact, the rank of $(f(\sigma\tau^{-1}))_{\sigma,\tau\in G}$ is the number of $\chi \in \hat{G}$ such that $\sum_{\sigma\in G} \chi(\sigma) f(\sigma) \neq 0$.

b. We have

$$\prod_{\substack{\chi\in\hat{G} \\ \chi\neq 1}} \left(\sum_{\sigma\in G} \chi(\sigma) f(\sigma) \right) = \det(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma,\tau\neq 1}.$$

PROOF. We compare two bases of the complex vector space V of functions $G \to \mathbb{C}$: the set of characters $\hat{G}$ and the set of δ-functions

$$\delta_\sigma(\tau) = \begin{cases} 1 & \tau = \sigma, \\ 0 & \tau \neq \sigma \end{cases}$$

for $\sigma \in G$. Consider the linear transformation $T\colon V \to V$ given by

$$T(g)(\tau) = \sum_{\sigma\in G} f(\sigma) g(\sigma\tau).$$

Applied to $g = \chi$, we obtain

$$T(\chi) = \sum_{\sigma\in G} f(\sigma)\chi(\sigma)\chi,$$

so χ is an eigenvector with eigenvalue $\sum_{\sigma\in G} \chi(\sigma) f(\sigma)$. It follows that $\det T$ is the product of the latter sums over all χ. On the other hand,

$$T(\delta_\sigma)(\rho) = \sum_{\tau\in G} f(\tau)\delta_\sigma(\rho\tau) = \sum_{\tau\in G} f(\tau)\delta_{\sigma\tau^{-1}}(\rho) = \sum_{\tau\in G} f(\tau^{-1}\sigma)\delta_\tau(\rho)$$

so

$$T(\delta_\sigma) = \sum_{\tau\in G} f(\sigma\tau^{-1})\delta_\tau$$

so the (τ,σ)-entry of the matrix of T with respect to this basis is $f(\sigma\tau^{-1})$. In that the determinant and rank of T are independent of the choice of basis, we have part a.

For part b, we consider the codimension 1 subspace W of V that consisting of the $g\colon G \to \mathbb{C}$ with $\sum_{\sigma\in G} g(\sigma) = 0$. One basis of these functions is given by $\hat{G} - \{1\}$, and another is given by the functions

$\delta_\sigma - |G|^{-1}$ for $\sigma \neq 1$. Also, we see immediately that $T(W) \subseteq W$. The determinant of $T|_W$ with respect to the character basis is clearly the left-hand side of the desired equality. On the other hand, noting that

$$\sum_{\tau \in G} (\delta_\tau - |G|^{-1}) = 0,$$

we have

$$T(\delta_\sigma - |G|^{-1}) = \sum_{\tau \in G} f(\sigma\tau^{-1})(\delta_\tau - |G|^{-1}) = \sum_{\substack{\tau \in G \\ \tau \neq 1}} (f(\sigma\tau^{-1}) - f(\sigma))(\delta_\tau - |G|^{-1}),$$

which has the desired coefficients. □

We omit a proof of the following.

LEMMA 1.5.19. *For a field K and a finite group G, let V and W be $K[G]$-modules of finite K-dimension. Suppose that there is a field extension L of K such that $V \otimes_K L \cong W \otimes_K L$ as $L[G]$-modules. Then $V \cong W$ as $K[G]$-modules.*

PROPOSITION 1.5.20. *Let F be an abelian extension with Galois group G of either $\mathbb{Q}$ or an imaginary quadratic field. Then $E_F \otimes_{\mathbb{Z}} \mathbb{Q} \cong I_G \otimes_{\mathbb{Z}} \mathbb{Q}$ as $\mathbb{Q}[G]$-modules.*

PROOF. By Proposition 1.2.4, we have $E_F \otimes_{\mathbb{Z}} \mathbb{R} \cong V_0$, where V_0 is as in Notation 1.2.3. That is V_0 is a hyperplane in the $\mathbb{R}$-span of the archimedean places of F, in this case consisting of the formal sums with coefficients summing to zero (since F is either totally real or purely imaginary). Since E has just one archimedean place, all of the places of F are conjugate under the action determined by precomposition of a representative by the inverse of an element of G. Fixing an embedding $\phi : F \to \mathbb{C}$ then provides an isomorphism $V_0 \cong I_G \otimes_{\mathbb{Z}} \mathbb{R}$, so $E_F \otimes_{\mathbb{Z}} \mathbb{R} \cong I_G \otimes_{\mathbb{Z}} \mathbb{R}$. By Lemma 1.5.19, we then have that $E_F \otimes_{\mathbb{Z}} \mathbb{Q} \cong I_G \otimes_{\mathbb{Z}} \mathbb{Q}$. □

THEOREM 1.5.21 (Brumer). *Leopoldt's conjecture holds for all finite abelian extensions of $\mathbb{Q}$ and all finite abelian extensions of any imaginary quadratic field.*

PROOF. By Proposition 1.5.20, we may pick $\alpha \in E_F$ be such that $\{\sigma(\alpha) \mid \sigma \in G - \{1\}\}$ is an independent set of r units of F. Let $\phi = \iota \circ \phi : K \to \mathbb{C}_p$, and consider the function $f : G \to \mathbb{C}_p$ defined by $f(\sigma) = \log_p \phi(\sigma^{-1}\alpha)$. Since

$$\prod_{\sigma \in G} \sigma^{-1}\alpha = \pm 1,$$

we have

$$\sum_{\sigma \in G} f(\sigma) = 0.$$

If $\sum_{\sigma\in G}\chi(\sigma)f(\sigma)=0$ for some nontrivial character $\chi\in\hat{G}$, then

$$\sum_{\sigma\in G-\{1\}}(1-\chi(\sigma))f(\sigma)=0.$$

Since $1-\chi(\sigma)\in\bar{\mathbb{Q}}$. By Theorem 1.5.17, we then have that the quantities $f(\sigma)$ for $\sigma\in G-\{1\}$ are $\mathbb{Q}$-linearly dependent, and hence $\mathbb{Z}$-linearly dependent. That is, there exist elements $k_\sigma\in\mathbb{Z}$, not all zero, such that

$$\prod_{\sigma\in G-\{1\}}(\sigma\alpha)^{k_\sigma}\in\mu(F).$$

This, however, contradicts our choice of α.

Now choose an ordering of G and form the matrix $(f(\sigma\tau^{-1}))_{\sigma,\tau\in G}$, the (σ,τ)-entry of which is $\log_p(\phi\circ\tau)(\sigma^{-1}\alpha)$. It then follows from Proposition 1.5.18a that this matrix has rank $r=|G|-1$, and the $\sigma=1$ row and $\tau=1$ column are linearly dependent on the others. If we remove them, the resulting r-by-r minor is the p-adic regulator matrix attached to the basis $\sigma^{-1}\alpha$ with $\sigma\in G-\{1\}$ and the embeddings $\phi\circ\tau$ for $\tau\in G-\{1\}$. Thus $R_p(F)\neq 0$, so Leopoldt's conjecture holds for F. $\square$

CHAPTER 2

Module theory

2.1. Pseudo-isomorphisms

DEFINITION 2.1.1. For an integral domain R, a *pseudo-null* R-module is an R-module M with annihilator $\mathrm{Ann}_R(M)$ of height at least 2.

DEFINITION 2.1.2. Let R be an integral domain. An R-module homomorphism $f\colon A \to B$ is a *pseudo-isomorphism* if it has pseudo-null kernel and cokernel.

The existence of a pseudo-isomorphism from one object to another is not in general an equivalence relation on the category of finitely generated R-modules, as it is not symmetric.

EXAMPLE 2.1.3. The quotient of $\mathbb{F}_p[x,y]$ by the maximal ideal (x,y) of height 2 is pseudo-null. However, as (x,y) is not principal, there is no pseudo-isomorphism $\mathbb{F}_p[x,y] \to (x,y)$.

Nevertheless, we can make the following definition, which does provide an equivalence relation.

DEFINITION 2.1.4. We say that two modules A and B over an integral domain R are *pseudo-isomorphic* if $A_\mathfrak{p} \cong B_\mathfrak{p}$ for all height one prime ideals $\mathfrak{p}$ of R.

NOTATION 2.1.5. We write $A \simeq B$ if A and B are pseudo-isomorphic modules over an integral domain R.

If there exists a pseudo-isomorphism from one R-module to another, then they are pseudo-isomorphic. Recall that a prime ideal $\mathfrak{p}$ of R lies in the support of a R-module A if and only if $A_\mathfrak{p} \neq 0$.

LEMMA 2.1.6. *Let $f\colon A \to B$ be a pseudo-isomorphism of R-modules, where R is an integral domain. Then A and B are pseudo-isomorphic.*

PROOF. Since localization is an exact functor, for any height one prime ideal $\mathfrak{p}$ of R, we have an exact sequence

$$0 \to (\ker f)_\mathfrak{p} \to A_\mathfrak{p} \to B_\mathfrak{p} \to (\operatorname{coker} f)_\mathfrak{p} \to 0.$$

Since any prime ideal $\mathfrak{q}$ in the support of $\mathrm{Ann}_R(\ker f)$ or $\mathrm{Ann}_R(\operatorname{coker} f)$ has height at least 2, while $R_\mathfrak{p}$ has Krull dimension one, we have $\mathfrak{q}R_\mathfrak{p} = R_\mathfrak{p}$. Since $(\ker f)_\mathfrak{p}$ and $(\operatorname{coker} f)_\mathfrak{p}$ then have no prime ideals in their support, they are both zero. □

LEMMA 2.1.7. *Let A and B be modules over a commutative ring R with A finitely presented, and let S be a multiplicative subset of R. Then we have a canonical isomorphism*

$$\mathrm{Hom}_{S^{-1}R}(S^{-1}A, S^{-1}B) \cong S^{-1}\,\mathrm{Hom}_R(A,B).$$

PROOF. As

$$S^{-1}A \cong S^{-1}R \otimes_R A,$$

adjointness of Hom and $\otimes$ yields

$$\mathrm{Hom}_{S^{-1}R}(S^{-1}A, S^{-1}B) \cong \mathrm{Hom}_R(A, S^{-1}B). \tag{2.1.1}$$

The result now follows from (2.1.1) and

$$\mathrm{Hom}_R(A, S^{-1}R \otimes_R B) \cong S^{-1}R \otimes_R \mathrm{Hom}_R(A,B). \tag{2.1.2}$$

To see that (2.1.2) holds, note first that it holds if $A = R$. It then holds for every free R-module A of finite rank, as finite direct sums commute with Hom in the first variable and direct sums commute with tensor products. In general, choose a resolution

$$P_1 \to P_0 \to A$$

with P_0 and P_1 finitely generated free R-modules, and use the fact that the contravariant functors of A in question are exact on right-exact sequences of R-modules, in particular as $S^{-1}R$ is R-flat. □

We recall from the theory of primary decomposition that every ideal I in a noetherian ring is a minimal finite intersection of primary ideals, and the minimal ideals among the finitely many associated primes of I that are the radicals of these primary ideals are the isolated primes of I.

LEMMA 2.1.8. *Any finitely generated torsion module over a noetherian ring R has only finitely many height one prime ideals in its support.*

PROOF. A prime ideal $\mathfrak{p}$ is in the support of a finitely generated R-module M if and only if and only if it contains $I = \mathrm{Ann}_R(M)$. Any height one prime ideal containing I is an isolated prime in its primary decomposition, so there can be only finitely many. □

From now on in this section, we use Λ to denote an integrally closed noetherian domain. Note that the localization of Λ at any height one prime is still a integrally closed noetherian domain, and it has a unique nonzero prime, so it is a DVR.

LEMMA 2.1.9. *Let A and B be torsion Λ-modules. Let X be the finite set of height one prime ideals in the support of A or B. Set*

$$S = \Lambda - \bigcup_{\mathfrak{p}\in X} \mathfrak{p}.$$

Let $f\colon A \to B$ be a Λ-module homomorphism. Then f is a pseudo-isomorphism if and only if the localized map

$$S^{-1}f\colon S^{-1}A \to S^{-1}B$$

is an isomorphism.

PROOF. First, note that X is indeed finite by Lemma 2.1.8. Let $X = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, where the $\mathfrak{p}_i$ are distinct. As localization is an exact functor, it suffices to show that a finitely generated torsion Λ-module M with height one support in X is pseudo-null if and only if $S^{-1}M = 0$.

If M is pseudo-null, then its annihilator has height at least 2, so is not contained in any prime ideal of height one. Thus, for each $1 \leq i \leq r$, there exists an element $y_i \in \mathrm{Ann}_\Lambda(M)$, with $y_i \notin \mathfrak{p}_i$. Since there also exists an element $x_i \in \mathfrak{p}_i$ with $x_i \notin \mathfrak{p}_j$ for all $j \neq i$, we have

$$x = y_1x_2x_3\cdots x_r + x_1y_2x_3\cdots x_r + \cdots + x_1x_2\cdots x_{r-1}y_r \in S \cap \mathrm{Ann}_\Lambda(M)$$

and so $S^{-1}M = 0$.

Conversely, suppose that $S^{-1}M = 0$. Then $M_\mathfrak{p} = 0$ for all $\mathfrak{p} \in S$, and hence for all height one prime ideals $\mathfrak{p}$, which is to say that for each $\mathfrak{p}$, there exists $s \in \mathrm{Ann}_\Lambda(M)$ with $s \notin \mathfrak{p}$, from which it follows that $\mathrm{Ann}_\Lambda(M) \not\subseteq \mathfrak{p}$ for any height one prime ideal $\mathfrak{p}$. Therefore, $\mathrm{Ann}_\Lambda(M)$ has height at least 2. □

PROPOSITION 2.1.10. *Let A be a finitely generated, torsion Λ-module. Then A is pseudo-isomorphic to a direct sum $\bigoplus_{i=1}^{s} \Lambda/\mathfrak{p}_i^{k_i}$ with $\mathfrak{p}_i$ a height one prime of Λ and $k_i \geq 1$ for all $1 \leq i \leq s$ and for $s \geq 0$. Moreover, this decomposition is unique up to ordering.*

PROOF. Let S be the complement of the union of the height one prime ideals in the support of A. Then $S^{-1}A$ is a torsion module over the principal ideal domain $S^{-1}\Lambda$, so we have an isomorphism

$$g\colon S^{-1}A \xrightarrow{\sim} \bigoplus_{i=1}^{s} S^{-1}(\Lambda/\mathfrak{p}_i^{k_i})$$

with the $\mathfrak{p}_i$ and k_i as in the statement. By Lemma 2.1.7, there exists a Λ-module homomorphism $f\colon A \to \bigoplus_{i=1}^{s} \Lambda/\mathfrak{p}_i^{k_i}$ with $S^{-1}f = g$. By Lemma 2.1.9, the map f is a pseudo-isomorphism. The uniqueness is clear from the uniqueness in the structure theorem for finitely generated $S^{-1}\Lambda$-modules. □

The following is now clear.

COROLLARY 2.1.11. *Two finitely generated, torsion Λ-modules A and B are pseudo-isomorphic if and only if there exists a pseudo-isomorphism $f\colon A \to B$.*

REMARK 2.1.12. A module M over an integral domain R is torsion if and only if $M_{(0)} = 0$, which is to say that its localization at 0 is trivial. In particular, the R-torsion submodule of such a module M is the kernel of the localization map to $M_{(0)}$.

LEMMA 2.1.13. *Let A be a finitely generated Λ-module, let T denote its Λ-torsion submodule, and set $Z = A/T$. Then there is a pseudo-isomorphism*

$$A \to T \oplus Z.$$

PROOF. Supposing without loss of generality that $T \neq 0$, let S be the complement of the union of the height one primes in the support of T. Then $S^{-1}\Lambda$ is a principal ideal domain, and by the structure theorem for finitely generated modules over principal ideal domains, we have a projection map

$$\rho' \colon S^{-1}A \to S^{-1}T,$$

which realizes the $S^{-1}\Lambda$-torsion submodule $S^{-1}T$ of $S^{-1}A$ as a direct summand. (To see that $S^{-1}T$ is the $S^{-1}\Lambda$-torsion submodule of $S^{-1}A$, note that it is torsion and the quotient $S^{-1}Z = S^{-1}A/S^{-1}T$ is $S^{-1}\Lambda$-torsion-free, as the fact that $Z \to Z_{(0)}$ is injective implies that $S^{-1}Z \to S^{-1}Z_{(0)} = Z_{(0)}$ is as well.) In other words, if we let $\nu \colon A \to Z$ be the quotient map and ν' denote its localization, then $(\rho', \nu') \colon S^{-1}A \to S^{-1}T \oplus S^{-1}Z$ is an isomorphism.

By Lemma 2.1.7, there exist $\rho \in \mathrm{Hom}(A, T)$ and $s \in S$ such that $\rho = s\rho'$. We consider the map

$$(\rho, \nu) \colon A \to T \oplus Z.$$

Its localization is an isomorphism as multiplication by s is an isomorphism on $S^{-1}T$. Since the kernel and cokernel are a subgroup and a quotient of T, respectively, they are supported on S, and the triviality of their localizations at S implies their pseudo-nullity. Thus, (ρ, ν) is a pseudo-isomorphism. □

NOTATION 2.1.14. For a Λ-module A, let us use

$$A^* = \mathrm{Hom}_\Lambda(A, \Lambda)$$

to denote its Λ-dual.

Note that Lemma 2.1.7 tells us that $(A^*)_\mathfrak{p} \cong (A_\mathfrak{p})^*$ for any prime ideal $\mathfrak{p}$ of Λ, the latter module being defined as

$$(A_\mathfrak{p})^* = \mathrm{Hom}_{\Lambda_\mathfrak{p}}(A_\mathfrak{p}, \Lambda_\mathfrak{p}),$$

so we simply write $A^*_\mathfrak{p}$. Let $\mathscr{Q}$ denote the quotient field of Λ.

LEMMA 2.1.15. *Let Z be a finitely generated, torsion-free Λ-module. The map $Z \to Z^{**}$ is an injective pseudo-isomorphism.*

PROOF. For any height one prime ideal $\mathfrak{p}$, the modules $Z_\mathfrak{p}$ and $Z^{**}_\mathfrak{p}$ are free, being finitely generated torsion-free modules over the principal ideal domain $\Lambda_\mathfrak{p}$. Moreover, the natural map $Z_\mathfrak{p} \to Z^{**}_\mathfrak{p}$ is an isomorphism, being identified with the map a finite rank free $\Lambda_\mathfrak{p}$-module to its $\Lambda_\mathfrak{p}$-double dual. That is, $Z \to Z^{**}$ is a pseudo-isomorphism, which is injective as Z is torsion-free. □

LEMMA 2.1.16. *Let A be a finitely generated Λ-module. Inside $A^*_{(0)}$, we have*

$$A^* = \bigcap_{\mathfrak{p} \in X_1} A^*_{\mathfrak{p}},$$

where X_1 denotes the set of height 1 primes of Λ

PROOF. Since A^* is torsion-free, it sits inside each $A^*_{\mathfrak{p}}$, hence in the intersection. Let $f \in A^*_{(0)}$ lie in $A^*_{\mathfrak{p}}$ for each $\mathfrak{p}$ of height one. Then $f\colon A \to \Lambda_{\mathfrak{p}}$ for all $\mathfrak{p}$, so f has image in $\Lambda = \bigcap_{\mathfrak{p} \in X_1} \Lambda_{\mathfrak{p}}$. It follows that $f \in A^*$, hence the result. □

DEFINITION 2.1.17. We say that a finitely generated Λ-module A is *reflexive* if the natural map $A \to A^{**}$ is an isomorphism.

Note that a reflexive Λ-module is necessarily torsion-free, since the dual of a finitely generated Λ-module is torsion-free.

LEMMA 2.1.18. *A finitely generated, torsion-free Λ-module Z is reflexive if and only if Z is the intersection of the $Z_{\mathfrak{p}}$ over all height one prime ideals $\mathfrak{p}$ of Λ.*

PROOF. We note that Lemma 2.1.16 implies that

$$Z^{**} = \bigcap_{\mathfrak{p} \in X_1} Z^{**}_{\mathfrak{p}},$$

and we recall that the natural map $Z_{\mathfrak{p}} \to Z^{**}_{\mathfrak{p}}$ is an isomorphism. As the diagram

$$\begin{array}{ccc} Z & \longrightarrow & Z^{**} \\ \downarrow & & \downarrow \wr \\ \bigcap_{\mathfrak{p} \in X_1} Z_{\mathfrak{p}} & \xrightarrow{\sim} & \bigcap_{\mathfrak{p} \in X_1} Z^{**}_{\mathfrak{p}} \end{array}$$

commutes, we have the result. □

We have the following immediate corollary of Lemmas 2.1.16 and 2.1.18.

COROLLARY 2.1.19. *Let A be a finitely generated Λ-module. Then A^* is reflexive.*

We recall that a noetherian local ring Ω is regular if its maximal ideal $\mathfrak{m}$ is generated by the terms of a regular sequence $(x_i)_{i=1}^d$, which is to say that x_i is not a zero divisor in $\Omega/(x_1, \ldots, x_{i-1})$ for $1 \leq i \leq d$. In this case, Ω has Krull dimension d. Equivalently, a noetherian local ring Ω is regular of Krull dimension d if its maximal ideal can be generated by d elements, or if $\dim_{\Omega/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = d$.

PROPOSITION 2.1.20. *Let Ω be a regular local ring of Krull dimension 2. Then every finitely generated, reflexive Ω-module is free.*

PROOF. Let A be a finitely generated and reflexive Ω-module. As Ω is regular, it has a regular sequence so a principal prime ideal $\mathfrak{p} = (f)$. We first claim that $A/\mathfrak{p}A$ is a free $\Omega/\mathfrak{p}$-module. As $\Omega/\mathfrak{p}$ is regular of Krull dimension 1, its maximal ideal is principal (and it is a domain), so it is a DVR. Thus, it suffices to show that $A/\mathfrak{p}A$ is torsion-free over $\Omega/\mathfrak{p}$. For this, note that the exact sequence

$$0 \to \mathrm{Hom}_\Omega(A^*, \Omega) \xrightarrow{f} \mathrm{Hom}_\Omega(A^*, \Omega) \to \mathrm{Hom}_\Omega(A^*, \Omega/\mathfrak{p})$$

implies that the map

$$A^{**}/\mathfrak{p}A^{**} \to \mathrm{Hom}_\Omega(A^*, \Omega/\mathfrak{p})$$

is injective. As

$$\mathrm{Hom}_\Omega(A^*, \Omega/\mathfrak{p}) \cong \mathrm{Hom}_{\Omega/\mathfrak{p}}(A^*/\mathfrak{p}A^*, \Omega/\mathfrak{p})$$

is $\Omega/\mathfrak{p}$-torsion free, the module $A^{**}/\mathfrak{p}A^{**}$ is $\Omega/\mathfrak{p}$-torsion free. But A is reflexive, so $A^{**}/\mathfrak{p}A^{**} \cong A/\mathfrak{p}A$, proving the claim.

Next, let $s = \dim_{\Omega/\mathfrak{m}} A/\mathfrak{m}A$, where $\mathfrak{m}$ is the maximal ideal of Ω. By Nakayama's Lemma, there exists a minimal Ω-generating set of A with s elements, which is to say a surjective map $\pi\colon \Omega^s \to A$. Since $A/\mathfrak{p}A$ is $\Omega/\mathfrak{p}$-free, and by what we have just said of rank s, the induced surjection $(\Omega/\mathfrak{p})^s \to A/\mathfrak{p}A$ is necessarily an isomorphism. Therefore, multiplication by f is surjective on $\ker\pi$, and Nakayama's lemma then tells us that $\ker\pi = 0$. □

REMARK 2.1.21. Any regular local ring is a UFD by a theorem of Auslander and Buchsbaum. In particular, regular local rings are integrally closed domains.

THEOREM 2.1.22. *Let Λ be a regular local ring of Krull dimension at most 2. Let A be a finitely generated Λ-module. Then there exists a pseudo-isomorphism*

$$A \to \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/\mathfrak{p}_i^{k_i}$$

for some $r, s \geq 0$ and height one primes $\mathfrak{p}_i$ and integers $k_i \geq 1$ for $1 \leq i \leq s$. Moreover, r and s are unique, and the prime powers are unique up to ordering.

PROOF. Suppose first that A is torsion-free. By Lemma 2.1.15, the map $A \to A^{**}$ is an injective pseudo-isomorphism, and by Proposition 2.1.20, we have that $A^{**} \cong \Lambda^r$ for some r. This is then the unique r for which there exists a pseudo-isomorphism $A \to \Lambda^r$, being that it is then the dimension of $A_{(0)}$ over the quotient field of Λ.

The result for torsion modules is Proposition 2.1.10. We can combine the torsion-free and torsion cases by applying Lemma 2.1.13 and the decompositions in each case. The uniqueness follows from the uniqueness in the two cases. □

2.2. Power series rings

Let $\mathscr{O}$ be a complete commutative local noetherian ring with maximal ideal $\mathfrak{m}$ and finite residue field of characteristic p. We study the ring $\Lambda = \mathscr{O}[\![T]\!]$, beginning with the following analogue of the division algorithm.

PROPOSITION 2.2.1 (Division algorithm). *Let $f, g \in \Lambda$, and suppose that $f \notin \mathfrak{m}\Lambda$. Let n be the largest integer such that $f \in \mathfrak{m}\Lambda + (T^n)$. Then we may write*

$$g = qf + r$$

for a unique $q \in \Lambda$ and $r \in \mathscr{O}[T]$ with $\deg r < n$.

PROOF. Suppose without loss of generality that $n > 0$. Let $u \in \mathscr{O}^\times$ be the coefficient of T^n in f. Let $a \in \Lambda$ and $b \in \mathscr{O}[T]$ be such that

$$f = aT^n + b,$$

where $\deg b < n$. Note that $b \in \mathfrak{m}\Lambda$ by choice of n, and since $a - u$ lies in the maximal ideal of Λ, we have $a \in \Lambda^\times$. Let $q_0' \in \Lambda$ and $r_0 \in \mathscr{O}[T]$ be such that

$$g = q_0' T^n + r_0,$$

where $\deg r_0 < n$. Setting $q_0 = a^{-1} q_0'$, we have

$$g = q_0 a T^n + r_0 \equiv q_0 f + r_0 \bmod \mathfrak{m}\Lambda.$$

Let $g_1 = g - q_0 f - r_0 \in \mathfrak{m}\Lambda$, and repeat the process to obtain $q_1 \in \mathfrak{m}\Lambda$ and $r_1 \in \mathfrak{m}\mathscr{O}[T]$ with $\deg r_1 < n$ and

$$g_1 \equiv q_1 f + r_1 \bmod \mathfrak{m}^2\Lambda.$$

Note then that

$$g \equiv (q_0 + q_1) f + (r_0 + r_1) \bmod \mathfrak{m}^2\Lambda.$$

Recursively, we may then construct

$$q = q_0 + q_1 + q_2 + \cdots \in \Lambda \quad \text{and} \quad r = r_0 + r_1 + r_2 + \cdots \in \mathscr{O}[T]$$

such that $g = qf + r$ and $\deg r < n$.

As for uniqueness, if $g = q'f + r'$ with $r' \in \mathscr{O}[T]$ and $\deg r' < n$, then

$$(q - q')f + (r - r') = 0.$$

We then need only show that if $c \in \Lambda$ and $d \in \mathscr{O}[T]$ with $\deg d < n$ satisfy $cf + d = 0$, then $c = d = 0$. Suppose that this is not the case, and let $k \geq 0$ be such that $c, d \in \mathfrak{m}^k\Lambda$ but not both c and d are contained in $\mathfrak{m}^{k+1}\Lambda$. We see that cf is congruent to a multiple of T^n modulo $\mathfrak{m}^{k+1}\Lambda$, which forces $d \in \mathfrak{m}^{k+1}\Lambda$, as $\deg d < n$. But then $cf \in \mathfrak{m}^{k+1}\Lambda$, and since $f \notin \mathfrak{m}\Lambda$, this forces $c \in \mathfrak{m}^{k+1}\Lambda$, a contradiction. □

DEFINITION 2.2.2. A *distinguished (or Weierstrass) polynomial* $f \in \Lambda$ is a polynomial with leading coefficient 1 that satisfies

$$f(T) \equiv T^{\deg f} \bmod \mathfrak{m}\Lambda.$$

THEOREM 2.2.3 (Weierstrass preparation). *Let $g \in \Lambda$ with $g \notin \mathfrak{m}\Lambda$. Then there exist a unique distinguished polynomial f and unit $u \in \Lambda^\times$ such that*

$$g = uf.$$

PROOF. We begin with existence. Let n be the maximal such that $g \in \mathfrak{m}\Lambda + (T^n)$, and let $u_0 \in \mathscr{O}^\times$ be the coefficient of T^n in g. Using the division algorithm, write

$$T^n = qg + r$$

for some unique $q \in \Lambda$ and $r \in \mathscr{O}[T]$ with $\deg r < n$. Since all of the terms of g of degree less than n lie in $\mathfrak{m}$, we have $r \in \mathfrak{m}\Lambda$. If we set $f = T^n - r$, then f is a distinguished polynomial. Moreover, the constant coefficient q_0 of q satisfies $q_0 u_0 \equiv 1 \bmod T$, so is a unit in $\mathscr{O}$, and therefore $q \in \Lambda^\times$. Letting $u = q^{-1}$, we have $g = uf$, as desired. The uniqueness of f and u is forced by the uniqueness of q and r. □

We then have the following corollaries of the Weierstrass preparation theorem.

COROLLARY 2.2.4. *Suppose that $\mathscr{O}$ is a PID. Then the ring Λ is a unique factorization domain.*

PROOF. Let $\pi \in \mathfrak{m}$ be a generator. For $g \in \pi^n\Lambda - \pi^{n+1}\Lambda$, we may apply the Weierstrass preparation theorem to factor $\pi^{-n}g$ into a polynomial f times a unit, and then use the fact that $\mathscr{O}[T]$ is a UFD to factor f into a product of irreducible polynomials, each of which is a Weierstrass polynomial times a unit. This gives the desired factorization of g as a product of a power of π, finitely many irreducible Weierstrass polynomials, and a unit. Clearly any other factorization is equivalent (up to unit and ordering) to such a factorization. □

REMARK 2.2.5. In fact, it is more generally true that if $\mathscr{O}$ is a regular local ring, then so is $\Lambda = \mathscr{O}[\![T]\!]$. For such $\mathscr{O}$, the ring $\mathscr{O}[\![T_1, T_2, \ldots, T_r]\!]$ is then of course a UFD as well.

Suppose from now on that $\mathscr{O}$ is the valuation ring of a finite extension of $\mathbb{Q}_p$. Let $\pi \in \mathscr{O}$ be a uniformizer. We may view $\mathscr{O}$ as sitting inside $\mathbb{C}_p$. Given $f \in \Lambda$ and $a \in \mathbb{C}_p$ with $|a|_p < 1$, the evaluation $f(a)$ converges to an element of $\mathbb{C}_p$.

COROLLARY 2.2.6. *Let $g \in \Lambda$ be nonzero. There exist only finitely many $a \in \mathbb{C}_p$ with $|a|_p < 1$ such that $g(a) = 0$.*

PROOF. By Weierstrass preparation, we have $g = \pi^\mu u f$ with $\mu \geq 0$, $u \in \Lambda^\times$, and f a Weiserstrass polynomial. As u is a unit, one cannot have $a \in \mathbb{C}_p$ with $|a|_p < 1$ such that $u(a) = 0$. Therefore, $g(a) = 0$ if and only if $f(a) = 0$, and so the result follows from the fact that f is a polynomial. □

COROLLARY 2.2.7. *Let $g \in \mathscr{O}[T]$, and let f be a distinguished polynomial in $\mathscr{O}[T]$ with f dividing g in Λ. Then $g/f \in \mathscr{O}[T]$.*

PROOF. Let $n = \deg f$. Suppose $\alpha \in \mathbb{C}_p$ is a root of f. If $|\alpha|_p > 1$, then $0 = |f(\alpha)|_p = |\alpha|_p^n > 1$, which is impossible. If $|\alpha|_p = 1$, then

$$0 = f(\alpha) \equiv \alpha^n \bmod \mathfrak{m}_{\mathbb{C}_p},$$

where $\mathfrak{m}_{\mathbb{C}_p}$ denotes the maximal ideal of $\mathbb{C}_p$, which is again impossible. If $|\alpha|_p < 1$, then set $q = g/f \in \Lambda$. Since $q(\alpha)$ converges, we have $g(\alpha) = 0$. Let $\mathscr{O}'$ denote the valuation ring of the splitting field of f. We divide g and f by $T - \alpha$ inside $\mathscr{O}'[T]$ and repeat the process with the resulting polynomials, which we denote f_1 and g_1. After n iterations, we have obtain $f_n = 1$, and since f is monic, g_n is the polynomial $q \in \mathscr{O}[T]$. □

Next, let us consider ideals in Λ.

DEFINITION 2.2.8. Two elements $f, g \in \Lambda$ are said to be *relatively prime* if the only elements in Λ that divide both f and g are units.

LEMMA 2.2.9. *Suppose that $f, g \in \Lambda$ are relatively prime. Then (f, g) has finite index in Λ.*

PROOF. Suppose that $h \in (f, g)$ is a polynomial of minimal degree (which exists by Weierstrass preparation), and suppose it is exactly divisible by a power π^n of π. Assume first that h has positive degree. Let $h' \in \Lambda$ be defined by $h = \pi^n h'$. Without loss of generality, suppose that h' does not divide f. The division algorithm produces $q \in \Lambda$ and $r \in \mathscr{O}[T]$ with $\deg r < \deg h'$ such that $f = qh' + r$. Then $\pi^n r \in (f, g)$, which forces $r = 0$ by the minimality of the degree of h. But then h' divides f, which is a contradiction, so h must be of degree 0.

So now, suppose that n is minimal such that $\pi^n \in (f, g)$. At least one of f and g is not divisible by π: suppose it is f, and assume without loss of generality that f is a distinguished polynomial. We have $(\pi^n, f) \subseteq (f, g)$, but

$$\Lambda/(\pi^n, f) \cong (\mathscr{O}/\pi^n\mathscr{O})[T]/(\bar{f}),$$

where $\bar{f}$ is the image of f in $\mathscr{O}/\pi^n\mathscr{O}[T]$, and the quotient ring is a finite ring by the division algorithm, as $\mathscr{O}$ has finite residue field. □

PROPOSITION 2.2.10. *Every prime ideal of Λ is one of 0, (π, T), (π), or (f), where f is an irreducible distinguished polynomial.*

PROOF. Suppose that $\mathfrak{p}$ is a nonzero prime ideal in Λ with $\mathfrak{p} \neq (\pi)$. By the primality of $\mathfrak{p}$, there then exists a distinguished polynomial f in $\mathfrak{p}$ that is irreducible and not divisible by π . So choose such an f: if $\mathfrak{p} = (f)$, we are done. Otherwise, there exists $g \in \mathfrak{p}$ with $g \notin (f)$, and therefore by Lemma 2.2.9, there exists $\pi^n \in (f,g)$ for some $n \geq 1$. Since $\mathfrak{p}$ is prime, we then have $\pi \in \mathfrak{p}$, and since $f \equiv T^{\deg f} \bmod \pi$, we have $T^{\deg f} \in \mathfrak{p}$. Again, primality of $\mathfrak{p}$ then forces $T \in \mathfrak{p}$, and finally, $\mathfrak{p} = (\pi, T)$ by the maximality of (π, T). □

REMARK 2.2.11. We have that $\Lambda/(\pi) \cong (\mathscr{O}/\mathfrak{m})[\![T]\!]$, while $\Lambda/(f)$ for a distinguished polynomial f is free of rank $\deg f$ over $\mathscr{O}$.

LEMMA 2.2.12. *A finitely generated Λ-module is pseudo-null if and only if it is finite.*

PROOF. Suppose that M is a finitely generated, pseudo-null Λ-module. To say that $\mathrm{Ann}_\Lambda(M)$ has height at least 2 is to say that it contains two relatively prime elements, hence has finite index in Λ. On the other hand, if M is a finite Λ-module, then

$$\mathrm{Ann}_\Lambda(M) = \bigcap_{m \in M} \mathrm{Ann}_\Lambda(m),$$

and $\mathrm{Ann}_\Lambda(m)$ must be of finite index in Λ, since m generates a finite Λ-module isomorphic to $\Lambda/\mathrm{Ann}_\Lambda(m)$. It follows that $\mathrm{Ann}_\Lambda(M)$ has finite index in Λ, and therefore has height 2. □

It follows that a pseudo-isomorphism of Λ-modules, for $\mathscr{O}$ a valuation ring in a finite extension of $\mathbb{Q}_p$, is a Λ-module homomorphism with finite kernel and cokernel.

THEOREM 2.2.13 (Structure theorem for finitely generated Λ-modules). *Let M be a finitely generated Λ-module. Then there exists a pseudo-isomorphism*

$$M \to \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(\pi^{l_j})$$

for some $r,s,t \geq 0$, $k_i \geq 1$ and f_i a distinguished irreducible Λ-polynomial for $1 \leq i \leq s$, and $l_j \geq 1$ for $1 \leq j \leq t$. Moreover, these quantities are unique up to reordering.

PROOF. This follows directly from Theorem 2.1.22 and the fact that the height one prime ideals in Λ are (π) and the ideals (f) for f an irreducible distinguished polynomial. □

2.3. Completed group rings

For a profinite group G, we use $U \trianglelefteq^o G$ to denote that U is an open normal subgroup of G.

DEFINITION 2.3.1. Let G be a profinite group, and let $\mathscr{O}$ be a commutative ring. We define the completed $\mathscr{O}$-group ring of G to be the inverse limit

$$\mathscr{O}[\![G]\!] = \varprojlim_{U \trianglelefteq^o G} \mathscr{O}[G/U]$$

with respect to the quotient maps $\mathscr{O}[G/V] \to \mathscr{O}[G/U]$ for $V \leq U$.

REMARK 2.3.2. In the case that G is finite, we have $\mathscr{O}[\![G]\!] = \mathscr{O}[G]$, the usual group ring.

We shall study completed group rings only for certain very special classes of rings $\mathscr{O}$ and profinite groups G. In particular, let us assume that $\mathscr{O}$ is local and complete with respect to a maximal ideal $\mathfrak{m}$, which is to say that

$$\mathscr{O} \cong \varprojlim_{n} \mathscr{O}/\mathfrak{m}^n\mathscr{O}.$$

REMARK 2.3.3. Since $\mathscr{O}$ is complete with respect to the maximal ideal $\mathfrak{m}$, we have

$$\mathscr{O}[\![G]\!] \cong \varprojlim_{\substack{U \trianglelefteq^o G \\ n \geq 0}} (\mathscr{O}/\mathfrak{m}^n\mathscr{O})[G/U]$$

DEFINITION 2.3.4. The augmentation ideal I_G of $\mathscr{O}[\![G]\!]$ is equal to

$$\ker(\mathscr{O}[\![G]\!] \xrightarrow{\varepsilon} \mathscr{O}),$$

where ε is the augmentation map, the inverse limit of the $\mathscr{O}$-linear maps $\mathscr{O}[G/U] \to \mathscr{O}$ that take every group element to 1.

REMARK 2.3.5. The map ε is surjective, and therefore it induces an isomorphism

$$\mathscr{O}[\![G]\!]/I_G \cong \mathscr{O}$$

We require the following lemma.

LEMMA 2.3.6. *Let k be a field of characteristic p, and let G be a finite abelian p-group. Then $k[G]$ is a local ring with maximal ideal the augmentation ideal in $k[G]$.*

PROOF. Suppose that $G \cong \bigoplus_{i=1}^r \mathbb{Z}/p^{n_i}\mathbb{Z}$ for some $n_i \geq 1$ and $r \geq 0$, and let g_i be the inverse image of a generator of the ith component under this isomorphism. It is easy to see that

$$k[G] \cong k[X_1, X_2, \ldots, X_r]/(X_1^{p^{n_1}} - 1, X_2^{p^{n_2}} - 1, \ldots, X_r^{p^{n_r}} - 1)$$

under the map that takes g_i to X_i. Moreover, $X_i^{p^{n_i}} - 1 = (X_i - 1)^{p^{n_i}}$ for each i since k has characteristic p. Setting $T_i = X_i - 1$ the resulting ring

$$k[T_1, T_2, \ldots, T_r]/(T_1^{p^{n_1}}, T_2^{p^{n_2}}, \ldots, T_r^{p^{n_r}})$$

is local with maximal ideal $(T_1, T_2, \ldots, T_r)$. (This is well-known, but note that if $f \notin (T_1, T_2, \ldots, T_r)$, then f has nontrivial constant coefficient, and we may construct an inverse by successive approximation, working modulo higher and higher total degrees.) The inverse image of this ideal under our isomorphism is the augmentation ideal of $k[G]$. □

We now let $\mathscr{O}$ be a commutative noetherian local ring that is complete with the topology defined by its maximal ideal $\mathfrak{m}$.

PROPOSITION 2.3.7. *Let $\mathscr{O}$ be a complete commutative noetherian local ring with finite residue field characteristic p, and let G be a topologically finitely generated abelian pro-p group. Then the algebra $\mathscr{O}[\![G]\!]$ is a local ring with maximal ideal $\mathfrak{m}\mathscr{O}[\![G]\!] + I_G$.*

PROOF. We note that

$$\mathscr{O}[\![G]\!]/(\mathfrak{m} + I_G) \cong \mathscr{O}/\mathfrak{m},$$

so $\mathfrak{m} + I_G$ is maximal. If $\mathfrak{M}$ is any maximal ideal of $\mathscr{O}[\![G]\!]$, then we have an injection

$$\mathscr{O}/(\mathfrak{M} \cap \mathscr{O}) \to \mathscr{O}[\![G]\!]/\mathfrak{M},$$

which forces $\mathscr{O}/(\mathfrak{M} \cap \mathscr{O})$ to be a field, hence $\mathfrak{M} \cap \mathscr{O}$ to be maximal in $\mathscr{O}$, and therefore $\mathfrak{M} \cap \mathscr{O}$ to be equal to $\mathfrak{m}$.

Moreover, we have

$$\mathscr{O}[\![G]\!]/\mathfrak{m}\mathscr{O}[\![G]\!] \cong k[\![G]\!],$$

where $k = \mathscr{O}/\mathfrak{m}$. This follows from the fact that $\mathfrak{m}\mathscr{O}[\![G]\!]$ is an inverse limit of a countable inverse system of modules $\mathfrak{m} \cdot (\mathscr{O}/\mathfrak{m}^n)[G/U]$ with surjective maps, as this implies that $\varprojlim^1$ of the system vanishes. (Here, the countability of the system is guaranteed by the assumption of finite generation on G.)

The problem is reduced to showing that the augmentation ideal of $k[\![G]\!]$ is its only maximal ideal. As the quotient of $k[\![G]\!]$ by a maximal ideal surjects onto the quotient of $k[G/U]$ by the image of that maximal ideal for every open normal subgroup U of G, it suffices to demonstrate our claim in the case of a finite abelian p-group G. However, that result is just Lemma 2.3.6. □

For any $r \geq 0$, recall that

$$\mathscr{O}[\![T_1, T_2, \ldots, T_r]\!] \cong \varprojlim_n \mathscr{O}[T_1, T_2, \ldots, T_r]/(T_1^n, T_2^n, \ldots, T_r^n).$$

The latter $\mathscr{O}$-modules in the inverse limit are free of finite rank over $\mathscr{O}$, and so can be given the $\mathfrak{m}$-adic topology, and the inverse limit then defines a topology on the power series ring itself.

The following lemma will be of use to us.

LEMMA 2.3.8. *Suppose that $\mathscr{O}$ is a complete commutative local noetherian ring with finite residue field, and let $\mathfrak{m}$ denote its maximal ideal. Let $r \geq 1$. The following sets of ideals provide bases of open neighborhoods of 0 that all define the same topology on the ring $R = \mathscr{O}[T_1, T_2, \ldots, T_r]$:*

i. $\{I_{s,t} \mid s,t \geq 1\}$, *where* $I_{s,t} = \mathfrak{m}^s R + (T_1^t, T_2^t, \ldots, T_r^t)$,

ii. $\{\mathfrak{M}^n \mid n \geq 1\}$, *where* $\mathfrak{M} = \mathfrak{m}R + (T_1, T_2, \ldots, T_r)$,

iii. $\{J_{s,t} \mid s,t \geq 1\}$, *where*

$$J_{s,t} = \mathfrak{m}^s R + (\omega_t(T_1), \omega_t(T_2), \ldots, \omega_t(T_r))$$

and we define

$$\omega_n(T) = (T+1)^{p^n} - 1$$

for any T and any $n \geq 0$.

In particular, R is isomorphic to the inverse limit of the quotients modulo the ideals in any of these sets.

PROOF. To show that two of the sets of ideals define the same topology is exactly to show that every ideal in each of the two sets contains an ideal in the other set. Note that

$$(T_1, T_2, \ldots, T_r)^{(t-1)r+1} \subseteq (T_1^t, T_2^t, \ldots, T_r^t).$$

We then see that

$$I_{1,t} \supseteq \mathfrak{M}^{(t-1)r+1} \quad \text{and} \quad J_{1,t} \supseteq \mathfrak{M}^{(p^t-1)r+1},$$

and from this we obtain that

$$I_{s,t} \supseteq I_{1,t}^s \supseteq \mathfrak{M}^{s((t-1)r+1)} \quad \text{and} \quad J_{s,t} \supseteq J_{1,t}^s \supseteq \mathfrak{M}^{s((p^t-1)r+1)}.$$

On the other hand, we have

$$\mathfrak{M}^n \supseteq I_{n,n} \quad \text{and} \quad \mathfrak{M}^n \supset J_{n,n},$$

where the latter containment uses that

$$\omega_n(T_i) = \sum_{j=1}^{p^n} \binom{p^n}{j} T_i^j \in (p^n T_i, p^{n-1} T_i^p, p^{n-2} T_i^{p^2}, \ldots, T_i^{p^n}) \subset (\mathfrak{m}^n + \mathfrak{m}^{n-1} T_i + \cdots + T_i^n) R \subset \mathfrak{M}^n.$$

Therefore, the topology defined by the powers of $\mathfrak{M}$ agrees both with the topologies defined by the ideals $I_{s,t}$ and by the ideals $J_{s,t}$. The final remark follows from the first part, as the set of $I_{s,t}$ defines the natural topology on the power series ring. □

THEOREM 2.3.9. *Let $\mathscr{O}$ be a complete commutative local noetherian ring with finite residue field of characteristic p. Suppose that $G \cong \mathbb{Z}_p^r$ for some r, and let $\{\gamma_i \mid 1 \leq i \leq r\}$ be a generating set of G. Then there is a unique topological isomorphism*

$$\mathscr{O}[\![G]\!] \xrightarrow{\sim} \mathscr{O}[\![T_1, T_2, \ldots, T_r]\!]$$

that takes $\gamma_i - 1$ to T_i.

PROOF. Let U_n be the open subgroup of G generated by $\{\gamma_i^{p^n} \mid 1 \leq i \leq r\}$ for some $n \geq 0$. We note that

$$\mathscr{O}[G/U_n] \to \mathscr{O}[T_1, T_2, \ldots, T_r]/(\omega_n(T_1), \omega_n(T_2), \ldots, \omega_n(T_r))$$

via the map that takes γ_i to $T_i + 1$. Moreover, note that $\omega_m(T_i)$ divides $\omega_n(T_i)$ for $m \leq n$, and these isomorphisms between group and polynomial rings are compatible with the canonical quotient maps on both sides. Since the groups U_n form a basis of open neighborhoods of 0 in G, we have

$$\mathscr{O}[\![G]\!] \cong \varprojlim_n \mathscr{O}[T_1, T_2, \ldots, T_r]/(\omega_n(T_1), \omega_n(T_2), \ldots, \omega_n(T_r))$$

On the other hand, we have

$$\mathscr{O}[\![T_1, T_2, \ldots, T_r]\!] \cong \varprojlim_n \mathscr{O}[T_1, T_2, \ldots, T_r]/(T_1^n, T_2^n \ldots, T_r^n).$$

Since $\mathscr{O} \cong \varprojlim \mathscr{O}/\mathfrak{m}^s$ as well, that the two inverse limits are isomorphic follows from the equality of the topologies defined by the sets of ideals in (i) and (iii) of Lemma 2.3.8. □

REMARK 2.3.10. We remark that the theorem implies that $\mathscr{O}[\![\mathbb{Z}_p^k]\!]$ is noetherian, as a power series ring in finitely many variables over a noetherian ring is noetherian, and Lemma 2.3.8 implies that it is complete with respect to its unique maximal ideal.

2.4. Invariants of Λ-modules

Let $\mathscr{O}$ be the valuation ring of a p-adic field, and let π be a uniformizer of the maximal ideal $\mathfrak{m}$ of $\mathscr{O}$. Set $\Lambda = \mathscr{O}[\![T]\!]$. We can use the structure theorem to construct invariants attached to a finitely generated Λ-module.

DEFINITION 2.4.1. Let M be a finitely generated Λ-module, pseudo-isomorphic to

$$\Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(\pi^{l_j})$$

for some $r, s, t \geq 0$, $k_i \geq 1$ and f_i a distinguished irreducible Λ-polynomial for $1 \leq i \leq s$, and $l_j \geq 1$ for $1 \leq j \leq t$.

i. The λ and μ-*invariants* of M are

$$\lambda(M) = \sum_{i=1}^{s} k_i \deg f_i \quad \text{and} \quad \mu(M) = \sum_{j=1}^{t} l_j,$$

respectively.

ii. The *characteristic polynomial* of M is

$$\operatorname{char}(M) = \pi^{\mu(M)} \prod_{i=1}^{s} f_i^{k_i},$$

and the *characteristic ideal* of M is the ideal $\operatorname{char}_\Lambda(M)$ of Λ generated by $\operatorname{char}(M)$.

We remark that the characteristic polynomial is multiplicative in exact sequences, as follows from the following lemma.

LEMMA 2.4.2. *Let*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

be a short exact sequence of finitely generated, torsion Λ*-modules. Then* $\operatorname{char}(B) = \operatorname{char}(A)\operatorname{char}(C)$.

PROOF. Let X be the set of height one prime ideals in the support of B, and let $S = \Lambda - \bigcup_{\mathfrak{p}\in X} \mathfrak{p}$. Identifying $S^{-1}A$, $S^{-1}B$, and $S^{-1}C$ with direct sums of quotients of $S^{-1}\Lambda$ by height one prime ideals, that the characteristic ideals of these modules are multiplicative in $S^{-1}\Lambda$ is a standard result in the theory of modules over a principal ideal domain. The lemma follows easily from this. □

We next consider the quotients of finitely generated, torsion Λ-modules. Recall that

$$\omega_n(T) = (T+1)^{p^n} - 1$$

for any $n \geq 0$.

REMARK 2.4.3. Suppose Γ is a procyclic group isomorphic to $\mathbb{Z}_p$, and let $\gamma \in \Gamma$ be a topological generator. Let Γ_n denote the quotient of Γ of order p^n. Recall that we have an isomorphism $\mathcal{O}[\![\Gamma]\!] \xrightarrow{\sim} \Lambda$ that takes $\gamma - 1$ to T. Then $\gamma^{p^n} - 1$ is taken to ω_n, so we have that

$$\mathcal{O}[\Gamma_n] \cong \Lambda/(\omega_n).$$

We then have that

$$\Lambda \cong \varprojlim_n \Lambda/(\omega_n).$$

Moreover, the quotient $M/\omega_n M$ of a Λ-module M is identified with the Γ^{p^n}-coinvariant group $M_{\Gamma^{p^n}}$ of M.

LEMMA 2.4.4. *If M is a finitely generated Λ-module, then the canonical maps*

$$M \xrightarrow{\sim} \varprojlim_n M/\omega_n M \xrightarrow{\sim} \varprojlim_{m,n} M/(\pi^m, \omega_n)M$$

are isomorphisms.

PROOF. Since Λ is noetherian and M is finitely generated, there exists a presentation of M as a Λ-module:

$$\Lambda^r \to \Lambda^s \to M \to 0$$

for some $r, s \geq 0$. Since tensor product is right exact and

$$\Lambda/(\pi^m, \omega_n) \otimes_\Lambda M \cong M/(\pi^m, \omega_n)M,$$

we have that

$$(\Lambda/(\pi^m, \omega_n))^r \to (\Lambda/(\pi^m, \omega_n))^s \to M/(\pi^m, \omega_n)M \to 0.$$

is exact as well. As the inverse limit is exact on finite groups, the resulting inverse limit

$$\Lambda^r \to \Lambda^s \to \varprojlim_{m,n} M/(\pi^m, \omega_n)M \to 0$$

is exact, so there is a canonical isomorphism

$$M \xrightarrow{\sim} \varprojlim_{m,n} M/(\pi^m, \omega_n)M.$$

Since the latter map factors as

$$M \to \varprojlim_n M/\omega_n M \to \varprojlim_{m,n} M/(\pi^m, \omega_n)M,$$

we are done if we can show the second of these maps is injective. By left exactness of the inverse limit, this will follow from the injectivity of the maps

$$M_n \to \varprojlim_m M_n/\pi^m M_n,$$

where we have set $M_n = M/\omega_n M$. For this, note that Nakayama's Lemma tells us that $A = \bigcap_m \pi^m M_n = 0$, since $\pi A = A$. □

REMARK 2.4.5. The proof of Lemma 2.4.4 goes through with ω_n replaced by any sequence f_n of distinguished polynomials with $f_m \mid f_n$ for $m \leq n$ and $f_m \neq f_n$ if $m < n$.

For $n \geq m$, we set $\omega_{n,m} = \omega_n/\omega_m$. Let us also set $\omega_{n,-1} = \omega_n$.

LEMMA 2.4.6. *Let M be a finitely generated torsion Λ-module containing no elements of finite order. Then there exists an integer $n_0 \geq -1$ such that $\omega_{n,n_0} M = p^{n-n_0} M$ for all $n \geq n_0$.*

PROOF. Since M has no p-torsion, we have $\mu(M) = 0$. The structure theorem implies the existence of a pseudo-isomorphism

$$\phi : M \to \bigoplus_{i=1}^{s} \Lambda/(f_i)$$

with f_i distinguished, and which must be injective as, again, M has no p-torsion. As $\prod_{i=1}^{s} f_i$ annihilates M, we have that $T^{\lambda(M)}$ annihilates $M/\pi M$. It follows that $(T+1)^{p^m}$ acts as the identity on $M/\pi M$ for any m with $p^m \geq \lambda(M)$. Fix such an m, and let n_0 be an integer such that $p^{n_0} \geq p^m(e+1)$, where $e+1$ is the ramification index of π in $\mathscr{O}$.

For $\theta \in \mathrm{End}_\Lambda(M)$ given by the action of $T+1$, the exact sequence

$$0 \to \mathrm{End}_\Lambda(M) \xrightarrow{\pi} \mathrm{End}_\Lambda(M) \to \mathrm{End}_\Lambda(M/\pi M)$$

implies that

$$\theta^{p^m} - 1 \in \pi \,\mathrm{End}_\Lambda(M).$$

For any $n \geq n_0$, we then have

$$\theta^{p^n} - 1 = ((\theta^{p^m} - 1) + 1)^{p^{n-m}} - 1 \in (\pi^{p^{n-m}}, p\pi)\,\mathrm{End}_\Lambda(M) = p\pi\,\mathrm{End}_\Lambda(M).$$

Let $\psi \in \mathrm{End}_\Lambda(M)$ with $\theta^{p^n} = 1 + p\pi\psi$. Since

$$\omega_{n+1,n} = \sum_{c=0}^{p-1} (T+1)^{cp^n},$$

we have that $\omega_{n+1,n}$ acts on M as

$$\sum_{c=0}^{p-1} (1 + p\pi\psi)^c \in p + \sum_{c=0}^{p-1} cp\pi\psi + p^2\,\mathrm{End}_\Lambda(M) \subseteq p + p\pi\,\mathrm{End}_\Lambda(M).$$

For $\bar{M} = M/p\pi M$, we therefore have that $\omega_{n+1,n} \cdot \bar{M} = p \cdot \bar{M}$. This forces

$$\omega_{n+1,n} \cdot M = p \cdot M$$

by Nakayama's lemma, which implies the result. □

We now have the following result on the orders of quotients of finitely generated, torsion Λ-modules.

THEOREM 2.4.7. *Let M be a finitely generated, torsion Λ-module, and let $n_0 \geq -1$ be such that* $\mathrm{char}(M)$ *and ω_{n,n_0} are relatively prime for all nonnegative $n \geq n_0$. Set $\lambda = \lambda(M)$ and $\mu = \mu(M)$. Let q denote the order of the residue field k of $\mathscr{O}$, and let e denote the ramification index of $\mathscr{O}$ over $\mathbb{Z}_p$. Then there exists an integer $\nu \in \mathbb{Z}$ such that*

$$|M/\omega_{n,n_0}M| = q^{p^n\mu + ne\lambda + \nu}$$

for all sufficiently large $n \geq 0$.

PROOF. Our proof consists of four steps. In the first, we treat the case of finite M. In the second, we reduce to the case of direct sums of quotients of Λ. In the third, we treat the quotients of Λ by powers of π, and in the fourth, we treat the quotients of Λ by distinguished polynomials. For simplicity of notation, let us set $\omega_n' = \omega_{n,n_0}$.

Step 1: Note first that if M is finite, then $M/\omega_n' M \cong M$ for n sufficiently large, as follows from Lemma 2.4.4, noting Remark 2.4.5. In this case, q^ν is then just the order of M. To see that ν is an integer and not just a rational number, note that M has a filtration $\{\pi^i M \mid i \geq 0\}$ and the graded quotients $\pi^i M/\pi^{i+1}M$ are finite-dimensional k-vector spaces, so of order a power of q. It follows that

$$|M| = \prod_{i=0}^{\infty} |\pi^i M/\pi^{i+1}M|$$

is a power of q as well.

Step 2: In the general case, consider the map

$$\phi : M \to N = \bigoplus_{i=1}^{s} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(\pi^{l_j})$$

constructed in Theorem 2.2.13. It has finite kernel and cokernel, and the induced maps

$$\phi_n : M/\omega_n' M \to N/\omega_n' N$$

fit into a commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \ker\phi & \xrightarrow{\omega_n'} & \ker\phi & \longrightarrow & \ker\phi_n & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & M & \xrightarrow{\omega_n'} & M & \longrightarrow & M/\omega_n' M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\phi_n} & & \\
0 & \longrightarrow & N & \xrightarrow{\omega_n'} & N & \longrightarrow & N/\omega_n' N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{coker}\phi & \xrightarrow{\omega_n'} & \operatorname{coker}\phi & \longrightarrow & \operatorname{coker}\phi_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where the map $\omega_n' : N \to N$ is injective since one cannot have $\omega_n' g \in (f_i^{k_i})$ (or in (π^{l_j})) for some i (resp., j) unless $g \in (f_i^{k_i})$ (resp., (π^{l_j})) as ω_n' is relatively prime to each f_i by assumption (and to π by definition). Now, for sufficiently large n, we have that multiplication by ω_n' is the zero map on $\ker\phi$

and $\operatorname{coker}\phi$, as $\ker\phi$ and $\operatorname{coker}\phi$ are finite. Therefore, the snake lemma tells us that, for such n, we have $\operatorname{coker}\phi \cong \operatorname{coker}\phi_n$ and an exact sequence

$$0 \to \ker\phi \to \ker\phi_n \to \operatorname{coker}\phi \to 0.$$

Defining $\eta \geq 0$ by

$$q^\eta = |\ker\phi| = \frac{|\ker\phi_n|}{|\operatorname{coker}\phi_n|},$$

we have that

$$|M/\omega_n' M| = q^\eta \prod_{i=1}^{s} |\Lambda/(\omega_n', f_i^{k_i})| \cdot \prod_{j=1}^{t} |\Lambda/(\omega_n', \pi^{l_j})|$$

for the same sufficiently large n. This reduces the theorem to modules of the form $M = \Lambda/(\pi^l)$ for some $l \geq 1$ or $M = \Lambda/(f)$ with f a (a power of an irreducible) distinguished polynomial relatively prime to every ω_n'.

Step 3: Suppose now that $M = \Lambda/(\pi^l)$ for some $l \geq 1$. We then have

$$M/\omega_n' M = \Lambda/(\omega_n', \pi^l) \cong (\mathscr{O}/\pi^l\mathscr{O})[\![T]\!]/(\omega_n'),$$

Since ω_n' is a distinguished polynomial of degree $p^n - p^{n_0}$, the latter ring is isomorphic to $(\mathscr{O}/\pi^l\mathscr{O})^{p^n}$ as an $\mathscr{O}$-module. We therefore have that

$$|M/\omega_n' M| = q^{p^n l - p^{n_0} l}.$$

Note that $\mu(M) = l$, and we can take $\nu = -p^{n_0} l$ for this M.

Step 4: Finally, suppose that $M = \Lambda/(f)$ for some distinguished polynomial f relatively prime to every ω_n'. By Lemma 2.4.6, we have that there exists $n_1 \geq n_0$ such that

$$\omega_{n,n_1} M = p^{n-n_1} M$$

for all $n \geq n_1$. We also have an exact sequence

$$0 \to M/\omega_{n_1}' M \xrightarrow{\omega_{n,n_1}} M/\omega_n' M \to M/\omega_{n,n_1} M \to 0,$$

and therefore we have

$$M/\omega_{n,n_1} M \cong M/p^{n-n_1} M \cong (\mathscr{O}/\pi^{e(n-n_1)}\mathscr{O})^\lambda,$$

the latter isomorphism being of $\mathscr{O}$-modules. Defining $\nu \in \mathbb{Z}$ by

$$q^\nu = |M/\omega_{n_1}' M| \cdot q^{-n_1 e\lambda},$$

we then have

$$|M/\omega_n' M| = q^{ne\lambda + \nu},$$

as desired.

□

We next wish to consider results which give us conditions that allow us to compute invariants of Λ-modules from their quotients. For this, the following lemma is useful.

LEMMA 2.4.8. *Let $\phi: M \to N$ be a pseudo-isomorphism of Λ-modules, and let $f \in \Lambda$ be a distinguished polynomial. Then the induced map $\phi_f: M/fM \to N/fN$ is also a pseudo-isomorphism, and moreover, we have*

$$|\ker \phi_f| \leq |\ker \phi||\operatorname{coker} \phi| \quad \text{and} \quad |\operatorname{coker} \phi_f| \leq |\operatorname{coker} \phi|.$$

Similarly, using $A[f]$ to denote the kernel of $f: A \to A$ for any Λ-module A, the induced map ${}_f\phi: M[f] \to N[f]$ is also a pseudo-isomoprhism, and we have

$$|\ker {}_f\phi| \leq |\ker \phi| \quad \text{and} \quad |\operatorname{coker} {}_f\phi| \leq |\ker \phi||\operatorname{coker} \phi|.$$

PROOF. Consider first the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M/\ker\phi & \xrightarrow{\phi} & N & \longrightarrow & \operatorname{coker}\phi & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow f & & \downarrow f & & \\ 0 & \longrightarrow & M/\ker\phi & \xrightarrow{\phi} & N & \longrightarrow & \operatorname{coker}\phi & \longrightarrow & 0. \end{array}$$

The snake lemma then yields an exact sequence

$$0 \to (M/\ker\phi)[f] \to N[f] \to (\operatorname{coker}\phi)[f] \to M/(fM+\ker\phi) \to N/fN \to \operatorname{coker}\phi_f \to 0. \tag{2.4.1}$$

The kernel of ϕ_f has order at most the products of the orders of the kernels of the maps $M/fM \to M/(fM+\ker\phi)$ and $M/(fM+\ker\phi) \to N/fN$. The first clearly has order at most $|\ker\phi|$, and by (2.4.1), the second has order at most $|\operatorname{coker}\phi|$. The statement on $\operatorname{coker}\phi_f$ is also clear from the exact sequence.

As for ${}_f\phi$, the snake lemma applied to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker\phi & \longrightarrow & M & \xrightarrow{\phi} & M/\ker\phi & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow f & & \downarrow f & & \\ 0 & \longrightarrow & \ker\phi & \longrightarrow & M & \xrightarrow{\phi} & M/\ker\phi & \longrightarrow & 0. \end{array}$$

yields exactness of

$$0 \to (\ker\phi)[f] \to M[f] \to (M/\ker\phi)[f] \to \ker\phi/f\ker\phi,$$

Together with (2.4.1), this implies that ${}_f\phi$ has finite kernel contained in $\ker\phi$ and finite cokernel of order at most $|\ker\phi| \cdot |\operatorname{coker}\phi|$. □

DEFINITION 2.4.9. Let A be a finitely generated $\mathcal{O}$-module. The π-rank $r_\pi(A)$ of A is the dimension of $A/\pi A$ as a vector space over $k = \mathcal{O}/\pi\mathcal{O}$.

PROPOSITION 2.4.10. *Let M be a finitely generated, torsion Λ-module. Then $\mu(M) = 0$ if and only if the quantities $r_\pi(M/\omega_n M)$ are bounded as n varies.*

PROOF. Consider a pseudo-isomorphism

$$\phi : M \to N = \bigoplus_{i=1}^{s} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(\pi^{l_j}).$$

Then $\phi_{\omega_n} : M/\omega_n M \to N/\omega_n N$ has finite kernel and cokernel of bounded order by Lemma 2.4.8, so it suffices to check the result for N. Note that the π-rank of $\Lambda/(f, \omega_n)$ for f a distinguished polynomial is bounded by $\deg f$, since $\Lambda/(f) \cong \mathcal{O}^{\deg f}$ as an $\mathcal{O}$-module. On the other hand, $\Lambda/(\pi^l, \omega_n)$ is isomorphic to $(\mathcal{O}/\pi^l)^{p^n}$ as an $\mathcal{O}$-module, so has unbounded π-rank. □

Similarly, we have the following proposition for the λ-invariant.

PROPOSITION 2.4.11. *Let M be a finitely generated, torsion Λ-module. Then $\lambda(M)$ is equal to the following quantities:*

i. $\operatorname{rank}_{\mathcal{O}} M$ *and*

ii. the maximal integer λ such that M has a quotient isomorphic to $(\mathcal{O}/\pi^n\mathcal{O})^\lambda$ as an $\mathcal{O}$-module for every n.

PROOF. Consider a pseudo-isomorphism

$$\phi : M \to N = \bigoplus_{i=1}^{s} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(\pi^{l_j}).$$

Let $n > \mu(M)$. Then $\Lambda/(\pi^{l_j})$ has trivial $\mathcal{O}$-rank and no quotient of the form $\mathcal{O}/\pi^n\mathcal{O}$, since $n > l_j$. On the other hand, $\Lambda/(f_i^{k_i})$ is isomorphic to $\mathcal{O}^{k_i \deg f_i}$ as an $\mathcal{O}$-module by Remark 2.2.11, so has a quotient of the form $(\mathcal{O}/\pi^n\mathcal{O})^m$ for exactly those $m \leq k_i \deg f_i$. Therefore, the result holds for N.

By definition, $\mathcal{O}$-rank is not affected by pseudo-isomorphism, so $\lambda(M) = \operatorname{rank}_{\mathcal{O}} M$. Moreover, if $\lambda = \operatorname{rank}_{\mathcal{O}} M$, then the quotient of M modulo its π-power torsion subgroup is a finitely generated torsion-free $\mathcal{O}$-module of rank λ, hence is isomorphic to $\mathcal{O}^\lambda$ and has a quotient isomorphic to $(\mathcal{O}/\pi^n\mathcal{O})^m$ for exactly those $m \leq \lambda$. □

Finally, for finitely generated Λ-modules which are not necessarily Λ-torsion, we have the following result on Λ-ranks.

PROPOSITION 2.4.12. *Let M be a finitely generated Λ-module. Then we have*

$$\operatorname{rank}_\Lambda(M) = \operatorname{rank}_{\mathscr{O}}(M/TM) - \operatorname{rank}_{\mathscr{O}}(M[T]).$$

Moreover, we have

$$\operatorname{rank}_{\mathscr{O}}(M/\omega_n M) = p^n \operatorname{rank}_\Lambda(M) + c$$

for some $c \geq 0$ for all sufficiently large n.

PROOF. Again consider a pseudo-isomorphism

$$\phi : M \to N = \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(\pi^{l_j}).$$

Then $\operatorname{rank}_\Lambda(M) = \operatorname{rank}_\Lambda(N)$, and by Lemma 2.4.8, we have

$$\operatorname{rank}_{\mathscr{O}}(M/TM) = \operatorname{rank}_{\mathscr{O}}(N/TN) \quad \text{and} \quad \operatorname{rank}_{\mathscr{O}}(M[T]) = \operatorname{rank}_{\mathscr{O}}(N[T]),$$

or more strongly, that $M[T] \to N[T]$ is a pseudo-isomorphism.

Given this, the proof of the first part is reduced to case that $M = N$. Since $\Lambda/T\Lambda$ has $\mathscr{O}$-rank 1 and $\Lambda/(f)$ for a distinguished polynomial f has

$$\Lambda/(f,T) \cong \mathscr{O}/f(0)\mathscr{O},$$

we have that the $\mathscr{O}$-rank of the latter module is nonzero, and then equal to 1, if and only if T divides f. Finally, $\Lambda/(T,\pi^l) \cong \mathscr{O}/\pi^l\mathscr{O}$ for $l \geq 1$ and so has trivial $\mathscr{O}$-rank. It follows that $\operatorname{rank}_{\mathscr{O}}(N/TN) = r + s$, where s is the number of f_i equal to T. As for $N[T]$, note that $\Lambda[T] = 0$ and $\Lambda/(\pi^l)[T] = 0$, while $\Lambda/(f)[T]$ is nonzero, and then of $\mathscr{O}$-rank 1, if and only if T divides f. Therefore, we have $\operatorname{rank}_{\mathscr{O}} N[T] = s$, and part a follows.

We note that $\operatorname{rank}_{\mathscr{O}[\![\omega_n]\!]}(M) = p^n \operatorname{rank}_\Lambda(M)$, since Λ has rank p^n over $\mathscr{O}[\![\omega_n]\!]$. The first part applied with T replaced by ω_n then implies

$$\operatorname{rank}_{\mathscr{O}}(M/\omega_n M) = p^n \operatorname{rank}_\Lambda(M) + \operatorname{rank}_{\mathscr{O}}(M[\omega_n]).$$

It suffices then to show that $\operatorname{rank}_{\mathscr{O}}(M[\omega_n])$ is bounded in n. But this follows as $\omega_{n,m}$ is relatively prime to $\operatorname{char}_\Lambda(M)$ for n sufficiently large for all m. □

2.5. Pontryagin duality

Let A be a locally compact, Hausdorff topological abelian group.

DEFINITION 2.5.1. The *Pontryagin dual* of A is defined to be the topological group

$$A^\vee = \operatorname{Hom}_{\text{cts}}(A, \mathbb{R}/\mathbb{Z})$$

with the compact-open topology, which is to say, with basis of open sets of the form

$$\mathscr{B}(K,U) = \{f \in A^\vee \mid f(K) \subseteq U\},$$

where $K \subset A$ is compact and $U \subset \mathbb{R}/\mathbb{Z}$ is open.

Of course, if $f\colon A \to B$ is a continuous map of locally compact, Hausdorff abelian groups, then there is a natural map $f^\vee\colon B^\vee \to A^\vee$ given by $f^\vee(\varphi) = \varphi \circ f$.

The following is the key theorem regarding the Pontryagin dual, which we state without proof.

THEOREM 2.5.2 (Pontryagin duality). *Let $\mathscr{L}$ denote the category of locally compact, Hausdorff topological abelian groups, let $\mathscr{C}$ denote the category of compact, Hausdorff topological abelian groups, and let $\mathscr{D}$ denote the category of discrete topological abelian groups. Then the Pontryagin dual provides a self-inverse contravariant functor from $\mathscr{L}$ to its itself. Moreover, it induces contravariant equivalences of categories between $\mathscr{C}$ and $\mathscr{D}$ in both directions.*

REMARK 2.5.3. If A is a profinite or discrete torsion, then in fact

$$A^\vee = \mathrm{Hom}_{\mathrm{cts}}(A, \mathbb{Q}/\mathbb{Z}),$$

while if A is pro-p or discrete p-torsion, then we have

$$A^\vee = \mathrm{Hom}_{\mathrm{cts}}(A, \mathbb{Q}_p/\mathbb{Z}_p).$$

Moreover, we note that if A is discrete, then every homomorphism from it is continuous. On the other hand, if A is a finitely generated $\mathbb{Z}_p$-module, then every $\mathbb{Z}_p$-linear homomorphism is continuous, so

$$A^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Q}_p/\mathbb{Z}_p).$$

REMARK 2.5.4. If A has the additional structure of a topological G-module for a profinite group G, then $A^\vee$ has the continuous G-action given by

$$(g \cdot f)(a) = f(g^{-1}a)$$

for $g \in G$, $f \in A^\vee$ and $a \in A$.

REMARK 2.5.5. Pontryagin duality induces a nondegenerate continuous pairing

$$A \times A^\vee \to \mathbb{Q}_p/\mathbb{Z}_p, \qquad (a,f) \mapsto f(a).$$

If A is also a topological G-module, then the latter pairing is G-equivariant.

Here is another interesting result.

PROPOSITION 2.5.6.

a. If A is a compact, Hausdorff topological $\mathbb{Z}_p$-module, then A is profinite.

b. If A is a discrete topological $\mathbb{Z}_p$-module, then A is $\mathbb{Z}_p$-torsion.

PROOF. Let us start with part b. Since A is discrete, every element $a \in A$ has $p^n a = 0$ for some $n \geq 0$ by continuity of the action. As for part a, we note that the dual of a compact $\mathbb{Z}_p$-module is A a discrete $\mathbb{Z}_p$-module, hence $\mathbb{Z}_p$-torsion. Then $A^\vee$ is the direct limit of the finite submodules generated by any finite set of its elements, so A is the topologically the inverse limit of the Pontryagin duals of those submodules, and therefore A is profinite. □

COROLLARY 2.5.7. *Every finite topological $\mathbb{Z}_p$-module has the discrete topology.*

EXAMPLE 2.5.8. Since $\mathbb{Z}_p$ is procyclic, a continuous homomorphism from it is determined by where 1 is sent. Since $\mathbb{Z}_p$ is a free pro-p group, we can send 1 to any element. Therefore, we have $\mathbb{Z}_p^\vee = \mathbb{Q}_p/\mathbb{Z}_p$.

DEFINITION 2.5.9. We say an locally compact module over a profinite ring R is *cofinitely generated* if its Pontryagin dual is a finitely generated right R-module.

2.6. Iwasawa adjoints

We continue to suppose that $\Lambda = \mathscr{O}[\![T]\!]$ for a valuation ring $\mathscr{O}$ of a p-adic field with uniformizer π. Let F denote the quotient field of $\mathscr{O}$. We will be most interested in Pontryagin duals of Λ-modules.

DEFINITION 2.6.1. Let $\iota : \Lambda \to \Lambda$ be the unique continuous $\mathscr{O}$-linear ring homomorphism satisfying $\iota(T) = (T+1)^{-1} - 1$.

We can convert the canonical right action on the Pontryagin dual of a Λ-module to a left action using an involution, as follows.

PROPOSITION 2.6.2. *If M is a locally compact, Hausdorff topological Λ-module, then $M^\vee$ is as well, with respect to the action*

$$(\lambda \cdot \varphi)(m) = \varphi(\iota(\lambda)m) \tag{2.6.1}$$

for $\lambda \in \Lambda$, $m \in M$, and $\varphi \in M^\vee$.

Let $s \geq 0$ be such that π^s generates the different of $\mathscr{O}/\mathbb{Z}_p$. Then the $\mathscr{O}$-balanced pairing

$$\mathscr{O} \times \mathscr{O} \to \mathbb{Z}_p, \qquad (x,y) \mapsto \mathrm{Tr}_{F/\mathbb{Q}_p}(\pi^{-s}xy) \tag{2.6.2}$$

is perfect. For a locally compact, Hausdorff topological Λ-module M, we have a left Λ-module structure on $\mathrm{Hom}_{\mathscr{O}}(M, F/\mathscr{O})$ as in (2.6.1), with φ now in $\mathrm{Hom}_{\mathscr{O}}(M, F/\mathscr{O})$.

PROPOSITION 2.6.3. *For every finitely or cofinitely generated $\mathscr{O}$-module A, there exists an isomorphism*

$$A^\vee \cong \mathrm{Hom}_{\mathscr{O}}(A, F/\mathscr{O}).$$

These can be chosen to be natural in A in a manner that is canonical up to the choice of uniformizer π of $\mathscr{O}$. Moreover, if A is a Λ-module, then the isomorphism is of Λ-modules.

PROOF. The perfect pairing of (2.6.2) yields an isomorphism $\mathscr{O} \cong \mathrm{Hom}(\mathscr{O}, \mathbb{Z}_p)$ and therefore the composite $\mathscr{O}$-module isomorphism

$$F/\mathscr{O} \cong \mathscr{O} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}, \mathbb{Q}_p/\mathbb{Z}_p).$$

Since A is (co)finitely generated over $\mathbb{Z}_p$, we have the following Λ-module isomorphisms

$$A^\vee \cong \mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}_{\mathscr{O}}(A, \mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}, \mathbb{Q}_p/\mathbb{Z}_p)) \cong \mathrm{Hom}_{\mathscr{O}}(A, F/\mathscr{O}),$$

and naturality is easily checked. □

We have the following analogue of Proposition 2.5.6.

PROPOSITION 2.6.4.

a. Every compact Λ-module is an inverse limit of finite Λ-modules.

b. Every discrete Λ-module is a direct limit of finite Λ-modules.

PROOF. By Pontryagin duality, it suffices to prove part b. For this, we again note that the continuity of the Λ-action on a discrete module M ensures that, for any $m \in M$, the annihilator $\mathrm{Ann}_\Lambda(m)$ is an open ideal of Λ. But then M is the union of its finite Λ-submodules $\Lambda \cdot m$ for $m \in M$. □

Note that if M is a finitely generated Λ-module, we endow it with the topology under which $(\pi^m, \omega_n)M$ forms a basis of open submodules of M.

DEFINITION 2.6.5. Let M be a finitely generated, torsion Λ-module, and set $M_n = M/\omega_{n,m}M$ for $n \geq m$ and some fixed $m \geq -1$ with $\omega_{n,m}$ relatively prime to $\mathrm{char}(M)$ for all n. Set

$$\alpha(M) = \varprojlim_n M_n^\vee \cong (\varinjlim_n M_n)^\vee,$$

where $M_n \to M_{n+1}$ is induced by the map $m \mapsto \omega_{n+1,n}m$ on M. Then the Λ-module $\alpha(M)$ is called the Iwasawa adjoint to M.

REMARKS 2.6.6.

a. We leave it to the reader to check that the definition of $\alpha(M)$ does not depend on m.

b. If $\phi\colon M \to N$ is a Λ-module homomorphism, where M and N are finitely generated and Λ-torsion, then we obtain a natural Λ module homomorphism $\alpha(\phi)\colon \alpha(N) \to \alpha(M)$.

LEMMA 2.6.7. *The contravariant functor α is left exact.*

PROOF. To see the exactness, note that

$$M_n \cong M \otimes_\Lambda \Lambda/(\omega_{n,m}),$$

the tensor product is right exact, the Pontryagin dual is an exact contravariant functor, and the inverse limit is exact on finite abelian groups. □

LEMMA 2.6.8. *If M is a finite Λ-module, then $\alpha(M) = 0$.*

PROOF. Since M is finite, the map $\omega_{n,m}\colon M \to M$ is zero for n sufficiently large relative to a fixed m. The result follows. □

LEMMA 2.6.9. *If M is a finitely generated, torsion Λ-module with $\mu(M) = 0$, then there are natural isomorphisms*

$$\alpha(M) \cong \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p) \cong \mathrm{Hom}_{\mathscr{O}}(M, \mathscr{O})$$

as Λ-modules. Here, Λ acts on both $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ and $\mathrm{Hom}_{\mathscr{O}}(M, \mathscr{O})$ by

$$(\lambda \cdot \phi)(m) = \phi(\iota(\lambda)m).$$

PROOF. Let N be the p-power torsion submodule of M. By Lemma 2.6.7 and Lemma 2.6.8, the map $\alpha(M/N) \to \alpha(M)$ is an isomorphism, so we can and do suppose that M is p-torsion-free.

Since M is finitely generated over $\mathbb{Z}_p$, we have that for sufficiently large m and $n \geq m$ that $\omega_{n,m}$ acts on M by multiplication by p^{n-m} by Lemma 2.4.6. Therefore, we see that

$$\alpha(M) \cong \varprojlim_n (M/p^n M)^\vee \cong \varprojlim_n \mathrm{Hom}_{\mathbb{Z}_p}(M/p^n M, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p).$$

For the other isomorphism, we note that

$$\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p) \cong \mathrm{Hom}_{\mathbb{Z}_p}(M \otimes_{\mathscr{O}} \mathscr{O}, \mathbb{Z}_p) \cong \mathrm{Hom}_{\mathscr{O}}(M, \mathrm{Hom}(\mathscr{O}, \mathbb{Z}_p)) \cong \mathrm{Hom}_{\mathscr{O}}(M, \mathscr{O}),$$

the latter isomorphism using the pairing of (2.6.2), and all of these isomorphisms are of Λ-modules. □

PROPOSITION 2.6.10. *Let $\phi\colon M \to N$ be a pseudo-isomorphism of finitely generated, torsion Λ-modules. Then the induced map $\alpha(\phi)\colon \alpha(N) \to \alpha(M)$ an injective pseudo-isomorphism.*

PROOF. As the inverse limit is exact on finite modules, in order to show that $\alpha(\phi)$ is a pseudo-isomorphism it suffices to show that the maps $N_n^\vee \to M_n^\vee$ have kernel and cokernel of bounded order. By exactness of the Pontryagin dual, this reduces to proving that $M_n \to N_n$ has kernel and cokernel of bounded order, which follows from Lemma 2.4.8.

Finally, by Lemma 2.6.7, we have that the sequence

$$0 \to \alpha(\mathrm{coker}\,\phi) \to \alpha(N) \xrightarrow{\alpha(\phi)} \alpha(M)$$

is exact. The injectivity of $\alpha(\phi)$ then follows from Corollary 2.6.8. □

DEFINITION 2.6.11. For a Λ-module M, we let M^ι denote the Λ-module that is M as a set but on which the Λ-action $\cdot_\iota$ is

$$\lambda \cdot_\iota m = \iota(\lambda)m$$

for $\lambda \in \Lambda$ and $m \in M$.

LEMMA 2.6.12.

a. For any positive integer ℓ, we have $\alpha(\Lambda/(\pi^l)) \cong \Lambda/(\pi^l)$.

b. For any distinguished polynomial f, we have $\alpha(\Lambda/(f)) \cong \Lambda/(\iota(f))$.

PROOF. For part a, set $\gamma = T+1$ and let $M = \Lambda/(\pi^l)$. Then any element in $M_n = M/\omega_n M$ (taking $m = -1$) may be uniquely written as

$$f = \sum_{i=0}^{p^n-1} a_i \gamma^i$$

modulo $\omega_n = \gamma^{p^n} - 1$, for some $a_i \in \mathscr{O}/\pi^l\mathscr{O}$ for $0 \le i \le p^n - 1$. Let us identify $M_n^\vee$ with $\mathrm{Hom}_{\mathscr{O}}(M_n, F/\mathscr{O})$ as in Proposition 2.6.3. We define a map

$$\psi_n \colon M_n \to M_n^\vee$$

by setting

$$\psi_n(f)(\gamma^i) = \frac{a_i}{\pi^l},$$

and extending $\mathscr{O}$-linearly. Then ψ_n is clearly an injective homomorphism, and it is also easily seen that the $\psi_n(\gamma^i)$ form a $\mathscr{O}$-basis of $M_n^\vee$, so ψ_n is surjective as well. Moreover, ψ_n is a map of Λ-modules as

$$\psi_n(\gamma f)(\gamma^i) = \frac{a_{i-1}}{\pi^l} = \psi_n(f)(\gamma^{i-1}) = (\gamma \cdot \psi_n(f))(\gamma^i).$$

The diagram

$$\begin{array}{ccc} M_{n+1} & \xrightarrow{\psi_{n+1}} & M_{n+1}^\vee \\ \downarrow & & \downarrow \omega_{n+1,n}^\vee \\ M_n & \xrightarrow{\psi_n} & M_n^\vee \end{array}$$

commutes since

$$\omega_{n+1,n}^\vee(\psi_{n+1}(f))(\gamma^i) = \psi_{n+1}(f)(\iota(\omega_{n+1,n})\gamma^i) = \sum_{j=0}^{p-1} \psi_{n+1}(f)(\gamma^{i+p^n j}) = \psi_n(f)(\gamma^i).$$

In the inverse limit, we obtain $\alpha(\Lambda/(\pi^l)) \cong \Lambda/(\pi^l)$.

For part b, suppose that $M = \Lambda/(f)$ with f a distinguished polynomial of degree d. Let us define $\varepsilon\colon \Lambda \to \mathscr{O}$ by setting $\varepsilon(g)$ equal to the coefficient of T^{d-1} in r, where $r \in \mathscr{O}[T]$ is the unique polynomial of degree less than d with $g = qf + r$ for some $q \in \Lambda$. We then define

$$\theta\colon \Lambda/(f) \to \mathrm{Hom}_{\mathscr{O}}(\Lambda/(f), \mathscr{O})^{\iota}$$

by

$$\theta(\bar{g})(\bar{h}) = \varepsilon(gh),$$

where $\bar{g}, \bar{h} \in \Lambda/(f)$ and $g, h \in \Lambda$ are lifts of $\bar{g}$ and $\bar{h}$ respectively. This is clearly well-defined, and moreover it is a Λ-module homomorphism, since

$$\theta(\lambda\bar{g})(\bar{h}) = \varepsilon(\lambda gh) = \theta(\bar{g})(\lambda\bar{h}) = (\lambda \cdot \theta(\bar{g}))(\bar{h}).$$

If $r \in \mathscr{O}[T]$ is nonzero of degree less k than d, then letting $\bar{r}$ denote the image of r in $\Lambda/(f)$, we have

$$\theta(\bar{r})(T^{d-1-k}) = \varepsilon(T^{d-1-k}r) \neq 0,$$

which means that $\bar{r} \notin \ker\theta$, so θ is injective. A count of $\mathscr{O}$-ranks now tells us that α has finite cokernel.

In fact, θ is surjective, as for any $0 \leq k \leq d-1$ and $g = \sum_{i=0}^{d-1} a_i T^i$, we have that

$$T^k g - \sum_{j=1}^{k} a_{d-j} T^{k-j} f \equiv \sum_{i=k}^{d-1} a_{i-k} T^i \bmod \pi,$$

since f is distinguished, and hence

$$\theta(T^k)(\bar{g}) \equiv a_{d-1-k} \bmod \pi.$$

Since the functions $\phi_k \in \mathrm{Hom}_{\mathscr{O}}(\Lambda/(f), \mathscr{O})^{\iota}$ with $\phi_k(g) = a_{d-1-k}$ generate $\mathrm{Hom}_{\mathscr{O}}(\Lambda/(f), \mathscr{O})^{\iota}$ and agree with the $\theta(T^k)$ modulo π, the $\theta(T^k)$ do as well by Nakayama's lemma. In other words, θ is an isomorphism $\Lambda/(f) \to \alpha(\Lambda/(f))^{\iota}$, and part b follows as $(\Lambda/(f))^{\iota} \cong \Lambda/(\iota(f))$. □

THEOREM 2.6.13. *Let M be a finitely generated, torsion Λ-module. Then $\alpha(M)$ is a finitely generated, torsion Λ-module that is pseudo-isomorphic to M^{ι}. Moreover, $\alpha(M)$ contains no nontrivial finite Λ-submodules.*

PROOF. Consider a pseudo-isomorphism

$$\theta\colon N = \bigoplus_{i=1}^{s} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(\pi^{l_j}) \to M,$$

which exists by the structure theorem and Proposition 2.1.11. Note that $\alpha(\theta)\colon \alpha(M) \to \alpha(N)$ is an injective pseudo-isomorphism. If we can show that $\alpha(N)$ is pseudo-isomorphic to N^{ι}, then clearly $\alpha(M)$ will be pseudo-isomorphic to M^{ι}, as pseudo-isomorphism is an equivalence relation on finitely generated, torsion Λ-modules. Moreover, if $\alpha(N)$ has no nonzero finite Λ-submodules, then neither

does $\alpha(M)$, being isomorphic to a submodule of $\alpha(N)$. By the additivity of the adjoint functor, it then suffices to assume that M is a quotient of Λ by a height one prime ideal, but this is covered by Lemma 2.6.12. □

2.7. The group ring of a cyclic p-group

Let us suppose that G is a cyclic group of order p. In this section, we wish to study the structure theory of modules over $\mathbb{Z}_p[G]$ that are finitely generated, free $\mathbb{Z}_p$-modules. From our study of modules over $\Lambda = \mathbb{Z}_p[\![T]\!]$ (or representation theory over $\mathbb{Q}_p$), we are easily able to classify such modules up to pseudo-isomorphism.

Let $N_G \in \mathbb{Z}_p[G]$ denote the norm element, and let $X = \mathbb{Z}_p[G]/N_G$, which is noncanonically isomorphic to the augmentation ideal I_G via the map $x \mapsto (g-1)x$, for $g \in G$ a generator.

LEMMA 2.7.1. *Let A be a finitely generated $\mathbb{Z}_p[G]$-module, where G is cyclic of order p. Then there are $s,t \geq 0$ and a homomorphism*

$$\phi : A \to X^s \oplus \mathbb{Z}_p^t$$

with finite kernel and cokernel, and $\ker \phi = 0$ *if and only if A is p-torsion free.*

PROOF. We remark that for a given generator g of G, we have an isomorphism

$$\psi : \Lambda/(\omega_1) \xrightarrow{\sim} \mathbb{Z}_p[G]$$

determined by $\psi(T) = g-1$. Any element of A generates a cyclic $\mathbb{Z}_p[G]$-module, which may then be viewed as a quotient of $\Lambda/(\omega_1)$. Since $\omega_1 = T \cdot \omega_{1,0}$ and $\omega_{1,0}$ is irreducible, we have $\Lambda/(\omega_1, f)$ is finite for a power series $f \in \Lambda$ if f is not a unit times a product of a power of T and a power of $\omega_{1,0}$. This leaves three possibilities for nontrivial p-torsion free quotients of $\Lambda/(f)$, which are $\Lambda/(f) \cong \mathbb{Z}_p[G]$, $\Lambda/(T) \cong \mathbb{Z}_p$, and $\Lambda/(\omega_{1,0}) \cong X$, since $\psi(\omega_{1,0}) = N_G$. Therefore, the structure theorem for finitely generated Λ-modules tells us that A is pseudo-isomorphic to a direct sum of copies of the latter two $\mathbb{Z}_p[G]$-modules, $\mathbb{Z}_p$ and X. □

REMARK 2.7.2. The $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p[G]$ is pseudo-isomorphic to $X \oplus \mathbb{Z}_p$. Explicitly, letting ε denote the augmentation map, we have

$$\begin{aligned} \mathbb{Z}_p[G] &\to X \oplus \mathbb{Z}_p, \qquad a \mapsto ((g-1)a, \varepsilon(a)) \\ X \oplus \mathbb{Z}_p &\to \mathbb{Z}_p[G], \qquad (x,b) \mapsto x + bN_G, \end{aligned}$$

and both of these maps are injective with cokernel isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

We now state the main result of the section.

THEOREM 2.7.3. *Let A be a finitely generated $\mathbb{Z}_p[G]$-module that is p-torsion free. Then there is an isomorphism*

$$\phi : A \to \mathbb{Z}_p[G]^r \oplus X^s \oplus \mathbb{Z}_p^t$$

of $\mathbb{Z}_p[G]$-modules for some $r,s,t \geq 0$.

PROOF. Since $\mathbb{Z}_p[G]$ is $\mathbb{Z}_p[G]$-projective, we also have that if $B \cong \mathbb{Z}_p[G]^r$ is the maximal $\mathbb{Z}_p[G]$-free quotient of A, then setting $A' = \ker(A \to B)$, we have an isomorphism

$$A \cong A' \oplus \mathbb{Z}_p[G]^r,$$

where A' has no free $\mathbb{Z}_p[G]$-quotient. We may therefore assume that A itself has no free $\mathbb{Z}_p[G]$-quotient.

Consider the sequence

$$0 \to A^G \to A \to I_G A \to 0.$$

Since A is p-torsion free, we must have $(I_G A)^G = 0$, since there is an injective pseudo-isomorphism

$$\psi : A \to X^s \oplus \mathbb{Z}_p^t$$

for some $s,t \geq 0$, and $(I_G X)^G = 0$, while $I_G \mathbb{Z}_p = 0$. In particular, we have that $A^G \cong \mathbb{Z}_p^t$, and there is an injective pseudo-isomorphism from $I_G A$ to X^u for the above u, since $I_G X \simeq X$.

Let $\{x_1, \ldots, x_m\}$ be a minimal generating set of $I_G A$ as a $\mathbb{Z}_p[G]$-module. We note that $\mathbb{Z}_p[G]x_i$ is isomorphic to a finite index submodule of X, and it is therefore a power $I_G^n X$ for some n. (Here, note that $pX \in I_G X$.) The map $X \to I_G^n$ given by $x \mapsto (g-1)^n x$ for a generator $g \in G$, is an isomorphism, so in fact we have $\mathbb{Z}_p[G]x_i \cong X$.

If $y \in \mathbb{Z}_p[G]x_i \cap \mathbb{Z}_p[G]x_j$, then by minimality we clearly must have

$$y \in I_G x_i \cap I_G x_j$$

since $\mathbb{Z}_p[G]x_i \cong X$ has $I_G x_i$ as its unique maximal improper submodule. We then have $x_i' \in \mathbb{Z}_p[G]x_i$ and $x_j' \in \mathbb{Z}_p[G]x_j$ with

$$y = (g-1)x_i' = (g-1)x_j',$$

which forces $x_i' - x_j' \in (I_G A)^G$. In other words, we have $x_i' = x_j'$, contradicting minimality. We therefore have $m = s$ and $I_G A \cong I_G^s$.

We now know that A fits in an exact sequence

$$0 \to \mathbb{Z}_p^t \to A \xrightarrow{\pi} X^s \to 0,$$

which we claim splits. To see this, write $X^s = \langle x_1, \ldots, x_s \rangle$. Then $z_i = N_G \tilde{x}_i$ is an element of $\mathbb{Z}_p^t$, and the sequence splits if and only if $z_i \in p\mathbb{Z}_p^t$ for all i, since this means exactly that there exist $y_i \in \mathbb{Z}_p^t$ with $z_i = p y_i$ and therefore $N_G(\tilde{x}_i - y_i) = 0$, which tells us that $\langle \tilde{x}_i - y_i \rangle \cong X$. The $\mathbb{Z}_p[G]$-linear map taking

x_i to $\tilde{x}_i - y_i$ then determines the splitting. If not, we have that some $\tilde{x}_i$ generates a direct summand of A isomorphic to $\mathbb{Z}_p[G]$, since z_i (for some i) may be taken as part of a basis $\{z_i, w_2, \ldots, w_t\}$ of $\mathbb{Z}_p^t$, and

$$A = \langle \tilde{x}_1, \ldots, \tilde{x}_s, w_2, \ldots, w_t \rangle \cong \mathbb{Z}_p[G] \oplus \langle \tilde{x}_1, \ldots, \tilde{x}_{i-1}, \tilde{x}_{i+1}, \ldots, \tilde{x}_s, w_2, \ldots, w_t \rangle.$$

Since we have assumed that A has no $\mathbb{Z}_p[G]$-quotient, the latter cannot happen, so the sequence splits, as desired. □

2.8. Eigenspaces

In this section, we suppose that Δ is a finite abelian group. For a fixed prime p, we consider the group

$$\Delta^* = \mathrm{Hom}(\Delta, \overline{\mathbb{Q}_p}^\times)$$

of p-adic characters of Δ. Let $\mathscr{O}$ denote the $\mathbb{Z}_p$-algebra generated by the roots of unity of order dividing the exponent of Δ, and let E denote the quotient field of $\mathscr{O}$. For $\chi \in \Delta^*$, we let $\mathscr{O}_\chi$ the $\mathbb{Z}_p$-algebra generated by the values of χ, and let E_χ denote its fraction field. Cearly, the ring $\mathscr{O}$ contains $\mathscr{O}_\chi$.

What we shall call eigenspaces of a $\mathbb{Z}_p[\Delta]$-module shall in general, in fact, be quotients. Note that $\chi \in \Delta^*$ induces a map $\tilde{\chi}\colon \mathscr{O}[\Delta] \to \mathscr{O}$, which restricts to a map $\mathbb{Z}_p[\Delta] \to \mathscr{O}_\chi$.

DEFINITION 2.8.1. Let A be an $\mathscr{O}[\Delta]$-module, and let $\psi \in \Delta^*$. We define the *ψ-eigenspace* of A as

$$A^\psi = A \otimes_{\mathscr{O}[\Delta]} \mathscr{O},$$

where the map $\mathscr{O}[\Delta] \to \mathscr{O}$ in the tensor product is $\tilde{\chi}$.

REMARK 2.8.2. If $p \nmid |\Delta|$, then the canonical map $A \to A^\psi$ induces an isomorphism

$$\{a \in A \mid \delta a = \psi(\delta) a \text{ for all } \delta \in \Delta\} \xrightarrow{\sim} A^\psi.$$

It is the former module that might more typically be called an eigenspace. It can be interpreted as the Δ-invariant group of the twist $A(\psi)$ of A that is A as an $\mathscr{O}$-module but on which $\delta \in \Delta$ acts as $\psi(\delta)\delta$ does on A. Our eigenspace A^ψ is instead the Δ-coinvariant group of $A(\psi)$.

NOTATION 2.8.3. For $\psi \in \Delta^*$, set

$$e_\psi = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \psi(\delta)\delta^{-1} \in E[\Delta].$$

Note that

$$\sigma e_\psi = \psi(\sigma) e_\psi$$

for every $\sigma \in \Delta$, and in particular

$$\mathscr{O}[\Delta] e_\psi = \mathscr{O} e_\psi$$

as an $\mathscr{O}[\Delta]$-submodule of $E[\Delta]$.

PROPOSITION 2.8.4. *We have a canonical decomposition of rings and $E[\Delta]$-modules*

$$E[\Delta] \cong \prod_{\psi \in \Delta^*} E e_\psi.$$

If $p \nmid |\Delta|$, we similarly have a decomposition

$$\mathscr{O}[\Delta] \cong \prod_{\psi \in \Delta^*} \mathscr{O} e_\psi.$$

PROOF. One need only remark that the e_ψ are mutually orthogonal idempotents that sum to 1, as is a basic fact of character theory (in this case for a finitely generated abelian group). □

The following lemma is useful to note.

LEMMA 2.8.5. *Let $\psi \in \Delta^*$. For any $E[\Delta]$-module A (or $\mathscr{O}[\Delta]$-module A if $p \nmid |\Delta|$), we have $A^\psi = e_\psi A$.*

PROOF. If $a \in e_\psi A$, then $e_\psi a = a$, as e_ψ is an idempotent. Conversely, if $a \in A^{(\psi)}$, then

$$e_\psi a = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \psi(\delta)^{-1} \delta a = a,$$

as $\delta a = \psi(\delta) a$. □

The following is a consequence of Proposition 2.8.4.

PROPOSITION 2.8.6. *For every $E[\Delta]$-module A, there is an internal direct sum decomposition*

$$A \cong \bigoplus_{\psi \in \Delta^*} A^\psi.$$

If $p \nmid |\Delta|$, then this decomposition holds for $\mathscr{O}[\Delta]$-modules as well.

PROOF. We have

$$A \cong A \otimes_{\mathscr{O}[\Delta]} \mathscr{O}[\Delta] \cong A \otimes_{\mathscr{O}[\Delta]} \bigoplus_{\psi \in \Delta^*} \mathscr{O} e_\psi \cong \bigoplus_{\psi \in \Delta^*} A \otimes_{\mathscr{O}[\Delta]} \mathscr{O} e_\psi \cong \bigoplus_{\psi \in \Delta^*} e_\psi A \otimes_{\mathscr{O}[\Delta]} \mathscr{O}[\Delta] \cong \bigoplus_{\psi \in \Delta^*} A^\psi,$$

with the second step being Proposition 2.8.4 and the last step following from Lemma 2.8.5. □

Eigenspaces of an $\mathscr{O}[\Delta]$-module behave well under tensor products and homomorphism groups, as seen in the following result.

LEMMA 2.8.7. *Let A and B be $\mathscr{O}[\Delta]$-modules with $A = A^\chi$ and $B = B^\psi$ for some $\chi, \psi \in \Delta^*$. We then have*

$$A \otimes_{\mathscr{O}} B = (A \otimes_{\mathscr{O}} B)^{\chi\psi}$$

and

$$\mathrm{Hom}_{\mathscr{O}}(A, B) = \mathrm{Hom}_{\mathscr{O}}(A, B)^{\chi^{-1}\psi}.$$

PROOF. For $a \in A$ and $b \in B$, we have

$$\delta(a \otimes b) = \delta(a) \otimes \delta(b) = \chi(\delta)a \otimes \psi(\delta)b = \chi\psi(\delta) \cdot a \otimes b.$$

For $\phi \in \mathrm{Hom}_{\mathscr{O}}(A,B)$, we have

$$(\delta \cdot \phi)(a) = \delta\phi(\delta^{-1}a) = \psi(\delta)\phi(\chi(\delta)^{-1}a) = \psi\chi^{-1}(\delta)\phi(a).$$

□

We next consider a slightly different notion of eigenspaces, in this case for $\mathbb{Z}_p[\Delta]$-modules.

DEFINITION 2.8.8. Let A be a $\mathbb{Z}_p[\Delta]$-module, and let $\chi \in \Delta^*$. The χ-eigenspace $A^{(\chi)}$ of A is defined as

$$A^{(\chi)} = A \otimes_{\mathbb{Z}_p[\Delta]} \mathscr{O}_\chi,$$

where the map $\mathbb{Z}_p[\Delta] \to \mathscr{O}_\chi$ is given by $\tilde{\chi}$.

NOTATION 2.8.9. For $\chi \in \Delta^*$, set

$$\tilde{e}_\chi = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \mathrm{Tr}_{E_\chi/\mathbb{Q}_p}(\chi(\delta))\delta^{-1} \in \mathbb{Z}_p[\Delta],$$

where $\mathrm{Tr}_{E_\chi/\mathbb{Q}_p} \colon E_\chi \to \mathbb{Q}_p$ denotes the trace map.

NOTATION 2.8.10. For a field E, let G_E denote its absolute Galois group, which is to say the Galois group of the extension of E given by a fixed separable closure.

DEFINITION 2.8.11. We say that two p-adic characters $\chi, \psi \colon \Delta \to \overline{\mathbb{Q}_p}^\times$ are *conjugate* if there exists $\sigma \in G_{\mathbb{Q}_p}$ such that $\chi = \sigma \circ \psi$.

REMARK 2.8.12. If χ and ψ are conjugate, then $\mathscr{O}_\chi = \mathscr{O}_\psi$.

REMARK 2.8.13. If A is also a $\mathbb{Q}_p$-vector space or $p \nmid |\Delta|$, then the canonical map $\tilde{e}_\chi A \to A^{(\chi)}$ is an isomorphism. Note that while $A^{(\chi)}$ has an $\mathscr{O}_\chi$-module structure, the $\mathbb{Z}_p[\Delta]$-module $\tilde{e}_\chi A$ is only endowed with such a structure when a choice of character ψ in the conjugacy class of χ is made.

Let Σ denote the set of conjugacy classes in Δ^*. We let $[\chi]$ denote the conjugacy class of $\chi \in \Delta^*$. We then have the following.

LEMMA 2.8.14. *Let A be a $\mathbb{Z}_p[\Delta]$-module, and let $\chi \in \Delta^*$. We have*

$$A^{(\chi)} \otimes_{\mathscr{O}_\chi} \mathscr{O} \cong (A \otimes_{\mathbb{Z}_p} \mathscr{O})^\chi.$$

If A is also a $\mathbb{Q}_p$-vector space or $p \nmid |\Delta|$, then we also have

$$A^{(\chi)} \otimes_{\mathbb{Z}_p} \mathscr{O} \cong \bigoplus_{\psi \in [\chi]} (A \otimes_{\mathbb{Z}_p} \mathscr{O})^\psi$$

PROOF. For the first isomorphism, we merely note that

$$A^{(\chi)} \otimes_{\mathscr{O}_\chi} \mathscr{O} \cong A \otimes_{\mathbb{Z}_p[\Delta]} e_\chi \mathscr{O}_\chi \otimes_{\mathscr{O}_\chi} \mathscr{O} \cong A \otimes_{\mathbb{Z}_p[\Delta]} e_\chi \mathscr{O} \cong (A \otimes_{\mathbb{Z}_p} \mathscr{O})^\chi.$$

Let $\Delta_\chi = \Delta/\ker\chi$, which is a cyclic group, generated by an element we call δ_χ. Note that $\psi \in \Delta^*$ is conjugate to χ if and only if ψ factors through Δ_χ and there exists $\sigma \in G_{\mathbb{Q}_p}$ such that $\psi(\delta_\chi) = \sigma(\chi(\delta_\chi))$. Hence, the characters in $[\chi]$ are in one-to-one correspondence with the $G_{\mathbb{Q}_p}$-conjugates of $\chi(\delta_\chi)$. Let $\xi = \chi(\delta_\chi)$, and suppose that $\Phi \in \mathbb{Z}_p[X]$ is its minimal polynomial. We then have

$$\mathscr{O} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\xi] \cong \mathscr{O} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[X]/(\Phi(X)) \cong \mathscr{O}[X]/(\Phi(X)) \cong \prod_{\xi'} \mathscr{O}[X]/(X - \xi') \cong \prod_{\xi'} \mathscr{O},$$

where ξ' runs over the $G_{\mathbb{Q}_p}$-conjugates of ξ, and the composite map takes $1 \otimes \xi$ to ξ' in the ξ'-coordinate. Reinterpreting this, we have

$$\mathscr{O} \otimes_{\mathbb{Z}_p} e_\chi \mathscr{O}_\chi \cong \bigoplus_{\psi \in [\chi]} e_\psi \mathscr{O}$$

as $\mathscr{O}[\Delta]$-modules, where the map takes $1 \otimes e_\chi$ to e_ψ in the ψ-coordinate. (Note that $e_\psi = \sigma e_\chi$ if $\psi = \sigma\chi$, if we let σ act on the coefficients of e_χ.) Therefore, we may conclude that

$$A^{(\chi)} \otimes_{\mathbb{Z}_p} \mathscr{O} \cong A \otimes_{\mathbb{Z}_p[\Delta]} e_\chi \mathscr{O}_\chi \otimes_{\mathbb{Z}_p} \mathscr{O} \cong \bigoplus_{\psi \in [\chi]} A \otimes_{\mathbb{Z}_p[\Delta]} e_\psi \mathscr{O} \cong \bigoplus_{\psi \in [\chi]} (A \otimes_{\mathbb{Z}_p} \mathscr{O})^\psi.$$

□

PROPOSITION 2.8.15. *For every $\mathbb{Q}_p[\Delta]$-module A, and every $\mathbb{Z}_p[\Delta]$-module A if $p \nmid |\Delta|$, there is a direct sum decomposition*

$$A \cong \bigoplus_{[\chi] \in \Sigma} A^{(\chi)}$$

of $\mathbb{Z}_p[\Delta]$-modules, where the sum is over the conjugacy classes in Σ.

PROOF. We define

$$\Phi \colon A \to \bigoplus_{[\chi] \in \Sigma} A^{(\chi)}$$

as the product of the surjective maps $A \to A \otimes_{\mathbb{Z}_p[\Delta]} e_\chi \mathscr{O}_\chi$ that take a to $a \otimes e_\chi$. We first show that Φ is an isomorphism after tensoring with $\mathscr{O}$. That is,

$$\Phi \otimes \mathrm{id}_{\mathscr{O}} \colon A \otimes_{\mathbb{Z}_p} \mathscr{O} \to \bigoplus_{[\chi] \in \Sigma} A^{(\chi)} \otimes_{\mathbb{Z}_p} \mathscr{O}.$$

By Lemma 2.8.14, the right-hand side is isomorphic to

$$\bigoplus_{[\chi] \in \Sigma} \bigoplus_{\psi \in [\chi]} (A \otimes_{\mathbb{Z}_p} \mathscr{O})^\psi \cong \bigoplus_{\psi \in \Delta^*} (A \otimes_{\mathbb{Z}_p} \mathscr{O})^\psi$$

under the map that takes $(a \otimes e_\chi) \otimes 1$ to $(a \otimes 1) \otimes e_\psi$. The composite map is then the map that takes $a \otimes 1$ to $(a \otimes 1) \otimes e_\psi$, and this is an isomorphism by Proposition 2.8.6. Thus, we have that $\Phi \otimes \mathrm{id}_{\mathscr{O}}$ is an isomorphism, and as $\mathscr{O}$ is a free $\mathbb{Z}_p$-module, we have that Φ is an isomorphism. □

Even if $p \mid |\Delta|$, we have a weaker direct sum decomposition of $\mathbb{Z}_p[\Delta]$-modules.

NOTATION 2.8.16. Let Υ denote the set of maximal ideals of $\mathbb{Z}_p[\Delta]$.

REMARK 2.8.17. Every $\mathfrak{m} \in \Upsilon$ is the kernel of a composite map $\tilde{\chi}\colon \mathbb{Z}_p[\Delta] \xrightarrow{\tilde{\chi}} \mathscr{O} \to \overline{\mathbb{F}_p}$. Thus, Υ may be identified with the set of equivalence classes of characters in Δ^* under which two characters are considered equivalent if the above compositions are $G_{\mathbb{F}_p}$-conjugate. We write $\psi \in \mathfrak{m}$ if $\psi \in \Delta^*$ lies in the equivalence class corresponding to $\mathfrak{m}$.

The proof of the following is left to the reader. Perhaps the easiest way to think of it is that each $A_\mathfrak{m}$ is just $A^{(\rho)}$ for ρ a p-adic character of the prime-to-p part of the group Δ.

PROPOSITION 2.8.18. *For any $\mathbb{Z}_p[\Delta]$-module A, there is a canonical direct sum decomposition*

$$A \cong \bigoplus_{\mathfrak{m} \in \Upsilon} A_\mathfrak{m}$$

We have $A_\mathfrak{m}^{(\chi)} \cong A^{(\chi)}$ for $\chi \in \mathfrak{m}$, and if $p \nmid |\Delta|$, then $\mathfrak{m} = [\chi]$ and $A_\mathfrak{m} \cong A^{(\chi)}$ for any $\chi \in \mathfrak{m}$. If A is a $\mathbb{Q}_p$-vector space, then we have that

$$A_\mathfrak{m} \cong \bigoplus_{[\chi] \subset \mathfrak{m}} A^{(\chi)}.$$

CHAPTER 3

Iwasawa theory

Throughout this chapter, F will denote a fixed number field, and we let p be a prime.

3.1. $\mathbb{Z}_p$-extensions

DEFINITION 3.1.1. A Galois extension F_∞ of F is said to be a *$\mathbb{Z}_p$-extension* if $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$.

Fix a $\mathbb{Z}_p$-extension F_∞ of F, and set $\Gamma = \mathrm{Gal}(F_\infty/F)$. The fixed field of Γ^{p^n} is a number field F_n with $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$. We set

$$\Gamma_n = \Gamma/\Gamma^{p^n} = \mathrm{Gal}(F_n/F).$$

DEFINITION 3.1.2. The *absolute Galois group* of a field E is the Galois group $G_E = \mathrm{Gal}(E^{\mathrm{sep}}/E)$ of a separable closure E^{sep} of E over E.

For a field E of characteristic not p, let μ_{p^∞} denote the group of p-power roots of unity in a separable closure E^{sep} of E.

DEFINITION 3.1.3. For a field E of characteristic not p, the *p-adic cyclotomic character* is the map $\chi\colon G_E \to \mathbb{Z}_p^\times$ defined by $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for all $\zeta \in \mu_{p^\infty}$.

Let us fix a primitive nth root of unity in $\overline{\mathbb{Q}}$ for each $n \geq 1$, subject to the condition that $\zeta_{nm}^m = \zeta_n$ for all $m \geq 1$.

REMARK 3.1.4. For a number field F, the p-adic cyclotomic character $\chi\colon G_F \to \mathbb{Z}_p^\times$ induces an injection of $\mathrm{Gal}(F(\mu_{p^\infty})/F)$ onto an open subgroup of $\mathbb{Z}_p^\times$. It is an isomorphism if $F = \mathbb{Q}$.

It is easy to see that

$$\mathbb{Z}_p^\times \cong \begin{cases} (1+p\mathbb{Z}_p) \times \mu_{p-1}(\mathbb{Z}_p) & p \text{ odd} \\ (1+4\mathbb{Z}_2) \times \langle -1 \rangle & p = 2, \end{cases}.$$

Let $q = p$ if p is odd and $q = 4$ if $p = 2$. Every element of $1 + q\mathbb{Z}_p$ is a p-adic power of some topological generator u of $1 + q\mathbb{Z}_p$, such as $1 + q$, which is to say that the map that takes $a \in \mathbb{Z}_p$ to u^a is an isomorphism from $\mathbb{Z}_p$ to $1 + q\mathbb{Z}_p$. We therefore have

$$\mathbb{Z}_p^\times \cong \begin{cases} \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} & p \text{ odd} \\ \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} & p = 2. \end{cases} \tag{3.1.1}$$

As a consequence, we have the following result.

LEMMA 3.1.5. *Any open subgroup of $\mathbb{Z}_p^\times$ has a unique quotient isomorphic to $\mathbb{Z}_p$ for any p.*

PROOF. That the quotient of $\mathbb{Z}_p^\times$ by its group of torsion elements is isomorphic to $\mathbb{Z}_p$ follows from (3.1.1). We then need only remark that any open subgroup of $\mathbb{Z}_p$ has the form $p^n\mathbb{Z}_p$ for some $n \geq 0$, so is itself isomorphic to $\mathbb{Z}_p$. □

Together, Remark 3.1.4 and Lemma 3.1.5 allow us to make the following definition.

DEFINITION 3.1.6. The *cyclotomic $\mathbb{Z}_p$-extension F_{cyc}* of F is the unique subfield of $F(\mu_{p^\infty})$ that is a $\mathbb{Z}_p$-extension of F.

In fact, if F is totally real, then its cyclotomic $\mathbb{Z}_p$-extension F_{cyc} will lie in the maximal totally real subfield of $F(\mu_{p^\infty})$ (and therefore will equal it in the case that $p = 2$).

Next, we study ramification in $\mathbb{Z}_p$-extensions.

PROPOSITION 3.1.7. *Suppose that v is a place of F not over p. Then v is unramified in any $\mathbb{Z}_p$-extension F_∞/F.*

PROOF. The inertia subgroup of v in $\Gamma = \mathrm{Gal}(F_\infty/F)$ is a closed subgroup of Γ and therefore equal to Γ^{p^n} for some $n \geq 0$, unless it is trivial. In the case that v is archimedean, only the latter case is possible as an inertia group at v has order at most 2 in general. In general, in the former case, F_n is its fixed field, and the completion of F_n at a prime over v has a tamely, totally ramified $\mathbb{Z}_p$-extension that is the completion of F_∞. On the other hand, the completion of F_n being a characteristic zero local field, such an extension does not exist. □

LEMMA 3.1.8. *There exists a prime v over p in F and an $n \geq 0$ such that F_∞/F_n is totally ramified at v.*

PROOF. By Proposition 3.1.7, no prime not over p ramifies in F_∞/F, so if no primes over p ramify, then F_∞/F would be unramified everywhere. However, the Hilbert class field of F is of finite degree, so this is not possible. That is, there exists a v over p such that that the inertia group at v in Γ is nontrivial, hence equal to some Γ^{p^n}. □

In the case of the cyclotomic $\mathbb{Z}_p$-extension, we can say more.

PROPOSITION 3.1.9. *Let F_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F. No finite prime splits completely in F_{cyc}/F, and every prime over p is totally ramified in F_{cyc}/F_n for some $n \geq 0$.*

PROOF. If v split completely in F_{cyc}/F, then it would also have to split completely in the extension $F(\mu_{p^\infty})/F(\mu_q)$, since $F(\mu_{p^\infty}) = F_\infty(\mu_q)$, where $q = p$ for p odd and $q = 4$ for $p = 2$. But this means that $F_v(\mu_{p^\infty}) = F_v(\mu_q)$, which is to say that $F_v(\mu_q)$ contains μ_{p^∞}, which is impossible.

On the other hand, we know that $\mathbb{Q}_{\text{cyc}}/\mathbb{Q}$ is totally ramified at p, so the resulting local extension $\mathbb{Q}_{p,\text{cyc}}/\mathbb{Q}_p$ is totally ramified as well. But then the completion of F_{cyc} at a prime above v is simply the compositum $F_v \cdot \mathbb{Q}_{p,\text{cyc}}$, and therefore its intersection with the maximal unramified extension of $\mathbb{Q}_p$ must be of finite degree over $\mathbb{Q}_p$. In particular, $F_v \cdot \mathbb{Q}_{p,\text{cyc}}/F_v$ has an infinite inertia group, which therefore must have the form $\Gamma_{\text{cyc}}^{p^n}$ for some $n \geq 0$, where $\Gamma_{\text{cyc}} = \text{Gal}(F_{\text{cyc}}/F)$. □

We note the following interesting corollary.

COROLLARY 3.1.10. *Let v be a prime of F_{cyc} not lying above p. Suppose that E/F_{cyc} is a pro-p extension in which it does not ramify. Then v splits completely in E/F_{cyc}.*

PROOF. Since $F_{v,\text{cyc}}/F_v$ is an unramified $\mathbb{Z}_p$-extension by Propositions 3.1.7 and 3.1.9, it is the maximal unramified pro-p extension of F_v. It follows that for any prime w of E lying over v, we must have $E_w = F_{v,\text{cyc}}$, since the Galois closure of E_w/F_v is a pro-p extension of F_v containing $F_{v,\text{cyc}}$. □

Finally, we consider the maximal number of independent $\mathbb{Z}_p$-extensions of F, which is to say the $\mathbb{Z}_p$-rank of the Galois group of the maximal abelian V_p-ramified extension of F.

PROPOSITION 3.1.11. *Let $\tilde{F}$ denote the compositum of all $\mathbb{Z}_p$-extensions of F. Then* $\text{Gal}(\tilde{F}/F) \cong \mathbb{Z}_p^{r_2+1+\delta}$*, where δ is the Leopoldt defect of F.*

PROOF. This is a consequence of Theorem 1.5.7, since Proposition 3.1.7 tells us that the $\mathbb{Z}_p$-rank of the maximal abelian $V_{p\infty}$-ramified extension of F is the $\mathbb{Z}_p$-rank of $\text{Gal}(\tilde{F}/F)$. □

3.2. Limits of class groups

Let F_∞ be a $\mathbb{Z}_p$-extension of F with $\Gamma = \text{Gal}(F_\infty/F)$. We define F_n and Γ_n as before.

DEFINITION 3.2.1. We refer to $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ as the *Iwasawa algebra* of the extension F_∞/F.

DEFINITION 3.2.2. A Λ-module, or module over the Iwasawa algebra, is also called an *Iwasawa module*.

By definition, we have $\Lambda = \varprojlim \mathbb{Z}_p[\Gamma_n]$. Note that any $\mathbb{Z}_p[\Gamma_n]$-module is automatically an Iwasawa module, with Λ acting through the quotient map $\pi_n \colon \Lambda \to \mathbb{Z}_p[\Gamma_n]$. Therefore, given an inverse (resp., direct) system of $\mathbb{Z}_p[\Gamma_n]$-modules M_n with respect to maps that are Λ-module homomorphisms, the inverse (resp., direct) has the structure of a Λ-module.

DEFINITION 3.2.3. Let F_∞/F be a $\mathbb{Z}_p$-extension. For $n \geq m \geq 0$, let us set

$$N_{n,m} = N_{F_n/F_m} : A_n \to A_m \quad \text{and} \quad j_{n,m} = j_{F_n/F_m} : A_m \to A_n.$$

With respect to the systems defined by these maps, we set

$$X_\infty = \varprojlim_n A_n \quad \text{and} \quad A_\infty = \varinjlim_n A_n.$$

TERMINOLOGY 3.2.4. The direct limit $\varinjlim_n \mathrm{Cl}_{F_n}$ contains A_∞ as its p-part and is called the *class group* of F_∞.

The maps $N_{n,m}$ and $j_{n,m}$ are $\mathbb{Z}_p[\Gamma_n]$-module homomorphisms, and so both X_∞ and A_∞ have canonical structures of Λ-modules.

Recall that the Artin map sets up an isomorphism between A_n and $\mathrm{Gal}(H_n/F_n)$, where H_n is the p-Hilbert class field of F_n. Under this identification, the norm map $N_{n,m}$ becomes the map on Galois groups that is restriction. We then have the following.

REMARK 3.2.5. Let E be an algebraic extension of F, and for a set of primes S of F, let S_E be the set of primes of E lying above those in S. We will say that more simply that an extension of E is S-ramified if it is S_E-ramified.

PROPOSITION 3.2.6. *Let S be a set of primes of F. Let L_n denote the maximal S-ramified abelian pro-p extension of F_n for $n \geq 0$ or $n = \infty$. Then the inverse limit of restriction maps*

$$\mathrm{Gal}(L_\infty/F_\infty) \to \varprojlim_n \mathrm{Gal}(L_n/F_n)$$

is an isomorphism of Λ-modules.

PROOF. Since L_n/F_n is an S-ramified abelian pro-p extension, so is L_nF_∞/F_∞. Therefore, $L_n \subseteq L_\infty$. We claim that $\bigcup_n L_n = L_\infty$. Let $x \in L_\infty$. Then $F_\infty(x)/F_\infty$ is an S-ramified abelian p-extension. Let y be a field generator of the Galois closure of $F(x)$ as an extension of F. To show that $x \in L_n$ for some n, it therefore suffices to show that $y \in L_n$. Let m be such that $F_n(y) \cap F_\infty = F_m$. Then $F_m(y) \cap F_\infty = F_m$ as well, and the restriction map

$$\mathrm{Gal}(F_\infty(y)/F_\infty) \to \mathrm{Gal}(F_m(y)/F_m)$$

is surjective, so $F_m(y)/F_m$ is abelian.

Since L_∞/F_∞ is S-ramified, and F_∞/F is V_p-ramified, we have that $F_m(y)/F_m$ is $S \cap V_p$-ramified. If v is a place over p in F_m that is not in S_{F_m}, then since $F_\infty(y)/F_\infty$ is unramified over v, the same must be true of $F_n(y)/F_n$ for some n, and therefore $y \in L_\infty$.

It now follows that the inverse limit of restriction maps

$$\mathrm{Gal}(L_\infty/F_\infty) \xrightarrow{\sim} \varprojlim_n \mathrm{Gal}(L_n/F_\infty \cap L_n)$$

is an isomorphism, and since $\bigcup_n (F_\infty \cap L_n) = F_\infty = \bigcup_n F_n$, we have that

$$\varprojlim_n \mathrm{Gal}(L_n/F_\infty \cap L_n) \xrightarrow{\sim} \varprojlim_n \mathrm{Gal}(L_n/F_n)$$

is an isomorphism as well, as desired. □

COROLLARY 3.2.7. *The inverse limit of Artin maps provides a canonical identification between X_∞ and the Galois group of the maximal unramified abelian pro-p extension of F_∞.*

TERMINOLOGY 3.2.8. We call the Λ-module X_∞ the *unramified Iwasawa module*.

REMARK 3.2.9. If K is an algebraic extension of $\mathbb{Q}$, we may speak of its primes as the valuations on K extending the valuations of $\mathbb{Q}$. To say that an extension L of K is unramified at a prime v is exactly to say that every extension of v to a prime w of L is unramified in the sense that the extension L_w/K_v of completions is unramified, which is to say Galois with group restricting isomorphically to the Galois group of the corresponding extension of residue fields. (If v is archimedean, this just means that $L_w = K_v$.)

More generally, we make the following definition.

DEFINITION 3.2.10. Let S be a set of primes of F. The *S-ramified Iwasawa module* over F_∞ is the Galois group $\mathfrak{X}_{\infty,S}$ of the maximal S-ramified abelian pro-p extension of F_∞.

Let us choose a topological generator γ of Γ, which defines a unique continuous, $\mathbb{Z}_p$-linear isomorphism $\Lambda \xrightarrow{\sim} \mathbb{Z}_p[\![T]\!]$ that takes $\gamma - 1$ to T. Therefore, we may speak of characteristic ideals of Λ as elements of $\mathbb{Z}_p[\![T]\!]$. We have the following result on the structure of X_∞.

PROPOSITION 3.2.11. *The Λ-module X_∞ is finitely generated and torsion.*

PROOF. For $n \geq m$, set $\Sigma_{n,m} = \Sigma_{F_n/F_m}$ in the notation of Theorem 1.3.14, which also provides exact sequences fitting into commutative diagrams

$$\begin{array}{ccccccccc}
\ker \Sigma_{n',m} & \longrightarrow & (A_{n'})_{\Gamma_{n'}^{p^m}} & \xrightarrow{N_{n',m}} & A_m & \longrightarrow & \mathrm{coker}\, \Sigma_{n',m} & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle N_{n',n}} & & \| & & \downarrow & & \\
\ker \Sigma_{n,m} & \longrightarrow & (A_n)_{\Gamma_n^{p^m}} & \xrightarrow{N_{n,m}} & A_m & \longrightarrow & \mathrm{coker}\, \Sigma_{n,m} & \longrightarrow & 0
\end{array}$$

of $\mathbb{Z}_p[\Gamma_m]$-modules for $n' \geq n$. Let $I_v^{(m)}$ denote the inertia group at v in Γ^{p^m}, which can only be nontrivial for $v \in V_p$ which do not split completely in F_∞/F, and let

$$\Sigma^{(m)} \colon \bigoplus_{v \in V_p(F_m)} I_v^{(m)} \to \Gamma^{p^m}$$

be the natural map given by inclusion and product. In the inverse limit over n, we obtain exact sequences

$$\ker\Sigma^{(m)} \to (X_\infty)_{\Gamma^{p^m}} \to A_m \to \operatorname{coker}\Sigma^{(m)} \to 0. \tag{3.2.1}$$

Note that $\ker\Sigma^{(m)}$ is finitely generated over $\mathbb{Z}_p$ and A_m is finite. By Nakayama's Lemma, we see that X_∞ is a finitely generated Λ-module. Moreover, we see that $(X_\infty)_{\Gamma^{p^m}}$ is of bounded $\mathbb{Z}_p$-rank for all m. Were X_∞ to have nontrivial Λ-rank, then since there would exist a pseudo-isomorphism from X_∞ to the direct sum M of Λ^r and a torsion module, the ranks of $(X_\infty)_{\Gamma^{p^m}}$ would necessarily have been unbounded, since $\Lambda_{\Gamma^{p^m}} \cong \mathbb{Z}_p[\Gamma_m]$, and

$$(X_\infty)_{\Gamma^{p^m}} \to M_{\Gamma^{p^m}}$$

has finite cokernel. □

REMARK 3.2.12. If there exists a unique prime above p in F, and it is unsplit in F_m, then (3.2.1) implies that the map $(X_\infty)_{\Gamma^{p^m}} \to A_m$ is an injection. If, moreover, p is totally ramified in F_∞, then $(X_\infty)_{\Gamma^{p^m}} \to A_m$ is an isomorphism for every m.

We have the following theorem of Iwasawa that was mentioned in the introduction.

THEOREM 3.2.13 (Iwasawa). *Let $\lambda = \lambda(X_\infty)$ and $\mu = \mu(X_\infty)$. Then there exists $\nu \in \mathbb{Z}$ such that*

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

for all sufficiently large n.

PROOF. Let $N_n \colon X_\infty \to A_n$ be the inverse limit of norm maps $N_{n',n}$ for $n' \geq n$. Let us use Y_n to denote the kernel of N_n, which is a Λ-submodule of X_∞ that is pseudo-isomorphic to X_∞.

Fix m sufficiently large such that every prime over p that ramifies in F_∞/F_m is totally ramified. In particular, we have that N_m is surjective. We consider $n \geq m$. Let S_n be the set of primes (over p) in F_n that ramify in F_∞, and hence are totally ramified, and note that $|S_n| = |S_m| \neq 0$ by Lemma 3.1.8. Then the inertia group at $v \in S_n$ in Γ^{p^n} is Γ^{p^n} itself.

Let L_n be the maximal unramified abelian pro-p extension of F_n, and let L_∞ be the maximal unramified abelian pro-p extension of F_∞. We have $X_\infty \cong \operatorname{Gal}(L_\infty/F_\infty)$ and $A_n \cong \operatorname{Gal}(L_n/F_n)$, so $Y_n \cong \operatorname{Gal}(L_\infty/L_nF_\infty)$. Let E be the maximal unramified p-extension of F_n in L_∞. Since any $v \in S_n$ is totally ramified in F_∞/F_n, we have $E \cap F_\infty = F_n$. Since EF_∞/F_∞ is abelian, this tells us that E/F_n is abelian as well. Thus, E is equal to the maximal unramified abelian p-extension of F_n in L_∞. Consequently, $\operatorname{Gal}(L_\infty/L_n)$ is topologically generated by the inertia groups $J_v^{(n)}$ in $\operatorname{Gal}(L_\infty/F_n)$ for primes $v \in S_n$, and Y_n is the intersection of the latter group with $\operatorname{Gal}(L_\infty/F_\infty)$, i.e., it consists of those elements which restrict trivially to Γ.

In other words (for $n = m$), we have that Y_m is topologically generated as a pro-p group by elements $g = \sigma\tau^{-1} \in \mathrm{Gal}(L_\infty/F_\infty)$, where $\sigma \in J_v^{(m)}$ and $\tau \in J_w^{(m)}$ for primes $v, w \in S_m$ are such that σ and τ both restrict to γ^{p^m} for a fixed topological generator γ of Γ. We can compute the action of the element $\omega_{n,m} = \sum_{i=0}^{p^{n-m}-1} \gamma^{p^m i}$ on g as follows:

$$\omega_{n,m} \cdot g = \prod_{i=0}^{p^{n-m}-1} \tau^i g \tau^{-i} = (g\tau)^{p^{n-m}} \tau^{-p^{n-m}} = \sigma^{p^{n-m}} \tau^{-p^{n-m}}.$$

As the elements $\sigma^{p^{n-m}} \tau^{-p^{n-m}}$ topologically generate Y_n, this implies that $\omega_{n,m} Y_m = Y_n$.

Since $A_n = X_\infty/Y_n$, we conclude that

$$|A_n| = |X_\infty/Y_m| \cdot |Y_m/\omega_{n,m} Y_m|$$

for all $n \geq m$. Since Y_m is pseudo-isomorphic to X_∞, we have $\lambda = \lambda(Y_m)$ and $\mu = \mu(Y_m)$. Since $|X_\infty/Y_m|$ is a constant power of p, Theorem 2.4.7 yields the result. □

Finally, we compare X_∞ and A_∞.

PROPOSITION 3.2.14. *The Λ-modules $\alpha(X_\infty)$ and $A_\infty^\vee$ are pseudo-isomorphic, and in particular $A_\infty^\vee$ is finitely generated and Λ-torsion. Moreover, $A_\infty^\vee$ has no nonzero finite Λ-submodules.*

PROOF. As in the proof of Theorem 3.2.13, we let Y_n denote the kernel of the inverse limit of norm maps $N_n \colon X_\infty \to A_n$ for each $n \geq 0$. We showed that there exists $m \geq 0$ sufficiently large so that N_n is surjective and $\omega_{n,m} Y_m = Y_n$ for all $n \geq m$. We consider a directed system of short exact sequences with morphisms as in the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Y_m/\omega_{n,m}Y_m & \longrightarrow & X_\infty/\omega_{n,m}Y_m & \longrightarrow & X_\infty/Y_m & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \omega_{n',n}} & & \downarrow{\scriptstyle \omega_{n',n}} & & \downarrow{\scriptstyle \omega_{n',n}} & & \\ 0 & \longrightarrow & Y_m/\omega_{n',m}Y_m & \longrightarrow & X_\infty/\omega_{n',m}Y_m & \longrightarrow & X_\infty/Y_m & \longrightarrow & 0 \end{array}$$

for $n' \geq n \geq m$. Since X_∞/Y_m is a finite Λ-module, in the direct limit we obtain isomorphisms

$$\alpha(Y_m)^\vee = \varinjlim_n Y_m/\omega_{n,m}Y_m \xrightarrow{\sim} \varinjlim_n X_\infty/\omega_{n,m}Y_m \xrightarrow{\sim} \varinjlim_n A_n = A_\infty.$$

Since Y_m injects into X_∞ with finite cokernel, Proposition 2.6.10 yields that the natural map $\alpha(X_\infty) \to \alpha(Y_m)$ is an injective pseudo-isomorphism. Since $A_\infty^\vee \cong \alpha(Y_m)$, the final statement follows from Theorem 2.6.13. □

Again noting Theorem 2.6.13, we have the following corollary.

COROLLARY 3.2.15. *The Λ-module $A_\infty^\vee$ is is pseudo-isomorphic to X_∞^ι, and in particular, X_∞ and $A_\infty^\vee$ have the same λ and μ-invariants.*

We end with a still open conjecture of Iwasawa, which is known in the case of abelian fields by work of Ferrero-Washington: see Theorem 6.2.1.

CONJECTURE 3.2.16 (Iwasawa's μ-conjecture). *If F_∞ is the cyclotomic $\mathbb{Z}_p$-extension F_{cyc} of F, then $\mu(X_\infty) = 0$.*

We will also have cause to study two modules related to X_∞ and A_∞.

DEFINITION 3.2.17. Let F_∞/F be a $\mathbb{Z}_p$-extension. For $S = V_p$, let us set $A'_n = A_{F_n,S}$. We then define

$$X'_\infty = \varprojlim_n A'_n \quad \text{and} \quad A'_\infty = \varinjlim_n A'_n$$

with respect to the maps $N_{n,m}$ and $j_{n,m}$ on these groups.

DEFINITION 3.2.18. We call X'_∞ the *completely split Iwasawa module*, while A'_∞ is the *p-part of the p-class group* $\varinjlim_n \mathrm{Cl}_{F_n,V_p}$ of F_∞.

We summarize without proof the results for X_∞ and A_∞ that also hold for X'_∞ and A'_∞ by much the same arguments.

PROPOSITION 3.2.19. *The Λ-module X'_∞ is finitely generated and torsion. It is canonically isomorphic via an inverse limit of Artin maps to the Galois group of the maximal unramified abelian pro-p extension of F_∞ in which every prime over p splits completely. Moreover, $(X'_\infty)^\iota$ is pseudo-isomorphic to $(A'_\infty)^\vee$, and the latter module has no nonzero finite Λ-submodules.*

For the cyclotomic $\mathbb{Z}_p$-extension, we note that we could just have well have chosen any set of primes containing V_p in defining X'_∞.

PROPOSITION 3.2.20. *Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension. Then the natural maps*

$$X'_\infty \to \varprojlim_n A_{F_n,S} \quad \text{and} \quad A'_\infty \to \varinjlim_n A_{F_n,S}$$

are respectively an isomorphism and a surjective pseudo-isomorphism for any finite set S of primes of F containing V_p.

3.3. The p-ramified Iwasawa module

In this section, we focus for simplicity on the case that $S = V_{p\infty}$, though there is no theoretical obstruction to considering a larger finite set. We make the following definition.

DEFINITION 3.3.1. Let F_∞/F be a $\mathbb{Z}_p$-extension. Let $\mathfrak{X}_n = \mathfrak{X}_{F_n,V_{p\infty}}$ for $n \geq 0$, and let

$$\mathfrak{X}_\infty \cong \varprojlim_n \mathfrak{X}_n$$

be the $V_{p\infty}$-ramified Iwasawa module, which we refer to as the *p-ramified Iwasawa module*.

Consider the following weakening of the Leopoldt conjecture.

CONJECTURE 3.3.2 (Weak Leopoldt conjecture). *Let F_∞/F be a $\mathbb{Z}_p$-extension. Then the Leopoldt defects $\delta(F_n)$ are bounded in $n \geq 0$.*

We will abbreviate $\delta(F_n)$ by δ_n.

The weak Leopoldt conjecture has the following consequence for the p-ramified Iwasawa module.

THEOREM 3.3.3. *Let F_∞/F be a $\mathbb{Z}_p$-extension for which the weak Leopoldt conjecture holds. Then*

$$\operatorname{rank}_\Lambda \mathfrak{X}_\infty = r_2(F).$$

PROOF. Let M_∞ be such that $\mathfrak{X}_\infty = \operatorname{Gal}(M_\infty/F_\infty)$, and define M_n for $n \geq 0$ by

$$\mathfrak{X}_n = \operatorname{Gal}(M_n/F_n).$$

We then have that $(\mathfrak{X}_\infty)_{\Gamma_n} \cong \operatorname{Gal}(M_n/F_\infty)$, and therefore we have an exact sequence

$$0 \to (\mathfrak{X}_\infty)_{\Gamma_n} \to \mathfrak{X}_n \to \Gamma_n \to 0.$$

Since any archimedean place splits completely in a $\mathbb{Z}_p$-extension, we have $r_2(F_n) = p^n r_2(F)$ and hence $\operatorname{rank}_{\mathbb{Z}_p} \mathfrak{X}_n = p^n r_2(F) + 1 + \delta_n$. It follows that $\operatorname{rank}_{\mathbb{Z}_p}(\mathfrak{X}_\infty)_{\Gamma_n} = p^n r_2(F) + \delta_n$ for all n. Since δ_n is bounded in n, the result then follows from Proposition 2.4.12. □

We prove the weak Leopoldt conjecture in the case of the cyclotomic $\mathbb{Z}_p$-extension. Let $\mathscr{E}_n = \mathscr{E}_{F_n}$ for each $n \geq 0$, and let $\mathscr{U}_{n,v}$ be the p-completion of $\mathscr{O}_{F_{n,v}}^\times$ for any prime v of F_n.

THEOREM 3.3.4. *Suppose that F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension of F. Then the weak Leopoldt conjecture holds for F_∞/F. In fact, if F contains μ_{2p}, then $\delta_n \leq \lambda(X'_\infty)$ for every n.*

PROOF. Assume first that F contains μ_{2p}. Let $r = \operatorname{rank}_{\mathbb{Z}_p} \mathscr{E}_n$, and choose units such that $\alpha_1, \ldots, \alpha_r \in \mathscr{O}_{F_n}^\times$ generate $\mathscr{E}_n$ modulo its torsion subgroup as a $\mathbb{Z}_p$-module and such that the images of $\alpha_{\delta_n+1}, \ldots, \alpha_r$ under

$$\iota_n \colon \mathscr{E}_n \to \bigoplus_{v \in V_p(F_n)} \mathscr{U}_{n,v}$$

generate $\iota_n(\mathscr{E}_n)$ modulo its torsion subgroup.

Let p^k be the exponent of the p-power torsion in $\iota_n(\mathscr{E}_n)$. Then, for each $1 \leq i \leq \delta_n$, there exist $a_{ij} \in \mathbb{Z}_p$ for each $\delta_n + 1 \leq j \leq r$ such that

$$\iota_n(\alpha_i) \prod_{j=\delta_n+1}^{r} \iota_n(\alpha_j^{a_{ij}})$$

has trivial p^kth power. Fix $l \geq 1$. For every i and j as above, choose $b_{ij} \in \mathbb{Z}$ such that

$$b_{ij} \equiv a_{ij} \bmod p^l \mathbb{Z}_p,$$

and then set

$$\beta_i = \alpha_i \prod_{j=\delta_n+1}^{r} \alpha_j^{b_{ij}}.$$

It follows that $\iota_n(\beta_i)^{p^k} \in \iota_n(\mathscr{E}_n)^{p^{k+l}}$ for each i.

Since $\alpha_1, \dots, \alpha_r$ form a $\mathbb{Z}_p$-linear basis of the maximal p-torsion-free quotient of $\mathscr{E}_n$, the images of the elements $\beta_1, \dots, \beta_{\delta_n}$ in $F_n^\times / F_n^{\times p^l}$ generate a subgroup isomorphic to $(\mathbb{Z}/p^l\mathbb{Z})^{\delta_n}$. By Kummer theory, the group $F_n^\times \cap F_\infty^{\times p}$ is exactly $\mu_{p^\infty} F_n^{\times p}$, and since the closed subgroup of $\mathscr{E}_n$ generated by $\beta_1, \dots, \beta_{\delta_n}$ is p-torsion-free, the images of these elements generate a subgroup of $F_\infty^\times / F_\infty^{\times p^l}$ that is also isomorphic to $(\mathbb{Z}/p^l\mathbb{Z})^{\delta_n}$.

Now consider

$$K = F_\infty\big(\beta_1^{1/p^l}, \dots, \beta_{\delta_n}^{1/p^l}\big),$$

and note that $\mathrm{Gal}(K/F_\infty)$ is isomorphic to $(\mathbb{Z}/p^l\mathbb{Z})^{\delta_n}$. Since $\iota_n(\beta_i)^{p^k} \in \iota_n(\mathscr{E}_n)^{p^{l+k}}$ and β_i^{1/p^l} is a p^{l+k}th root of $\beta_i^{p^k}$, we have that every prime of v over p splits completely in this extension. Since $\mathrm{Gal}(K/F_\infty)$ is already a quotient of $\mathfrak{X}_\infty$, it is then a quotient of X'_∞. In other words, we have surjections

$$X'_\infty \to (\mathbb{Z}/p^l\mathbb{Z})^{\delta_n}$$

for every l. Since X'_∞ is Λ-torsion, Proposition 2.2.13 tells us that $\delta_n \le \lambda(X'_\infty)$.

Now, if F does not contain μ_{2p}, we still have $\delta(F_n) \le \delta(F_n(\mu_{2p}))$, and since the latter numbers are bounded, we have the result. □

We next study sequences into which $\mathfrak{X}_\infty$ fits. For this, we need to define several more Λ-modules.

DEFINITION 3.3.5. Let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F, and let $S = V_{p\infty}$. We let

$$\mathscr{E}_\infty = \varprojlim_n \mathscr{E}_{F_n} \quad \text{and} \quad \mathscr{E}'_\infty = \varprojlim_n \mathscr{E}_{F_n,S}.$$

where the inverse limits are taken under norm maps. Letting $\mathscr{U}_{n,v}$ denote the pro-p-completion of $\mathscr{O}_{F_{n,v}}^\times$ for $v \in S(F_n)$, we set

$$\mathscr{U}_{\infty,v} = \varprojlim_n \mathscr{U}_{n,v} \quad \text{and} \quad \mathscr{F}_{\infty,v} = \varprojlim_n \widehat{F_{n,v}^\times},$$

for $v \in S(F_\infty)$, with the inverse limits taken with respect to the local norm maps. Set

$$\mathscr{U}_\infty = \prod_{v \in S(F_\infty)} \mathscr{U}_{\infty,v} \quad \text{and} \quad \mathscr{F}_\infty = \prod_{v \in S(F_\infty)} \mathscr{F}_{\infty,v}.$$

Let ι_∞ and ι'_∞ denote the canonical maps

$$\iota_\infty \colon \mathscr{E}_\infty \to \mathscr{U}_\infty \quad \text{and} \quad \iota'_\infty \colon \mathscr{E}'_\infty \to \mathscr{F}_\infty.$$

PROPOSITION 3.3.6. *Let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F. Assume, moreover, that p is odd or F has no real places. We have a map of canonical exact sequences of Λ-modules*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker \iota_\infty & \longrightarrow & \mathscr{E}_\infty & \xrightarrow{\iota_\infty} & \mathscr{U}_\infty & \longrightarrow & \mathfrak{X}_\infty & \longrightarrow & X_\infty & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & \ker \iota'_\infty & \longrightarrow & \mathscr{E}'_\infty & \xrightarrow{\iota'_\infty} & \mathscr{F}_\infty & \longrightarrow & \mathfrak{X}_\infty & \longrightarrow & X'_\infty & \longrightarrow & 0. \end{array}$$

PROOF. This is simply the inverse limit of the sequences of Theorem 1.5.4 for the fields F_n, which remains exact as the modules in question are profinite. The assumptions are simply to insure that the number of terms in the direct sum of local unit or multiplicative groups is finite: otherwise, one need merely replace the direct sums by inverse limits of direct sums at the finite level. □

DEFINITION 3.3.7. We set

$$A'_\infty = \varinjlim_n A_{F_n, V_{p^\infty}}.$$

REMARK 3.3.8. An element $\gamma \in \Gamma$ acts on $H^1(G_{F_\infty,S}, \mu_{p^\infty})$ through its action on cocycles: i.e., for a cocycle f, $\gamma \in \Gamma$, and $\sigma \in G_{F,S}$ we have

$$(\gamma \cdot f)(\sigma) = \gamma \cdot f(\tilde{\gamma}^{-1} \sigma \tilde{\gamma}),$$

where $\tilde{\gamma}$ is any lift of γ to $G_{F,S}$. Giving this cohomology group the discrete topology, with respect to which it is p-power torsion, we have that Γ acts continuously and $\mathbb{Z}_p$-linearly, and hence we obtain a Λ-action.

Kummer theory allows us to prove the following proposition.

PROPOSITION 3.3.9. *Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension, and let $S = V_{p^\infty}$. There is canonical map of exact sequences*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & H^1(G_{F_\infty,S}, \mu_{p^\infty}) & \longrightarrow & A_\infty & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow\!\!\downarrow & & \\ 1 & \longrightarrow & \mathscr{O}_{F_\infty,S}^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & H^1(G_{F_\infty,S}, \mu_{p^\infty}) & \longrightarrow & A'_\infty & \longrightarrow & 0 \end{array}$$

of Λ-modules.

PROOF. Recall from Theorem 1.4.5 that we have exact sequences

$$1 \to \mathscr{O}_{F_n,S}^\times / \mathscr{O}_{F_n,S}^{\times p^m} \to H^1(G_{F_n,S}, \mu_{p^m}) \to A'_n[p^m] \to 0,$$

where $A'_n = A_{F_n,S}$. The direct limit as n heads towards infinity yields

$$1 \to \mathscr{O}_{F_\infty,S}^\times / \mathscr{O}_{F_\infty,S}^{\times p^m} \to H^1(G_{F_\infty,S}, \mu_{p^m}) \to A'_\infty[p^m] \to 0.$$

For any abelian group B, with respect to the maps $B/p^mB \to B/p^{m+1}B$ induced by multiplication by p, we have

$$\varinjlim_m B/p^mB \cong B \otimes_{\mathbb{Z}} \left(\varinjlim_m \frac{1}{p^m}\mathbb{Z}/\mathbb{Z} \right) \cong B \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p,$$

where the maps are the natural inclusion maps on the right-hand side of the middle term. Applying this to $B = \mathscr{O}_{F_\infty,S}^\times$ and noting that

$$A'_\infty = \varinjlim_m A'_\infty[p^m]$$

since A'_∞ is p-power torsion, we have the lower exact sequence. (Note that this did not require F_∞ to be the cyclotomic $\mathbb{Z}_p$-extension).

Now, note that $H^1(G_{F_\infty,S}, \mu_{p^\infty})$ is isomorphic via Kummer theory to the direct limit of the groups $\mathscr{B}_{n,m}/F_n^{\times p^m}$, where $\mathscr{B}_{n,m}$ is the subgroup of $x \in F_n^\times$ such that $x\mathscr{O}_{F_n,S} = \mathfrak{a}^{p^m}$ for some fractional ideal $\mathfrak{a}$ of $\mathscr{O}_{F_n,S}$. We then have maps

$$\mathscr{B}_{n,m}/F_n^{\times p^m} \to A'_n[p^m], \qquad x \mapsto [\mathfrak{a}]',$$

where $[\mathfrak{a}]'$ denotes the class of $\mathfrak{a}$ in A'_n, of which the map

$$\theta' \colon H^1(G_{F_\infty,S}, \mu_{p^\infty}) \to A'_\infty$$

is the direct limit. Given any $x \in \mathscr{B}_{n,m}$, note that there exists $n' > n$ independent of x such that $x\mathscr{O}_{F_{n'}} = \mathfrak{b}^{p^m}$ for some fractional ideal $\mathfrak{b}$ of $\mathscr{O}_{F_{n'}}$ since every prime over p is totally ramified in F_∞/F_t for sufficiently large t. We then have a map

$$\mathscr{B}_{n,m}/F_n^{\times p^m} \to A_{n'}[p^m], \qquad x \mapsto [\mathfrak{b}].$$

In this way, we obtain in the direct limit a map

$$\theta \colon H^1(G_{F_\infty,S}, \mu_{p^\infty}) \to A_\infty$$

which is θ' after composing with the natural projection $A_\infty \to A'_\infty$, which implies that the diagram in the statement of the proposition commutes.

We need only verify exactness in the upper sequence in the statement of the proposition. The kernel of θ is identified by Kummer theory with exactly those

$$x \otimes p^{-m} \in F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

such that $x\mathscr{O}_{F_\infty}$ is the p^mth power of a principal ideal (z), which is to say that

$$x \otimes p^{-m} = xz^{-p^m} \otimes p^{-m} \in \mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p.$$

Moreover, if $\mathfrak{b} \in A_\infty$, then $\mathfrak{b} \in A_\infty[p^m]$ for some $m \geq 1$, and then $\mathfrak{b}$ is the image of some element $\mathfrak{b}_n \in A_n[p^m]$ by definition of the direct limit. We have then that $\mathfrak{b}_n^{p^m} = x\mathscr{O}_{F_n}$ for some $x \in F_n^\times$, and so $\theta(x \otimes p^{-m}) = [\mathfrak{b}]$. Hence, θ is surjective. $\square$

COROLLARY 3.3.10. *Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension, and let $S = V_{p\infty}$. Then there is a canonical exact sequence*

$$1 \to \mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathscr{O}_{F_\infty,S}^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\theta} A_\infty \to A'_\infty \to 0$$

of Λ-modules.

PROOF. This follows from Proposition 3.3.9 via the snake lemma. □

DEFINITION 3.3.11. Let M be a $\mathbb{Z}_p[G_E]$-module for a field E of characteristic not p. For $i \in \mathbb{Z}$, the ith Tate twist of M is the $\mathbb{Z}_p[G_E]$-module $M(i)$ that is M as a $\mathbb{Z}_p$-module, but on which G_E acts via the new action $\cdot_i$ given by

$$\sigma \cdot_i m = \chi(\sigma)^i \sigma m$$

for $\sigma \in G_E$ and $m \in M$.

EXAMPLE 3.3.12. Given a field E of characteristic not p, a choice of compatible system ζ_{p^n} of primitive p^nth roots of unity in a separable closure, i.e., such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for each $n \geq 1$, gives rise to isomorphisms

$$\mathbb{Z}_p(1) \xrightarrow{\sim} \varprojlim_n \mu_{p^n}, \qquad a \mapsto (\zeta_{p^n}^a)_n,$$
$$\mathbb{Q}_p/\mathbb{Z}_p(1) \xrightarrow{\sim} \mu_{p^\infty}, \qquad \frac{a}{p^n} \mapsto \zeta_{p^n}^a$$

of $\mathbb{Z}_p[G_E]$-modules.

REMARK 3.3.13. The Tate twist $\mathbb{Z}_p(i)$ for $i \in \mathbb{Z}$ may be viewed as a Λ-module that is isomorphic to $\mathbb{Z}_p$ as a $\mathbb{Z}_p$-module, and on which $\gamma \in \Gamma = \mathrm{Gal}(F_\infty/F)$ acts by $\chi(\gamma)^i$, where $\chi\colon \Gamma \to \mathbb{Z}_p^\times$ is the homomorphism induced by the cyclotomic character. More generally, if B is any Λ-module, then we may speak of its Tate twist $B(i) \cong B \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(i)$, which is a new Λ-module that is B with a modified action of Γ given by $\gamma \cdot_i b = \chi(\gamma)^i \gamma b$.

COROLLARY 3.3.14. *Suppose that $\mu_{2p} \subset F$ and F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension. Then we have an exact sequence*

$$0 \to A_\infty^\vee(1) \to \mathfrak{X}_\infty \to \mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p(1)) \to 0$$

of finitely generated Λ-modules.

PROOF. By assumption, we have $\mu_{p^\infty} \subset F_\infty$. Hence, we have

$$H^1(G_{F_\infty,S}, \mu_{p^\infty}) \cong \mathrm{Hom}_{\mathrm{cts}}(\mathfrak{X}_\infty, \mu_{p^\infty}) \cong \mathfrak{X}_\infty^\vee(1).$$

Taking the Tate twist of the Pontryagin dual of the sequence of Proposition 3.3.9, we obtain an exact sequence

$$0 \to A_\infty^\vee(1) \to \mathfrak{X}_\infty \to \mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) \to 0.$$

The result now follows from the following calculation for an abelian group B:

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}_p}(B \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) &\cong \mathrm{Hom}_{\mathbb{Z}_p}(B \otimes_{\mathbb{Z}} \mathbb{Z}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \\ &\cong \mathrm{Hom}_{\mathbb{Z}_p}(B \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)) \\ &\cong \mathrm{Hom}_{\mathbb{Z}_p}(B \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p),\end{aligned}$$

where in the second-to-last step we have used the adjointness of Hom and $\otimes$. □

3.4. CM fields

In this subsection, we shall consider the behavior of inverse and direct limits of p-parts of class groups in the cyclotomic $\mathbb{Z}_p$-extension F_∞ of F in the case that F is a CM field. We remark that F_∞ is itself a CM field, and for the most part, we could take F_∞ to be any CM $\mathbb{Z}_p$-extension of F in this section (though conjecturally, as we shall see later, there no others). We assume that p is odd throughout this subsection.

PROPOSITION 3.4.1. *The natural maps*

$$j_n^- : A_n^- \to A_\infty^-$$

are injective for all n. Moreover, the natural maps

$$N_n^- : X_\infty^- \to A_n^-$$

are all surjective.

PROOF. The second statement is easy, since the cokernel of N_n is isomorphic as a Λ-module the maximal unramified quotient of Γ^{p^n}, and Γ has trivial minus part.

For the first statement, it suffices to show that $j_{n+1,n}^- : A_n^- \to A_{n+1}^-$ is injective for each n. Let $G = \mathrm{Gal}(F_{n+1}/F_n)$, and let $\mathscr{O}_n$ denote the ring of integers of F_n. As the maps in Proposition 1.3.5 are easily seen to be Galois equivariant, we have that $\ker j_{n+1,n}^-$ is isomorphic to a submodule of $H^1(G, \mathscr{O}_{n+1}^\times)^-$.

Let $\mu(F_n)$ denote the group of p-power roots of unity in F_n for each n. The exact sequence

$$1 \to \mu(F_{n+1}) \to \mathscr{O}_{n+1}^\times \to \mathscr{O}_{n+1}^\times/\mu(F_{n+1}) \to 1$$

of $\mathbb{Z}_p[\mathrm{Gal}(F_n/F_n^+)]$-modules, gives rise to a long exact sequence in Tate cohomology

$$\cdots \to \hat{H}^0(G, \mathscr{O}_{n+1}^\times/\mu(F_{n+1})) \to H^1(G, \mu(F_{n+1})) \to H^1(G, \mathscr{O}_{n+1}^\times) \to H^1(G, \mathscr{O}_{n+1}^\times/\mu(F_{n+1})) \to \cdots,$$

also of $\mathbb{Z}_p[\mathrm{Gal}(F_n/F_n^+)]$-modules, so it remains exact after taking minus parts.

Now, for any $\mathbb{Z}_p[\mathrm{Gal}(F_{n+1}/F_n^+)]$-module A, we have a canonical isomorphism

$$\hat{H}^{-1}(G,A)^- \xrightarrow{\sim} H^1(G,A)^- \otimes_{\mathbb{Z}_p} G \cong H^1(G,A)^-$$

of $\mathbb{Z}_p[\mathrm{Gal}(F_n/F_n^+)]$-modules, as $\mathrm{Gal}(F_n/F_n^+)$ acts trivially on G (as it acts by lifting and conjugating). Since $\hat{H}^i(G,\mathscr{O}_{n+1}^\times/\mu(F_{n+1}))^-$ is a p-group that is a subquotient of $(\mathscr{O}_{n+1}^\times/\mu(F_{n+1}))^-$ for $i=0,-1$, and the latter group has trivial p-part, we have that there is an isomorphism

$$\hat{H}^{-1}(G,\mu(F_{n+1}))^- \xrightarrow{\sim} H^1(G,\mathscr{O}_{n+1}^\times)^-.$$

Note that $\mu(F_{n+1})^p = \mu(F_n)$. The map $N_G\colon \mu(F_{n+1}) \to \mu(F_{n+1})$ induced by the norm element is given by raising to the pth power so has $\ker(N_G) = \mu_p(F)$, while $I_G\mu(F_{n+1}) = \mu_p(F)$, so we have

$$\hat{H}^{-1}(G,\mu(F_{n+1}))^- = 0,$$

finishing the proof. □

We also have the following fact regarding X_∞^-.

PROPOSITION 3.4.2. *The Λ-module X_∞^- has no nonzero finite Λ-submodules.*

PROOF. Let M be a finite Λ-submodule of X_∞^-. Since M is finite, there exists $m \geq 0$ such that $M \to M_{\Gamma^{p^m}}$ is an isomorphism, which is to say that Γ^{p^m} acts trivially on M. Let $x \in M$, and suppose that x is an element of order p in M. Set $x_n = N_n(x)$. Then $x_n \neq 0$ for sufficiently large n, which we may take be at least m. For such an n, note that $j_{n+1,n}(x_n) \neq 0$ by Proposition 3.4.1. We also have

$$j_{n+1,n}(x_n) = j_{n+1,n}(N_{n+1,n}(x_{n+1})) = px_{n+1}$$

by the triviality of the action of Γ^{p^n} on M. In particular, $px_{n+1} \neq 0$, whch forces $px \neq 0$, contradicting the existence of x. Hence $M = 0$. □

Note that $\mu(X_\infty) = \mu(X_\infty^+) + \mu(X_\infty^-)$ and $\lambda(X_\infty) = \lambda(X_\infty^+) + \lambda(X_\infty^-)$, since $X_\infty \cong X_\infty^- \oplus X_\infty^+$.

PROPOSITION 3.4.3. *Suppose that $\mu_p \subset F$. Then $\mu(X_\infty) = 0$ if and only if $\mu(X_\infty^-) = 0$.*

PROOF. If $\mu(X_\infty^-) = 0$, then Lemma 2.4.10 tells us that the p-ranks of the $(X_\infty)^-_{\Gamma^{p^n}}$ are bounded in n. Since N_n^- is surjective, the p-ranks of the A_n^- are then bounded as well. By the reflection theorem, the p-ranks of the A_n^+ are then bounded, as $r_p(A_n^+) \leq r_p(A_n^-) + 1$. In turn, this implies that the p-ranks of the $(X_\infty)^+_{\Gamma^{p^n}}$ are bounded (since the kernel to A_n^+ has p-rank less than or equal to the number of ramified primes minus 1 in F_∞/F_n, and this number is bounded in n). Again applying Lemma 2.4.10, we have that $\mu(X_\infty^+) = 0$. □

CONJECTURE 3.4.4 (Greenberg). *The Iwasawa module X_∞^+ is finite.*

REMARK 3.4.5. Greenberg's conjecture means exactly that $\lambda(X_\infty^+) = \mu(X_\infty^+) = 0$. Therefore, under the assumption of Iwasawa's μ-conjecture, Greenberg's conjecture is equivalent to the statement that $\lambda(X_\infty^+) = 0$.

PROPOSITION 3.4.6. *Greenberg's conjecture holds if and only if $A_\infty^+ = 0$.*

PROOF. This is an immediate consequence of Corollary 3.2.15, since $(A_\infty^+)^\vee$ has no finite Λ-submodules and hence can be finite if and only if it is zero. □

PROPOSITION 3.4.7. *Suppose that $\mu_p \subset F$. We have an isomorphism*

$$(A_\infty^-)^\vee(1) \xrightarrow{\sim} \mathfrak{X}_\infty^+$$

and an exact sequence

$$0 \to (A_\infty^+)^\vee(1) \to \mathfrak{X}_\infty^- \to \mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p(1)) \to 0.$$

In particular, Greenberg's conjecture implies that

$$\mathfrak{X}_\infty^- \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p(1)).$$

PROOF. Dirichlet's unit theorem tells us that

$$\mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong (\mathscr{O}_{F_\infty^+}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p) \times \mu_{p^\infty}$$

as $\mathbb{Z}_p[\mathrm{Gal}(F/F^+)]$-modules. We have

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p(1))^- = \mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p(1)),$$

and

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathscr{O}_{F_\infty}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p(1))^+ \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mu_{p^\infty}, \mathbb{Z}_p(1)) = 0.$$

The first statement is then a consequence of Corollary 3.3.14, and the second is then a consequence of Proposition 3.4.6. □

COROLLARY 3.4.8. *The finitely generated, Λ-torsion modules $(X_\infty^-)^\iota(1)$ and $\mathfrak{X}_\infty^+$ are pseudo-isomorphic.*

PROOF. This is an immediate consequence of Proposition 3.4.7 and Corollary 3.2.15. □

To obtain even finer information, we can pass to eigenspaces.

COROLLARY 3.4.9. *Let F be totally real, let $\chi\colon G_F \to \overline{\mathbb{Z}_p}^\times$ be a finite odd character of prime-to-p order, and let E be an abelian extension of F of degree prime to p containing $F_\chi(\mu_p)$. Considering Iwasawa modules for the cyclotomic $\mathbb{Z}_p$-extension E_∞/E, we have*

$$\mathfrak{X}_\infty^{(\omega\chi^{-1})} \cong (A_\infty^{(\chi)})^\vee(1) \simeq (X_\infty^{(\chi)})^\iota(1)$$

as $\Lambda[\mathrm{Gal}(E/F)]$*-modules.*

REMARK 3.4.10. In Corollary 3.4.9, the Iwasawa modules in question, $\mathfrak{X}_\infty$, A_∞, and X_∞, have an action of $\mathrm{Gal}(E/F)$ that commutes with the Λ-action, since

$$\mathrm{Gal}(E_\infty/F) \cong \mathrm{Gal}(F_\infty/F) \times \mathrm{Gal}(E/F)$$

in that E_∞/F is abelian and $\mathrm{Gal}(E/F)$ has prime-to-p order.

3.5. Kida's formula

Suppose that F is a number field and E is a cyclic extension with Galois group G. The exact sequence of Theorem 1.3.14 is not quite canonical as written, since one of the maps depends on a choice of generator of G, but it becomes canonical when written in the form

$$\begin{aligned} 0 \to \ker j_{E/F} \otimes_{\mathbb{Z}} G \to \hat{H}^{-1}(G, \mathscr{O}_E^\times) \to I_E^G/I_F \otimes_{\mathbb{Z}} G \to \mathrm{Cl}_E^G / j_{E/F}(\mathrm{Cl}_F) \otimes_{\mathbb{Z}} G \\ \to \mathscr{O}_F^\times / N_{E/F}\mathscr{O}_E^\times \to \ker \Sigma_{E/F} \to (\mathrm{Cl}_E)_G \xrightarrow{N_{E/F}} \mathrm{Cl}_F \to \mathrm{coker}\, \Sigma_{E/F} \to 0, \end{aligned}$$

which is to say that the map

$$\mathrm{Cl}_E^G / j_{E/F}(\mathrm{Cl}_F) \otimes_{\mathbb{Z}} G \to \mathscr{O}_F^\times / N_{E/F}\mathscr{O}_E^\times$$

of Remark 1.3.15 is canonical, noting that there is a canonical isomorphism

$$H^1(G,A) \otimes_{\mathbb{Z}} G \cong \hat{H}^{-1}(G,A)$$

for any $\mathbb{Z}[G]$-module A. Moreover, if E is Galois over $F_0 \subset F$, the maps in the above sequence are all $\mathrm{Gal}(F/F_0)$-equivariant.

Suppose now that we consider the cyclotomic $\mathbb{Z}_p$-extensions F_∞/F and E_∞/F. Then we may consider the inverse limit of the above exact sequences for the extensions E_n/F_n, and we obtain the following result, in which we distinguish Iwasawa modules over F_∞ and E_∞ by writing them in the notation of functions of the base field; e.g., $X_\infty(E)$ is the Galois group of the maximal unramified abelian pro-p extension of E_∞.

THEOREM 3.5.1. *Let E/F be a cyclic of prime power order Galois extension of number fields with $G = \mathrm{Gal}(E/F)$. Let F_∞ denote the cyclotomic extension of F, and let $E_\infty = EF_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of E. We suppose that $E \cap F_\infty = F$, so we have $G \cong \mathrm{Gal}(E_\infty/F_\infty)$. Let*

$$j_\infty \colon X_\infty(F) \to X_\infty(E)^G$$

denote the direct limit of the maps j_{E_n/F_n}. For $v \in V(F_\infty)$, let I_v denote the inertia group of v in G. Let

$$\Sigma_\infty \colon \bigoplus_{v \in V(F_\infty)} I_v \to G$$

denote the product of the inclusion maps. We then have a canonical exact sequence of Λ-modules:

$$0 \to \ker j_\infty \otimes_{\mathbb{Z}} G \to \hat{H}^{-1}(G, \mathscr{E}_\infty(E)) \to \varprojlim_n I_{E_n}^G / I_{F_n} \otimes_{\mathbb{Z}} G \to \operatorname{coker} j_\infty \otimes_{\mathbb{Z}} G$$
$$\to \hat{H}^0(G, \mathscr{E}_\infty(E)) \to \ker \Sigma_\infty \to X_\infty(E)_G \to X_\infty(F) \to \operatorname{coker} \Sigma_\infty \to 0.$$

If F is a CM field and p is odd, then E is also CM, and the sequence of Theorem 3.5.1 is $\mathrm{Gal}(F/F^+)$-equivariant. Taking minus parts, we are able to obtain the following.

LEMMA 3.5.2. *Let E/F be a Galois extension of CM fields with $G = \mathrm{Gal}(E/F) \cong \mathbb{Z}/p\mathbb{Z}$, for p odd. Suppose that $\mu(X_\infty^-(F)) = 0$. Let $\delta = 1$ if $\mu_p \subset F$ and 0 otherwise. Let T denote the set of primes of F_∞^+ that split in F_∞/F_∞^+, ramify in E_∞/F_∞, and do not lie over p. Then the Herbrand quotient $h(X_\infty^-(E))$ exists and equals $p^{\delta - |T|}$. Moroever, $\mu(X_\infty^-(E)) = 0$.*

PROOF. Note that $G = G^+$ and $\mathscr{E}_\infty^-(E) = \mathbb{Z}_p(1)^\delta$, so

$$\hat{H}^i(G, \mathscr{E}_\infty(E))^- \cong \hat{H}^i(G, \mathscr{E}_\infty^-(E)) \cong \hat{H}^i(G, \mathbb{Z}_p(1))^\delta.$$

One checks immediately that $\hat{H}^0(G, \mathbb{Z}_p(1)) \cong \mu_p$ and $\hat{H}^{-1}(G, \mathbb{Z}_p(1)) = 0$. In particular j_∞ is injective on minus parts.

We remark first that $I_{E_n}^G / I_{F_n}$ is generated by the classes of the ramified primes of E_n that are ramified over F_n, and is a direct sum of copies of $\mathbb{Z}/p\mathbb{Z}$, one for each such prime. Now, a norm compatible sequence of nontrivial images of primes in the $I_{E_n}^G / I_{F_n}$ as n varies must consist of primes above p, for a prime ideal not over p in E_n is inert in E_{n+1}/E_n for large enough n, and then therefore is not a norm from the extension. On the other hand, those above p are totally ramified in E_{n+1}/E_n for large enough n, so do form part of a unique norm compatible sequence. We therefore have that

$$\varprojlim_n I_{E_n}^G / I_{F_n} \cong \bigoplus_{v \in V_p(F_\infty)} I_v.$$

Since G is of order p, we have either $I_v = G$ or $I_v = 0$ if v is a prime of F_∞. We note that $I_v^- = 0$ if $u \in V_{F_\infty^+}$ does not split in F_∞/F_∞^+ and v lies above u while $(I_v \oplus I_{v'})^- \cong I_u$ if u splits into v and v'. Noting also that $G^- = 0$, we obtain an exact sequence

$$0 \to \bigoplus_{v \in S_p} G \to (X_\infty^-(E))^G / j_\infty(X_\infty^-(F)) \to \mu_p^\delta \to \bigoplus_{v \in S} G \to X_\infty^-(E)_G \to X_\infty^-(F) \to 0, \tag{3.5.1}$$

where S denotes the set of primes of F_∞^+ that split in F_∞/F_∞^+ and ramify in E_∞/F_∞, and $S_p \subseteq S$ is the subset of primes over p.

The exact sequence (3.5.1) tells us that $\mu((X_\infty^-(E))_G) = 0$, since $\mu(X_\infty^-(F)) = 0$. But if A_G is finitely generated over $\mathbb{Z}_p$, then A is finitely generated over $\mathbb{Z}_p[G]$, and hence over $\mathbb{Z}_p$ since G is finite. Therefore, we have $\mu(X_\infty^-(E)) = 0$.

Since $j_\infty^-: X_\infty^-(F) \to X_\infty^-(E)^G$ is injective and $N_\infty^-: X_\infty^-(E) \to X_\infty^-(F)$ is surjective, we have

$$\operatorname{coker} j_\infty^- \cong \tfrac{X_\infty^-(E)^G}{N_G X_\infty^-(E)} = \hat{H}^0(G, X_\infty^-(E)),$$
$$\ker N_\infty^- \cong \ker(X_\infty^-(E)_G \xrightarrow{N_G} X_\infty^-(E)^G) = \hat{H}^{-1}(G, X_\infty^-(E)).$$

Therefore, we have

$$h(X_\infty^-(E)) = \frac{|\operatorname{coker} j_\infty^-|}{|\ker N_\infty^-|} = p^{|S_p^-|+\delta-|S^-|} = p^{\delta-|T|}.$$

□

We are now ready to prove Kida's formula. Kida's formula may be thought of as an analogue of the Riemann-Hurwitz formula, which describes the growth of genus of Riemann surfaces in branched covers.

THEOREM 3.5.3 (Kida). *Let p be an odd prime, and let E/F be a finite p-extension of CM-number fields. Let E_∞ (resp., F_∞) be the cyclotomic $\mathbb{Z}_p$-extension of E (resp., F), and suppose that $E \cap F_\infty = F$. Assume that $\mu(X_\infty^-(F)) = 0$. Then $\mu(X_\infty^-(E)) = 0$, and we have*

$$\lambda(X_\infty^-(E)) - \delta = [E:F](\lambda(X_\infty^-(F)) - \delta) + \sum_{w \in Q_E} (|I_w| - 1),$$

where $\delta = 1$ if $\mu_p \subset F$ and 0 otherwise,

$$Q_E = \{w \in V(E_\infty^+) - V_p(E_\infty^+) \mid w \text{ splits in } E_\infty/E_\infty^+\},$$

and I_w is the ramification group of w in $\operatorname{Gal}(E_\infty^+/F_\infty^+)$.

PROOF. First, we reduce the result to cyclic groups of order p by induction on the order of $G = \operatorname{Gal}(E_\infty^+/F_\infty^+) \cong \operatorname{Gal}(E/F)$. Let K be an intermediate field in E/F, let $G' = \operatorname{Gal}(K/F)$, and let $G'' = \operatorname{Gal}(E/K)$ (which can be taken to be of order p). For $v \in V_{K_\infty^+}$, let I_v' denote the ramification group of v in G', and for $w \in V_{E_\infty^+}$, let I_w'' denote the ramification group of w in G''. The statement on μ-invariants then follows immediately by induction and Lemma 3.5.2. Then, by induction, we have

$$\begin{aligned}
\lambda(X_\infty^-(E)) - \delta &= [E:K](\lambda(X_\infty^-(K)) - \delta) + \sum_{w \in Q_E} (|I_w''| - 1) \\
&= [E:K]\Big([K:F](\lambda(X_\infty^-(F)) - \delta) + \sum_{v \in Q_K} (|I_v'| - 1)\Big) + \sum_{w \in Q_E} (|I_w''| - 1) \\
&= [E:F](\lambda(X_\infty^-(F)) - \delta) + [E:K] \sum_{v \in Q_K} (|I_v'| - 1) + \sum_{w \in Q_E} (|I_w''| - 1).
\end{aligned}$$

For any $v \in Q_K$ and $w \in Q_E$ lying above v, Corollary 3.1.10 tells us that $[G'' : I''_w]$ is the number of primes of Q_E lying above v. We then have

$$[E:K]\sum_{v\in Q_K}(|I'_v|-1) = |G''|\sum_{w\in Q_E}[G'':I''_w]^{-1}(|I'_v|-1)$$
$$= \sum_{w\in Q_E}(|I_w|-|I''_w|) = \sum_{w\in Q_E}(|I_w|-1) - \sum_{w\in Q_E}(|I''_w|-1),$$

finishing the inductive step.

Now, we are reduced to the case that $[E:F]=p$. Note that in this case, a prime $w \in Q_E$ is either totally ramified (of degree p) or completely split in E/F, so

$$\sum_{w\in Q_E}(|I_w|-1) = \sum_{v\in T}(p-1) = (p-1)|T|,$$

where T is, as in Lemma 3.5.2, the set of primes of Q_F that ramify in E_∞^+/F_∞^+. By Proposition 3.4.2 and the fact that $\mu(X_\infty^-(E))=0$, we have that $X_\infty^-(E)$ is free of finite rank over $\mathbb{Z}_p$. It is also a $\mathbb{Z}_p[G]$-module, and therefore

$$X_\infty^-(E) \cong \mathbb{Z}_p[G]^r \oplus X^s \oplus \mathbb{Z}_p^t$$

for some r,s,t. It follows immediately that

$$\lambda(X_\infty^-(E)) = pr+(p-1)s+t = p(r+t)+(p-1)(s-t).$$

We compute, under these isomorphisms

$$X_\infty^-(E)^G \cong (N_G)^r \oplus \mathbb{Z}_p^t \quad \text{and} \quad N_G X_\infty^-(E) \cong (N_G)^r \oplus (p\mathbb{Z}_p)^t$$
$$X_\infty^-(E)[N_G] = X^r \oplus X^s \quad \text{and} \quad I_G X_\infty^-(E) = X^r \oplus (I_G X)^s,$$

so

$$h(X_\infty^-(E)) = \frac{|\hat{H}^0(G,X_\infty^-(E))|}{|\hat{H}^{-1}(G,X_\infty^-(E))|} = p^{t-s}.$$

By Lemma 3.5.2, we therefore have that

$$s-t = |T|-\delta.$$

One sees immediately from Theorem 3.5.1 that the inverse limit of norm maps

$$X_\infty^-(E)_G \to X_\infty^-(F)$$

is a pseudo-isomorphism. We then have that

$$\lambda(X_\infty^-(F)) = \lambda(X_\infty^-(E)_G) = \mathrm{rank}_{\mathbb{Z}_p}(X_\infty^-(E)_G) = r+t.$$

It follows that

$$\lambda(X_\infty^-(E))-\delta = p\lambda(X_\infty^-(F))+(p-1)(|T|-\delta)-\delta = p(\lambda(X_\infty^-(F))-\delta)+(p-1)|T|,$$

finishing the proof. □

CHAPTER 4

Cyclotomic fields

4.1. Dirichlet L-functions

In this section, we summarize, largely without proof, various results regarding L-functions of Dirichlet characters.

DEFINITION 4.1.1. A multiplicative function $\chi\colon \mathbb{Z} \to \mathbb{C}$ is called a *Dirichlet character* if it is periodic of some period $n \geq 1$ and $\chi(a) \neq 0$ for $a \in \mathbb{Z}$ if and only if $(a,n) = 1$. The integer n is called the *modulus* of χ.

EXAMPLE 4.1.2. There is a unique Dirichlet character 1 which has value 1 at every $a \in \mathbb{Z}$, and it is known as the trivial character.

DEFINITION 4.1.3.

a. The *conductor* f_χ of a Dirichlet character χ is the smallest integer f dividing its period such that there exists a Dirichlet character ψ of modulus f with $\chi(a) = \psi(a)$ for all $a \in \mathbb{Z}$ with $(a,n) = 1$.

b. We say that a Dirichlet character is *primitive* if its conductor equals its modulus.

DEFINITION 4.1.4. We say that a Dirichlet character χ is *even* (resp., *odd*) if $\chi(-1) = 1$ (resp., $\chi(-1) = -1$.)

Every character $\phi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ gives rise to a Dirichlet character $\chi\colon \mathbb{Z} \to \mathbb{C}$ of period n with $\chi(a) = \phi(a \pmod n)$ for $a \in \mathbb{Z}$ with $(a,n) = 1$. The resulting character χ has conductor f, where f is minimal such that ϕ factors through $(\mathbb{Z}/f\mathbb{Z})^\times$.

DEFINITION 4.1.5. Let $\phi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$, and suppose that the induced Dirichlet character has conductor f. The *primitive Dirichlet character attached to* ϕ is the primitive Dirichlet character of conductor f that satisfies $\phi(a) = \chi(a')$ for $a \in \mathbb{Z}$, $(a,f) = 1$, where $a' \in \mathbb{Z}$ is any integer with $a' \equiv a \bmod f$ and $(a',n) = 1$.

Let $F/\mathbb{Q}$ be an abelian field, and let $n \geq 1$ be such that $F \subseteq \mathbb{Q}(\mu_n)$. The cyclotomic character then allows us to identify $\mathrm{Gal}(F/\mathbb{Q})$ with a quotient of $(\mathbb{Z}/n\mathbb{Z})^\times$.

NOTATION 4.1.6. The set $X(F)$ of primitive Dirichlet characters of $F \subseteq \mathbb{Q}(\mu_N)$ consists of the primitive characters of conductor dividing n attached to characters of $(\mathbb{Z}/n\mathbb{Z})^\times$ that factor through $\mathrm{Gal}(F/\mathbb{Q})$.

REMARK 4.1.7. A Dirichlet character $\chi \in X(F)$ is even if and only if the associated character on $\mathrm{Gal}(F/\mathbb{Q})$ is even.

To any Dirichlet character, we can attach an L-series.

DEFINITION 4.1.8. Let χ be a Dirichlet character. The *Dirichlet L-series* attached to χ is the complex-valued function on $s \in \mathbb{C}$ with $\mathrm{Re}\, s > 1$ defined by

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

EXAMPLE 4.1.9. For $\chi = 1$, one has $L(1, s) = \zeta(s)$, the Riemann ζ-function.

We note that Dirichlet L-series have Euler product expansions.

PROPOSITION 4.1.10. *One has*

$$L(\chi, s) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}}$$

for all $s \in \mathbb{C}$ *with* $\mathrm{Re}\, s > 1$.

THEOREM 4.1.11. *The L-series* $L(\chi, s)$ *has a meromorphic continuation to all of* $\mathbb{C}$ *that is analytic if* $f_\chi > 1$, *while* $\zeta(s)$ *is holomorphic aside from a simple pole at* $s = 1$ *with residue* 1.

DEFINITION 4.1.12. The *Dirichlet L-function* $L(\chi, s)$ of a Dirichlet character χ is the meromorphic continuation of the L-series $L(\chi, s)$ to $\mathbb{C}$.

DEFINITION 4.1.13. The Γ-*function* is the unique meromorphic function on $\mathbb{C}$ that satisfies

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t}\, dt$$

for all $s \in \mathbb{C}$ with $\mathrm{Re}\, s > 0$ and

$$\Gamma(s+1) = s\Gamma(s)$$

for all s for which it is defined.

REMARK 4.1.14. The Γ-function has poles, which are all simple, at exactly the nonpositive integers. It also satisfies $\Gamma(n) = (n-1)!$ for any positive integer n.

DEFINITION 4.1.15. The *Gauss sum* attached to a Dirichlet character χ of modulus n is the value

$$\tau(\chi) = \sum_{a=1}^{n} \chi(a) e^{2\pi i a/n}.$$

DEFINITION 4.1.16. For a Dirichlet character χ, we let $\bar{\chi}$ denote its *complex conjugate*, which satisfies $\bar{\chi}(a) = \overline{\chi(a)}$ for all $a \in \mathbb{Z}$.

We mention a couple of basic lemmas regarding Gauss sums that will be of use.

LEMMA 4.1.17. *Let χ be a primitive Dirichlet character. Then we have*

$$\chi(b)\tau(\bar{\chi}) = \sum_{a=1}^{f_\chi} \bar{\chi}(a) e^{2\pi i ab/f_\chi}$$

for all $b \in \mathbb{Z}$.

PROOF. If $\chi(b) = 0$, then setting $d = (b, f_\chi)$ and $m = d^{-1} f_\chi$, we have

$$\sum_{a=1}^{f_\chi} \bar{\chi}(a) e^{2\pi i ab/f_\chi} = \sum_{a=1}^{m} \sum_{c=1}^{d} \bar{\chi}(a+mc) e^{2\pi i ab/f_\chi},$$

and

$$\sum_{c=1}^{d} \bar{\chi}(a+mc) = 0$$

for all a. If $\chi(b) \neq 0$, then

$$\chi(b)\tau(\bar{\chi}) = \sum_{a=1}^{f_\chi} \bar{\chi}(ab^{-1}) e^{2\pi i a/f_\chi},$$

which gives the desired equality upon reordering the sum. □

LEMMA 4.1.18. *For a primitive Dirichlet character χ, we have*

$$|\tau(\chi)| = f_\chi^{1/2}.$$

PROOF. Note that $\overline{\tau(\chi)} = \chi(-1)\tau(\bar{\chi})$. We then have

$$|\tau(\chi)| = \chi(-1) \sum_{a=1}^{f_\chi} \chi(a)\tau(\bar{\chi}) e^{2\pi i a/f_\chi},$$

and by Lemma 4.1.17, this equals

$$\chi(-1) \sum_{a=1}^{f_\chi} \left(\sum_{b=1}^{f_\chi} \bar{\chi}(b) e^{2\pi i ab/f_\chi} \right) e^{2\pi i a/f_\chi} = \chi(-1) \sum_{b=1}^{f_\chi} \bar{\chi}(b) \sum_{a=1}^{f_\chi} e^{2\pi i a(b+1)/f_\chi}.$$

The latter sum of exponentials is zero unless $b = f_\chi - 1$, in which case it is f_χ. Hence,

$$|\tau(\chi)| = |\chi(-1)|^2 f_\chi = f_\chi.$$

□

DEFINITION 4.1.19. For a primitive Dirichlet character χ, we set

$$\delta_\chi = (1-\chi(-1))/2, \quad \varepsilon_\chi = \frac{\tau(\chi)}{i^{\delta_\chi}\sqrt{f_\chi}}, \text{ and } \quad \Lambda(\chi,s) = \left(\frac{f_\chi}{\pi}\right)^{s/2}\Gamma\left(\frac{s+\delta_\chi}{2}\right)L(\chi,s),$$

THEOREM 4.1.20. *Let χ be a primitive Dirichlet character. Then the L-functions of χ and $\bar{\chi}$ satisfy the functional equation*

$$\Lambda(\chi,s) = \varepsilon_\chi \Lambda(\bar{\chi}, 1-s)$$

for all $s \in \mathbb{C}$.

We give the relationship between Dirichlet L-functions and the Dedekind zeta function of an abelian field.

PROPOSITION 4.1.21. *Let F be an abelian field. Then*

$$\zeta_F(s) = \prod_{\chi \in X(F)} L(\chi,s).$$

PROOF. It suffices to check this on s with $\mathrm{Re}\, s > 1$ by uniqueness of the meromorphic continuations. In turn, it suffices to check that for each prime p, we have

$$\prod_{\mathfrak{p} \in V_p(F)} (1-(N\mathfrak{p})^{-s}) = \prod_{\chi \in X(F)} (1-\chi(p)p^{-s}). \tag{4.1.1}$$

As $F/\mathbb{Q}$ is Galois, we have $N\mathfrak{p} = p^{-fs}$, where f is the common residue degree of the primes over p in F, so the lefthand side is just $(1-p^{-fs})^g$, where $g = |V_p(F)|$. Note that $\chi(p) = 0$ if p ramified in the fixed field of the kernel of χ. Thus, the product reduces to $\chi \in X(E)$, where E is the maximal subextension of $F/\mathbb{Q}$ that is unramified at p. Viewing $\chi \in X(E)$ as a Galois character, so $\chi(p)$ is the value of χ on the Frobenius at p, which is a generator of a cyclic subgroup of order f in $\mathrm{Gal}(E/\mathbb{Q})$. Since $fg = [E:\mathbb{Q}]$, there are g characters χ such that $\chi(f) = \zeta_f^i$ for a fixed primitive fth root of unity ζ_f and given integer i with $0 \le i \le f-1$. The righthand side of (4.1.1) is then simply

$$\prod_{i=0}^{f-1}(1-\zeta_f p^{-s})^g = (1-p^{-fs})^g,$$

as required. □

COROLLARY 4.1.22. *Let χ be a Dirichlet character with associated primitive character nontrivial. Then $L(\chi,1) \neq 0$.*

PROOF. Since $\zeta_F(s)$ has a simple pole at $s=1$, as does $L(\chi_0,s)$, for χ_0 the trivial character of modulus $[F:\mathbb{Q}]$, while $L(\chi,s)$ is analytic for $\chi \neq \chi_0$, this is a direct result of Proposition 4.1.21. □

4.2. Bernoulli numbers

DEFINITION 4.2.1. For $n \geq 0$, the nth *Bernoulli number* B_n is the value of the nth derivative of $\frac{t}{e^t-1}$ at 0.

In other words, B_n is the rational number appearing in the Taylor expansion

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

EXAMPLE 4.2.2. We have

$$\frac{e^t-1}{t} = \sum_{n=0}^{\infty} \frac{t^n}{(n+1)!} = 1 + \frac{1}{2}t + \frac{1}{6}t^2 + \cdots,$$

so $B_0 = 1$, $B_1 = -\frac{1}{2}$, and $B_2 = \frac{1}{6}$ after inverting the series.

REMARK 4.2.3. Note that

$$\frac{-t}{e^{-t}-1} = \frac{te^t}{e^t-1} = \frac{t}{e^t-1} + t,$$

so

$$\frac{t}{e^t-1} + \frac{1}{2}t$$

is an even function, and therefore we have $B_n = 0$ for all odd $n \geq 2$.

We shall require generalizations of these numbers attached to Dirichlet characters.

DEFINITION 4.2.4. Let χ be a primitive Dirichlet character, and let m be any multiple of f_χ. Then the *generalized Bernoulli number* $B_{n,\chi}$ is the algebraic number appearing in the series expansions

$$\sum_{a=1}^{m} \chi(a) \frac{te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

REMARK 4.2.5. The independence from m in the definition of $B_{n,\chi}$ is easily seen to boil down to the fact that

$$\sum_{i=0}^{r-1} \frac{x^i}{x^r-1} = \frac{1}{x-1},$$

taking $r = m/f_\chi$ and $x = e^{f_\chi t}$.

REMARK 4.2.6. We have $B_{n,1} = B_n$ for all $n \geq 2$, but $B_{1,1} = \frac{1}{2} = -B_1$.

REMARK 4.2.7. We have that $B_{n,\chi} = 0$ for $n \not\equiv \delta_\chi \bmod 2$, aside from $B_{1,1}$.

We also have Bernoulli polynomials.

DEFINITION 4.2.8. The nth *Bernoulli polynomial* $B_n(X) \in \mathbb{Q}[X]$ is the polynomial appearing in the series expansion

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!}.$$

EXAMPLE 4.2.9. We have $B_0(X) = 1$ and $B_1(X) = X - \frac{1}{2}$.

LEMMA 4.2.10. *Let χ be a primitive Dirichlet character, and let m be a multiple of f_χ. We have*

$$B_{n,\chi} = m^{n-1} \sum_{a=1}^{m} \chi(a) B_n(\tfrac{a}{m})$$

for $n \geq 1$.

PROOF. We have

$$\sum_{n=0}^{\infty} m^{n-1} \sum_{a=1}^{m} \chi(a) B_n\left(\frac{a}{m}\right)\frac{t^n}{n!} = \sum_{a=1}^{m} \chi(a) m^{-1} \sum_{n=0}^{\infty} B_n\left(\frac{a}{m}\right)\frac{(mt)^n}{n!} = \sum_{a=1}^{m} \chi(a)\frac{te^{at}}{e^{mt}-1}.$$

□

COROLLARY 4.2.11. *Let χ be a primitive, nontrivial Dirichlet character of conductor dividing m. Then we have*

$$B_{1,\chi} = \frac{1}{m}\sum_{a=1}^{m} \chi(a) a.$$

PROOF. We compute easily that $B_1(x) = x - 1/2$. The result then follows from Lemma 4.2.10 and the fact that the sum over all $\chi(a)$ for $1 \leq a \leq m$ is zero, since χ is nontrivial. □

DEFINITION 4.2.12. A value of $L(\chi, s)$ at $s \in \mathbb{Z}$ is known as an L-value, or as a special value of the L-function $L(\chi, s)$.

The following proposition gives a relationship between L-values and generalized Bernoulli numbers.

PROPOSITION 4.2.13. *Let χ be a primitive Dirichlet character. Then we have*

$$L(\chi, 1-n) = -\frac{B_{n,\chi}}{n}$$

for all positive integers n.

PROOF. Let $x \in \mathbb{R}$ with $0 < x \leq 1$, and consider the complex function

$$f(t) = \frac{te^{(1-x)t}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(1-x)\frac{t^n}{n!}.$$

For $s \in \mathbb{C}$, set

$$g(s) = \lim_{\varepsilon \to 0^+} \int_{\gamma_\varepsilon} f(t) t^{s-2} dt,$$

where the path γ_ε consists of the horizontal infinite path along the real axis to ε, following by a counterclockwise traversal around the circle C_ε of radius ε, followed by the horizontal infinite path from ε along the positive real axis. Here, $t^{s-2} = e^{(s-2)\log t}$, where we take the branch of the logarithm given by the positive real axis. Then

$$g(s) = \lim_{\varepsilon \to 0^+} \left((e^{2\pi i s} - 1) \int_\varepsilon^\infty f(t) t^{s-2} dt + \int_{C_\varepsilon} f(t) t^{s-2} dt \right).$$

If $\operatorname{Re} s > 1$, the second term vanishes in the limit, and this simplifies to

$$(e^{2\pi i s} - 1)^{-1} g(s) = \int_0^\infty f(t) t^{s-2} dt = \sum_{k=0}^\infty \int_0^\infty t^{s-1} e^{-(x+k)t} dt = \sum_{k=0}^\infty (x+k)^{-s} \Gamma(s) = \Gamma(s)\zeta(s,x),$$

where we set $\zeta(s,x) = \sum_{k=0}^\infty (x+k)^{-s}$. The latter function can be meromorphically continued to all of $\mathbb{C}$ which is again analytic away from $s = 1$. We therefore have

$$g(s) = (e^{2\pi i s} - 1)\Gamma(s)\zeta(s,x)$$

for all $s \in \mathbb{C} - \{1\}$.

For $s = 1 - n$, we obtain

$$\lim_{s \to 1-n} (e^{2\pi i s} - 1)\Gamma(s)\zeta(s,x) = \lim_{\varepsilon \to 0^+} \int_{C_\varepsilon} f(t) t^{-1-n} dt = 2\pi i \cdot \frac{B_n(1-x)}{n!}$$

by Cauchy's integral formula. We have

$$\lim_{s \to 1-n} (e^{2\pi i s} - 1)\Gamma(s) = 2\pi i \lim_{s \to 1-n} s\Gamma(s) = 2\pi i \frac{(-1)^{n-1}}{(n-1)!},$$

so we obtain

$$\zeta(1-n,x) = (-1)^{n-1} \frac{B_n(1-x)}{n} = -\frac{B_n(x)}{n}.$$

Finally, setting $f = f_\chi$, we need only note that

$$L(\chi, 1-n) = \sum_{a=1}^f \chi(a) f^{n-1} \zeta(1-n, \tfrac{a}{f}) = -\frac{1}{n} \sum_{a=1}^f \chi(a) f^{n-1} B_n(\tfrac{a}{f}) = -\frac{B_{n,\chi}}{n}.$$

□

THEOREM 4.2.14. *Let χ be a nontrivial primitive Dirichlet character. We have*

$$L(\chi, 1) = \begin{cases} \dfrac{\pi i \tau(\chi)}{f_\chi} B_{1,\bar{\chi}} & \text{if } \chi \text{ is odd,} \\ -\dfrac{\tau(\chi)}{f_\chi} \displaystyle\sum_{a=1}^{f_\chi} \bar{\chi}(a) \log |1 - e^{2\pi i a / f_\chi}| & \text{if } \chi \text{ is even .} \end{cases}$$

PROOF. If χ is odd, then the functional equation and the fact that $\Gamma(1/2) = \pi^{1/2}$ imply that

$$L(\chi,1) = -\frac{\pi i \tau(\chi)}{f_\chi} L(\bar{\chi},0) = \frac{\pi i \tau(\chi)}{f_\chi} B_{1,\bar{\chi}}.$$

Now let χ be even, and set $f = f_\chi$. By Lemma 4.1.17, we then have

$$L(\chi,1) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{1}{\tau(\bar{\chi})} \sum_{a=1}^{f} \frac{\bar{\chi}(a) e^{2\pi i a n/f}}{n} = -\frac{1}{\tau(\bar{\chi})} \sum_{a=1}^{f} \bar{\chi}(a) \log(1 - e^{2\pi i a/f}).$$

By Lemma 4.1.18 (and Lemma 4.1.17), we have that $\tau(\bar{\chi})\tau(\chi) = f$, and the evenness of $\bar{\chi}$ plus the fact that the sum is taken over all a mod f tell us that we may replace $\log(1 - e^{2\pi i a/f})$ with

$$\log|1 - e^{2\pi i a/f}| = \frac{1}{2}(\log(1 - e^{2\pi i a/f}) + \log(1 - e^{2\pi i (f-a)/f})).$$

□

Combining the analytic class number formula with Proposition 4.1.21 and Theorem 4.1.11, we obtain the following, which we will at times also refer to as the analytic class number formula.

COROLLARY 4.2.15. *Let F be an abelian field. Then we have*

$$\prod_{\substack{\chi \in X(F) \\ \chi \neq 1}} L(\chi,1) = \frac{2^{r_1(F)} (2\pi)^{r_2(F)} h_F R_F}{w_F |d_F|^{1/2}}.$$

We note the following.

LEMMA 4.2.16. *Let F be a CM field. Set $Q_F = [E_F : \mu(F) E_F^+]$. Then $Q_F \in \{1,2\}$ and*

$$[E_F : E_F^+] = \tfrac{Q_F}{2} w_F.$$

PROOF. Let τ be the generator of $\mathrm{Gal}(F/F^+)$. For $\alpha \in E_F$, we have $|\alpha^{1-\tau}| = 1$ under any complex embedding of F, so $\alpha^{1-\tau} \in \mu(F)$. Consider the commutative diagram

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \langle -1 \rangle & \longrightarrow & \mu(F) & \longrightarrow & \mu(F)^2 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & E_F^+ & \longrightarrow & E_F & \xrightarrow{1-\tau} & \mu(F) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & E_F^+/\langle -1 \rangle & \longrightarrow & E_F/\mu(F) & \xrightarrow{1-\tau} & \mu(F)/\mu(F)^2 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

The snake lemma tells us that the cokernels K of the two maps $\tau - 1$ are isomorphic. The lower two rows yield

$$[E_F : E_F^+] = \frac{w_F}{|K|} \quad \text{and} \quad [E_F : \mu(F)E_F^+] = \frac{2}{|K|},$$

and the result follows. □

We remark that for cyclotomic fields, Q_F is computable.

LEMMA 4.2.17. *Let $F = \mathbb{Q}(\mu_m)$ for some $m \geq 1$ with $m \not\equiv 2 \bmod 4$. Then*

$$Q_F = \begin{cases} 1 & m \text{ is a prime power} \\ 2 & \text{otherwise.} \end{cases}$$

PROOF. Let τ be the generator of $\mathrm{Gal}(F/F^+)$. Note that

$$Q_F = 2|\mathrm{coker}(E_F \xrightarrow{1-\tau} \mu(F))|^{-1}$$

by the proof of Lemma 4.2.16. If m is not a prime power, then $1-\zeta_m$ is a unit, and $(1-\zeta_m)^{1-\tau} = -\zeta_m$, which generates $\mu(F)$. Thus $Q_F = 2$ in this case. Conversely, if $\alpha^{1-\tau} = -\zeta_m$ generates $\mu(F)$ for some $\alpha \in E_F$, we would have $\alpha^{-1}(1-\zeta_m) \in F^+$. If m were a power of a prime p, then $\alpha^{-1}(1-\zeta_m)$ would generate the unique prime over p in F. Since this prime is ramified in F/F^+, its generator cannot lie in F^+. This forces Q_F to be 1 if m is a prime power. □

NOTATION 4.2.18. For a CM field F, we set $R_F^+ = R_{F^+}$

LEMMA 4.2.19. *Let F be a CM field. Then*

$$R_F = 2^{r_2(F)-2} \frac{w_F}{[E_F : E_F^+]} R_F^+.$$

PROOF. Let

$$r = r_2(F) - 1 = \mathrm{rank}\, E_F = \mathrm{rank}\, E_F^+.$$

Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_r \in E_F^+$ satsify

$$\langle -1, \alpha_1, \alpha_2, \ldots, \alpha_r \rangle = E_F^+.$$

Then

$$\mu(F) \cdot \langle \alpha_1, \alpha_2, \ldots, \alpha_r \rangle = \mu(F)E_F^+,$$

which has index $2[E_F : E_F^+]/w_F$ in E_F, so Lemma 1.2.10 tells us that

$$R_F = \frac{w_F}{2[E_F : E_F^+]} R_F(\alpha_1, \alpha_2, \ldots, \alpha_r).$$

On the other hand, note that each c_i in Definition 1.2.5 is 2 for F but 1 for F^+, so

$$R_F(\alpha_1, \alpha_2, \ldots, \alpha_r) = 2^r R_F^+,$$

as desired. □

Corollary 4.2.15 implies the following.

THEOREM 4.2.20. *Suppose that F is a CM abelian field. Then*

$$h_F^- = 2[E_F : E_F^+] \prod_{\substack{\chi \in X(F) \\ \chi \text{ odd}}} \frac{-B_{1,\chi}}{2} \quad \text{and} \quad h_F^+ = \frac{1}{R_F^+} \prod_{\substack{\chi \in X(F) \\ \chi \neq 1 \text{ even}}} \left(\frac{-1}{2} \sum_{a=1}^{f_\chi} \chi(a) \log |1 - e^{2\pi i a/f_\chi}| \right).$$

PROOF. Let E be an arbitrary abelian field. We remark that for $\chi \in X(E)$, the quantity f_χ is the conductor of the corresponding character $(\mathbb{Z}/f_\chi\mathbb{Z})^\times \to \mathbb{C}^\times$. Therefore, the conductor-discriminant fomula tells us that

$$|d_E| = \prod_{\chi \in X(E)} f_\chi. \tag{4.2.1}$$

Moreover, a comparison of the functional equations of the Dirichlet L-functions and the Artin L-functions yields that

$$\prod_{\chi \in X(E)} \varepsilon_\chi = 1,$$

so

$$\prod_{\chi \in X(E)} \tau(\chi) = i^{r_2(E)} |d_E|^{1/2}. \tag{4.2.2}$$

Taking the quotient of the analytic class number formula for F by that for F^+ and applying Theorem 4.2.14, we obtain

$$\prod_{\substack{\chi \in X(F) \\ \chi \text{ odd}}} \frac{\pi i \tau(\chi)}{f_\chi} B_{1,\bar{\chi}} = \frac{\pi^{r_2(F)}}{|d_F/d_{F^+}|^{1/2}} \frac{R_F/R_F^+}{w_F/w_{F^+}} h_F^-. \tag{4.2.3}$$

Applying (4.2.1) and (4.2.2) for $E = F$ and $E = F^+$, we see that

$$\prod_{\substack{\chi \in X(F) \\ \chi \text{ odd}}} \frac{\pi i \tau(\chi)}{f_\chi} = \frac{(-\pi)^{r_2(F)}}{|d_F/d_{F^+}|^{1/2}},$$

and Lemma 4.2.19 tells us that

$$\frac{R_F/R_F^+}{w_F/w_{F^+}} = 2^{r_2(F)-1}[E_F : E_F^+],$$

since $w_{F^+} = 2$. Equation (4.2.3) is then immediately reduced to the desired form.

On the other hand, the analytic class number formula for F^+ and Theorem 4.2.14,

$$\prod_{\substack{\chi\in X(F)\\ \chi\neq 1 \text{ even}}}\left(\frac{-\tau(\chi)}{f_\chi}\sum_{a=1}^{f_\chi}\bar{\chi}(a)\log|1-e^{2\pi ia/f_\chi}|\right)=\frac{2^{r_1(F^+)}h_F^+R_F^+}{2|d_{F^+}|^{1/2}},$$

Applying (4.2.1) and (4.2.2) and noting that replacing $\bar{\chi}(a)$ by $\chi(a)$ in the resulting sum makes no difference in the result, we obtain the formula for h_F^+. □

4.3. Cyclotomic units

The product appearing in the formula for h_F^+ in Theorem 4.2.20 may appear itself something like a regulator. This is essentially the case.

DEFINITION 4.3.1. If F is an abelian field contained in $\mathbb{Q}(\mu_m)$ for $m\geq 1$, we let $S=V_{m\infty}$ and define the group of *cyclotomic S-units* $C_{F,S}$ of F to be the subgroup

$$C_{F,S}=\langle 1-\zeta_m^a \mid 1\leq a<m\rangle\cap F^\times$$

of $\mathscr{O}_{F,S}^\times$, where ζ_m is a primitive mth root of unity. The group of *cyclotomic units* of F is then defined as the intersection $C_F=E_F\cap C_{F,S}$.

REMARK 4.3.2. The definition of C_F is independent of the multiple m of the conductor of F^+.

We have the following result of Hasse, which is due to Kummer in the case of $\mathbb{Q}(\mu_p)$ for a prime p. We will prove a generalization of this result to arbitrary cyclotomic fields in Theorem 4.7.1.

THEOREM 4.3.3 (Hasse). *Let $F=\mathbb{Q}(\mu_{p^n})$ for an odd prime p and $n\geq 1$. Then we have*

$$h_F^+=[E_F^+:C_F^+].$$

PROOF. The set

$$\left\{\xi_a=\frac{\zeta_{p^n}^{a/2}-\zeta_{p^n}^{-a/2}}{\zeta_{p^n}^{1/2}-\zeta_{p^n}^{-1/2}}\,\middle|\,1<a<p^n/2,\,(a,p)=1\right\}$$

forms an independent set of generators of C_F^+. Let us let R_{cyc} denote the regulator of the latter set. Then R_{cyc} is the absolute value of the determinant of the matrix with rows and columns indexed by the integers a prime to p with $1<a<p^n/2$ with entries in the row and column corresponding to (a,b) given by $\log|\sigma_a(\xi_b)|$, where $\sigma_a(\zeta_{p^n})=\zeta_{p^n}^a$. Now

$$\log|\sigma_a(\xi_b)|=\log|1-\zeta_{p^n}^{ab}|-\log|1-\zeta_{p^n}^a|.$$

Proposition 1.5.18 applied to the group $\mathrm{Gal}(F^+/\mathbb{Q})$ yields

$$R_{\mathrm{cyc}} = \left| \prod_{\substack{\chi \in X(F^+) \\ \chi \neq 1}} \left(\sum_{\substack{b=1 \\ (b,p)=1}}^{p^n/2-1} \chi(b) \log|1-\zeta_{p^n}^b| \right) \right| = \left| \prod_{\substack{\chi \in X(F^+) \\ \chi \neq 1}} \frac{1}{2} \sum_{\substack{c=1 \\ (c,p)=1}}^{p^n-1} \chi(c) \log|1-\zeta_{p^n}^c| \right|.$$

As χ has conductor dividing p^n and

$$1-\zeta_n^c = \prod_{j=0}^{k-1} (1-\zeta_{nk}^{c+jk})$$

for $n,k \geq 1$ and $c \not\equiv 0 \bmod n$, we have

$$\sum_{\substack{c=1 \\ (c,p)=1}}^{p^n-1} \chi(c) \log|1-\zeta_{p^n}^c| = \sum_{\substack{c=1 \\ (c,p)=1}}^{f_\chi-1} \chi(c) \log|1-\zeta_{f_\chi}^c|,$$

the middle step by Theorem 4.2.14. By Theorem 4.2.20, it then follows that $R_{\mathrm{cyc}} = h_F^+ R_F^+$. On the other hand, we have $R_{\mathrm{cyc}} = R_F^+ [E_F^+ : C_F^+]$ by Lemma 1.2.10. □

A standard choice of primitive mth roots of unity for $m \geq 1$, viewing $\overline{\mathbb{Q}}$ as a subset of $\mathbb{C}$, is to take $\zeta_m = e^{2\pi i/m}$ for $m \geq 1$. This choice has the advantage that $\zeta_n^{n/m} = \zeta_m$ for m dividing n. Let us make such a choice. We first remark that the elements $1-\zeta_m$ for m divisible by two distinct primes are in fact units.

LEMMA 4.3.4. *If m is divisible by two distinct primes, then $1-\zeta_m \in C_{\mathbb{Q}(\mu_m)}$.*

PROOF. For a positive integer d, let Φ_d denote the dth cyclotomic polynomial. We have

$$\Phi_m(1) = \prod_{\substack{i=1 \\ (i,m)=1}}^{m} (1-\zeta_m^i),$$

so it suffices to show that $\Phi_m(1) = \pm 1$. We have

$$\frac{x^m-1}{x-1} = \prod_{\substack{d|m \\ d>1}} \Phi_d(x).$$

Plugging in $x=1$, we obtain

$$m = \prod_{\substack{d|m \\ d>1}} \Phi_d(1).$$

Note $\Phi_{p^k}(1) = p^k$ for any power p^k of a prime p. Expressing $m = \prod_{i=1}^g p_i^{k_i}$ as a product of powers of distinct primes p_i, we then also have

$$m = \prod_{i=1}^{g} \Phi_{p_i^{k_i}}(1).$$

Since each $\Phi_d(1)$ is an integer, it follows that $\Phi_m(1) = \pm 1$, as desired. □

Next, we note the following the compatibility of the elements $1-\zeta_m$ under norms.

LEMMA 4.3.5. *For $m \geq 1$ and a prime ℓ, we have*

$$N_{\mathbb{Q}(\mu_{m\ell})/\mathbb{Q}(\mu_m)}(1-\zeta_{m\ell}) = \begin{cases} 1-\zeta_m & \text{if } \ell \mid m, \\ -\zeta_m^{\ell-1}\dfrac{1-\zeta_m}{1-\zeta_m^{\ell-1}} & \text{if } \ell \nmid m. \end{cases}$$

PROOF. Note that

$$\prod_{i=1}^{\ell}(1-\zeta_{m\ell}\zeta_\ell^i) = 1-\zeta_m.$$

If ℓ divides m, then the left-hand side runs over the conjugates of $1-\zeta_{m\ell}$ under $\mathrm{Gal}(\mathbb{Q}(\mu_{m\ell})/\mathbb{Q}(\mu_m))$, so the product equals the norm.

If ℓ does not divide m, then let $a,b \in \mathbb{Z}$ with $a\ell + bm = 1$. We then have $\zeta_m^a\zeta_\ell^b = \zeta_{m\ell}$, so the conjugates of $\zeta_{m\ell}$ have the form $\zeta_{m\ell}\zeta_\ell^i$ with $i \not\equiv -b \bmod \ell$. Note that $b \equiv m^{-1} \bmod \ell$, so moving this term from the product to the other side, we have

$$N_{\mathbb{Q}(\mu_m\ell)/\mathbb{Q}(\mu_m)}(1-\zeta_{m\ell}) = \frac{1-\zeta_m}{1-\zeta_m^{-\ell-1}} = -\zeta_m^{\ell-1}\frac{1-\zeta_m}{1-\zeta_m^{\ell-1}}.$$

□

4.4. Reflection theorems

We now refine Theorem 1.4.15 by working with eigenspaces. Start with a totally real field F. Let

$$\chi\colon G_F \to \overline{\mathbb{Q}}^\times$$

be a character with finite image. Any embedding φ of $\overline{F}$ in $\mathbb{C}$ fixes an element $c_\varphi \in G_F$ that is the restriction of complex conjugation in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, since F is taken to a subfield of $\mathbb{R}$ under the embedding. All such complex conjugations in G_F arise in this way, and they form $[F:\mathbb{Q}]$ distinct conjugacy classes in $G_\mathbb{Q}$ for the real embeddings of F in $\overline{F} = \overline{\mathbb{Q}}$. In G_F^{ab}, these complex conjugations restrict to exactly $[F:\mathbb{Q}]$ distinct elements, with the elements of the same class restricting to the same element.

DEFINITION 4.4.1. We say that a character $\chi\colon G_F \to \overline{\mathbb{Q}}^\times$ of a totally real field F is *totally even* if χ is trivial on all complex conjugations and *totally odd* if χ is nontrivial on all complex conjugations. If $F = \mathbb{Q}$, we say more simply that χ is *even* or *odd* in the respective cases.

We let F_χ denote the extension of F that is the fixed field of the kernel of χ, which will itself be totally real if χ is totally even and CM if χ is totally odd. If $F = \mathbb{Q}$, these are the only cases.

We now suppose that χ has order prime to a given odd prime p. We fix an embedding $\iota_p\colon \overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$, which allows us to view χ as a character with values in $\overline{\mathbb{Q}_p}^\times$, and hence in $\overline{\mathbb{Z}_p}^\times$.

One key character of interest to us is the Teichmüller character

$$\omega\colon G_F \to \mathbb{Q}_p^\times$$

which has image contained in $\mu_{p-1}(\mathbb{Z}_p)$ and is defined by the equality

$$\sigma(\zeta) = \zeta^{\omega(\sigma)}$$

for any $\sigma \in G_F$ and $\zeta \in \mu_p$. Note that the Teichmüller character is an odd character on G_F.

THEOREM 4.4.2 (Leopoldt's Spiegelungsatz). *Let F be a totally real field, and let $\chi\colon G_F \to \overline{\mathbb{Q}_p}^\times$ be a totally odd character of finite order prime to p. Let E be an abelian extension of F of degree prime to p that contains $F_\chi(\mu_p)$. Then we have*

$$r_p(A_E^{(\omega\chi^{-1})}) - \delta_\chi \leq r_p(A_E^{(\chi)}) \leq r_p(A_E^{(\omega\chi^{-1})}) + r_p((\mathscr{O}_E^\times/\mathscr{O}_E^{\times p})^{(\omega\chi^{-1})}),$$

where δ_χ is 0 unless $\chi = \omega$ and the extension $E(\mu(F)^{1/p})/E$ is unramified, in which case it is 1.

PROOF. Let $\Delta = \mathrm{Gal}(E/F)$. Let $\mathscr{O}$ be the ring generated over $\mathbb{Z}_p$ by the character values of Δ. Let k denote the residue field of $\mathscr{O}$, and let k_ψ denote the residue field of $\mathscr{O}_\psi$, the ring of values of ψ, for any $\psi \in \Delta^*$. As $\mathscr{O}$ is unramified over $\mathbb{Z}_p$, we have $[\mathscr{O} : \mathscr{O}_\psi] = [k : k_\psi]$.

For a $\mathbb{Z}_p[\Delta]$-module B, we let $B_\mathscr{O} = B \otimes_{\mathbb{Z}_p} \mathscr{O}$. We remark that Lemma 2.8.7 implies that

$$r_p(B_\mathscr{O}^\psi) = [k : k_\psi] r_p(B^{(\psi)}).$$

Note also that we have

$$r_p(B_\mathscr{O}^\psi) = [k : \mathbb{F}_p] \dim_k((B/pB)_\mathscr{O}^\psi),$$

so

$$r_p(B^{(\psi)}) = [k_\psi : \mathbb{F}_p]^{-1} \dim_k((B/pB)_\mathscr{O}^\psi). \tag{4.4.1}$$

Since $\mathscr{O}_\chi = \mathscr{O}_{\omega\chi^{-1}}$ and since $\delta_\chi = 0$ unless $\chi = \omega$, in which case $k_\chi = \mathbb{F}_p$, equation (4.4.1) tells us that the desired inequalities are equivalent to

$$\dim_k(A_\mathscr{O}^{\omega\chi^{-1}}) - \delta_\chi \leq \dim_k(A_\mathscr{O}^\chi) \leq \dim_k(A_\mathscr{O}^{\omega\chi^{-1}}) + \dim_k((\mathscr{O}_E^\times/\mathscr{O}_E^{\times p})_\mathscr{O}^{\omega\chi^{-1}}),$$

where we have set $A = A_E/pA_E$ to shorten notation.

Note that we have the following isomorphisms of groups

$$\mathrm{Hom}_{\mathbb{Z}_p}(A_E, \mu_p)_\mathscr{O} \cong \mathrm{Hom}_{\mathbb{Z}_p}(A_E, (\mu_p)_\mathscr{O}) \cong \mathrm{Hom}_\mathscr{O}((A_E)_\mathscr{O}, (\mu_p)_\mathscr{O})$$

the first step following from the freeness of $\mathscr{O}$ over $\mathbb{Z}_p$ and the second from the adjointness of Hom and $\otimes$. Moreover, Lemma 2.8.7 implies that

$$\mathrm{Hom}_\mathscr{O}((A_E)_\mathscr{O}, (\mu_p)_\mathscr{O})^\psi \cong \mathrm{Hom}_\mathscr{O}((A_E)_\mathscr{O}^{\omega\psi^{-1}}, (\mu_p)_\mathscr{O})$$

for any $\psi \in \Delta^*$. Recalling Lemma 1.4.6, we then have an exact sequence

$$0 \to ((B \cap \mathscr{O}_E^\times)/\mathscr{O}_E^{\times p})_{\mathscr{O}}^{\psi} \to \mathrm{Hom}_{\mathscr{O}}((A_E)_{\mathscr{O}}^{\omega\psi^{-1}}, (\mu_p)_{\mathscr{O}}) \to (A_E)_{\mathscr{O}}^{\psi}[p],$$

where B is the set of elements of $E^\times$ that have pth roots that generate unramified extensions of E. Since $(\mu_p)_{\mathscr{O}}$ is a one-dimensional k-vector space, we have

$$\mathrm{Hom}_{\mathscr{O}}((A_E)_{\mathscr{O}}^{\omega\psi^{-1}}, (\mu_p)_{\mathscr{O}}) \cong \mathrm{Hom}_k(A_{\mathscr{O}}^{\omega\psi^{-1}}, k),$$

which as the k-dual of a k-vector space has dimension equal to $\dim_k(A_{\mathscr{O}}^{\omega\psi^{-1}})$.

In the case that $\psi = \chi$, we then have that

$$\dim_k(A_{\mathscr{O}}^{\omega\chi^{-1}}) \leq \dim_k(((B \cap \mu(E))/\mu(E)^p)_{\mathscr{O}}^{\chi}) + \dim_k(A_{\mathscr{O}}^{(\chi)}) = \delta_\chi + \dim_k(A_E^{(\chi)}),$$

since the p-power roots of unity in E have trivial χ-eigenspace unless $[\chi] = [\omega]$, which happens if and only if $\chi = \omega$, as ω takes its values in $\mathbb{Z}_p$. On the other hand, if we take $\psi = \omega\chi^{-1}$, then we have

$$\dim_k(A_{\mathscr{O}}^{\chi}) \leq \dim_k((\mathscr{O}_E^\times/\mathscr{O}_E^{\times p})_{\mathscr{O}}^{\omega\chi^{-1}}) + \dim_k(A_{\mathscr{O}}^{\omega\chi^{-1}}),$$

finishing the proof. □

In the special case that $F = \mathbb{Q}$ and $E = \mathbb{Q}(\mu_p)$, we remark that $\delta_\omega = 0$, as $\mathbb{Q}(\mu_{p^2})/F$ is ramified at the unique prime over p. Moreover, we have the following.

LEMMA 4.4.3. *Let k be an even integer. Then*

$$(\mathscr{O}_{\mathbb{Q}(\mu_p)}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{(\omega^k)} \cong \begin{cases} \mathbb{Z}_p & k \not\equiv 0 \bmod (p-1) \\ 0 & k \equiv 0 \bmod (p-1) \end{cases}.$$

COROLLARY 4.4.4. *For any even integer k, we have*

$$r_p(A_{\mathbb{Q}(\mu_p)}^{(\omega^k)}) \leq r_p(A_{\mathbb{Q}(\mu_p)}^{(\omega^{1-k})}) \leq r_p(A_{\mathbb{Q}(\mu_p)}^{(\omega^k)}) + 1.$$

COROLLARY 4.4.5. *We have $A_{\mathbb{Q}(\mu_p)}^{(\omega)} = A_{\mathbb{Q}(\mu_p)}^{(1)} = 0$.*

PROOF. We know that

$$A_{\mathbb{Q}(\mu_p)}^{(1)} = A_{\mathbb{Q}(\mu_p)}^{\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})} \cong A_{\mathbb{Q}} = 0.$$

As Theorem 4.4.2 and Lemma 4.4.3 tell us that $r_p(A_{\mathbb{Q}(\mu_p)}^{(1)}) = r_p(A_{\mathbb{Q}(\mu_p)}^{(\omega)})$, so we are done. □

4.5. Stickelberger theory

Let us fix an integer $m \geq 1$ and a primitive mth root of unity ζ_m throughout this section.

DEFINITION 4.5.1. Let $F = \mathbb{Q}(\mu_m)$, and let $G = \mathrm{Gal}(F/\mathbb{Q})$.

a. For $a \in \mathbb{Z}$ with $(a,m) = 1$, let $\sigma_a \in G$ be such that $\sigma_a(\zeta_m) = \zeta_m^a$. The *Stickelberger element* θ_F is the element of $\mathbb{Q}[G]$ given by

$$\theta_F = \frac{1}{m} \sum_{\substack{a=1 \\ (a,m)=1}}^{m} a\sigma_a^{-1}.$$

b. The *Stickelberger ideal* of F is the ideal $\mathscr{I}_F = \mathbb{Z}[G]\theta_F \cap \mathbb{Z}[G]$ of $\mathbb{Z}[G]$.

LEMMA 4.5.2. *Let J denote the ideal of $\mathbb{Z}[G]$ generated by elements of the form $\sigma_b - b$ for $b \in \mathbb{Z}$ with $(b,m) = 1$. Then $J = \{x \in \mathbb{Z}[G] \mid x\theta_F \in \mathbb{Z}[G]\}$.*

PROOF. Let us use $\langle \alpha \rangle$ to denote the fractional part of $\alpha \in \mathbb{Q}$. We note

$$\sigma_b\theta_F = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \frac{a}{m}\sigma_b\sigma_a^{-1} = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \left\langle \frac{ab}{m} \right\rangle \sigma_a^{-1}.$$

Since $\langle \frac{ab}{m} \rangle - \langle \frac{a}{m} \rangle b \in \mathbb{Z}$, we have $(\sigma_b - b)\theta_F \in \mathscr{I}_F$ for all $b \in \mathbb{Z}$ prime to m, and hence $J\theta_F \subseteq \mathbb{Z}[G]$.

Now take $x = \sum_b e_b\sigma_b$ with $x\theta_F \in \mathbb{Z}[G]$. Writing this out, we have

$$\sum_{\substack{a=1 \\ (a,m)=1}}^{m} \left(\sum_{\substack{b=1 \\ (b,m)=1}}^{m} e_b \left\langle \frac{ab}{m} \right\rangle \right) \sigma_a^{-1} \in \mathbb{Z}[G],$$

which implies that

$$\sum_{\substack{b=1 \\ (b,m)=1}}^{m} e_b b \in m\mathbb{Z}.$$

But note that $m = (m+1) - \sigma_1 \in J$, so $m\mathbb{Z} \subset J$. We then have

$$x = \sum_{\substack{b=1 \\ (b,m)=1}}^{m} e_b(\sigma_b - b) + \sum_{\substack{b=1 \\ (b,m)=1}}^{m} e_b b \in J,$$

finishing the proof. □

DEFINITION 4.5.3. Let q be a power of a prime ℓ and $\chi\colon \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a character, which we extend to a function $\chi\colon \mathbb{F}_q \to \mathbb{C}$ by $\chi(0) = 0$. The *Gauss sum* attached to χ is

$$g(\chi) = -\sum_{\alpha \in \mathbb{F}_q^\times} \chi(\alpha) e^{2\pi i \mathrm{Tr}(\alpha)/\ell}$$

where $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_\ell}$ is the trace map.

LEMMA 4.5.4. *Let q be a power of a prime ℓ prime to m. Let $\chi\colon \mathbb{F}_q^\times \to \mu_m$ be a character, so $g(\chi) \in \mathbb{Q}(\mu_{\ell m})$. Let $b \in \mathbb{Z}$ be relatively prime to m, and let $\sigma_b \in \mathrm{Gal}(\mathbb{Q}(\mu_{\ell m})/\mathbb{Q}(\mu_\ell))$ be the unique lift of $\sigma_b \in G$. Then*

$$g(\chi)^{\sigma_b - b} \in \mathbb{Q}(\mu_m).$$

In particular, we have $g(\chi)^m \in \mathbb{Q}(\mu_m)$.

PROOF. For $\tau \in \mathrm{Gal}(\mathbb{Q}(\mu_{\ell m})/\mathbb{Q}(\mu_m))$ with $\tau(\zeta_\ell) = \zeta_\ell^c$, we have

$$g(\chi)^\tau = -\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) e^{2\pi i \mathrm{Tr}(c\alpha)/\ell} = \chi(c)^{-1} g(\chi).$$

On the other hand, we have $g(\chi)^{\sigma_b} = g(\chi^b)$ as σ_b fixes μ_ℓ, so we see that

$$(g(\chi)^{\sigma_b - b})^\tau = g(\chi^b)^\tau g(\chi)^{-b\tau} = \chi^b(c)^{-1}\chi(c)^{-b} g(\chi)^{\sigma_b - b} = g(\chi)^{\sigma_b - b},$$

as desired. □

LEMMA 4.5.5. *Let q be a power of a prime ℓ and $\chi\colon \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a character. Then*

$$g(\chi) g(\bar{\chi}) = \chi(-1)\ell.$$

We state Stickelberger's theorem for $F = \mathbb{Q}(\mu_m)$. A similar result holds for abelian fields in general.

THEOREM 4.5.6 (Stickelberger). *Let $F = \mathbb{Q}(\mu_m)$, set $G = \mathrm{Gal}(F/\mathbb{Q})$. Then the Stickelberger ideal of F annihilates the class group: $\mathscr{I}_F \cdot \mathrm{Cl}_F = 0$.*

PROOF. Fix $C \in \mathrm{Cl}_F$, and let $\mathfrak{l}$ be a prime ideal representing C in $\mathscr{O}_F$ that lies above a completely split prime ℓ of $\mathbb{Q}$. Note that $\ell \equiv 1 \bmod m$, and let $c \in \mathbb{Z}$ be a primitive root modulo ℓ. Let $\chi\colon \mathbb{F}_\ell^\times \to \mathbb{C}^\times$ denote the character with $\chi(c) = e^{2\pi i/m}$. There is unique prime $\mathfrak{L}$ of $\mathbb{Q}(\mu_{\ell m})$ lying above $\mathfrak{l}$, and $\mathfrak{L}^{\ell-1} = \mathfrak{l} \cdot \mathbb{Z}[\mu_{\ell m}]$. We use $v_{\mathfrak{L}}$ to denote the additive valuation attached to $\mathfrak{L}$. For $b \in \mathbb{Z}$ prime to m, and $\sigma_b \in \mathrm{Gal}(\mathbb{Q}(\mu_{\ell m})/\mathbb{Q}(\mu_\ell))$ the unique lift of $\sigma_b \in \mathrm{Gal}(F/\mathbb{Q})$, we set

$$t_b = v_{\sigma_b^{-1}\mathfrak{L}}(g(\chi)).$$

By Lemma 4.5.5, we have that $g(\chi) \mid (\ell)$, so $t_b \leq \ell - 1$, and by Lemma 4.5.4, we have in the smaller field F that

$$v_{\sigma_b^{-1}\mathfrak{l}}(g(\chi)^{\ell-1}) = t_b.$$

In other words, we have the factorization

$$g(\chi)^{\ell-1}\mathscr{O}_F = \prod_{\substack{b=1 \\ (b,m)=1}}^{m} (\sigma_b^{-1}\mathfrak{l})^{t_b},$$

so

$$\sum_{\substack{b=1\\(b,m)=1}}^{m} t_b \sigma_b^{-1}$$

annihilates the class of $\mathfrak{l}$.

Now take $\tau \in \mathrm{Gal}(F(\mu_\ell)/F)$ given by $\tau(\zeta_\ell) = \zeta_\ell^c$. Then since every prime over ℓ is totally ramified $F(\mu_\ell)/F$, we have that τ is in the inertia group of all such primes. Note that

$$v_{\sigma_b^{-1}\mathfrak{L}}(\zeta_\ell - 1) = 1$$

for all b. We calculate

$$\frac{g(\chi)}{(\zeta_\ell - 1)^{t_b}} \equiv \frac{g(\chi)^\tau}{(\zeta_\ell^c - 1)^{t_b}} \equiv \frac{\chi(c)^{-1} g(\chi)}{c^{t_b}(\zeta_\ell - 1)^{t_b}} \bmod \sigma_b^{-1}\mathfrak{L}.$$

This forces $e^{2\pi i/m} \equiv c^{-t_b} \bmod \sigma_b^{-1}\mathfrak{L}$ and therefore modulo $\sigma_b^{-1}\mathfrak{l}$, since both sides of the latter congruence lie in F. In other words, we have

$$e^{2\pi i b/m} \equiv c^{-t_b} \bmod \mathfrak{l}.$$

On the other hand, there exists some a prime to m such that

$$e^{2\pi i/m} \equiv c^{-(\ell-1)a/m} \bmod \mathfrak{l}.$$

We therefore have that

$$t_b \equiv \frac{(\ell-1)ab}{m} \bmod (\ell - 1),$$

forcing

$$t_b = (\ell - 1)\left\langle \frac{ab}{m} \right\rangle.$$

It follows that

$$(\ell - 1) \sum_{\substack{b=1\\(n,m)=1}}^{m} \left\langle \frac{ab}{m} \right\rangle \sigma_b^{-1} = (\ell - 1)\sigma_a \theta_F$$

annihilates C.

Now suppose $x \in \mathbb{Z}[G]$ is such that $x\theta_F \in \mathscr{I}_F$. We then have

$$(g(\chi)^{\sigma_a^{-1}x})^{\ell-1}\mathscr{O}_F = \mathfrak{l}^{(\ell-1)x\theta_F}.$$

By Lemmas 4.5.2 and 4.5.4, we have $g(\chi)^{\sigma_a^{-1}x} \in F$. Therefore, the identity

$$(g(\chi)^{\sigma_a^{-1}x})\mathscr{O}_F = \mathfrak{l}^{x\theta_F}$$

actually holds, and so we see that $x\theta_F$ annihilates C. So, $\mathscr{I}_F$ annihilates C, and we are done. □

This has an interesting application for the field $\mathbb{Q}(\mu_p)$.

THEOREM 4.5.7 (Herbrand). *Let p be an odd prime, and set $F = \mathbb{Q}(\mu_p)$. Let $j \not\equiv 1 \bmod p-1$ be an odd integer, and suppose that $A_F^{(\omega^j)} \neq 0$. Then $B_{1,\omega^{-j}} \in p\mathbb{Z}_p$. Moreover, we have $A_F^{(\omega)} = 0$.*

PROOF. By Stickelberger's theorem, we have that $\mathscr{I}_F \cdot A_F = 0$. In particular, we have that $\mathscr{I}_j = e_{\omega^j}\mathscr{I}_F$ annihilates $A_F^{(\omega^j)}$, where $e_{\omega^j} \in \mathbb{Z}_p[G]$ is the idempotent attached to ω^j. Note that for, b prime to p, we have

$$e_{\omega^j}(\sigma_b - b)\theta_F = (\omega^j(b) - b)\frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-j}(a)e_{\omega^j} = (\omega^j(b) - b)B_{1,\omega^{-j}}e_{\omega^j},$$

where we have applied Corollary 4.2.11 in the last step. It follows that $(\omega^j(b) - b)B_{1,\omega^{-j}}$ annihilates $A_F^{(\omega^j)}$ for all b prime to p. Choosing b to be a primitive root of 1, we have that $\omega^j(b) \not\equiv b \bmod p$, so if $A_F^{(\omega^j)}$ is nontrivial, then $B_{1,\omega^{-j}}$ must be divisible by p. For $j = 1$, we note that

$$(\omega^j(1+p) - (1+p))B_{1,\omega^{-1}} = -pB_{1,\omega^{-1}} = -\sum_{i=1}^{p} \omega(a)^{-1}a \equiv 1 \bmod p,$$

so we get that 1 annihliates $A_F^{(\omega)}$, hence the result. □

As with the plus part, the minus part of the class number of a cyclotomic field of prime power roots of unit can be interpreted as an index, as in the following result of Iwasawa. The proof is deferred to its generalization to arbitrary cyclotomic fields in Theorem 4.7.1.

THEOREM 4.5.8 (Iwasawa). *Let $F = \mathbb{Q}(\mu_{p^n})$ for a prime p and $n \geq 1$. Then*

$$h_F^- = [\mathbb{Z}[G]^- : \mathscr{I}_F^-].$$

4.6. Distributions

DEFINITION 4.6.1. Let $\{X_i \mid i \in I\}$ be a collection of finite sets, were I is a directed set under $\leq$, and let $\pi_{ij} \colon X_i \to X_j$ for $i \geq j$ be a collection surjective maps. Let A be an abelian group. An A-valued distribution on the collection (X_i, π_{ij}) is a set of maps $\psi_i \colon X_i \to A$ for $i \in I$ that satisfy the distribution relation

$$\psi_j(x) = \sum_{y \in \pi_{ij}^{-1}(x)} \psi_i(y)$$

for all $j \leq i$ and $x \in X_i$.

REMARK 4.6.2. Given a collection (X_i, π_{ij}) as above, we may consider the inverse limit

$$X = \varprojlim_{i \in I} X_i.$$

Let $\pi_i\colon X \to X_i$ be the map induced by the system. Let $\mathrm{Step}(X,A)$ denote the set of A-valued step functions on X. Supposing now that A is a ring, a distribution $\{\psi_i\colon X_i \to A \mid i \in I\}$ on the collection (X_i, π_{ij}) (or more simply, on X) gives rise to an A-module homomorphism

$$\tilde{\psi}\colon \mathrm{Step}(X,A) \to A$$

as follows. If χ_Y denotes the characteristic function of a compact-open subset Y of X, then we let

$$\tilde{\psi}(\chi_{\pi_i^{-1}(x)}) = \psi_i(x)$$

for any $i \in I$ and $x \in X_i$. We take $\tilde{\psi}$ as the A-linear extension of this map to the group of all step functions. The distribution relation insures that it is well-defined. Conversely, given an A-module homomorphism $\tilde{\psi}\colon \mathrm{Step}(X,A) \to A$, we may define $\psi_i(x)$ to be $\tilde{\psi}(\chi_{\pi_i^{-1}}(x))$, and the ψ_i provide a distribution on X.

EXAMPLE 4.6.3. Let I be the set of positive integers, ordered in the usual manner. Let $X_i = \mathbb{Z}/p^i\mathbb{Z}$, and let π_{ij} for $j \leq i$ be the reduction modulo p^j map. Let $a \in \mathbb{Z}_p$. Define

$$\psi_i(x) = \begin{cases} 1 & \text{if } x \equiv a \bmod p^i, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\{\psi_i \mid i \geq 0\}$ is an R-valued distribution for any ring R, called the δ-distribution at a. The corresponding functional δ_a satisfies $\delta_a(f) = f(a)$, where $f \in \mathrm{Step}(\mathbb{Z}_p, R)$ is any congruence function.

Let us focus on a specific case of interest.

DEFINITION 4.6.4. Let A be an abelian group, and let D be a divisible abelian group with finitely topologically generated Pontryagin dual.

a. By an A-valued *distribution* on D, we mean a function $\psi\colon D \to A$ with the property that

$$\psi(d) = \sum_{\substack{c \in D \\ nc = d}} \psi(c) \tag{4.6.1}$$

for all positive integers n and $d \in D$.

b. By an A-valued *punctured distribution* on D, we mean a function $\psi\colon D - \{0\} \to A$ satisfying the distribution relation (4.6.1) for all positive integers n and $d \in D - \{0\}$.

REMARK 4.6.5. For an abelian group A and a torsion divisible abelian group D, the A-valued distributions on D are in one-to-one correspondence with the A-valued distributions $\{\psi_n \mid n \geq 1\}$ on the collection of n-torsion subgroups $D[n]$ in D for $n \geq 1$, together with the transition maps $\pi_{n,m}\colon D[n] \to D[m]$ for m dividing n given by multiplication by $\frac{n}{m}$. That is, ψ and the maps ψ_n take the same values on the

elements of $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. If A is a ring, then the maps ψ also give rise to a functional $\tilde{\psi}\colon \mathrm{Step}(\varprojlim_n D[n], A) \to A$, as noted above.

REMARK 4.6.6. Punctured distributions on D do not quite give rise to distributions on the sets $D[n] - \{0\}$, since multiplication by $\frac{n}{m}$ does not preserve these sets.

EXAMPLE 4.6.7. Let I be the set of positive integers, ordered by divisibility. Fix $k \geq 0$, and for $0 \leq a < n$ with $n \geq 1$, set

$$\psi_n^{(k)}\left(\frac{a}{n}\right) = n^{k-1}B_k\left(\frac{a}{n}\right).$$

For m dividing n, we have

$$\psi_n^{(k)}\left(\frac{a}{m}\right) = m^{k-1}B_k\left(\frac{a}{m}\right) = \sum_{j=0}^{n/m-1} n^{k-1}B_k\left(\frac{a+jm}{n}\right) = \sum_{\substack{b=0 \\ b\equiv a \bmod m}}^{n-1} \psi_n^{(k)}\left(\frac{b}{n}\right).$$

Thus, we can safely make the following definition.

DEFINITION 4.6.8. For $k \geq 0$, the kth *Bernoulli distribution* $\psi^{(k)}$ is the $\mathbb{Q}$-valued distribution on $\mathbb{Q}/\mathbb{Z}$ defined by

$$\psi^{(k)}\left(\frac{a}{n}\right) = n^{k-1}B_k\left(\left\langle\frac{a}{n}\right\rangle\right),$$

where $\langle\alpha\rangle$ denotes the smallest nonegative rational number representing $\alpha \in \mathbb{Q}/\mathbb{Z}$.

We also mention the following example of something close to a distribution.

EXAMPLE 4.6.9. Define $\psi\colon \mathbb{Q}/\mathbb{Z} - \{0\} \to \mathbb{Q}(\mu_\infty)^\times$ by $\psi(\frac{i}{n}) = 1 - \zeta_n^i$. If $m \mid n$ and $i \not\equiv 0 \bmod m$, we have

$$\psi\left(\frac{i}{m}\right) = 1 - \zeta_m^i = \prod_{k=0}^{n/m-1}(1 - \zeta_n^{i+km}) = \prod_{\substack{j=0 \\ j\equiv i \bmod m}}^{n-1} \psi\left(\frac{j}{n}\right),$$

so ψ satisfies the distribution relations under multiplication. Thus ψ is a punctured distribution on $\mathbb{Q}/\mathbb{Z}$.

We will be interested in the following resulting distribution.

NOTATION 4.6.10. Let ψ_{cyc} be the $\mathbb{R}$-valued punctured distribution on $\mathbb{Q}/\mathbb{Z}$ given by

$$\psi_{\mathrm{cyc}}(\alpha) = -\frac{1}{2}\log|1 - e^{2\pi i\langle\alpha\rangle}|$$

for $\alpha \in \mathbb{Q}/\mathbb{Z}$.

REMARK 4.6.11. Note that an A-valued (punctured) distribution ψ on $\mathbb{Q}/\mathbb{Z}$ gives rise to an A-valued map $\tilde{\psi}$ on (nontrivial) Dirichlet characters χ in that Dirichlet characters are step functions on $\hat{\mathbb{Z}}$ (that are zero at zero). In particular, if χ has modulus dividing m, then

$$\tilde{\psi}(\chi) = \sum_{a=0}^{m-1} \chi(a)\psi\left(\frac{a}{m}\right).$$

EXAMPLE 4.6.12. By Lemma 4.2.10, we have

$$\psi^{(n)}(\chi) = B_{n,\chi}$$

for a primitive Dirichlet character χ. In particular, $\psi^{(n)}(\chi) = 0$ if $n \not\equiv \chi(-1) \bmod 2$, unless $n = 1$ and $\chi = 1$. Similarly, $\psi_{\mathrm{cyc}}(\chi) = 0$ unless χ is even.

4.7. Sinnott's theorem

In this section, we fix $m > 1$ with $m \not\equiv 2 \bmod 4$. We set $F = \mathbb{Q}(\mu_m)$ and $G = \mathrm{Gal}(F/\mathbb{Q})$. The goal of this section is to prove the following generalization of the results of Hasse and Iwasawa for F, which is due to Sinnott.[1]

THEOREM 4.7.1 (Sinnott). *Let $F = \mathbb{Q}(\mu_m)$ for $m > 1$ with $m \not\equiv 2 \bmod 4$. Then we have*

$$[E_F^+ : C_F^+] = 2^a h_F^+ \quad \textit{and} \quad [\mathbb{Z}[G]^- : \mathscr{I}_F^-] = 2^b h_F^-,$$

where

$$a = \begin{cases} 0 & \text{if } g = 1 \\ 2^{g-2} + 1 - g & \text{if } g \geq 2 \end{cases} \quad \textit{and} \quad b = \begin{cases} 0 & \text{if } g = 1 \\ 2^{g-2} - 1 & \text{if } g \geq 2, \end{cases}$$

for g the number of primes dividing m.

NOTATION 4.7.2. For $\chi \in \hat{G}$, we have the idempotent

$$e_\chi = \frac{1}{\varphi(m)} \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \chi(a)\sigma_a^{-1} \in \mathbb{C}[G].$$

We also have idempotents

$$e^\pm = \frac{1 \pm \sigma_{-1}}{2} \in \mathbb{Q}[G].$$

The following is essentially immediate from the definitions.

LEMMA 4.7.3. *We have $e^\pm A = \frac{1}{2}\mathbb{Z}[G]^\pm$ inside $\mathbb{Q}[G]$. In particular, we see that*

$$[e^\pm \mathbb{Z}[G] : \mathbb{Z}[G]^\pm] = 2^{\varphi(m)/2}.$$

[1] This section is roughly written at present and might be safely skipped for now, aside from the statement of the theorem.

NOTATION 4.7.4. For any $\mathbb{Z}[G]$-module A, set $A_0 = \ker(N_G \colon A \to A)$.

REMARK 4.7.5. For a $\mathbb{Z}[G]$-module A, we note that $e^-(1-e_1)A = e^-A$.

NOTATION 4.7.6. For each prime p dividing m, set

$$\lambda_p = \sum_{\chi \in \hat{G}} (1 - \bar{\chi}(p)) e_\chi \in \mathbb{Q}[G].$$

For each positive integer f dividing m, set $G_f = \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}(\mu_f))$. Let U denote the $\mathbb{Z}[G]$-module generated by the elements

$$u_f = N_{G_f} \prod_{p|f} \lambda_p \in \mathbb{Q}[G]$$

for positive integers f dividing m, where the product is taken over primes dividing f.

We briefly sketch a proof of the following proposition.

PROPOSITION 4.7.7. *Let g be the number of primes dividing m. Then we have the following equalities:*

$$(e^{\pm}\mathbb{Z}[G] : e^{\pm}U) = \begin{cases} 1 & \text{if } g = 1 \\ 2^{2^{g-2}} & \text{if } g \geq 2. \end{cases}$$

PROOF. If $g = 1$, then U is generated by N_G and λ_p for the unique prime p dividing m. We have $u_1 = N_G = |G|e_1$ and $u_p = \lambda_p = 1 - e_1$. Then

$$[e_1\mathbb{Z}[G] + \mathbb{Z}[G] : U] = |G| = [e_1\mathbb{Z}[G] + \mathbb{Z}[G] : \mathbb{Z}[G]],$$

so $[\mathbb{Z}[G] : U] = 1$. Moreover, note that $e^-e_1 = 0$, and from this it is easily seen that $e^-\mathbb{Z}[G] = e^-U$, and as a result, $[e^+\mathbb{Z}[G] : e^+U] = 1$ as well.

For $g \geq 2$, we indicate only a few details of the proof. One uses the fact that U is the product over primes p dividing m of the modules U_p generated by N_{I_p} and λ_p, where $I_p < \mathrm{Gal}(F/\mathbb{Q})$ is the inertia group at p, to see that $(\mathbb{Z}[G] : U) = 1$. On the other hand,

$$(\mathbb{Z}[G] : U) = (e^+\mathbb{Z}[G] : e^+U)(\mathbb{Z}[G]^- : U^-).$$

One checks that the order of

$$\hat{H}^{-1}(\mathrm{Gal}(F/F^+), U) = U^-/(\sigma_{-1} - 1)U \cong e^-\mathbb{Z}[G]/e^-U$$

is $2^{2^{g-1}}$. We then have

$$(e^+\mathbb{Z}[G] : e^+U)(e^-\mathbb{Z}[G] : e^-U) = 2^{2^{g-1}},$$

and the proof is finished upon showing that $(e^-\mathbb{Z}[G] : e^-U) = 2^{2^{g-2}}$, which we omit. □

Recall that I_G denotes the augmentation ideal in $\mathbb{Z}[G]$.

COROLLARY 4.7.8. *Let g be the number of primes dividing m. Then*

$$(e^+I_G : e^+U_0) = \begin{cases} \varphi(m)^{-1} & \text{if } g = 1 \\ 2^{2^{g-2}}\varphi(m)^{-1} & \text{if } g \geq 2, \end{cases}$$

PROOF. The quotient $e^+\mathbb{Z}[G]/e^+I_G$ is isomorphic to $\mathbb{Z}$ via the augmentation map, while e^+U/e^+U_0 is generated by the class of $u_1 = N_G$, and the image of $N_G \in e^+\mathbb{Z}[G]$ under the augmentation map is $|G| = \varphi(M)$. It follows that

$$(e^\pm\mathbb{Z}[G] : e^\pm U) = \varphi(M)(e^+I_G : e^+U_0),$$

and we apply Proposition 4.7.7. □

NOTATION 4.7.9. For a punctured $\mathbb{C}$-valued distribution ψ on $\mathbb{Q}/\mathbb{Z}$, let T_ψ be the subgroup of $\mathbb{C}[G]$ generated by the elements

$$\eta_\psi(c) = \sum_{\substack{b=1 \\ (b,m)=1}}^{m} \psi\left(\frac{bc}{m}\right)\sigma_b^{-1}$$

for positive integers c with $c \not\equiv 0 \bmod m$.

REMARK 4.7.10. The group T_ψ is a $\mathbb{Z}[G]$-module, as $\sigma_a\eta_\psi(c) = \eta_\psi(ac)$ for a prime to m. As a $\mathbb{Z}[G]$-module, it is then generated by the elements $\eta_\psi(d)$ for d positive dividing m.

At times, we will view the elements of $\hat{G}$ also as primitive Dirichlet characters.

PROPOSITION 4.7.11. *Let ψ be a punctured $\mathbb{C}$-valued distribution on $\mathbb{Q}/\mathbb{Z}$. Then*

$$(1 - e_1)T_\psi = \omega_\psi U,$$

where

$$\omega_\psi = \sum_{\chi \in \hat{G} - \{1\}} \psi(\bar{\chi})e_\chi \in \mathbb{C}[G].$$

PROOF. For $d \geq 1$ dividing m, set $f = \frac{m}{d}$. Let χ be a nontrivial character of $\hat{G}$. Then $e_\chi\eta_\psi(d)$ vanishes if f does not divide the conductor f_χ of χ, and if $f \mid f_\chi$, then

$$e_\chi\eta_\psi(d) = e_\chi \sum_{\substack{b=1 \\ (b,m)=1}}^{m} \psi\left(\frac{b}{f}\right)\bar{\chi}(b) = e_\chi\frac{\varphi(m)}{\varphi(f)}\left(\prod_{p|f}(1 - \bar{\chi}(p))\right)\psi(\bar{\chi}).$$

Noting that $e_\chi\omega_\psi = e_\chi\psi(\bar{\chi})$, that $e_\chi\lambda_p = e_\chi(1 - \bar{\chi}(p))$, and that

$$e_\chi N_{G_f} = \begin{cases} e_\chi\frac{\varphi(m)}{\varphi(f)} & \text{if } f_\chi \mid f \\ 0 & \text{otherwise,} \end{cases}$$

we conclude that

$$e_\chi \eta_\psi(d) = e_\chi \omega_\psi u_f.$$

This holds for all $\chi \neq 1$, and we also ahve that $e_1\omega_\psi = 0$, so we obtain $(1-e_1)\eta_\psi(d) = \omega_\psi u_f$. In that this holds for all d, the result follows. □

LEMMA 4.7.12. *Let ψ be a punctured $\mathbb{C}$-valued distribution on $\mathbb{Q}/\mathbb{Z}$. In the notation of Proposition 4.7.11, if $\psi(\chi) = 0$ for all nontrivial $\chi \in \hat{G}$ with $\chi(-1) = \mp 1$, then*

$$(e^{\pm}U_0 : (1-e_1)T_\psi) = \left| \prod_{\substack{\chi \in \hat{G} - \{1\} \\ \chi(-1) = \pm 1}} \psi(\chi) \right|.$$

PROOF. By our condition on χ, the element ω_ψ of Proposition 4.7.11 is

$$\omega_\psi = \sum_{\substack{\chi \in \hat{G} - \{1\} \\ \chi(-1) = \pm 1}} \psi(\chi) e_\chi.$$

Then $\omega_\psi \in (1-e_1)e^{\pm}\mathbb{C}[G]$ by assumption on ψ, and Proposition 4.7.11 implies that

$$(1-e_1)T_\psi = \omega_\psi U = (1-e_1)e^{\pm}\omega_\psi U_0.$$

Note that $e_1\lambda_p = 0$ for any prime p dividing m, so $e_1 u_f = 0$ if f is a positive divisor of m other than 1. Since the u_f generate U as a $\mathbb{Z}[G]$-module and $u_1 = N_G$, we therefore have $U = U_0 + N_G\mathbb{Z}$. It follows that $(1-e_1)U = U_0$. Multiplication by ω_ψ determines an $\mathbb{C}$-linear endomorphism of $(1-e_1)e^{\pm}\mathbb{C}[G]$ that takes $e^{\pm}U_0$ onto $(1-e_1)T_\psi$. The idempotent e_χ for nontrivial $\chi \in \hat{G}$ with $\chi(-1) = \pm 1$ is an eigenvector of this endomorphism with eigenvalue $\psi(\chi)$. The determinant is of course the product of these eigenvalues. The result then follows by Lemma 1.2.9. □

REMARK 4.7.13. For any $\mathbb{Z}[G]$-module A that is free over $\mathbb{Z}$, we have $A_0 = A \cap (1-e_1)A$, since $e_1 A_0 = 0$ and the kernel of N_G is the image of e_1 on $A \otimes_{\mathbb{Z}} \mathbb{Q}$.

EXAMPLE 4.7.14. The $\mathbb{R}$-vector space V spanned by the elements of G has V_0 equal to the elements with coefficients summing to 0. For S the set of primes above m in F, we have $T = T_{\psi_{\mathrm{cyc}}} = \rho(C_{F,S})$ is contained in V, and note that $T_0 = \rho(C_F)$ by the product formula.

LEMMA 4.7.15. *For $\psi = \psi_{\mathrm{cyc}}$ and $T = T_{\psi_{\mathrm{cyc}}}$, we have*

$$[(1-e_1)T : T_0] = 2^{-g}\varphi(m).$$

PROOF. Note that

$$(1-e_1)T/T_0 \cong ((1-e_1)T + T)/T \cong (e_1 T + T)/T \cong e_1 T/T^G.$$

We have

$$e_1 T = \frac{1}{\varphi(m)} N_G \rho(C_{F,S}) = \frac{1}{\varphi(m)} \rho(C_{F,S}^{N_G}).$$

Note that $|(1-\zeta_f)^{N_G}| = 1$ if f is not a prime power, and $(1-\zeta_{p^k})^{N_G} = p^{\varphi(m)/\varphi(p^k)}$. It follows that

$$e_1 T = \frac{1}{2} \sum_{p|m} \frac{1}{\varphi(p^{k_p})} \log p \cdot N_G \mathbb{Z},$$

where $k_p \geq 1$ is the additive p-adic valuation of m.

Next, note that $\alpha \in C_{F,S}$ satisfies $j(\alpha) \in T^G$ if and only if $j(\alpha^{\sigma-1}) = 0$ for all $\sigma \in G$, which is equivalent to $\alpha^{\sigma-1} \in \mu(F)$, which is in turn equivalent to $\alpha^{1+\tau} \in \mathbb{Q}^\times$, with τ complex conjugation. Let

$$P = \{\alpha \in C_{F,S} \mid \alpha^{1+j} \in \mathbb{Q}^\times\},$$

and note that $T^G = \rho(P) = \frac{1}{2}\rho(P^{1+\tau})$. For an odd prime p dividing m, set

$$\alpha_p = \prod_{a=1}^{(p-1)/2} (1-\zeta_p^a),$$

and set $\alpha_2 = 1-\zeta_4$ if m is even. Then each α_p for p dividing m lies in P, so $P^{1+\tau}$ contains the group H generated by all primes dividing m. Since $P^{1+\tau}$ is a subgroup of the positive rationals, the quotient $P^{1+\tau}/H$ is torsion-free, and on the other hand $(P^{1+j})^{\varphi(m)} = (P^{1+j})^{N_G} \subseteq H$, which forces $P^{1+\tau} = H$. Thus

$$T^G = \frac{1}{4} \sum_{p|m} \log p \cdot N_G \mathbb{Z}.$$

It follows that

$$[(1-e_1)T : T_0] = [e_1 T : T^G] = \prod_{p|m} \frac{\varphi(p^k)}{2} = \frac{\varphi(m)}{2^g}.$$

□

LEMMA 4.7.16. *Let $\rho : E_{F,S} \to V^+$ denote the $\mathbb{Z}[G]$-module homomorphism*

$$\rho(\alpha) = -\frac{1}{2} \sum_{\sigma \in G} \log|\sigma(\alpha)|\sigma^{-1}.$$

Then

$$(e^+ I_G : \rho(E_F)) = \frac{R_F^+}{Q_F}.$$

PROOF. Let $X = (1-e_1)e^+V$, in which $\rho(E_F)$ forms a lattice of full rank $r = \frac{\varphi(m)}{2} - 1$. The lattice e^+I_G has a basis $e^+(1-\sigma_a^{-1})$ for $1 < a < \frac{m}{2}$ with $(a,m) = 1$. Fix a complex embedding of F, hence an absolute value. For an independent system of units $\alpha_1, \ldots, \alpha_r \in E_F^+$ generating E_F/μ_F, we have

$$\rho(\alpha_i) = -\sum_{\substack{a=1 \\ (a,m)=1}}^{\lceil \frac{m}{2} \rceil - 1} \log|\sigma_a(\alpha_i)|\sigma_a^{-1} = \sum_{\substack{a=2 \\ (a,m)=1}}^{\lceil \frac{m}{2} \rceil - 1} \log|\sigma_a(\alpha_i)|e^+(1-\sigma_a^{-1}).$$

Since the matrix with entries $\log|\eta_i^{\sigma_a}|$ has determinant $2^{-r}R_F$ by definition and $R_F = \frac{2^r}{Q_F}R_F^+$, we are done. □

LEMMA 4.7.17. *We have*

$$[e^-\mathbb{Z}[G]\theta_F : \mathscr{I}_F^-] = w_F.$$

.

PROOF. Let $\Theta_F = \mathbb{Z}[G]\theta_F$ for brevity. Since $(\sigma_a - a)\theta_F \in \mathscr{I}_F$ for all $a \in \mathbb{Z}$, we have that

$$\Theta_F = \mathscr{I}_F + \theta_F\mathbb{Z},$$

and therefore $\Theta_F/\mathscr{I}_F \cong \mathbb{Z}/m\mathbb{Z}$ as m is minimal with $m\theta_F$ integral. From the fact that $\langle\alpha\rangle + \rangle 1-\alpha\rangle = 1$ for $\alpha \notin \mathbb{Z}$, one see that $e^+\theta_F = \frac{1}{2}N_G\mathbb{Z}$. Since $(\sigma_2 - 2)\theta_F \in \mathscr{I}_F$ and $e^+(\sigma_2 - 2) = -\frac{1}{2}N_G$, we then have that $e^+\Theta_F = e^+\mathscr{I}_F$ and therefore $(\mathbb{Z}[G]\theta)_F^+ = \mathscr{I}_F^+$, which in turn implies that

$$\Theta_F^-/\mathscr{I}_F^- \cong \Theta_F/\mathscr{I}_F \cong \mathbb{Z}/m\mathbb{Z}.$$

If m is even, then $\sigma_{m/2}\theta_F = \frac{1}{2}N_G = e^+\theta_F$. Therefore, we have $e^+\Theta_F \subseteq \Theta_F$, and in turn this implies that $e^-\Theta_F \subseteq \Theta_F$. In other words, we have $[e^-\Theta_F : \Theta_F^-] = 1$.

If m is odd, then $e^-\sigma_a\theta_F = \sigma_a\theta_F - \frac{1}{2}N_G$, so

$$e^-\Theta_F + \Theta_F = \tfrac{1}{2}N_G\mathbb{Z} + \theta_F,$$

and therefore

$$e^-\Theta_F/\Theta_F^- \cong \tfrac{1}{2}N_G\mathbb{Z}/(\Theta_F \cap \tfrac{1}{2}N_G\mathbb{Z}).$$

Note that $N_G = (1+j)\theta_F \in \Theta_F$ but $\frac{1}{2}N_G \notin \Theta_F$ since $m\Theta_F \subset \mathbb{Z}[G]$ and m is odd. Therefore, we have $[e^-\Theta_F : \Theta_F^-] = 2$.

For arbitrary m, we conclude that

$$[e^-\mathbb{Z}[G]\theta_F : \mathscr{I}_F^-] = [e^-\Theta_F : \Theta_F^-][\Theta_F^- : \mathscr{I}_F^-] = \frac{w_F}{m} \cdot m = w_F.$$

□

We are now ready to prove Sinnott's theorem.

PROOF OF THEOREM 4.7.1. First consider $\psi = \psi_{\mathrm{cyc}}$, and set $T = T_\psi$. Since $T_0 = \rho(C_F)$, we may write our index as a product

$$[E_F^+ : C_F^+] = [\rho(E_F) : \rho(C_F)] = (\rho(E_F) : e^+ I_G)(e^+ I_G : e^+ U_0)(e^+ U_0 : (1-e_1)T)((1-e_1)T : T_0).$$

The latter four relative indices are computed by Lemma 4.7.16, Lemma 4.7.12, Corollary 4.7.8, and Lemma 4.7.15, respectively. Plugging in, we obtain

$$[E_F^+ : C_F^+] = \frac{Q_F}{R_F^+} \cdot \frac{(2^{2^{g-1}})^{1/2}}{\varphi(m)} \cdot \left| \prod_{\substack{\chi \in \hat{G} - \{1\} \\ \chi \text{ even}}} \psi_{\mathrm{cyc}}(\chi) \right| \cdot \frac{\varphi(m)}{2^g} = 2^a \frac{1}{R_F^+} \prod_{\substack{\chi \in \hat{G} - \{1\} \\ \chi \text{ even}}} \psi_{\mathrm{cyc}}(\chi) = 2^a h_F^+,$$

where the last equality follows from Theorem 4.2.20.

Next, consider $\psi = \psi^{(1)}$, the first Bernoulli distribution, which by definition has $T_{\psi^{(1)}} = e^- \mathbb{Z}[G]\theta_F$. We write the index in question as a product as follows:

$$[\mathbb{Z}[G]^- : \mathscr{I}_F^-] = (\mathbb{Z}[G]^- : e^- \mathbb{Z}[G])(e^- \mathbb{Z}[G] : e^- U)(e^- U : e^- \mathbb{Z}[G]\theta_F)(e^- \mathbb{Z}[G]\theta_F : \mathscr{I}_F^-).$$

The latter four relative indices are computed by Lemmas 4.7.3, Proposition 4.7.7, 4.7.12, and 4.7.17, respectively. Noting also that $2^b Q_F = 2^{2^{g-2}}$ if $g \geq 2$ and $2^b Q_F = 1$ if $g = 1$, we obtain

$$[\mathbb{Z}[G]^- : \mathscr{I}_F^-] = 2^{-\varphi(m)/2} \cdot 2^b Q_F \cdot \left| \prod_{\substack{\chi \in \hat{G} \\ \chi \text{ odd}}} \psi^{(1)}(\chi) \right| \cdot w_F = 2^b \cdot 2[E_F : E_F^+] \prod_{\substack{\chi \in \hat{G} \\ \chi \text{ odd}}} \frac{-B_{1,\chi}}{2} = 2^b h_F^-$$

where the second equality uses that $Q_F w_F = 2[E_F : E_F^+]$ by Lemma 4.2.16, and the final equality follows from Theorem 4.2.20. □

CHAPTER 5

Kubota-Leopoldt p-adic L-functions

5.1. p-adic measures

In this section, we study $\mathbb{C}_p$-valued distributions.

DEFINITION 5.1.1. We say that a $\mathbb{C}_p$-valued distribution $\{\psi_i\}_{i\in I}$ on an inverse system of finite sets X_i is *bounded* if there exists a constant $B \in \mathbb{R}_{\geq 0}$ such that $|\psi_i(x)| \leq B$ for all $x \in X_i$ for all $i \in I$, where $|\cdot|$ is the unique extension of the p-adic valuation on $\mathbb{Q}_p$ to $\mathbb{C}_p$.

REMARK 5.1.2. To say that $\{\psi_i\}$ is bounded is the same as saying the corresponding functional ψ on step functions on the profinite space $X = \varprojlim_i X_i$ satisfies

$$|\psi(\chi)| \leq B\|\chi\|,$$

where $\|\chi\| = \sup_{x\in X} |\chi(x)|$ (which is actually a maximum, as X is compact).

NOTATION 5.1.3. For a topological subring $\mathscr{O}$ of $\mathbb{C}_p$, let $C(X,\mathscr{O})$ denote the space of continuous functions from X to $\mathscr{O}$, endowed with the compact-open topology.

REMARK 5.1.4. The set $\mathrm{Step}(X,\mathbb{C}_p)$ is dense in $C(X,\mathbb{C}_p)$.

DEFINITION 5.1.5. For a topological subring $\mathscr{O}$ of $\mathbb{C}_p$ and a profinite space X, an *$\mathscr{O}$-valued measure* on X is a bounded linear functional

$$\mu : C(X,\mathscr{O}) \to \mathscr{O}.$$

We write

$$\int_X g d\mu$$

for the value $\mu(g)$.

REMARK 5.1.6. Measures on X are in one-to-one correspondence with bounded distributions, since $\mathrm{Step}(X,\mathbb{C}_p)$ is dense in $C(X,\mathbb{C}_p)$.

EXAMPLE 5.1.7. The δ-distribution at $x \in X$ gives rise to the Dirac measure

$$\int_X g d\delta_x = g(x).$$

We briefly discuss measures on $\mathbb{Z}_p$.

REMARK 5.1.8. Let $g\colon \mathbb{Z}_p \to \mathbb{C}_p$ be a continuous function, and let μ be a $\mathbb{C}_p$-valued measure on $\mathbb{Z}_p$ with corresponding distribution $\{\mu_n\}$. Then

$$\int_{\mathbb{Z}_p} g d\mu = \lim_{n\to\infty} \sum_{a=0}^{p^n-1} g_n(a)\mu_n(a).$$

Let $\mathscr{O}$ denote the valuation ring of a finite extension of $\mathbb{Q}_p$.

PROPOSITION 5.1.9. *There is a canonical bijection between $\mathscr{O}$-valued measures μ on $\mathbb{Z}_p$ and elements λ of $\mathscr{O}[\![\mathbb{Z}_p]\!]$, seen explicitly as follows. Write $\lambda \in \mathscr{O}[\![\mathbb{Z}_p]\!]$ as $\lambda = (\lambda_n)_n$ with $\lambda_n \in \mathscr{O}[\mathbb{Z}/p^n\mathbb{Z}]$. Then μ is the measure associated to the distribution $\{\mu_n\}_{n\geq 1}$ with $\mu_n\colon \mathbb{Z}/p^n\mathbb{Z} \to \mathscr{O}$ corresponds to λ if and only if*

$$\lambda_n = \sum_{a=0}^{p^n-1} \mu_n(a)[a]_n$$

where $[a]_n \in \mathscr{O}[\mathbb{Z}/p^n\mathbb{Z}]$ is the group element attached to a.

PROOF. Clearly, the data of the λ_n determine the μ_n and conversely. One need only see that f is well-defined if and only if the μ_n satisfy the distribution relations. But, from the definitions, the element λ_{n+1} maps to λ_n if and only if

$$\mu_n(a) = \sum_{b=0}^{p^n-1} \mu_{n+1}(a+p^n b),$$

as required. □

REMARK 5.1.10. We have $\mu(\chi_{a+p^n\mathbb{Z}_p}) = \mu_n(a)$, so knowing each μ_n determines μ on step functions explicitly.

REMARK 5.1.11. Since $\mathscr{O}[\![T]\!] \cong \mathscr{O}[\![\mathbb{Z}_p]\!]$ via the continuous $\mathscr{O}$-linear isomorphism taking $T+1$ to the group element of 1, we have a canonical bijection between $\mathscr{O}$-valued measures on $\mathbb{Z}_p$ and power series in $\mathscr{O}[\![T]\!]$.

COROLLARY 5.1.12. *The power series f attached to an $\mathscr{O}$-valued measure μ on $\mathbb{Z}_p$ is given by*

$$f(T) = \sum_{i=0}^{\infty} \left(\int_{\mathbb{Z}_p} \binom{x}{i} d\mu(x) \right) T^i \in \mathscr{O}[\![T]\!].$$

PROOF. Let $f_n \in \mathscr{O}[\![T]\!]/(\omega_n)$ be the image of f. By Proposition 5.1.9, the measure μ attached to f given by the distribution $\{\mu_n\}_{n\geq 1}$ is related to f_n through the formula

$$f_n(T) = \sum_{a=0}^{p^n-1} \mu_n(a)(T+1)^a = \sum_{i=0}^{\infty} \sum_{a=0}^{p^n-1} \binom{a}{i} \mu_n(a) T^i,$$

so the inverse limit f of the f_n satisfies the desired equation. □

COROLLARY 5.1.13. *Let f be the power series attached to an $\mathscr{O}$-valued measure μ on $\mathbb{Z}_p$. If $t \in \mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal of $\mathscr{O}$, the value $f(t)$ may be calculated by*

$$f(t) = \int_{\mathbb{Z}_p} (1+t)^x d\mu(x),$$

where μ is the measure corresponding to f.

THEOREM 5.1.14 (Mahler). *We have*

$$C(\mathbb{Z}_p, \mathscr{O}) = \left\{ \sum_{i=0}^{\infty} c_i \binom{x}{i} \mid c_i \in \mathscr{O}, c_i \to 0 \right\},$$

and the representation of $g \in C(\mathbb{Z}_p, \mathscr{O})$ as a sum as in the latter set is unique.

PROOF. Suppose that there is a sequence $(c_i)_{i \geq 1}$ of elements of $\mathscr{O}$ that converges to 0. Since each $|\binom{x}{i}|$ is bounded by 1 on $\mathbb{Z}_p$, any $g = \sum_{i=0}^{\infty} c_i \binom{x}{i}$ with $c_i \to 0$ is the uniform limit of its continuous partial sums, hence continuous.

Consider the difference operator ∇ on $g \in C(\mathbb{Z}_p, \mathscr{O})$ defined by $\nabla(g)(x) = g(x+1) - g(x)$. Then

$$\nabla \binom{x}{i} = \binom{x+1}{i} - \binom{x}{i} = \binom{x}{i-1},$$

so if g has the form in the theorem, then $\nabla^i(g)(0) = c_i$. In other words, the representation of g as a sum is unique if it exists.

We now show existence. For this, it suffices to consider $\mathbb{Z}_p$-valued functions by choice of a basis and projection. We have a $\mathbb{Z}_p$-linear map from the set of sequences in $\mathbb{Z}_p$ that converge to 0 to $C(\mathbb{Z}_p, \mathbb{Z}_p)$ given by $(c_i)_{i \geq 0} \mapsto \sum_{i=0}^{\infty} c_i \binom{x}{i}$. It suffices to show that this map is surjective. This can be derived via recursion from the claim that the set of eventually zero sequences in $\mathbb{F}_p$ surjects onto $C(\mathbb{Z}_p, \mathbb{F}_p)$ via the reduction modulo p of this map.

Note that

$$C(\mathbb{Z}_p, \mathbb{F}_p) = \varinjlim_n \mathrm{Maps}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{F}_p),$$

For $0 \leq i \leq p^n - 1$, the map $x \mapsto \binom{x}{i} \bmod p$ lies in $\mathrm{Maps}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{F}_p)$, since

$$(1+T)^{x+p^n} \equiv (1+T)^x (1+T^{p^n}) \equiv (1+T)^x \bmod (p, T^{p^n}) \mathbb{Z}_p[\![T]\!].$$

Thus, our map restricts to a map

$$\{(c_i)_{0 \leq i < p^n} \mid c_i \in \mathbb{F}_p\} \to \mathrm{Maps}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{F}_p)$$

that is injective by our earlier uniqueness argument using ∇ and surjective by equality of $\mathbb{F}_p$-dimensions. This proves the desired surjectivity. □

The following is a matter of switching the order of a sum and an integral.

COROLLARY 5.1.15. *For $g = \sum_{i=0}^{\infty} c_i \binom{x}{i} \in C(\mathbb{Z}_p, \mathscr{O})$ and μ the measure attached to*

$$f = \sum_{i=0}^{\infty} a_i T^i \in \mathscr{O}[\![T]\!],$$

we have

$$\int_{\mathbb{Z}_p} g d\mu = \sum_{i=0}^{\infty} a_i c_i.$$

Typically, we are more interested in measures on $\mathbb{Z}_p^\times$, or the units in a slightly larger ring. Let us recall that $1+q\mathbb{Z}_p$, where $q = p$ if p is odd and $q = 4$ for $p = 2$, is isomorphic to $\mathbb{Z}_p$ via the map that takes u^a to a for any $a \in \mathbb{Z}_p$, where u is a fixed topological generator of $1+q\mathbb{Z}_p$, such as $1+q$. In this way, measures on $1+q\mathbb{Z}_p$ are made to correspond to measures on $\mathbb{Z}_p$.

DEFINITION 5.1.16. For an $\mathscr{O}$-valued measure ν on $1+q\mathbb{Z}_p$, let μ be the $\mathscr{O}$-valued measure on $\mathbb{Z}_p$ defined by

$$\int_{\mathbb{Z}_p} g(u^x) d\mu(x) = \int_{1+q\mathbb{Z}_p} g d\nu.$$

The power series in $\mathscr{O}[\![T]\!]$ attached to ν is the power series corresponding to μ by Proposition 5.1.9.

LEMMA 5.1.17. *The power series f attached to an $\mathscr{O}$-valued measure ν on $1+q\mathbb{Z}_p$ satisfies*

$$f(u^s - 1) = \int_{1+q\mathbb{Z}_p} x^s d\nu(x)$$

for $s \in \mathbb{Z}_p$, and f is uniquely determined by this formula.

PROOF. Let μ be the measure on $\mathbb{Z}_p$ corresponding to ν and f. Set $t = u^s - 1$ for some $s \in \mathbb{Z}_p$. Then Corollary 5.1.13 tells us that

$$f(u^s - 1) = \int_{\mathbb{Z}_p} u^{sx} d\mu(x) = \int_{1+q\mathbb{Z}_p} x^s d\nu(x).$$

We leave the last simple statement to the reader. □

REMARK 5.1.18. We can also attach a measure on $\mathbb{Z}_p$ to a measure on $\mathbb{Z}_p^\times$, by extension by zero. Similarly, we can restrict measures on $\mathbb{Z}_p$ to the latter multiplicative subgroups.

5.2. p-adic L-functions

DEFINITION 5.2.1. Let p be a prime number, and let $m \geq 1$ be prime to p. Set

$$\mathbb{Z}_{p,m} = \varprojlim_n (\mathbb{Z}/mp^n\mathbb{Z}).$$

Then

$$\mathbb{Z}_{p,m} \xrightarrow{\sim} \mathbb{Z}_p \times \mathbb{Z}/m\mathbb{Z},$$

and we let c_p denote the first coordinate of the image of $c \in \mathbb{Z}_{p,m}$.

Note that

$$\mathbb{Z}_{p,m}^{\times} = \varprojlim_n (\mathbb{Z}/mp^n\mathbb{Z})^{\times} \cong \mathbb{Z}_p^{\times} \times (\mathbb{Z}/m\mathbb{Z})^{\times},$$

and, setting $q = p$ for p odd and $q = 4$ for $p = 2$, we also have

$$\mathbb{Z}_{p,m}^{\times} \xrightarrow{\sim} (1 + q\mathbb{Z}_p) \times (\mathbb{Z}/qm\mathbb{Z})^{\times}.$$

DEFINITION 5.2.2. For $c \in \mathbb{Z}_{p,m}^{\times}$, we let c_p denote its image in $\mathbb{Z}_p^{\times}$ and $\langle c \rangle_p$ denote its image in $1 + q\mathbb{Z}_p$.

Note also that $\mathbb{Z}_{p,m}^{\times}$ is canonically isomorphic to the Galois group of $\mathbb{Q}(\mu_{mp^{\infty}})/\mathbb{Q}$. We will typically be interested in measures on $\mathbb{Z}_{p,m}^{\times}$.

Let us set $\Delta = (\mathbb{Z}/qm\mathbb{Z})^{\times}$. We have

$$\mathbb{Z}_p[\![\mathbb{Z}_{p,m}^{\times}]\!] \cong \mathbb{Z}_p[\Delta][\![1 + q\mathbb{Z}_p]\!] \cong \mathbb{Z}_p[\Delta][\![T]\!],$$

the latter isomorphism taking the group element u to $T + 1$.

Let $\mathscr{O}$ be the valuation ring of a finite extension of $\mathbb{Q}_p$. By the same discussion as before, replacing $\mathscr{O}$ by the group ring $\mathscr{O}[\Delta]$, we have the following.

LEMMA 5.2.3. *There is a canonical bijection between $\mathscr{O}$-valued measures on $\mathbb{Z}_{p,m}^{\times}$ and elements of $\mathscr{O}[\![T]\!][\Delta]$.*

Explicitly, the power series $f \in \mathscr{O}[\![T]\!][\Delta]$ attached to an $\mathscr{O}$-valued measure ν on $\mathbb{Z}_{p,m}^{\times}$ satisfies

$$f(u^s - 1) = \sum_{\sigma \in \Delta} \int_{1+q\mathbb{Z}_p} x^s d\nu(\sigma x) \cdot \sigma$$

If ν arises from a distribution $\psi = (\psi_n)$ on the groups $(\mathbb{Z}/mp^n\mathbb{Z})^{\times}$, then f is then given by the compatible system of elements

$$\sum_{\substack{a=1 \\ (a,mp)=1}}^{p^n m} \psi_n(a)[a]_n \in \mathscr{O}[(\mathbb{Z}/p^n m\mathbb{Z})^{\times}],$$

where $[a]_n$ denotes the group element of a.

The Bernoulli distribution will be the key to our definition of p-adic L-functions, but it is not necessarily integral. Therefore, we introduce the following modification.

DEFINITION 5.2.4. Set $N = p^n m$, let $c \in \mathbb{Z}_{p,m}^{\times}$, and take $k \geq 1$. For $x \in \mathbb{Z}/N\mathbb{Z}$, we view $\frac{x}{N}$ as an element of $\frac{1}{N}\mathbb{Z}/\mathbb{Z}$ and define

$$E_n^{(k)}(x) = \frac{1}{k} N^{k-1} B_k\left(\left\langle \frac{x}{N} \right\rangle\right)$$

and

$$E_{n,c}^{(k)}(x) = E_n^{(k)}(x) - c_p^k E_n^{(k)}(c^{-1}x).$$

Note that $E_n^{(k)} = \frac{1}{k}\psi_k^{(N)}$, so the $E_n^{(k)}$ and $E_{n,c}^{(k)}$ form distributions on $\mathbb{Q}/\mathbb{Z}$.

PROPOSITION 5.2.5. *For $N = p^n m$ with $n \geq 1$ and $k \geq 1$, we have $E_{n,c}^{(k)}(x) \in \mathbb{Z}_p$ and*

$$E_{n,c}^{(k)}(x) \equiv x^{k-1} E_{n,c}^{(1)}(x) \bmod p^n\mathbb{Z}_p$$

for all $x \in \mathbb{Z}/N\mathbb{Z}$.

PROOF. We have

$$\frac{te^{Xt}}{e^t - 1} = \left(1 - \frac{1}{2}t + \frac{1}{6}t^2 + \cdots\right)\sum_{i=0}^{\infty}\frac{X^i}{i!}t^i,$$

from which we see that the kth Bernoulli polynomial has the form

$$B_k(X) = X^k - \frac{k}{2}X^{k-1} + kf(X)$$

with $f \in \mathbb{Q}[X]$ of degree $k-2$ (or 0 if $k = 1$), the leading term of $f(X)$ being $\frac{k-1}{6}X^{k-2}$. Let $e_k \geq 0$ be minimal such that $p^{e_k} f(X) \in \mathbb{Z}_p[\![X]\!]$

Let $a \in \mathbb{Z}$ with $0 \leq a < N$ lift $x \in \mathbb{Z}/N\mathbb{Z}$, and let $b \in \mathbb{Z}$ with $0 \leq b < N$ and $y \in \mathbb{Z}_p$ be such that $\frac{c_p^{-1}a}{N} = \frac{b}{N} + y$. We then have

$$b^j \equiv c_p^{-j}a^j - jNc_p^{-j+1}a^{j-1}y \bmod N^2$$

for $j \geq 1$, which yields

$$E_{n,c}^{(k)}(x) \equiv \frac{1}{k}\left(\frac{1}{N}a^k - \frac{k}{2}a^{k-1} - c_p^k\left(\frac{1}{N}b^k - \frac{k}{2}b^{k-1}\right)\right) \equiv a^{k-1}\left(c_p y + \frac{1}{2}(c_p - 1)\right) \bmod p^{n-e_k}\mathbb{Z}_p.$$

Since this holds for all k, we have in particular that $E_{n,c}^{(1)}(x)$ is in $\mathbb{Z}_p$ for all n, noting that $c_p \equiv 1 \bmod 2\mathbb{Z}_p$, and that

$$E_{n,c}^{(k)}(x) \equiv x^{k-1}E_{n,c}^{(1)}(x) \bmod p^{n-e_k}\mathbb{Z}_p$$

is integral for sufficiently large n as well. By the distribution relation for the $E_{n,c}^{(k)}$, this integrality then holds for all n. If we choose $n \geq e_k'$, where e_k' is minimal such that $p^{e_k'}(f(X) - \frac{k-1}{6}X^{k-2}) \in \mathbb{Z}_p[X]$, then we can refine the above to to

$$E_{n,c}^{(k)}(x) \equiv x^{k-1}E_{n,c}^{(1)}(x) + Nx^{k-2}\frac{k-1}{6}(1 - c_p^2) \bmod p^n\mathbb{Z}_p$$

Since $c_p^2 \equiv 1 \bmod 6\mathbb{Z}_p$, this reduces to

$$E_{n,c}^{(k)}(x) \equiv x^{k-1}E_{n,c}^{(1)}(x) \bmod p^n\mathbb{Z}_p,$$

and the congruence then follows for arbitrary n by the distribution relation. □

REMARK 5.2.6. Together the $E_{n,c}^{(k)}$ form a $\mathbb{Z}_p$-valued measure $E_c^{(k)}$ on $\mathbb{Z}_{p,m}$, hence on $\mathbb{Z}_{p,m}^\times$ as well by restriction. We can integrate the resulting measure against functions on $\mathbb{Z}_{p,m}^\times$ that arise as limits of Dirichlet characters of conductor dividing $p^n m$ for some n.

DEFINITION 5.2.7. We let $E_c^{(k)}$ denote the measure defined by the $E_{n,c}^{(k)}$.

REMARK 5.2.8. Given $g \in C(\mathbb{Z}_{p,m}^\times, \mathscr{O})$, we have

$$\int_{\mathbb{Z}_{p,m}^\times} g(x) dE_c^{(k)}(x) = \int_{\mathbb{Z}_{p,m}^\times} g(x) x_p^{k-1} dE_c^{(1)}(x)$$

for every $k \geq 1$.

REMARK 5.2.9. When $\chi\colon \mathbb{Z}_{p,m} \to \mathscr{O}^\times$ is a continuous multiplicative function, we have

$$\int_{\mathbb{Z}_{p,m}} \chi(x) dE_c^{(k)}(x) = (1 - \chi(c) c_p^k) \frac{B_{k,\chi}}{k}.$$

Note that if χ has finite order, so is the map attached to a primitive Dirichlet character of conductor dividing mp^n for some n, then $\chi E_c^{(k)}$ defines an $\mathscr{O}$-valued measure on $\mathbb{Z}_{p,m}$, with volume given by the above formula. Here, the $\chi E_{n,c}^{(k)}$ are really only defined for $p^n m$ a multiple of the conductor of χ, but the ith terms of the distribution for i less than the minimal such n can be defined by the distribution relations.

DEFINITION 5.2.10. Let ν be an $\mathscr{O}$-valued measure on $\mathbb{Z}_{p,m}^\times$. We define its *p-adic Mellin transform* to be the $\mathscr{O}$-valued function $M_p(\nu)$ on $\mathbb{Z}_p$ given by

$$M_p(\nu)(s) = \int_{\mathbb{Z}_{p,m}^\times} \langle x \rangle_p^s x_p^{-1} d\nu(x).$$

REMARK 5.2.11. When p is odd, $x_p = \langle x \rangle_p \omega(x)$ for any $x \in \mathbb{Z}_{p,m}^\times$, where ω is the Teichmüller character, which factors through $(\mathbb{Z}/p\mathbb{Z})^\times$. For $p = 2$, we simply define $\omega\colon \mathbb{Z}_{2,m}^\times \to \mu_2(\mathbb{Z}_2)$ by the above formula.

REMARK 5.2.12. If ν is an $\mathscr{O}$-valued measure on $\mathbb{Z}_{p,m}^\times$, then so is $\psi\nu$ for any Dirichlet character ψ of conductor dividing $p^n m$ for some n. In particular, we have

$$M_p(\nu)(s) = \int_{\mathbb{Z}_{p,m}^\times} \langle x \rangle^{s-1} d(\omega^{-1}\nu).$$

DEFINITION 5.2.13. Let $\chi\colon \mathbb{Z}_{p,m}^\times \to \mathbb{C}_p^\times$ be a finite-order character. We define the *Kubota-Leopoldt p-adic L-function* of χ to be the $\mathbb{C}_p$-valued function on $\mathbb{Z}_p$ given by

$$L_p(\chi, s) = -(1 - \chi(c)\langle c \rangle_p^{1-s})^{-1} M_p(\chi E_c^{(1)})(1-s)$$

for $s \in \mathbb{Z}_p$ and $c \in \mathbb{Z}_{p,m}^\times$ such that $\chi(c) \neq 1$ if $\chi \neq 1$.

Rewriting this, we have

$$\begin{aligned} -(1 - \chi(c)\langle c \rangle_p^{1-s}) L_p(\chi, s) &= \int_{\mathbb{Z}_{p,m}^\times} \chi(x) \langle x \rangle_p^{1-s} x_p^{-1} dE_c^{(1)}(x) \\ &= \int_{\mathbb{Z}_{p,m}^\times} \langle x \rangle_p^{-s} d(\chi\omega^{-1} E_c^{(1)})(x). \end{aligned} \tag{5.2.1}$$

REMARK 5.2.14. The factor $(1-\chi(c)\langle c\rangle_p^{1-s})^{-1}$ in the definition of $L_p(\chi,s)$ removes the dependence of the definition of the p-adic L-function on the value c. Note that such a factor (without the inverse) was used in defining $E_c^{(1)}$ in the first place.

A finite order character $\chi\colon \mathbb{Z}_{p,m}^\times \to \mathbb{C}^\times$ takes values in $\overline{\mathbb{Q}}$ and may be viewed as a p-adic character through a choice of embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}_p}$, we have the following.

PROPOSITION 5.2.15. *Let χ be a primitive Dirichlet character of conductor $p^n m$ for some $n \geq 0$, and let χ also denote the resulting character $\chi\colon \mathbb{Z}_{p,m}^\times \to \mathbb{C}_p^\times$, fixing a place over p in $\overline{\mathbb{Q}}$. For $k \geq 1$, we have*

$$L_p(\chi,1-k) = -(1-\chi\omega^{-k}(p)p^{k-1})\frac{B_{k,\chi\omega^{-k}}}{k} = (1-\chi\omega^{-k}(p)p^{k-1})L(\chi\omega^{-k},1-k).$$

PROOF. Set $\chi_k = \chi\omega^{-k}$. We note that

$$(1-\chi_k(c)c_p^k)L_p(\chi,1-k) = \int_{\mathbb{Z}_{p,m}^\times} \chi_k(x)x_p^{k-1}dE_c^{(1)}(x) = \int_{\mathbb{Z}_{p,m}^\times} \chi_k(x)dE_c^{(k)}(x),$$

and we split the latter integral into a difference of an integral over $\mathbb{Z}_{p,m}$ by an integral over $p\mathbb{Z}_{p,m}$, given that χ_k is trivial on elements of $\mathbb{Z}_{p,m}$ not prime to m. By Remark 5.2.9, the former is

$$\int_{\mathbb{Z}_{p,m}} \chi_k(x)dE_c^{(k)}(x) = (1-\chi_k(c)c_p^k)\frac{B_{k,\chi_k}}{k}.$$

Since $E_{n,c}^{(k)}(pb) = E_{n-1,c}^{(k)}(b)$ for $b \in \mathbb{Z}/mp^n\mathbb{Z}$, the latter is

$$\begin{aligned}\int_{p\mathbb{Z}_{p,m}} \chi_k(x)dE_c^{(k)}(x) &= \sum_{a=1}^{mp^{n-1}} \chi_k(pa)E_{n,c}^{(k)}(pa)\\ &= \chi_k(p)p^{k-1}\sum_{a=1}^{mp^{n-1}} \chi_k(a)E_{n-1,c}^{(k)}(a)\\ &= \chi_k(p)p^{k-1}\int_{\mathbb{Z}_{p,m}} \chi_k(x)dE_c^{(k)}(x).\end{aligned}$$

Taking the difference of the two terms, we have the result. □

COROLLARY 5.2.16. *The p-adic L-function of χ is independent of the choice of c in its definition.*

PROOF. The function $L_p(\chi,s)$ is continuous, and its values at the dense subset of $\mathbb{Z}_p$ consisting of the nonnegative integers are independent of c by Proposition 5.2.15. □

5.3. Iwasawa power series

DEFINITION 5.3.1. A finite order p-adic character χ on $\mathbb{Z}_{p,m}^{\times}$ is a *of the first kind* if χ is trivial on $1+q\mathbb{Z}_p$ and *of the second kind* if it is trivial on Δ.

In general, a finite order p-adic character χ on $\mathbb{Z}_{p,m}^{\times}$ is a unique product $\chi = \chi_{\mathrm{t}}\chi_{\mathrm{w}}$ of a p-adic character χ_{t} of the first kind and a p-adic character χ_{w} of the second kind. We use the subscripts "t" and "w" to indicate "tame" and "wild", respectively, though the terminology is technically incorrect if $p=2$. If we view χ as corresponding to a primitive Dirichlet character of conductor mp^n for $n \geq 0$, then χ is of the first kind if and only if it has conductor dividing mq, and χ is of the second kind if and only if it has p-power order and conductor p^n for some $n \geq 1$ (and then necessarily at least 2 if $p=2$). If χ is of the second kind, it is necessarily even.

NOTATION 5.3.2. For any Dirichlet character χ, let $\Lambda_\chi = \mathscr{O}_\chi[\![T]\!]$, where $\mathscr{O}_\chi$ is the $\mathbb{Z}_p$-algebra generated by the values of χ, fixing a choice of a embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$. Let K_χ denote the quotient field of $\mathscr{O}_\chi$, and let $Q(\Lambda_\chi)$ denote the quotient field of Λ_χ, which contains $K_\chi[\![T]\!]$.

PROPOSITION 5.3.3. *Let χ be a primitive even Dirichlet character of conductor m or mq. There exists a unique element $F_\chi \in Q(\Lambda_\chi)$ such that*

$$F_\chi(\xi u^s - 1) = L_p(\chi\rho, s)$$

for all $s \in \mathbb{Z}_p$ and ξ of p-power order, where ρ is of the second kind satisfying $\rho(u) = \xi^{-1}$.

PROOF. It follows from (5.2.1) that

$$-(1-\chi\rho(c)\langle c\rangle_p^{1-s})L_p(\chi\rho,s) = \sum_{\sigma\in\Delta}\left(\int_{1+q\mathbb{Z}_p}\langle x\rangle_p^{-s}\rho(x)dE_c^{(1)}(x)\right)\chi\omega^{-1}(\sigma).$$

Let $a \in \mathbb{Z}_p$ be such that $\langle c\rangle_p = u^a$, and set

$$h_{\chi,c}(T) = \chi(c)\langle c\rangle_p(1+T)^{-a} - 1.$$

Then

$$h_{\chi,c}(\xi u^s - 1) = \chi(c)\langle c\rangle_p\xi^{-a}u^{-sa} - 1 = -(1-\chi\rho(c)\langle c\rangle_p^{1-s}).$$

Similarly, if we let $f_{\chi,c} \in \mathscr{O}_\chi[\![T]\!]$ be such that

$$f_{\chi,c}(u^s - 1) = -(1-\chi(c)\langle c\rangle_p^{1-s})L_p(\chi, s)$$

for all $s \in \mathbb{Z}_p$, then

$$f_{\chi,c}(\xi u^s - 1) = -(1-\chi\rho(c)\langle c\rangle_p^{1-s})L_p(\chi\rho, s).$$

Thus $F_\chi = \frac{f_{\chi,c}}{h_{\chi,c}}$ has the desired property. In that the integral power series $f_{\chi,c}$ satisfies $f_{\chi,c}((1+q)^s - 1) = h_{\chi,c}((1+q)^s-1)L_p(\chi,s)$ for all $s \in \mathbb{Z}_p$, it is unique, and therefore so is F_χ. □

REMARK 5.3.4. In the notation of Proposition 5.3.3, we have If $\chi \neq 1$, then we may take $c \in \Delta \subset \mathbb{Z}_{p,m}^{\times}$ to be such that $\chi(c) \neq 1$, so $h_{\chi,c} = \chi(c) - 1$, and $(\chi(c)-1)F_\chi \in \Lambda_\chi$. If $\chi = 1$, then we may take $c = u \in 1 + q\mathbb{Z}_p$, so $h_{\chi,u} = u(T+1)^{-1} - 1$.

DEFINITION 5.3.5. Let $F_n = \mathbb{Q}(\mu_{mp^n})$, and let $G_n = \mathrm{Gal}(F_n/\mathbb{Q})$. For any $b \in \mathbb{Z}_{p,m}^{\times}$, set

$$\Theta_n^{(k)}(b) = \sum_{\substack{a=1 \\ (a,mp)=1}}^{mp^n} E_n^{(k)}(ab)\sigma_a^{-1}.$$

We set $\Theta_n^{(k)} = \Theta_n^{(k)}(1)$ and refer to $\Theta_n^{(k)}$ as the *kth higher Stickelberger element* for F_n.

Since the $E_n^{(k)}$ form a distribution, the $\Theta_n^{(k)}$ give a compatible system in the inverse limit. Set $G_\infty = \mathrm{Gal}(F_\infty/\mathbb{Q})$. We have a continuous isomorphism $\mathbb{Z}_{p,m}^{\times} \xrightarrow{\sim} G_\infty$ via $a \mapsto \sigma_a$, under which $1 + q\mathbb{Z}_p$ is idenitifed with $\Gamma = \mathrm{Gal}(F_\infty/F)$ for $F = \mathbb{Q}(\mu_{mq})$, and $\Delta = (\mathbb{Z}/mq\mathbb{Z})^{\times}$ is identified with the torsion subgroup of G_∞, which we also denote by Δ. For locally compact $\mathbb{Z}_p$-algebra R, we then have an identification

$$R[\![G_\infty]\!] = R[\Delta][\![\Gamma]\!] \cong R[\Delta][\![T]\!]$$

of topological rings, where $T = \gamma - 1$ for $\gamma = \sigma_u$.

NOTATION 5.3.6. Let

$$\Theta_\infty^{(k)}(b) = (\Theta_n^{(k)}(b))_n \in \mathbb{Q}_p[\Delta][\![T]\!],$$

and set $\Theta_\infty^{(k)} = \Theta_\infty^{(k)}(1)$.

REMARK 5.3.7. Since

$$(1 - c_p^k \sigma_c^{-1}) \sum_{\substack{a=1 \\ (a,mp)=1}}^{mp^n} E_n^{(k)}(a)\sigma_a^{-1} = \sum_{\substack{a=1 \\ (a,mp)=1}}^{mp^n} E_{n,c}^{(k)}(a)\sigma_a^{-1} \in \mathbb{Z}_p[G_n],$$

we have $(1 - c_p^k \sigma_c^{-1})\Theta_\infty^{(k)} \in \mathbb{Z}_p[\Delta][\![T]\!]$. Aside from the use of σ_a^{-1} in place of σ_a, the latter is the power series corresponding to the measure given by the $E_{n,c}^{(k)}$ on $\mathbb{Z}_{p,m}^{\times}$.

NOTATION 5.3.8. For any nontrivial primitive even Dirichlet character χ of conductor m or mq, let

$$f_\chi = -\widetilde{\omega\chi^{-1}}(\Theta_\infty^{(1)}),$$

where $\widetilde{\omega\chi^{-1}} \colon \mathbb{Q}_p[\Delta][\![T]\!] \to K_\chi[\![T]\!]$ is the unique continuous $\mathbb{Q}_p[\![T]\!]$-linear map that restricts to $\chi_1^{-1} = \omega\chi^{-1}$ on Δ. Set

$$f_1 = (1 - u(1+T)^{-1})\widetilde{\omega}(\Theta_\infty^{(1)}).$$

DEFINITION 5.3.9. For any primitive even Dirichlet character of conductor m or mq, the power series f_χ is called the *Iwasawa power series* of χ.

REMARK 5.3.10. For any nontrivial χ, the image of f_χ in $\mathrm{Gal}(F_n/\mathbb{Q})$ is

$$-\sum_{\substack{a=1\\(a,mp)=1}}^{mp^n}\left(\frac{a}{mp^n}-\frac{1}{2}\right)\chi\omega^{-1}(a)\sigma_{\langle a\rangle_p}^{-1}=-\frac{1}{mp^n}\sum_{\substack{a=1\\(a,mp)=1}}^{mp^n}a\chi\omega^{-1}(a)\sigma_{\langle a\rangle_p}^{-1},$$

where the second equality is by the nontriviality of χ_1. Then $-f_\chi$ becomes identified with

$$\left(\widetilde{\omega\chi^{-1}}(\theta_{F_n})\right)_n\in\mathbb{Q}_p[\![\Gamma]\!],$$

where $\omega\chi^{-1}$ is defined in the obvious fashion. In other words, f_χ is the negative of the $\omega\chi^{-1}$-specialization of the inverse limit of Stickelberger elements of the fields F_n.

For χ nontrivial, the power series f_χ agrees with F_χ defined above.

LEMMA 5.3.11. *For any primitive even Dirichlet character χ of conductor m or mq, we have $f_\chi=F_\chi$. For $\chi=1$, we have $f_1=h_1F_1$, where $h_1=1-u(1+T)^{-1}$.*

PROOF. We have

$$\begin{aligned}-(1-\chi(c))f_\chi(u^s-1)&=\widetilde{\omega\chi^{-1}}\left(\sum_{\substack{a=1\\(a,mp)=1}}^{mp}\int_{1+q\mathbb{Z}_p}x^{-s}dE_c^{(1)}(x)\sigma_a^{-1}\right)\\&=\int_{\mathbb{Z}_{p,m}^\times}\chi_1(x)\langle x\rangle_p^{-s}dE_c^{(1)}(x)\\&=\int_{\mathbb{Z}_{p,m}^\times}\chi(x)\langle x\rangle_p^{1-s}x_p^{-1}dE_c^{(1)}(x)\\&=-(1-\chi(c))L_p(\chi,s).\end{aligned}$$

It follows that $f_\chi=F_\chi$. The case that $\chi=1$ is similar and left to the reader. □

We now prove the integrality of the Iwasawa power series f_χ for odd p.

PROPOSITION 5.3.12. *Let χ be a primitive even Dirichlet character of conductor m or mq. Then $\frac{1}{2}f_\chi\in\Lambda_\chi$.*

PROOF. We prove this in the case that p is odd. For $\chi=1$, this is immediate from Lemma 5.3.11 and Remark 5.3.4. For χ nontrivial, we are already done if χ is not of p-power order, as $\chi(c)-1$ can be chosen to be a unit. In particular, we may suppose that $m\neq1$, so is divisible by a prime $\ell\neq p$. We claim that

$$\Theta_\infty^{(1)}-\ell^{-1}\Theta_\infty^{(1)}(\ell)\in\mathbb{Z}_p[\![G_\infty]\!].$$

To see this, note that

$$\Theta_n^{(1)} - \ell^{-1}\Theta_n^{(1)}(\ell) = \sum_{\substack{a=1 \\ (a,mp)=1}}^{mp^n} \left(\frac{a}{mp^n} - \ell^{-1} \left\langle \frac{\ell a}{mp^n} \right\rangle \right) \sigma_a^{-1} \in \mathbb{Z}_p[G_n]$$

for all n, since $\ell \in \mathbb{Z}_p^\times$ and $\ell\frac{a}{mp^n} - \langle \frac{\ell a}{mp^n} \rangle \in \mathbb{Z}$ by definition. Setting $m' = \frac{m}{\ell}$, for $\tilde{\Delta} \subset \{1, \dots, mp^n\}$ a set of representatives of Δ viewed inside $\mathbb{Z}/mp^n\mathbb{Z}$ and a fixed $b \in \mathbb{Z}_p$, we have that the coefficient of $\gamma^{-b} \in \mathscr{O}_\chi[G_n]$ of $\widetilde{\omega\chi^{-1}}\Theta_n^{(1)}(\ell)$ is

$$\sum_{a \in \tilde{\Delta}} \left\langle \frac{\ell ab}{mp^n} \right\rangle \omega\chi^{-1}(a) = \sum_{\substack{a=1 \\ a \in \tilde{\Delta}}}^{m'p^n} \frac{ab}{m'p^n} \sum_{i=0}^{\ell-1} \omega\chi^{-1}(a + im'p^n),$$

and the latter sum is 0 since ℓ divides the conductor of $\omega\chi^{-1}$. (Note that one value of $a + im'p^n$ in the sum will not be prime to m if $\ell \nmid m'$, but $\omega\chi^{-1}(a + im'p^n) = 0$ for this value.) Thus, $\widetilde{\omega\chi^{-1}}(\Theta_\infty^{(1)}(\ell)) = 0$, so

$$f_\chi = \widetilde{\omega\chi^{-1}}(\Theta_\infty^{(1)} - \ell^{-1}\Theta_\infty^{(1)}(\ell)) \in \Lambda_\chi.$$

□

Putting this all together, we have the following.

THEOREM 5.3.13. *Let χ be a primitive even p-adic Dirichlet character of the first kind. There exists a unique element $f_\chi \in \Lambda_\chi$ such that if χ is nontrivial, we have*

$$f_\chi(\xi u^s - 1) = L_p(\chi\rho, s),$$

and if $\chi = 1$, then for $h_1 = u(1+T)^{-1} - 1$, we have

$$f_1(\xi u^s - 1) = h_1(\xi u^s - 1)L_p(\rho, s)$$

for all $s \in \mathbb{Z}_p$ and ξ of p-power order, where ρ is of the second kind satisfying $\rho(u) = \xi^{-1}$.

Recall that X_∞ denotes the unramified Iwasawa module over F_∞. The interpretation of f_χ in terms of Stickelberger elements also gives the following.

PROPOSITION 5.3.14. *For any primitive Dirichlet character χ of conductor m or mq, the Iwasawa power series $\frac{1}{2}f_\chi \in \Lambda_\chi$ annihilates $X_\infty^{(\omega\chi^{-1})}$.*

PROOF. We again suppose that p is odd. Recall that $\Theta_\infty^{(1)} - \ell^{-1}\Theta_\infty^{(1)}(\ell)$ is integral, and

$$\widetilde{\omega\psi^{-1}}(\Theta_\infty^{(1)}(\ell)) = 0$$

for every nontrivial even character ψ of conductor m or mp. Write $\chi = \nu\rho$ where ν has order prime to p and ρ has p-power order. By varying ρ over its $G_{\mathbb{Q}_p}$-conjugates, this implies that $e_{\omega\nu^{-1}}\Theta_\infty^{(1)}(\ell) = 0$,

where $e_{\omega\nu^{-1}}$ is the idempotent for $\omega\nu^{-1}$ on the prime-to-p part of Δ. Then $e_{\omega\nu^{-1}}\Theta_\infty^{(1)} \in \mathscr{O}_\nu[\![G_\infty]\!]$. By Remark 5.3.10, it annihilates $e_{\omega\nu^{-1}}X_\infty$. By projection, we then have that f_χ annihilates the quotient $X_\infty^{(\omega\chi^{-1})}$. □

COROLLARY 5.3.15. *Suppose that p is odd. For any even $k \geq 2$ not divisible by $p-1$ and every $j \geq 1$, we have*

$$B_{1,\omega^{k-1}} \equiv \frac{B_{j,\omega^{k-j}}}{j} \bmod p.$$

In particular, we have

$$B_{1,\omega^{k-1}} \equiv \frac{B_k}{k} \bmod p.$$

PROOF. We have $L_p(0,\omega^k) = -B_{1,\omega^{k-1}}$ and $L_p(1-j,\omega^k) = -\frac{B_{j,\omega^{k-j}}}{j}$, so this follows from the fact that $\omega^k \neq 1$, then $L_p(\chi,s) = f_\chi(u^s-1)$, and $u^{1-j}-1 \equiv 0 \bmod p$. □

COROLLARY 5.3.16. *Suppose that p is odd and $j \equiv k \bmod p^{n-1}(p-1)$ are even positive integers not divisible by $p-1$. Then*

$$(1-p^{j-1})\frac{B_j}{j} \equiv (1-p^{k-1})\frac{B_k}{k} \bmod p^n.$$

PROOF. We have $L_p(1-j,\omega^j) = -(1-p^{j-1})\frac{B_j}{j}$. As

$$\omega^j(x)\langle x\rangle_p^{j-1} = x_p^j\langle x\rangle_p^{-1}$$

and $x_p^j \equiv x_p^k \bmod p^n$, we have the result so long as

$$1-\omega^j(c)\langle c\rangle_p^j = 1-c_p^j$$

can be taken to be a unit, which occurs if $j \not\equiv 0 \bmod p-1$. □

5.4. Coleman theory

Let E be an unramified extension of $\mathbb{Q}_p$ with valuation ring $\mathscr{O}$. Let q denote the order of the residue field of $\mathscr{O}$. Let $E_n = E(\mu_{p^{n+1}})$, and let $\mathscr{O}_n$ denote its valuation ring, for $n \geq 0$. Fix a sequence $(\zeta_{p^n})_n$ of primitive p^nth roots of unity in E_n such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for each $n \geq 1$. Let $\Lambda = \mathscr{O}[\![T]\!]$.

NOTATION 5.4.1. Let $[p]$ denote the continuous $\mathbb{Z}_p$-linear endomorphism of Λ given on $f \in \Lambda$ by

$$[p](f)(T) = f((1+T)^p - 1).$$

LEMMA 5.4.2. *The image of $[p]$ is equal to the set of all $f \in \Lambda$ such that*

$$f(\zeta_p^i(1+T)-1) = f(T)$$

for all $i \in \mathbb{Z}$.

PROOF. We need only show that every f with the above property is in the image of $[p]$, which is to say that it can be expanded in a power series in $P = [p](T) = (1+T)^p - 1$. For this, suppose inductively that we have written f as

$$f = \sum_{i=0}^{n-1} a_i P^i + P^n f_n$$

with $a_i \in \mathscr{O}$ for some $n \geq 0$. Then f_n also has the property that $f_n(\zeta_p^i(1+T)-1) = f_n(T)$ for all i. Taking $T = 0$, we see that $f_n(\zeta_p^i - 1) = f_n(0)$ for all i, and therefore

$$f_n - f_n(0) = P f_{n+1}$$

for some $f_{n+1} \in \Lambda$ having the desired property, and we set $a_n = f_n(0)$. We then have $f = \sum_{i=0}^{\infty} a_i P^i$ in the limit. □

PROPOSITION 5.4.3. *There exist unique maps $\mathscr{N} : \Lambda \to \Lambda$ and $\mathscr{S} : \Lambda \to p\Lambda$ satisfying*

$$([p] \circ \mathscr{N})(f)(T) = \prod_{i=0}^{p-1} f(\zeta_p^i(1+T)-1) \quad \text{and} \quad ([p] \circ \mathscr{S})(f)(T) = \sum_{i=0}^{p-1} f(\zeta_p^i(1+T)-1)$$

for all $f \in \Lambda$.

PROOF. For $f \in \Lambda$, consider

$$g(T) = \prod_{i=0}^{p-1} f(\zeta_p^i(1+T)-1),$$

which is clearly in Λ as its coefficients are fixed by $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. We have $g(T) = g(\zeta_p^i(1+T)-1)$ for all $i \in \mathbb{Z}$, so by Lemma 5.4.2, we have $g = [p](\mathscr{N}(f))$ for some $\mathscr{N}(f) \in \Lambda$, which is unique by the injectivity of $[p]$.

If we take

$$h = \sum_{i=0}^{p-1} f(\zeta_p^i(1+T)-1) \in \Lambda$$

then as

$$f(\zeta_p^i(1+T)-1) \equiv f(T) \bmod (1-\zeta_p),$$

for each i, we have $h(T) \in p\Lambda$. As in the case of $\mathscr{N}$, we have $h(T) = h(\zeta_p^i(1+T)-1)$ for all i, so $h = [p](\mathscr{S}(f))$ for a unique $\mathscr{S}(f) \in p\Lambda$. □

DEFINITION 5.4.4. *Coleman's norm operator $\mathscr{N} : \Lambda \to \Lambda$* and *Coleman's trace operator $\mathscr{S} : \Lambda \to \Lambda$* are the maps characterized by Proposition 5.4.3.

LEMMA 5.4.5. *If $f \in \Lambda$ and $n \geq 1$, then $f \equiv 1 \bmod p^n$ if and only if $[p](f) \equiv 1 \bmod p^n$.*

PROOF. We consider the nontrivial direction. Let $m \geq 0$ be maximal with $f \equiv 1 \bmod p^m$, and let $k \geq 0$ be maximal such that

$$f \equiv 1 + ap^m T^k \bmod (p^{m+1}, T^{k+1})$$

for some nonzero $a \in \mathscr{O}^\times$. Since $[p](T) \equiv T^p \bmod p$, we have

$$[p](f) \equiv 1 + p^m a T^{pk} \bmod (p^{m+1}, T^{k+1}).$$

So, if $[p](f) \equiv 1 \bmod p^n$, then $n \leq m$. □

Let φ denote the unique Frobenius element in $\mathrm{Gal}(E_\infty/\mathbb{Q}_p)$, where $E_\infty = \bigcup_n E_n$, which we also let act on Λ through its action on coefficients.

PROPOSITION 5.4.6. *If $f \in \Lambda^\times$, then $\mathscr{N}(f) \equiv \varphi(f) \bmod p$. If $f \equiv 1 \bmod p^n$ for some positive integer n, then $\mathscr{N}(f) \equiv 1 \bmod p^{n+1}$.*

PROOF. Take $f \in \Lambda^\times$, and suppose that $f \equiv 1 \bmod p^k$ for some $k \geq 0$. We then have

$$f(\zeta_p^i(1+T) - 1) \equiv f(T) \bmod p^k(1 - \zeta_p)$$

for each $i \in \mathbb{Z}$, and our assumption on f implies that

$$([p] \circ \mathscr{N})(f) = \prod_{i=1}^{p-1} f(\zeta_p^i(1+T) - 1) \equiv f(T)^p \bmod p^{k+1}.$$

If $k \geq 1$, then $f^p \equiv 1 \bmod p^{k+1}$, so Lemma 5.4.5 tells us that $\mathscr{N}(f) \equiv 1 \bmod p^{k+1}$ as well.

If $k = 0$, then we can at least say that $f(T)^p \equiv \varphi(f)(T^p) \equiv [p](f)(T) \bmod p$, so

$$[p]\left(\frac{\mathscr{N}(f)}{\varphi(f)}\right) \equiv 1 \bmod p,$$

and therefore Lemma 5.4.5 tells us that $\mathscr{N}(f) \equiv \varphi(f) \bmod p$. □

COROLLARY 5.4.7. *Suppose that $f \in \Lambda^\times$. For $n \geq m$, we have*

$$\mathscr{N}^n(\varphi^{-n}(f)) \equiv \mathscr{N}^m(\varphi^{-m}(f)) \bmod p^{m+1}.$$

PROOF. By repeated application of Proposition 5.4.6 with $k = 0$, we have

$$\mathscr{N}^{n-m}(f) \equiv \varphi^{n-m}(f) \bmod p,$$

and again by Proposition 5.4.6, the congruence follows by applying $\mathscr{N}^m \circ \varphi^{-n}$ to $\frac{\mathscr{N}^{n-m}(f)}{\varphi^{n-m}(f)}$. □

COROLLARY 5.4.8. *Suppose that $f \in \Lambda^\times$. Then $g = \lim_{i \to \infty} \mathscr{N}^i(\varphi^{-i}(f))$ exists, and $\mathscr{N}(g) = \varphi(g)$.*

PROOF. By Corollary 5.4.7, the limit g in question exists, and we have

$$\mathscr{N}(g) = \lim_{i\to\infty} \mathscr{N}^{i+1}(\varphi^{-i}(f)) = \varphi \lim_{i\to\infty} \mathscr{N}^{i+1}(\varphi^{-(i+1)}(f)) = \varphi(g).$$

□

THEOREM 5.4.9 (Coleman). *Suppose that $u = (u_n)_{n\geq 0}$ forms a norm compatible sequence of units with $u_n \in \mathscr{O}_n^\times$. Then there exists a unique $f \in \Lambda^\times$ such that $f(\zeta_{p^n} - 1) = \varphi^n(u_n)$ for all $n \geq 0$, and it has the property that $\mathscr{N}(f) = \varphi(f)$.*

PROOF. We choose arbitrary $f_n \in \Lambda^\times$ that satisfy $f_n(\zeta_{p^n} - 1) = \varphi^n(u_n)$ for each n, and we set $g_n = \mathscr{N}^n(\varphi^{-n}(f_{2n}))$. As $(g_n)_n$ is a sequence in a compact set Λ, it has a limit point, which we call f. We claim that this f has the desired property.

For any $n \geq m$, we have

$$\begin{aligned}\varphi^m(u_m) = \varphi^m(N_{E_n/E_m}(u_n)) = \varphi^{m-n} \prod_{i=0}^{p^{n-m}-1} f_n(\zeta_{p^{n-m}}^i \zeta_{p^n} - 1) \\ = (\mathscr{N}^{n-m}\varphi^{m-n} f_n)([p]^{n-m}(\zeta_{p^n} - 1)) \\ = (\mathscr{N}^{n-m}\varphi^{m-n} f_n)(\zeta_{p^m} - 1).\end{aligned}$$

Since $2n - m \geq n$, Corollary 5.4.7, tells us that

$$\mathscr{N}^{2n-m}\varphi^{m-2n} f_{2n} \equiv \mathscr{N}^n \varphi^{-n} f_{2n} \bmod p^{n+1},$$

so

$$\varphi^m(u_m) = \mathscr{N}^{2n-m}\varphi^{m-2n} f_{2n}(\zeta_{p^m} - 1) \equiv g_n(\zeta_{p^m} - 1) \bmod p^{n+1}.$$

This forces $f(\zeta_{p^m} - 1) = \varphi^m(u_m)$ by taking the limit over the subsequence of $(g_n)_n$ converging to f.

The power series f is unique, as its difference with any other such power series would have infinitely many zeros in the maximal ideal of $\mathscr{O}_\infty$. Note that

$$\begin{aligned}\mathscr{N}(f)(\zeta_{p^n} - 1) = \mathscr{N}(f)([p](\zeta_{p^{n+1}} - 1)) = ([p] \circ \mathscr{N})(f)(\zeta_{p^{n+1}} - 1) \\ = \prod_{i=0}^{p-1} f(\zeta_{p^{n+1}}^i - 1) = N_{F_{n+1}/F_n}\varphi^{n+1}(u_{n+1}) = \varphi^{n+1}(u_n) = \varphi(f)(\zeta_{p^n} - 1)\end{aligned}$$

for all n, which similarly forces $\mathscr{N}(f) = \varphi(f)$. □

NOTATION 5.4.10. Let $\tilde{\Gamma} = \mathrm{Gal}(E_\infty/E)$. Let $U_\infty = \varprojlim_n \mathscr{O}_n^\times$ under norm maps.

We let $\sigma \in \tilde{\Gamma}$ act on $f \in \mathscr{O}[\![T]\!]$ by

$$(\sigma f)(T) = f((1+T)^{\chi(\sigma)} - 1),$$

where $\chi\colon \tilde{\Gamma} \to \mathbb{Z}_p^\times$ denotes the p-adic cyclotomic character. The group $\mathrm{Gal}(E_\infty/\mathbb{Q}_p) \cong \langle\varphi\rangle \times \tilde{\Gamma}$ then acts on $\mathscr{O}[\![T]\!]$ through the action of powers of Frobenius on coefficients and the action of $\tilde{\Gamma}$ described above.

NOTATION 5.4.11. Set

$$\mathscr{M} = \{f \in \Lambda^\times \mid \mathscr{N}(f) = \varphi(f)\}.$$

DEFINITION 5.4.12. The *Coleman power series* attached to $u = (u_n)_n \in U_\infty$ is the unique $f \in \mathscr{M}$ such that $f(\zeta_{p^n} - 1) = \varphi^n(u_n)$ for all $n \geq 0$.

COROLLARY 5.4.13. *The map $U_\infty \to \mathscr{M}$ that takes a norm compatible sequence to its associated Coleman power series is a continuous* $\mathrm{Gal}(E_\infty/\mathbb{Q}_p)$*-equivariant isomorphism.*

PROOF. That the map is an injective homomorphism is a consequence of uniqueness of the power series f attached to u by Theorem 5.4.9, and its image is in $\mathscr{M}$ by said theorem.

For any $f \in \mathscr{M}$, if we set $u_n = \varphi^{-n}(f(\zeta_{p^n} - 1))$, then

$$\varphi^n(u_n) = f(\zeta_{p^n} - 1) = \varphi^{-1}\mathscr{N}(f)(\zeta_{p^n} - 1) = \varphi^{-1}\prod_{i=0}^{p-1} f(\zeta_{p^{n+1}}\zeta_{p^n}^i - 1) = \varphi^n(N_{F_{n+1}/F_n}u_{n+1}).$$

Thus f is the power series attached to $(u_n)_n \in U_\infty$. Continuity follows from the construction of the map and is easily checked. □

LEMMA 5.4.14. *For all $f \in \Lambda$, we have*

$$\mathscr{S}([p](f)) = pf.$$

PROOF. By definition, we have that

$$([p] \circ \mathscr{S} \circ [p](f))(T) = \sum_{i=0}^{p-1} f([p](\zeta_p^i(1+T) - 1)) = pf([p](T)) = [p](pf)(T).$$

The result then follows by injectivity of $[p]$. □

NOTATION 5.4.15. Let

$$\Lambda^{\mathscr{S}=0} = \{f \in \Lambda \mid \mathscr{S}(f) = 0\} \quad \text{and} \quad \Lambda^{\mathscr{S}=p\varphi} = \{f \in \Lambda \mid \mathscr{S}(f) = p\varphi f\}.$$

PROPOSITION 5.4.16. *The sequence*

$$0 \to \mathbb{Z}_p \to \Lambda^{\mathscr{S}=p\varphi} \xrightarrow{1-[p]\varphi} \Lambda^{\mathscr{S}=0} \xrightarrow{f\mapsto \mathrm{Tr}_{E/\mathbb{Q}_p} f(0)} \mathbb{Z}_p \to 0$$

is exact.

PROOF. Any constant $a \in \mathbb{Z}_p$ satisfies $p\varphi a = pa = (\mathscr{S} \circ [p])(a) = \mathscr{S}(a)$, so sits inside $\Lambda^{\mathscr{S}=p\varphi}$. If $f \in \Lambda^{\mathscr{S}=p\varphi}$, then

$$\mathscr{S}((1-[p]\varphi)(f)) = p\varphi(f) - p\varphi(f) = 0$$

by Lemma 5.4.14, so $(1-[p]\varphi)(f) \in \Lambda^{\mathscr{S}=0}$. Thus, the sequence is well-defined.

Note that $(1-[p]\varphi)(a) = a - \varphi(a) = 0$ for $a \in \mathbb{Z}_p$ and $(1-[p]\varphi)(f)(0) = f(0) - \varphi(f(0))$ for $f \in \Lambda$, which is carried to 0 under $\mathrm{Tr}_{E/\mathbb{Q}_p}$. Thus, the sequence is a complex.

Injectivity of the first map is obvious, so we consider exactness at $\Lambda^{\mathscr{S}=p\varphi}$. If $f \in \Lambda^{\mathscr{S}=p\varphi}$ satisfies $[p]\varphi(f) = f$, then $f(0) \in \mathbb{Z}_p$, and we may replace f by $g = p^{-m}(f - f(0)) \in \Lambda^{\mathscr{S}=p\varphi}$ for $m \geq 0$ maximal, supposing $g \neq 0$. We then have

$$g \equiv bT^i \bmod (p, T^{i+1})$$

for some $b \in \mathscr{O}^\times$ and $i \geq 1$. But this congruence forces $\varphi(g)(T^p) \equiv 0 \bmod (p, T^{i+1})$, a contradiction. Thus, we have $f = f(0) \in \mathbb{Z}_p$.

We next consider exactness at $\Lambda^{\mathscr{S}=0}$. Suppose that $g \in \Lambda$ with $\mathrm{Tr}_{E/\mathbb{Q}_p} g(0) = 0$. Then $g(0) = (1-[p]\varphi)(b)$ for some $b \in \mathscr{O}$ by Hilbert's theorem 90, and

$$(1-[p]\varphi)(aT^i) \equiv aT^i \bmod (pT^i, T^{i+1})$$

for all $a \in \mathscr{O}$ and $i \geq 1$, so we can find a sequence in the image of $1-[p]\varphi$ that converges to g recursively, and thus $g = (1-p[\varphi])(f)$ for some $f \in \Lambda$. If moreover $g \in \Lambda^{\mathscr{S}=0}$, then

$$\mathscr{S}(f) = \mathscr{S}(g) + \mathscr{S}([p]\varphi(f)) = \mathscr{S}([p]\varphi(f)) = p\varphi(f).$$

Let $\xi \in \mu_{q-1}(E)$ satisfy $\mathrm{Tr}_{E/\mathbb{Q}_p} \xi = 1$. Note that $\xi(1+T) \in \Lambda^{\mathscr{S}=0}$, since

$$[p] \circ \mathscr{S}(\xi(1+T)) = \sum_{i=0}^{p-1} \zeta_p^i \xi(1+T) = 0,$$

and $[p]$ is injective. Thus, the final map is surjective. □

NOTATION 5.4.17.

a. Define $D\colon \Lambda \to \Lambda$ on $f \in \Lambda$ by $D(f) = (1+T)f'(T)$.

b. Define $\log\colon \Lambda^\times \to E[\![T]\!]$ to be the homomorphism satisfying

$$\log(1+f) = \sum_{i=1}^{\infty} \frac{(-1)^{i-1} f^i}{i}$$

for $f \in (p,T)$ and $\log(\xi) = 0$ for ξ any root of unity in $\mathscr{O}$.

c. Define $D\log\colon \Lambda^\times \to \Lambda$ on $f \in \Lambda^\times$ by $D\log(f) = (1+T)\frac{f'(T)}{f(T)}$.

REMARK 5.4.18. Note that $D\log = D \circ \log$. We also consider $D^k \log = D^{k-1} \circ D\log$ for $k \geq 1$.

LEMMA 5.4.19. *For any $f \in \Lambda^\times$, the quantity*

$$\frac{1}{p}\log\left(\frac{f^p}{[p]\varphi(f)}\right)$$

lies in Λ.

PROOF. We have

$$\varphi(f)((1+T)^p-1) \equiv \varphi(f)(T^p) \equiv f^p(T) \bmod p,$$

so $\frac{f^p}{[p]\varphi(f)} = 1+pg$ for some $g \in \Lambda$. We have

$$\frac{1}{p}\log(1+pg) = \sum_{i=1}^{\infty} \frac{(-1)^{i-1}p^{i-1}g^i}{i},$$

and the latter quantity clearly lies in Λ, since $i \geq v_p(i)+1$ for all $i \geq 1$. □

NOTATION 5.4.20. Define $\mathscr{L}\colon \Lambda^\times \to \Lambda$ on $f \in \Lambda^\times$ by

$$\mathscr{L}(f) = \log f - \frac{1}{p}\log([p]\varphi(f)).$$

PROPOSITION 5.4.21. *We have a commutative square*

$$\begin{array}{ccc} \mathscr{M} & \xrightarrow{\mathscr{L}} & \Lambda^{\mathscr{S}=0} \\ {\scriptstyle D\log}\downarrow & & \downarrow{\scriptstyle D} \\ \Lambda^{\mathscr{S}=p\varphi} & \xrightarrow{1-[p]\varphi} & \Lambda^{\mathscr{S}=0} \end{array}$$

of continuous $\mathrm{Gal}(E_\infty/\mathbb{Q}_p)$*-equivariant* $\mathbb{Z}_p$*-linear homomorphisms.*

PROOF. For any $g \in \Lambda$, we have

$$\begin{aligned} ([p]\circ\mathscr{S})(D(g)) &= \sum_{i=0}^{p-1} \zeta_p^i(1+T)g'(\zeta_p^i(1+T)-1) \\ &= \sum_{i=0}^{p-1} D(g(\zeta_p^i(1+T)-1)) \\ &= D(([p]\circ\mathscr{S})(g)), \end{aligned} \tag{5.4.1}$$

employing the chain rule in the second equality. Since $[p]$ is an injective endomorphism, it follows that $D(\Lambda^{\mathscr{S}=0}) \subseteq \Lambda^{\mathscr{S}=0}$.

For $h \in \mathscr{M}$, that $D\log h \in \Lambda^{\mathscr{S}=p\varphi}$ follows from the string of equalities

$$\begin{aligned}[p](\mathscr{S}(D\log h)) &= D(([p]\circ\mathscr{S})(\log h))\\ &= D\log(([p]\circ\mathscr{N})(h))\\ &= D\log(\varphi[p](h))\\ &= [p](p\varphi(D\log h)),\end{aligned}$$

the first using (5.4.1), the second using that log is a homomorphism, the third using $h \in \mathscr{M}$, and the fourth by definition of the endomorphism $[p]$. We also have $\mathscr{L}(h) \in \Lambda^{\mathscr{S}=0}$, since

$$\begin{aligned}[p]\circ\mathscr{S}(\mathscr{L}(h)) &= \sum_{i=0}^{p-1}\mathscr{L}(h)(\zeta_p^i(1+T)-1)\\ &= \sum_{i=0}^{p-1}\log(h)(\zeta_p^i(1+T)-1) - \log([p]\varphi(h)) = 0,\end{aligned}$$

the last step using $[p](T) = \prod_{i=0}^{p-1}(\zeta_p^i(1+T)-1)$.

Next, for any $h \in \Lambda^\times$, we have by the chain rule that

$$D\log([p]\circ h) = (1+T)\frac{(h\circ[p])'(T)}{h\circ[p](T)} = (1+T)^p\frac{h'([p](T))}{h([p](T))} = p[p](D\log h).$$

It follows from this that the diagram commutes. Galois-equivariance of log and then $\mathscr{L}$ is clear, and Galois-equivariance of D and then $D\log$ follows from the chain rule (for the $\tilde{\Gamma}$-action). □

LEMMA 5.4.22. *For every $n \geq 1$, we have*

$$\frac{1}{p}\mathscr{S}\left([p](T)^n\frac{1+T}{T}\right) = T^n\frac{1+T}{T}.$$

PROOF. Set $P = [p](T)$, and note that $P = \prod_{i=0}^{p-1}(\zeta_p^i(1+T)-1)$, and apply $D\log$ to both sides. We then have

$$p\frac{1+P}{P} = \sum_{i=0}^{p-1}\frac{\zeta_p^i(1+T)}{\zeta_p^i(1+T)-1}.$$

We have

$$[p]\left(\mathscr{S}\left(P^n\cdot\frac{1+T}{T}\right)\right) = P^n\sum_{i=0}^{p-1}\frac{\zeta_p^i(1+T)}{\zeta_p^i(1+T)+1} = pP^n\frac{1+P}{P} = [p]\left(pT^n\frac{1+T}{T}\right),$$

which yields the result. □

NOTATION 5.4.23. Let $\Omega = \mathbb{F}_q[\![T]\!]$, and define $\partial\colon \Omega^\times \to T\Omega$ by

$$\partial(f) = T\frac{f'(T)}{f(T)}$$

for $f \in \Omega$.

LEMMA 5.4.24. *We have*

$$T\Omega = \partial(\Omega^\times) + \{f^p \mid f \in T\Omega\}.$$

PROOF. We claim that

$$\partial(\Omega^\times) = \left\{ \sum_{i=1}^{\infty} a_i T^i \in \Omega \mid a_{pi} = a_i^p \text{ for all } i \geq 1 \right\}.$$

Let us denote the latter set by S. For this, we note that any $u \in \Omega^\times$ may be written uniquely as an infinite product

$$u = c \prod_{n=1}^{\infty} (1 - b_n T^n)$$

with $c \in \mathbb{F}_q^\times$ and $b_n \in \mathbb{F}_q$ for $n \geq 1$. Note that

$$\partial(1 - b_n T^n) = \frac{-n b_n T^n}{1 + b_n T^n} = -n \sum_{i=1}^{\infty} b_n^i T^{ni} \in S,$$

so $\partial(u) \in S$ as ∂ is a continuous homomorphism. Conversely, any element of S may be written as an infinite sum of terms of the form $-n\sum_{i=1}^{\infty} a^i T^{ni}$ for some $a \in \mathbb{F}_q$ and n prime to p (by using it to specify the coefficient of T^n and thereby of the T^{np^i} for $i \geq 1$), and such an element is equal to $\partial(1 - aT^n)$. Thus, we have the claim.

Note that we can pick the coefficients a_i with $p \nmid i$ of a power series in S arbitrarily. The fact that $\partial(\Omega^\times) = S$ implies the result since the pth powers of elements of $T\Omega$ are exactly the power series in $T^p\mathbb{F}_q[\![T^p]\!]$, for which we can pick the coefficients a_i with $p \mid i$ arbitrarily. □

PROPOSITION 5.4.25. *The map $D\log\colon \mathscr{M} \to \Lambda^{\mathscr{S}=p\varphi}$ is surjective and has kernel the group μ_{q-1} of roots of unity of $\mathscr{O}$ of prime-to-p order.*

PROOF. Clearly, the kernel of $D\log$ on $\Lambda^\times$ is $\mathscr{O}^\times$. Note that $a \in \mathscr{O}^\times \cap \mathscr{M}$ if and only if $a^p = \varphi(a)$. It is easy to see that no element of $1 + p\mathscr{O}$ can have this property, while every element of μ_{q-1} does. Thus, the kernel is as stated.

We claim first that it suffices to check the surjectivity of $D\log$ modulo p. Let $\Omega = \mathbb{F}_q[\![T]\!]$, and note that the formula for $D\log$ makes sense on $\Omega^\times$. Let $f \in \Lambda^{\mathscr{S}=p\varphi}$. Suppose by induction that there exists $h_k \in \mathscr{M}$ such that $D\log(h_k) \equiv f \bmod p^k\Lambda$. Then set

$$f' = \frac{1}{p^k}(f - D\log(h_k)) \in \Lambda^{\mathscr{S}=p\varphi},$$

and choose $h' \in \mathscr{M}$ such that $Dh' \equiv f' \bmod p\Lambda$. Setting $h_{k+1} = h_k + p^k h'$, we then have

$$D\log(h_{k+1}) \equiv f \bmod p^{k+1}\Lambda.$$

If we set $h = \lim_{k\to\infty} h_k$, then $D\log(h) = f$. Thus, we have the claim.

Next, we note that the reduction modulo p map $\mathscr{M} \to \Omega^\times$ is surjective. This is straightforward: if $\bar{f} \in \Omega^\times$, then choose any lift f of it to $\Lambda^\times$ and consider $g = \lim_{k\to\infty} \varphi^{-k}\mathscr{N}^k f$, which also lifts $\bar{f}$ but now lies in $\mathscr{M}$. To see that $D\log$ is surjective, it is then enough to see that the image Φ of $\Lambda^{\mathscr{S}=p\varphi}$ under reduction modulo p is contained in $\frac{1+T}{T}\partial(\Omega^\times)$.

Let $v \in \Phi$. By Lemma 5.4.24, we have that

$$\frac{T}{1+T}v = \partial(u) + f^p$$

for some $u \in \Omega^\times$ and $f \in T\Omega$. Note that $\frac{1}{p}\varphi^{-1}\mathscr{S}\colon \Lambda \to \Lambda$ reduces to an operator $\mathfrak{s}\colon \Omega \to \Omega$ that fixes both v and $\frac{1+T}{T}\partial(u)$, so fixes $\frac{1+T}{T}f^p$. On the other hand, Lemma 5.4.22 tells us that $\mathfrak{s}(\frac{1+T}{T}f^p) = \frac{1+T}{T}f$, since $[p](\varphi(f)) = f^p$ in Ω. But for $\frac{1+T}{T}f = \frac{1+T}{T}f^p$ to hold for $f \in T\Omega$, we must have $f = 0$. Therefore, $v = \frac{1+T}{T}\partial(u)$, finishing the proof. □

COROLLARY 5.4.26. *The map $D\colon \Lambda^{\mathscr{S}=0} \to \Lambda^{\mathscr{S}=0}$ is a bijection.*

PROOF. The kernel of D on Λ is $\mathbb{Z}_p$, but $\mathscr{S}(a) = pa$ for all $a \in \mathbb{Z}_p$, so D is an injection. Since $D\log$ is a surjection by Proposition 5.4.25, the exact sequence of Proposition 5.4.16 reduces us to the claim that the composite map $g \mapsto \mathrm{Tr}_{E/\mathbb{Q}_p} Dg(0)$ is surjective. For $a \in \mathscr{O}$, one may observe that $\mathscr{S}(a(1+T)) = 0$, so $a(1+T) \in \Lambda^{\mathscr{S}=0}$, and $D(a(1+T))(0) = a$. The corollary now follows by the surjectivity of trace in unramified extensions. □

We now have the following consequence of what we have proven.

PROPOSITION 5.4.27. *The diagram*

$$0 \to \mu_{q-1} \times \mathbb{Z}_p(1) \xrightarrow{(\xi,a)\mapsto \xi(1+T)^a} \mathscr{M} \xrightarrow{\mathscr{L}} \Lambda^{\mathscr{S}=0} \xrightarrow{f\mapsto \mathrm{Tr}_{E/\mathbb{Q}_p} f'(0)} \mathbb{Z}_p(1) \to 0$$

is an exact sequence in the category of compact abelian groups with continuous $\mathrm{Gal}(E_\infty/\mathbb{Q}_p)$*-actions.*

PROOF. We use Proposition 5.4.21, Proposition 5.4.25, and Corollary 5.4.26 to replace the middle terms in the exact sequence of Proposition 5.4.16. The fact that $D\log\colon \mathscr{M} \to \Lambda^{\mathscr{S}=p\varphi}$ has kernel μ_{q-1} is taken care of by adding it to the first term to preserve exactness. Note for this that the Coleman power series attached to the norm compatible sequence $(\zeta_{p^n}^a)_n$ for $a \in \mathbb{Z}_p$ is exactly $(1+T)^a$, and the map is clearly $\mathrm{Gal}(E_\infty/\mathbb{Q}_p)$-equivariant. Also, note that $Df(0) = f'(0)$, so the last map is as stated, and

$$f((1+T)^{\chi(a)} - 1)'|_{T=0} = \chi(a)f'(0),$$

so it is also $\mathrm{Gal}(E_\infty/\mathbb{Q}_p)$-equivariant. □

Recall that an $\mathscr{O}$-valued measure on $\mathbb{Z}_p$ is identified with an element of $\mathscr{O}[\![\mathbb{Z}_p]\!]$ which is isomorphic to Λ under the continuous $\mathscr{O}$-linear map that takes the group element of $[i]$ to $(1+T)^i$.

NOTATION 5.4.28. We define an operator $\Phi\colon \Lambda \to \Lambda$ on $f \in \Lambda$ by

$$\Phi(f) = f - \frac{1}{p}[p](\mathscr{S}(f)).$$

By definition, $f \in \Lambda$ satisfies $\Phi(f) = f$ if and only if $f \in \Lambda^{\mathscr{S}=0}$.

PROPOSITION 5.4.29. *A measure μ on $\mathbb{Z}_p$ is the extension by zero of a measure on $\mathbb{Z}_p^\times$ if and only if the power series attached to μ lies in $\Lambda^{\mathscr{S}=0}$. In other words, the continuous $\mathscr{O}$-linear isomorphism $\mathscr{O}[\![\mathbb{Z}_p]\!] \xrightarrow{\sim} \Lambda$ sending the group element 1 to $T+1$ restricts to an isomorphism $\mathscr{O}[\![\mathbb{Z}_p^\times]\!] \xrightarrow{\sim} \Lambda^{\mathscr{S}=0}$ of topological $\mathscr{O}$-modules.*

PROOF. Let f be the power series attached to μ, and let $\bar{f}_n \in \mathscr{O}[T]/((1+T)^{p^n}-1)$ denote its image. For the distribution $(\mu_n)_n$ attached to μ, we have that

$$f_n = \sum_{k=0}^{p^n-1} \mu_n(k)(1+T)^k \in \mathscr{O}[T]$$

lifts $\bar{f}_n$. Here, $\mu_n(k) = \int_{\mathbb{Z}_p} \chi_{k+p^n\mathbb{Z}_p} d\mu$ for $\chi_{k+p^n\mathbb{Z}_p}$ the chararacteristic function of $k+p^n\mathbb{Z}_p$. So, μ is the extension by zero of a measure on $\mathbb{Z}_p^\times$ if and only if $\mu_n(k) = 0$ for all $0 \le k \le p^n-1$ with $p \mid k$. We claim this occurs if and only if $\Phi(f) = f$, which will finish the proof.

Note that for any $a \in \mathscr{O}$, we have

$$\Phi(a(1+T)^k) = a(1+T)^k - \frac{1}{p}\sum_{i=0}^{p-1} a\zeta_p^{ik}(1+T)^k = \begin{cases} a(1+T)^k & \text{if } p \nmid k \\ 0 & \text{if } p \mid k. \end{cases}$$

Then

$$\Phi(f_n) = \sum_{\substack{k=0 \\ p\nmid k}}^{p^n-1} \mu_n(k)(1+T)^k \in \mathscr{O}[T],$$

and it is clear that

$$\Phi(f_n) \equiv f_n \bmod ((1+T)^{p^n}-1)$$

if and only if $\mu_n(k) = 0$ for all $p \mid k$. This holds for all n if and only if μ is the extension by zero of a measure on $\mathbb{Z}_p^\times$. □

Note that $\mathscr{O}[\![\mathbb{Z}_p^\times]\!] \xrightarrow{\sim} \Lambda^{\mathscr{S}=0}$ is $\mathrm{Gal}(E_\infty/\mathbb{Q}_p)$-equivariant, using the action of $\sigma \in \mathrm{Gal}(E_\infty/E)$ by multiplication by the group element of $\chi(\sigma)$ on $\mathscr{O}[\![\mathbb{Z}_p^\times]\!]$

DEFINITION 5.4.30. The *Coleman map* $\mathrm{Col}\colon U_\infty \to \mathscr{O}[\![\mathbb{Z}_p^\times]\!]$ is the map that takes $u \in U_\infty$ to the element of $\mathscr{O}[\![\mathbb{Z}_p^\times]\!]$ corresponding to $\mathscr{L}(f)$, where f is the Coleman power series attached to u.

Set $\zeta = (\zeta_{p^n})_n \in U_\infty$. For $\xi \in \mu_{q-1}$, let $\tilde{\xi} \in U_\infty$ be the unique norm compatible sequence of elements of μ_{q-1} with norm $\xi \in \mathscr{O}^\times$.

THEOREM 5.4.31. *There is an exact sequence*

$$0 \to \mu_{q-1} \times \mathbb{Z}_p(1) \xrightarrow{(\xi,a)\mapsto \xi\zeta^a} U_\infty \xrightarrow{\mathrm{Col}} \mathscr{O}[\![\mathbb{Z}_p^\times]\!] \xrightarrow{\lambda \mapsto \mathrm{Tr}_{E/\mathbb{Q}_p} \int_{\mathbb{Z}_p} x d\lambda(x)} \mathbb{Z}_p(1) \to 0$$

of continuous $\mathrm{Gal}(E_\infty/\mathbb{Q}_p)$*-equivariant homomorphisms.*

PROOF. The Coleman map is the composite

$$\mathrm{Col}\colon U_\infty \xrightarrow{\sim} \mathscr{M} \xrightarrow{\mathscr{L}} \Lambda^{\mathscr{S}=0} \xrightarrow{\sim} \mathscr{O}[\![\mathbb{Z}_p^\times]\!]$$

of the Coleman power series isomorphism with $\mathscr{L}$ and the isomorphism of Proposition 5.4.29. We use this to replace the middle part of the exact sequence of Proposition 5.4.27 with Col. That the first map is then as stated is immediate. That the final map is as stated comes from the fact that for $f \in \Lambda^{\mathscr{S}=0}$ corresponding to $\lambda \in \mathscr{O}[\![\mathbb{Z}_p^\times]\!]$ (which yields a measure on $\mathbb{Z}_p$ by extension by zero) and the distribution $(\lambda_n)_n$, we have

$$f'(0) = \lim_{n\to\infty} \sum_{k=0}^{p^n-1} k\lambda_n(k)(1+T)^{k-1}|_{T=0} = \lim_{n\to\infty} \sum_{k=0}^{p^n-1} k\lambda_n(k) = \int_{\mathbb{Z}_p} x d\lambda(x).$$

□

LEMMA 5.4.32. *Let μ be an $\mathscr{O}$-valued measure on $\mathbb{Z}_p$, and let $f \in \Lambda$ be the corresponding power series. For all $k \geq 0$, we have*

$$\int_{\mathbb{Z}_p} x^k d\mu(x) = (D^k f)(0).$$

PROOF. We have a linear functional defined by

$$L(g) = \int_{\mathbb{Z}_p} x g(x) d\mu(x)$$

for all $g \in C(\mathbb{Z}_p, \mathbb{C}_p)$. We then have

$$|L(g)| \leq \max_{a\in\mathbb{Z}_p} |g(a)|$$

for all g, so L is bounded and thus gives a measure μ_1, with a corresponding power series $h \in \Lambda$.

We claim that $h = Df$. To see this, write $f = \sum_{n=0}^\infty c_n T^n \in \Lambda$, where $c_n = \int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x)$. Note that

$$Df = \sum_{n=0}^\infty (nc_n + (n+1)c_{n+1})T^n.$$

Write $h = \sum_{n=0}^\infty e_n T^n$. Then

$$e_n = \int_{\mathbb{Z}_p} x \binom{x}{n} d\mu(x).$$

Since $x\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n}$, we have $e_n = (n+1)c_{n+1} + nc_n$ and therefore the claim.

Now, to prove the lemma, it suffices (by repeated application of the claim) to show that

$$\int_{\mathbb{Z}_p} x^k d\mu = \int_{\mathbb{Z}_p} d\mu_k,$$

where μ_k is the measure corresponding to $D^k f$. We can see this by induction, it being a consequence of the claim for $k = 1$. That is, if we know if for all measures with $k-1$ in place of k, then

$$\int_{\mathbb{Z}_p} x^{k-1} d\mu_1 = \int_{\mathbb{Z}_p} d\mu_k,$$

since $D^{k-1}(Df) = D^k f$. But by the claim, we have

$$\int_{\mathbb{Z}_p} x^{k-1} d\mu_1 = \int_{\mathbb{Z}_p} x^k d\mu,$$

so we are done. □

DEFINITION 5.4.33. For $k \geq 1$, the *kth Coates-Wiles homomorphism* $\delta_k : U_\infty \to \mathscr{O}$ takes $u \in U_\infty$ to $D^k \log(f)(0)$, where f is the Coleman power series attached to u.

LEMMA 5.4.34. *Let $\chi : \tilde{\Gamma} \xrightarrow{\sim} \mathbb{Z}_p^\times$ be the p-adic cyclotomic character. Then*

$$\delta_k(\sigma(u)) = \chi(\sigma)^k \delta_k(u)$$

for all $u \in U_\infty$ and $\sigma \in \tilde{\Gamma}$.

PROOF. Note that for any $g \in E[\![T]\!]$ and $a \in \mathbb{Z}_p$, we have

$$D(g((1+T)^a - 1)) = a(1+T)^a g'((1+T)^a - 1) = a(Dg)((1+T)^a - 1).$$

So, by recursion we see that

$$D^k(g((1+T)^a - 1)) = a^k (Dg)((1+T)^a - 1). \tag{5.4.2}$$

We can apply this with $g = \log f$ for f the Coleman power series attached to $u \in U_\infty$ and $a = \chi(\sigma)$ for $\sigma \in \tilde{\Gamma}$. For this, note that the Coleman power series attached to $\sigma(u)$ is $\sigma(f)(T) = f((1+T)^{\chi(\sigma)} - 1)$. Therefore, we have

$$D^k(\log \sigma(f)) = \chi(\sigma)^k (D^k \log f)(\sigma(T)),$$

and plugging in 0, we get the desired formula. □

PROPOSITION 5.4.35. *For $u \in U_\infty$, let $\lambda_u = \mathrm{Col}(u)$, which we view as an $\mathscr{O}$-valued measure on $\mathbb{Z}_p^\times$. We then have*

$$\int_{\mathbb{Z}_p^\times} x^k d\lambda_u = (1 - p^{k-1}\varphi)\delta_k(u)$$

for all $k \geq 1$.

PROOF. Let $f \in \Lambda^\times$ denote the power series attached to u, and note that

$$\begin{aligned}\int_{\mathbb{Z}_p^\times} x^k d\lambda_u &= (D^k \mathscr{L}(f))(0) \\ &= D^k \log(f)(0) - p^{-1} D^k \log(\varphi(f) \circ [p])(0) \\ &= \delta_k(u) - p^{k-1} D^k \log \varphi(f)(0) \\ &= (1 - p^{k-1}\varphi)\delta_k(u),\end{aligned}$$

the second-to-last step following from (5.4.2). □

CHAPTER 6

The Iwasawa main conjecture

6.1. Semi-local units modulo cyclotomic units

Let $F = \mathbb{Q}(\mu_{mp})$, where $p \nmid m$ and $m \not\equiv 2 \bmod 4$. Let us first observe that we have a map $\mathrm{Col}\colon \mathscr{U}_\infty^{(\chi)} \to \Lambda_\chi$. Note that each place of $\mathbb{Q}(\mu_m)$ over p is totally ramified in F_∞. Let V_p denote the set of places over p in any intermediate field. Recall that

$$\mathscr{U}_\infty \cong \bigoplus_{v \in V_p} \mathscr{U}_{v,\infty}.$$

Let $\mathscr{O}$ be the valuation ring of a place w of $\mathbb{Q}(\mu_m)$ over p. (Note that such places are totally ramified in $F = \mathbb{Q}(\mu_{mp})$, and even in F_∞.) Then $\mathscr{O}$ is free of rank one over $\mathbb{Z}_p[\Delta_p]$, for Δ_p the decomposition group at p in $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. Giving

$$\bigoplus_{v \in V_p} \mathscr{O}$$

the structure of a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})]$-module by allowing Δ to permute the factors, it is then is free of rank one as a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})]$-module, and we can think of 1 in the term for w as a generator. Similarly, then, we obtain

$$\tilde{\Lambda} = \mathbb{Z}_p[\![\mathbb{Z}_{p,m}^\times]\!] \cong \prod_{v \in V_p} \mathscr{O}[\![\mathbb{Z}_p^\times]\!],$$

and we can use this to define a Coleman map $\mathrm{Col}\colon \mathscr{U}_\infty \to \tilde{\Lambda}$ as the direct sum of the Coleman maps at the places over p.

PROPOSITION 6.1.1. *There is a homomorphism* $\mathrm{Col}\colon \mathscr{U}_\infty \to \tilde{\Lambda}$ *induced by the Coleman maps at the places of* F_∞ *above* p*, fitting in an exact sequence*

$$0 \to \mathbb{Z}_p[\Delta/\Delta_p](1) \to \mathscr{U}_\infty \xrightarrow{\mathrm{Col}} \tilde{\Lambda} \to \mathbb{Z}_p[\Delta/\Delta_p](1) \to 0$$

of $\tilde{\Lambda}$*-modules.*

COROLLARY 6.1.2. *Let* χ *be a nontrivial Dirichlet* p*-adic character of conductor dividing* mp*. Then the Coleman map induces a map* $\mathscr{U}_\infty^{(\chi)} \to \Lambda_\chi$ *which is an isomorphism if and only if* $\chi\omega^{-1}(p) - 1 \in \mathscr{O}_\chi^\times$.

We aim to prove the following theorem that, at least in the case of $F = \mathbb{Q}(\mu_p)$, was proven by Iwasawa.

THEOREM 6.1.3. *Let χ be a nontrivial, even primitive Dirichlet character of conductor m or mp, where p is an odd prime and m is a positive integer prime to p. Let $F = \mathbb{Q}(\mu_{mp})$, and let F_∞ be its cyclotomic $\mathbb{Z}_p$-extension. Then there is an exact sequence*

$$0 \to A_\chi(1) \to \mathscr{U}_\infty^{(\chi)}/\mathscr{C}_\infty^{(\chi)} \to \Lambda_\chi/(g'_\chi) \to 0,$$

where $A_\chi = \mathscr{O}_\chi/(\chi\omega^{-1}(p)-1)$, and where $g'_\chi = T^{-\delta}g_\chi$ for $\delta = 1$ if $\chi\omega^{-1}(p) = 1$ and $\delta = 0$ otherwise, where $g_\chi \in \Lambda_\chi$ satisfies

$$g_\chi(u^s - 1) = L_p(\chi, 1-s)$$

for all $s \in \mathbb{Z}_p$.

COROLLARY 6.1.4. *With the notation of Theorem 6.1.3, suppose that $\chi\omega^{-1}(p) - 1 \in \mathscr{O}_\chi^\times$. Then*

$$\mathscr{U}_\infty^{(\chi)}/\mathscr{C}_\infty^{(\chi)} \cong \Lambda_\chi/(g_\chi).$$

PROPOSITION 6.1.5. *Suppose that $p \nmid \varphi(m)$. Let χ be a nontrivial, even Dirichlet p-adic character of conductor dividing mp, and let f be the prime-to-p part of its conductor. The Λ_χ-module $\mathscr{C}_\infty^{(\chi)}$ is generated by the image of the norm compatible sequence $(1-\zeta_{fp^n})_n$.*

PROOF. Since only primes over p ramify in F_∞/F, the norm compatible sequences of elements of $F_n^\times$ are all norm compatible sequences of p-units. The group of norm compatible sequences of cyclotomic p-units in F_∞/F is generated as a $\tilde{\Lambda}$-module by $(1-\zeta_{dp^n})_n$ for d dividing m. Such a sequence is of true units if $f \neq 1$. From this, it is easy to see that $\mathscr{C}_\infty$ is similarly generated by the $(1-\zeta_{dp^n})_n$ and $((1-\zeta_{p^n})^{\sigma_c - 1})_n$, where $c \in \mathbb{Z}$ is a primitive root modulo p. The elements $e_\chi(1-\zeta_{dp^n})_n$ vanish unless f is a multiple of d. On the other hand, $e_\chi(1-\zeta_{dp^n})$ for d a multiple of f equals e_χ times the norm for $\mathbb{Q}(\zeta_{dp^n})/\mathbb{Q}(\zeta_{fp^n})$ of the elements $(1-\zeta_{dp^n})$. That is, $e_\chi(1-\zeta_{dp^n})_n$ is a $\tilde{\Lambda}$-multiple of $e_\chi(1-\zeta_{fp^n})_n$ for f dividing d. □

Let us now focus on the case that $F = \mathbb{Q}(\mu_p)$, for which we suppose that $E = \mathbb{Q}_p$. Note that $U_\infty = \mathscr{U}_\infty \times \mu_{p-1}$. Consider the cyclotomic unit

$$u_{n,c} = \frac{\zeta_{p^n}^{-c/2} - \zeta_{p^n}^{c/2}}{\zeta_{p^n}^{-1/2} - \zeta_{p^n}^{1/2}}$$

for c prime to p, and let $u_c = (u_{n,c})_n \in U_\infty$. Let $\tilde{\zeta}_{p,c} = \mathrm{Col}(u_{n,c})$.

PROPOSITION 6.1.6. *For $k \geq 1$, we have*

$$\int_{\mathbb{Z}_p^\times} x^k d\tilde{\zeta}_{p,c}(x) = (1-c^k)(1-p^{k-1})\zeta(1-k) = (1-c^k)L_p(\omega^k, 1-k).$$

PROOF. We employ the Coleman power series

$$f(T) = \frac{(1+T)^{-c/2} - (1+T)^{c/2}}{(1+T)^{-1/2} - (1+T)^{1/2}}$$

and the change of variables $T = e^t - 1$. By Lemma 5.4.32, we have that

$$\delta_k(u_c) = \frac{d^k}{dt^k} \log f(e^t - 1) \mid_{t=0} .$$

We have

$$\begin{aligned}\frac{d}{dt}\log f(e^t-1) &= \frac{1}{2}\left(\frac{1}{e^{-t}-1} - \frac{1}{e^t-1}\right) - \frac{c}{2}\left(\frac{1}{e^{-ct}-1} - \frac{1}{e^{ct}-1}\right) \\ &= \sum_{k=0}^{\infty} \frac{B_k}{2\cdot k!}((-t)^{k-1} - t^{k-1} + c((ct)^{k-1} - (-ct)^{k-1})) = \sum_{k=0}^{\infty} \frac{B_k}{k!}(c^k - 1)t^{k-1},\end{aligned}$$

so

$$\delta_k(u_c) = (c^k - 1)\frac{B_k}{k} = (1 - c^k)\zeta(1-k).$$

The result then follows from Proposition 5.4.35. □

We then have the following.

COROLLARY 6.1.7. *The $\mathbb{Z}_p$-valued measure $E_c^{(0)}$ on $\mathbb{Z}_p^\times$ satisfying*

$$\int_{\mathbb{Z}_p^\times} h(x) dE_c^{(0)}(x) = \int_{\mathbb{Z}_p^\times} x^{-1} h(x) dE_c^{(1)}(x)$$

for all $h \in C(\mathbb{Z}_p, \mathbb{C}_p)$ is equal to $\tilde{\zeta}_{p,c}$.

SKETCH OF PROOF OF THEOREM 6.1.3 FOR $\mathbb{Q}(\mu_p)$. Note that $\mathscr{C}_\infty$ is topologically generated by the elements u_c, and in particular it is generated as a $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] \cong \Lambda[\Delta]$-module, where $\Delta = \mathrm{Gal}(F_\infty/\mathbb{Q}_\infty)$, by u_c for any integer c that is a primitive root modulo p. Proposition 6.1.6 tells us that

$$\mathrm{Col}(\mathscr{C}_\infty) = \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]\tilde{\zeta}_{p,c}.$$

Note that $\tilde{\zeta}_p = (1 - \sigma_c)^{-1}\tilde{\zeta}_{p,c}$ is independent of c, though it is not quite integral, though it becomes integral up application of any element in the augmentation ideal I of $\Lambda[\Delta]$. If $k \not\equiv 0 \bmod p-1$, then $1 - c^k \in \mathbb{Z}_p^\times$. The "equivariant" version of Iwasawa's theorem is then proven: it reads

$$\mathscr{U}_\infty/\mathscr{C}_\infty \cong \Lambda[\Delta]/I\tilde{\zeta}_p.$$

Recall that a character ω^k of Δ defines an in this case surjective homomorphism $\widetilde{\omega^k}\colon \Lambda[\Delta] \to \Lambda$ of Λ-algebras. For even k, the image $\widetilde{\omega^k}(\tilde{\zeta}_p)$ is nonzero, and it is integral if and only if $k \not\equiv 0 \bmod p-1$. A simple check yields using Corollary 6.1.7 yields that the power series corresponding to $\widetilde{\omega^k}(\tilde{\zeta}_p)$ (or T times it if $k \equiv 0 \bmod p-1$) is g_{ω^k}, so we have Iwasawa's theorem. □

6.2. The Ferrero-Washington theorem

THEOREM 6.2.1 (Ferrero-Washington). *Let F be a finite abelian extension of $\mathbb{Q}$, and let F_∞ be its cyclotomic $\mathbb{Z}_p$-extension for a prime p. Then $\mu(X_\infty) = 0$.*

The following is immediate from the theorem and Proposition 3.4.2.

COROLLARY 6.2.2. *Let F be an abelian extension of $\mathbb{Q}$, and let F_∞ be its cyclotomic $\mathbb{Z}_p$-extension for an odd prime p. Then the p-torsion subgroup of X_∞^- is zero.*

In this section, we prove the Ferrero-Washington theorem in the case of $F = \mathbb{Q}(\mu_p)$ for an odd prime p. We follow their original proof in this case.

NOTATION 6.2.3. For $a \in \mathbb{Z}_p$ and a nonnegative integer m, let $[a]_m \in \mathbb{Z}$ denote the unique integer with $0 \leq a < p^{m+1}$ to which a is congruent modulo p^{m+1}. Let $\delta_0(a) = [a]_0$ and $\delta_m(a) = p^{-m}([a]_m - [a]_{m-1})$ if $m \geq 1$.

We may think of $\delta_m(a)$ as the coefficient of p^m in the usual p-adic expansion of a.

PROPOSITION 6.2.4. *The μ-invariant of X_∞ is nonzero if and only if there exists an even integer $k \not\equiv 0 \bmod p-1$ such that*

$$\sum_{\xi \in \mu_{p-1}(\mathbb{Z}_p)} \delta_m(a\xi)\xi^{k-1} \equiv 0 \bmod p$$

for all $m \geq 0$ and all $a \in \mathbb{Z}_p$.

PROOF. Since $X_\infty^{(\omega)}$ is trivial, we need only show that the μ-invariant μ_k of $X_\infty^{(\omega^{1-k})}$ is zero for every even k with $2 \leq k \leq p-3$. Since f_{ω^k} annihilates $X_\infty^{(\omega^{1-k})}$, it suffices to show that f_{ω^k} is not in $p\mathbb{Z}_p[\![T]\!]$. For $b \in \mathbb{Z}_p$, let $1 \leq i_m(b) \leq p^m$ be such that $\langle b \rangle_p \equiv (1+p)^{i_m(b)} \bmod p^{m+1}$. The expression for f_{ω^k} given by Remark 5.3.10 reduces to

$$f_{\omega^k} \equiv -\frac{1}{p^m} \sum_{\substack{b=1 \\ p \nmid b}}^{p^{m+1}} b\omega^{k-1}(b)(T+1)^{p^m - i_m(b)} \bmod \omega_m.$$

Since $\omega_m \equiv T^{p^m} \bmod p$, the congruence holds modulo (p, T^{p^m}) as well. To say that μ_k is nonzero is then equivalent to saying that every coefficient of a power of $T+1$ in each such expansion as we vary m is zero. Let $T_m(a)$ denote the set of positive integers $b < p^{m+1}$ that are prime to p and satisfy $i_m(b) \equiv i_m(a) \bmod p^m$. By what we have just said, we have $\mu_k > 0$ if and only if

$$\sum_{b \in T_m(a)} b\omega^{k-1}(b) \equiv 0 \bmod p^{m+1}$$

for all $a \in \mathbb{Z}_p$ and $m \geq 0$. Note that $i_m(b) \equiv i_m(a) \bmod p^{m+1}$ if and only if there exists $\xi \in \mu_{p-1}(\mathbb{Z}_p)$ such that $[b]_m = [\xi a]_m$. For given $a \equiv 1 \bmod p$ and ξ there is exactly one $0 < b < p^m$ with $p \nmid b$ having this property. Since $\omega(b) = \omega(\xi)$, we then have $\mu_k > 0$ if and only if

$$\sum_{\xi \in \mu_{p-1}(\mathbb{Z}_p)} [a\xi]_m \xi^{k-1} \equiv 0 \bmod p^{m+1}.$$

As $\delta_0(a\xi) = [a\xi]_0$ and $\delta_m(a\xi) = p^{-m}([a\xi]_m - [a\xi]_{m-1})$ for all $m \geq 1$, the result follows from the equivalence of $\mu_k > 0$ with the latter congruences. □

DEFINITION 6.2.5. A sequence $(b_i)_{i\geq 1}$ of tuples in $[0,1)^r$ is *uniformly distributed* if for every product $U \subseteq (0,1)^r$ of open intervals in $(0,1)$, the volume of U is proportional by a positive real number, independent of U, to the density of the b_i in U, which is to say the limit of $\frac{1}{N}|\{i \leq N \mid b_i \in U\}|$ as $N \to \infty$.

DEFINITION 6.2.6. For $r \geq 1$, we say that $(a_1, \ldots, a_r) \in \mathbb{Z}_p^r$ is *normal* if the sequence of tuples

$$(p^{-m}[a_1]_{m-1}, \ldots, p^{-m}[a_r]_{m-1})$$

with $m \geq 1$ is uniformly distributed in $[0,1)^r$.

We omit the proof of the following.

THEOREM 6.2.7 (Weyl). *A sequence $(b_{i,1}, \ldots, b_{i,r})_{i\geq 1}$ of tuples in $[0,1)^r$ is uniformly distributed if and only if for every tuple $(t_1, \ldots, t_r) \in \mathbb{Z}^r - \{0\}$, we have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} e^{2\pi i \sum_{j=1}^r b_{i,j} t_j} = 0.$$

PROPOSITION 6.2.8. *For $r \geq 1$, let $b_1, \ldots, b_r \in \mathbb{Z}_p$ be such that $b_1, \ldots, b_r$ are $\mathbb{Q}$-linearly independent. Then the complement of the set of $a \in \mathbb{Z}_p$ with $(ab_1, \ldots, ab_r)$ normal has Haar measure zero.*

PROOF. Let $t = (t_1, \ldots t_r) \in \mathbb{Z}^r - \{0\}$, and let $c = \sum_{j=1}^r b_j t_j$, which is nonzero by the linear independence of the b_j. For $a \in \mathbb{Z}_p$, we have

$$[ac]_{m-1} \equiv ac \equiv \sum_{j=1}^{r} ab_j t_j \equiv \sum_{j=1}^{r} [ab_j]_{m-1} t_j \bmod p^m.$$

Therefore, that $(ab_1, \ldots, ab_r)$ is normal is equivalent by the criterion of Weyl to the statement that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{m=1}^{N} e^{2\pi i p^{-m}[ac]_{m-1}} = 0$$

for all t. We claim that this holds outside a set of a of measure zero for each t. Since there are only countably many t, this implies the result. We also suppose that $t \notin p\mathbb{Z}^r$, as the convergence to zero of limit in question is unaffected by dividing by a power of p.

Set

$$p_N(a) = \frac{1}{N}\sum_{m=1}^{N} e^{2\pi i p^{-m}[ac]_{m-1}},$$

and note that

$$\int_{\mathbb{Z}_p} |p_N(a)|^2 da = \frac{1}{N} + \frac{1}{N^2}\sum_{\substack{m,n=1\\ m\neq n}}^{N} \int_{\mathbb{Z}_p} e^{2\pi i(p^{-n}[ac]_{n-1} - p^{-m}[ac]_{m-1})} da = \frac{1}{N},$$

each integral in the latter sum being zero, being a multiple of a sum over all p^nth (resp., p^mth) roots of unity if $n > m$ (resp., $m > n$). It follows that

$$\sum_{M=1}^{\infty} \int_{\mathbb{Z}_p} |p_{M^2}(a)|^2 da = \sum_{M=1}^{\infty} \frac{1}{M^2} = \frac{\pi^2}{6}$$

is finite, which forces $\lim_{M\to\infty} p_{M^2}(a) = 0$ outside of a set of measure zero. Note also that for any $N \in \mathbb{Z}$ with $M^2 \leq N < (M+1)^2$, we have

$$|p_N(a)| < |p_{M^2}(a)| + \frac{2M}{N} \leq |p_{M^2}(a)| + \frac{2}{M},$$

as $p_N(a) - p_{M^2}(a)$ is a sum of $N - M^2$ roots of unity. Thus $(p_N(a))_N$ has limit 0 outside of the same measure zero set. □

PROPOSITION 6.2.9. *Set $s = \frac{p-1}{2}$ and $r = \varphi(p-1)$. Let $b_1, \ldots, b_s \in \mathbb{Z}_p$ be such that $(b_1, \ldots, b_r)$ is normal, $b_i b_1^{-1} \notin \mathbb{Z}$ for all $2 \leq i \leq s$, and*

$$b_i = \sum_{j=1}^{r} c_{i,j} b_j$$

for some $c_{i,j} \in \mathbb{Z}$ for all $r < i \leq s$. Then there exist nonnegative integers m and n such that $\delta_n(b_j) = \delta_m(b_j)$ for all $2 \leq j \leq s$, while $\delta_n(b_1) = 1$ and $\delta_m(b_1) = 0$.

PROOF. Take $x_1 = \frac{1}{p}$, and let $x_2, \ldots, x_r \in (0,1)$ be such that the $x_1, \ldots, x_r$ are $\mathbb{Q}$-linearly independent. For $r < i \leq s$, set

$$x_i = \left\langle \sum_{j=1}^{r} c_{i,j} x_j \right\rangle.$$

If $x_i \in \mathbb{Q}$ for such an i, then $c_{i,j} = 0$ for $2 \leq j \leq r$ by the assumed linear indepedence, so $x_i = c_{1,j} x_1$. But this would imply that $b_i b_1^{-1} \in \mathbb{Z}$, contradicting our hypotheses. Thus, the x_i for $2 \leq i \leq s$ are all irrational.

Let $y_1 \in (0, \frac{1}{p})$, set $y_i = x_i$ for $2 \leq i \leq r$, and set $y_i = \langle \sum_{j=1}^{r} c_{i,j} y_j \rangle$ for $r < i \leq s$. Suppose that $x_1 - y_1$ is sufficiently small so that for each $2 \leq i \leq s$, we have an $0 \leq a < p$ such that $x_i, y_i \in (\frac{a}{p}, \frac{a+1}{p})$. Since $(b_1, \ldots, b_r)$ is normal, there exists an $m \geq 0$ such that

$$|p^{-m-1}[b_i]_m - y_i| < \varepsilon$$

for a given choice of $\varepsilon > 0$. for all $1 \leq i \leq r$. For $r < i \leq s$, we have

$$p^{-m-1}\left([b_i]_m - \sum_{j=1}^{r} c_{i,j}[b_j]_m\right) \in \mathbb{Z},$$

so

$$|p^{-m-1}[b_i]_m - y_i| \leq \sum_{j=1}^{r} |c_{i,j}||p^{-m-1}[b_j]_m - y_i| < \sum_{i=1}^{r} |c_{i,j}| \cdot \varepsilon,$$

noting that both terms are in $(0,1)$ in the middle step. We may take ε small enough that small enough $p^{-m-1}[b_i]_m$ lies in the same open interval $(\frac{a}{p}, \frac{a+1}{p})$ as y_i for all $1 \leq i \leq s$. We then have

$$p^{-1}\delta_m(b_i) < p^{-m}[b_i]_m < p^{-1}(\delta_m(b_i)+1),$$

so $\delta_m(b_i) = \lfloor py_i \rfloor$, and we note that $\lfloor py_i \rfloor = \lfloor px_i \rfloor$ for $i \geq 2$. Since $y_1 < \frac{1}{p}$, we have $\delta_m(b_1) = 0$.

Now repeat the argument, but this time replace y_1 with z_1 where $\frac{1}{p} < z_1 < \frac{2}{p}$ and $z_1 - x_1$ is small enough. We then again obtain an $n \geq 0$ such that $\delta_n(b_i) = \lfloor px_i \rfloor$, this time for all i, noting that $\lfloor px_1 \rfloor = 1$. Thus $\delta_n(b_i) = \delta_m(b_i)$ for all $i \geq 2$, while $\delta_n(b_1) = 1 > 0 = \delta_m(b_1)$. □

PROOF OF THEOREM 6.2.1 FOR $F = \mathbb{Q}(\mu_p)$ WITH p ODD. Set $s = \frac{p-1}{2}$ and $r = \varphi(p-1)$. Let ξ be a primitive $(p-1)$th root of unity. Note that $\xi^{s+1} = -\xi$, so for $a \in \mathbb{Z}_p$ we have $\delta_m(-a\xi) = p - 1 - \delta_m(a\xi)$ so long as $m \geq 1 + v_p(a)$. It follows that

$$\sum_{i=1}^{p-1} \delta_m(a\xi)\xi^{i(k-1)} = 2\sum_{i=1}^{s} \delta_m(a\xi)\xi^{i(k-1)} - (p-1)\sum_{i=1}^{s} \xi^{i(k-1)} \tag{6.2.1}$$

for all $a \in \mathbb{Z}_p$ and even integers k. The ξ^i with $1 \leq i \leq r$ are linearly independent: in fact, they form a $\mathbb{Z}$-basis of $\mathbb{Z}[\mu_{p-1}] \subset \mathbb{Z}_p$. Let $a \in \mathbb{Z}_p$ be such that $(a\xi, a\xi^2, \ldots, a\xi^r)$ is normal, and set $b_i = a\xi^i$ for each $1 \leq i \leq s$. Then the conditions of Proposition 6.2.9 are satisfied for the b_i, so we can find nonnegative integers m and n as in its statement.

Suppose that $\mu(X_\infty^-) > 0$. By Proposition 6.2.4, there exists an even $2 \leq k \leq p-1$ such that

$$\sum_{i=1}^{p-1} \delta_l(a\xi)\xi^{i(k-1)} \equiv 0 \bmod p$$

for all $l \geq 0$. Applying (6.2.1), we then have that

$$\begin{aligned} 2\xi^{k-1} &= 2\left(\sum_{i=1}^{s} \delta_n(a\xi)\xi^{i(k-1)} - \sum_{i=1}^{s} \delta_m(a\xi)\xi^{i(k-1)}\right) \\ &= \sum_{i=1}^{p-1} \delta_n(a\xi)\xi^{i(k-1)} - \sum_{i=1}^{p-1} \delta_m(a\xi)\xi^{i(k-1)} \equiv 0 \bmod p, \end{aligned}$$

providing the desired contradiction. □

6.3. The main conjecture over $\mathbb{Q}$

In its most classical form, the main conjecture of Iwasawa theory, or Iwasawa main conjecture, states that the characteristic ideals of odd eigenspaces of X_∞ are generated by the power series interpolating corresponding p-adic L-functions in the case that F is an abelian field and F_∞ is its cyclotomic $\mathbb{Z}_p$-extension. We refer to this as the main conjecture over the rationals, since it deals with fields cut out by abelian characters of the absolute Galois group over $\mathbb{Q}$. Its formulation in print is due to Greenberg. While the main conjecture was actually proven by Mazur and Wiles in 1984, we shall label it as a conjecture here in order to discuss its equivalent forms. We discuss its proof in later sections.

CONJECTURE 6.3.1 (The Iwasawa Main Conjecture). *Let p be an odd prime. Let χ be a nontrivial, even finite order p-adic character of $G_\mathbb{Q}$ of conductor not divisible by p^2, and let F be the the fixed field of the kernel of χ. For the cyclotomic $\mathbb{Z}_p$-extension F_∞ of F, we have*

$$\mathrm{char}_{\Lambda_\chi} X_\infty^{(\omega\chi^{-1})} = (f_\chi),$$

where $f_\chi \in \Lambda_\chi$ satisfies

$$f_\chi((1+p)^s - 1) = L_p(\chi, s)$$

for all $s \in \mathbb{Z}_p$.

We can reformulate the main conjecture in terms of the p-ramified Iwasawa module.

PROPOSITION 6.3.2. *The Iwasawa main conjecture is equivalent to the statement that*

$$\mathrm{char}_{\Lambda_\chi} \mathfrak{X}_\infty^{(\chi)} = (g_\chi),$$

where $g_\chi \in \Lambda_\chi$ satisfies

$$g_\chi((1+p)^{1-s} - 1) = L_p(\chi, s)$$

for all $s \in \mathbb{Z}_p$.

PROOF. By Corollary 3.4.9, we have a pseudo-isomorphism

$$\mathfrak{X}_\infty^{(\chi)} \simeq (X_\infty^{(\omega\chi^{-1})})^\iota(1),$$

and pseudo-isomorphic modules have the same characteristic ideal. We then have

$$g_\chi(T) = f_\chi(u(1+T)^{-1} - 1),$$

and the result follows. □

We can also reformulate the main conjecture as a comparison between global units modulo cyclotomic units and the plus part of the Iwasawa module. This formulation eschews the use of L-functions.

THEOREM 6.3.3. *The Iwasawa main conjecture is equivalent to the statement that*

$$\mathrm{char}_{\Lambda_\chi}(\mathscr{E}_\infty^{(\chi)}/\mathscr{C}_\infty^{(\chi)}) = \mathrm{char}_{\Lambda_\chi}(X_\infty^{(\chi)}).$$

PROOF. From the first exact sequence of Proposition 3.3.6, we obtain an exact sequence

$$0 \to \mathscr{E}_\infty^{(\chi)}/\mathscr{C}_\infty^{(\chi)} \to \mathscr{U}_\infty^{(\chi)}/\mathscr{C}_\infty^{(\chi)} \to \mathfrak{X}_\infty^{(\chi)} \to X_\infty^{(\chi)} \to 0.$$

Iwasawa's theorem tells us that the characteristic ideal of the second term has characteristic ideal (g_χ). Since the alternating product of characteristic ideals of Iwasawa modules in an exact sequence of finite length is 1, we have that

$$\mathrm{char}_{\Lambda_\chi}(\mathscr{E}_\infty^{(\chi)}/\mathscr{C}_\infty^{(\chi)}) = \mathrm{char}_{\Lambda_\chi}(X_\infty^{(\chi)})$$

if and only if $\mathrm{char}_{\Lambda_\chi}\mathfrak{X}_\infty^{(\chi)} = (g_\chi)$. The latter statement is an equivalent form of the main conjecture by Proposition 6.3.2. □

Mazur and Wiles proved the following interesting consequence of the main conjecture.

THEOREM 6.3.4 (Mazur-Wiles). *Let p, F, χ, and $\mathscr{O}_\chi$ be as in the Iwasawa main conjecture, and suppose that χ has prime-to-p order. We then have*

$$|A_F^{(\omega\chi^{-1})}| = |B_{1,\chi\omega^{-1}}|_\chi^{-1},$$

where $|\cdot|_\chi$ denotes the normalized multiplicative valuation on the unramified extension $\mathscr{O}_\chi$ of $\mathbb{Z}_p$.

In particular, the converse to Herbrand's theorem (due to Ribet) holds.

We also note that any one divisibility of characteristic ideals in the main conjecture for all χ of the Galois group of a given totally real abelian field implies the other. This is a consequence of the following result, which can be derived using the analytic class number formula (for instance, using Sinnott's work).

PROPOSITION 6.3.5. *Let F be an abelian, CM extension of $\mathbb{Q}$ of conductor not divisible by p^2, and let $G = \mathrm{Gal}(F^+/\mathbb{Q})$. Let $f = \prod_{\chi\in\hat{G}} f_\chi \in \mathbb{Z}_p[\![T]\!]$, and let $\mu(f) = \mu(\Lambda/(f))$ and $\lambda(f) = \lambda(\Lambda/(f))$. Then*

$$\mu(X_\infty^-) = \mu(f) \quad \text{and} \quad \lambda(X_\infty^-) = \lambda(f).$$

As a final note, we treat the powers of the variable T itself that appear in the ideals of the main conjecture.

PROPOSITION 6.3.6. *We have that $T \mid \mathrm{char}_\Lambda X_\infty^{(\omega\chi^{-1})}$ if and only if $\chi\omega^{-1}(p) = 1$.*

PROOF. Let $N_{F_\infty/F}\colon \mathscr{E}_\infty \to \mathscr{E}_F$ be projection to the first term of a norm compatible sequence. Consider the exact sequence

$$\mathscr{E}_F/N_{F_\infty/F}\mathscr{E}_\infty \to \ker\left(\bigoplus_{v\in V_p(F)} \Gamma_v \to \Gamma\right) \to (X_\infty)_\Gamma \to A_F$$

that exists by Theorem 1.3.14. We take $\omega\chi^{-1}$-eigenspaces. Since A_F is finite, $\mathscr{E}_F^{(\omega\chi^{-1})} = 0$, and $\Gamma^{(\omega\chi^{-1})} = 0$, we have that

$$(X_\infty^{(\omega\chi^{-1})})_\Gamma \simeq \left(\bigoplus_{v\in V_p(F)} \Gamma_v\right)^{(\omega\chi^{-1})},$$

and the latter isomorphic to $\mathbb{Z}_p$ or 0 depending on whether $\chi\omega^{-1}(p) = 1$ or not. □

THEOREM 6.3.7 (Ferrero-Greenberg). *We have $T^2 \nmid f_\chi$, and $T \mid f_\chi$ if and only if $\chi\omega^{-1}(p) = 1$.*

We can see from this (and Sinnott's work, for instance) that $T^2 \nmid \mathrm{char}_\Lambda X_\infty^{(\omega\chi^{-1})}$ for all χ as well, so the same power of T divides both f_χ and $\mathrm{char}_\Lambda X_\infty^{(\omega\chi^{-1})}$.

6.4. The Euler system of cyclotomic units

Let $m > 1$ be a positive integer, and let $F = \mathbb{Q}(\mu_m)^+$. Let $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. Consider the set $\mathscr{P}$ of nontrivial products of distinct prime numbers that split completely in F, which is to say are congruent to ± 1 modulo m. For any $r \in \mathscr{P}$, we set $F_r = F(\mu_r)$ for brevity, and we let $G_r = \mathrm{Gal}(F_r/F)$, which is isomorphic to $\mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})$ by restriction. For $\ell \mid r$, we view G_ℓ as the subgroup $\mathrm{Gal}(F_r/F_{r/\ell})$ of G_r. With this identification, if we let $N_r \in \mathbb{Z}[G_r]$ be the norm element, we then have

$$N_r = \prod_{\ell\mid r} N_\ell,$$

the product being (implicitly) taken over primes. Fix a generator σ_ℓ of G_ℓ for each prime $\ell \in \mathscr{P}$, and let φ_ℓ denote the Frobenius in G_r for any $r \in \mathscr{P}$ not divisible by ℓ.

DEFINITION 6.4.1. For $r \in \mathscr{P}$, the rth *derivative element* is

$$D_r = \prod_{\ell\mid r} D_\ell \in \mathbb{Z}[G_r]$$

where for a prime $\ell \in \mathscr{P}$, we set

$$D_\ell = \sum_{i=1}^{\ell-2} i\sigma_\ell^i.$$

The ℓth derivative element has the following key property.

LEMMA 6.4.2. *For $\ell \in \mathscr{P}$, we have*

$$(\sigma_\ell - 1)D_\ell = \ell - 1 - N_\ell.$$

PROOF. We have

$$\sigma_\ell D_\ell = \sum_{i=1}^{\ell-2} i\sigma_\ell^{i+1} = \sum_{i=1}^{\ell-1}(i-1)\sigma_\ell^i = \sum_{i=1}^{\ell-1} i\sigma_\ell^i - \sum_{i=1}^{\ell-1}\sigma_\ell^i = (D_\ell + \ell - 1) - N_\ell.$$

□

Fix a primitive mth root a unity ζ_m and a primitive ℓth root of unity ζ_ℓ for each $\ell \in \mathscr{P}$. For $r \in \mathscr{P}$, set $\zeta_r = \prod_{\ell | r} \zeta_\ell$. Let

$$\alpha_r = (\zeta_m \zeta_r - 1)(\zeta_m^{-1}\zeta_r - 1) \in F_r,$$

which is a cyclotomic unit if $r \neq 1$ or m is composite. It has two key properties: the first is that

$$\alpha_r \equiv \alpha_{r/\ell} \bmod \mathfrak{L}$$

for every prime $\mathfrak{L}$ of F_r over ℓ. The second is the so-called Euler system relation found in the following lemma. Note that we use additive notation for the multiplicative action of the group ring.

LEMMA 6.4.3. *We have $N_\ell \alpha_r = (\varphi_\ell - 1)\alpha_{r/\ell}$.*

PROOF. Set $s = \frac{r}{\ell}$. We have

$$N_\ell(\zeta_m\zeta_r - 1) = \prod_{i=1}^{\ell-1}(\zeta_m\zeta_\ell^i\zeta_s - 1) = \frac{\zeta_m^\ell \zeta_s^\ell - 1}{\zeta_m\zeta_s - 1} = (\varphi_\ell - 1)(\zeta_m\zeta_s - 1),$$

and replacing ζ_m with ζ_m^{-1}, we have the lemma. □

Fix an odd positive integer n, and let $\mathscr{P}_n$ denote the subset of elements of $\mathscr{P}$ that are products of primes that are 1 modulo n.

LEMMA 6.4.4. *If $r \in \mathscr{P}_n$, then $D_r\alpha_r \in (F_r^\times / F_r^{\times n})^{G_r}$.*

PROOF. We prove this by induction on the number of primes dividing r, the case that the number is zero, i.e., $r = 1$, being clear. If $r = \ell s$ for some prime ℓ and s in $\mathscr{P}_n$, then

$$(\sigma_\ell - 1)D_r\alpha_r = (\ell - 1 - N_\ell)D_s\alpha_r = (\ell - 1)D_s\alpha_r + (1 - \varphi_\ell)D_s\alpha_s$$

by the Euler system relation. The latter of course agrees with $(1 - \varphi_\ell)D_s\alpha_s$ modulo $(F_r^\times)^{\ell-1}$. Now, by induction we have $D_s\alpha_s \in F_s^{\times n}$, and since $\ell \in \mathscr{P}_n$, this tells us that $(\sigma_\ell - 1)D_r\alpha_r \in F_r^{\times n}$. Since this holds for all ℓ, we have proven the lemma. □

Note that $\mu_n \cap F = \{1\}$ since F is totally real and n is odd, and this and the fact that n and r are relatively prime tell us that $\mu_n \cap F(\mu_r) = \{1\}$. We therefore have that μ_n has trivial G_{F_r}-invariants, so the sequence of base terms in the Hochschild-Serre spectral sequence yields an isomorphism

$$(F_r^\times/F_r^{\times n})^{G_r} \xrightarrow{\sim} F^\times/F^{\times n}$$

inverse to the inflation map $H^1(G_F,\mu_n) \to H^1(G_{F_r},\mu_n)^{G_r}$. Let $\kappa_r \in F^\times/F^{\times n}$ denote the image of $D_r\alpha_r$ under this map.

TERMINOLOGY 6.4.5. The element κ_r is called the *Kolyvagin derivative* of α_r.

REMARK 6.4.6. Note that for any $y \in F_\ell^\times$, the element $(1-\sigma_\ell)y = \frac{y}{\sigma_\ell y}$ is necessarily a unit at primes over ℓ. As ℓ splits completely in F and all primes over it are totally ramified in F_ℓ/F, it makes sense to take the image of $(\sigma_\ell - 1)y$ in

$$(\mathscr{O}_F/\ell\mathscr{O}_F)^\times \cong \prod_{\mathfrak{l}|\ell}(\mathscr{O}_F/\mathfrak{l}\mathscr{O}_F)^\times \cong \prod_{\mathfrak{L}|\ell}(\mathscr{O}_{F_\ell}/\mathfrak{L}\mathscr{O}_{F_\ell})^\times.$$

Let $\tilde{\kappa}_r$ denote a lift of κ_r to $F^\times$. Write

$$D_r\alpha_r = \tilde{\kappa}_r\beta_r^n$$

for some $\beta_r \in F_r^\times$.

LEMMA 6.4.7. *The fractional ideal $\beta_r\mathscr{O}_{F_r}$ is invariant under G_r.*

PROOF. For $\sigma \in G_r$, the element $(\sigma-1)\beta_r$ is an nth root of $(\sigma-1)D_r\alpha_r$, since $\tilde{\kappa}_r \in F$. In particular, $(\sigma-1)\beta_r$ is a unit for all $\sigma \in G_r$, and the result follows from this. □

Let I_ℓ denote the subgroup of the ideal group I_F of F generated by the prime ideals $\mathfrak{l}$ in $\mathscr{O}_F$ dividing a rational prime ℓ. Then $I_F = \bigoplus_\ell I_\ell$, where the direct sum is taken over all primes.

LEMMA 6.4.8. *If $r \in \mathscr{P}_n$ and ℓ is prime with $\ell \nmid r$, then we may choose $\tilde{\kappa}_r$ so that $\beta_r \in F_r^\times$ is a unit at all primes over ℓ.*

PROOF. Note that the choice of $\tilde{\kappa}_r$ is canonical up to an element of $F^{\times n}$, so β_r is similarly-well determined exactly up to an element of $F^\times$. Since no prime over ℓ ramifies in F_r/F, we have that the G_r-fixed part of the summand of I_{F_r} generated by primes over ℓ is I_ℓ. By Lemma 6.4.7, we can find $a \in F^\times$ such that $a\beta_r$ is a unit at all primes over ℓ, as required. □

For $a \in F^\times/F^{\times n}$, we let $[a]_\ell$ to denote the image of $a\mathscr{O}_F$ in I_ℓ/nI_ℓ under the canonical projection.

LEMMA 6.4.9. *Let $\ell \in \mathscr{P}_n$. Then there exists a unique Δ-equivariant surjection*

$$\Pi_\ell \colon (\mathscr{O}_F/\ell\mathscr{O}_F)^\times \to I_\ell/nI_\ell$$

such that

$$\Pi_\ell((1-\sigma_\ell)x) = [N_\ell x]_\ell$$

for all $x \in F_\ell^\times/F_\ell^{\times n}$.

PROOF. Since F_ℓ/F is tamely ramified at each prime dividing ℓ, the Δ-equivariant map

$$p_\ell \colon F_\ell^\times/F_\ell^{\times n} \xrightarrow{1-\sigma_\ell} (\mathscr{O}_F/\ell\mathscr{O}_F)^\times$$

that exists by Remark 6.4.6 is surjective. Similarly, the Δ-equivariant map $q_\ell \colon F_\ell^\times/F_\ell^{\times n} \to I_\ell/nI_\ell$ given by $q_\ell(x) = [N_\ell x]_\ell$ is surjective as all primes dividing ℓ in F are totally ramified in F_ℓ.

For $x \in F_\ell^\times/F_\ell^{\times n}$, we have $p_\ell(x) = 0$ if and only if the order $\ell-1$ of the residue field of each prime $\mathfrak{L}$ over ℓ in F_ℓ divides the valuation $v_\mathfrak{L}(x)$, which of course implies that $\ell-1$ divides $v_\mathfrak{l}(N_\ell(x))$ for each prime $\mathfrak{l}$ of F over L. Since $\ell \in \mathscr{P}_n$, we then have $[N_\ell(x)]_\ell = 0$. Consequently, the map q_ℓ factors through the map p_ℓ, producing the unique map Π_ℓ. □

Let

$$\pi_\ell \colon \{a \in F^\times/F^{\times n} \mid [a]_\ell = 0\} \to I_\ell/nI_\ell$$

be the map that takes an element a to the value of Π_ℓ on the image of a in $(\mathscr{O}_F/\ell\mathscr{O}_F)^\times$.

REMARK 6.4.10. From the proof of Lemma 6.4.9, we have that $x \in \ker \pi_\ell$ if and only if x is an nth power modulo $\mathfrak{l}$ for all prime $\mathfrak{l}$ dividing ℓ.

PROPOSITION 6.4.11. *For any $r \in \mathscr{P}_n$ and prime ℓ, we have*

$$[\kappa_r]_\ell = \begin{cases} \pi_\ell(\kappa_{r/\ell}) & \text{if } \ell \mid r \\ 0 & \text{if } \ell \nmid r. \end{cases}$$

PROOF. If $\ell \nmid r$, then we saw in Lemma 6.4.8 that β_r may be chosen to be a unit at all primes over ℓ, in which case $\tilde{\kappa}_r$ will also be a unit at ℓ, and therefore $[\kappa_r]_\ell = 0$.

If $\ell \mid r$, then write $r = \ell s$. We choose β_s to be a unit at primes over ℓ. Since β_r^n is a unit times an element of $F^\times$, we have that $v_\mathfrak{L}(\beta_r^n)$ is a multiple of the ramification index $\ell-1$ for each prime $\mathfrak{L}$ of F_r over ℓ. Since such primes are unramified over F_ℓ, we can find $\nu \in F_\ell^\times$ such that $\beta_r \nu^{(\ell-1)/n}$ is a unit at all primes over ℓ. Since $N_\ell \nu$ and $\nu^{\ell-1}$ have the valuation at each $\mathfrak{L}$ over ℓ and $\beta_r^{-n}\mathscr{O}_{F_r} = \tilde{\kappa}_r\mathscr{O}_{F_r}$, we therefore have $[N_\ell \nu]_\ell = [\kappa_r]_\ell$.

Fix a prime $\mathfrak{L}$ over ℓ in F_r. Since $\mathfrak{L}$ is ramified over F, we have

$$(1-\sigma_\ell)\nu^{(\ell-1)/n} \equiv (\sigma_\ell - 1)\beta_r \bmod \mathfrak{L}.$$

Since $\tilde{\kappa}_r, \tilde{\kappa}_s \in F$, we have

$$(\sigma_\ell - 1)\beta_r^n = (\sigma_\ell - 1)D_r\alpha_r = (\ell - 1 - N_\ell)D_s\alpha_r$$
$$= (\ell-1)D_s\alpha_r - (\varphi_\ell - 1)D_s\alpha_s = (\ell-1)D_s\alpha_r - (\varphi_\ell - 1)\beta_s^n,$$

the third equality by the Euler system relation. Since $\alpha_r \equiv \alpha_s \bmod \mathfrak{L}$, and

$$(\varphi_\ell - 1)\beta_s \equiv (\ell - 1)\beta_s \bmod \mathfrak{L}$$

by definition of the Frobenius, we have

$$(\sigma_\ell - 1)\beta_r \equiv \frac{D_s\alpha_r^{(\ell-1)/n}}{(\varphi_\ell - 1)\beta_s} \equiv \left(\frac{D_s\alpha_s}{\beta_s^n}\right)^{(\ell-1)/n} \equiv \tilde{\kappa}_s^{(\ell-1)/n} \bmod \mathfrak{L}.$$

In other words, the elements $(1-\sigma_\ell)\nu$ and $\tilde{\kappa}_s$ differ by an $\frac{\ell-1}{n}$th root of unity modulo primes over ℓ in F_ℓ. We then have that $\Pi_\ell((1-\sigma_\ell)\nu) = \pi_\ell(\kappa_s)$. By Lemma 6.4.9, we have the result. □

Now suppose that p is an odd prime, and let $n = p^k$ for some $k \geq 1$. The following theorem guarantees the existence of enough primes for our application.

PROPOSITION 6.4.12. *Given an ideal class $\mathfrak{c} \in A_F$, a finite $\mathbb{Z}[\Delta]$-submodule M of $F^\times/F^{\times n}$, and a Galois-equivariant map $\theta\colon M \to \mathbb{Z}/n\mathbb{Z}[\Delta]$, there exist infinitely many primes $\mathfrak{l} \in \mathfrak{c}$ that lie over some prime $\ell \in \mathscr{P}_n$ such that M has trivial image in I_ℓ/nI_ℓ and there exists a unit $u \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that*

$$\pi_\ell(x) = u\theta(x)\mathfrak{l} \bmod nI_\ell$$

for all $x \in M$.

PROOF. Let $E = F(\mu_n)$ and H be the p-Hilbert class field of F. The inertia group at any prime over p in $\mathrm{Gal}(E/F)$ has index at most 2, so $H \cap E = F$ as p is odd. Note that $\mathrm{Gal}(E(\sqrt[n]{M})/E)$ injects into $\mathrm{Hom}(M, \mu_n)$ by Kummer theory. The element $\rho \in \mathrm{Gal}(E/F)$ corresponding to complex conjugation acts as 1 on M and as -1 on μ_m, so ρ acts as -1 on $\mathrm{Hom}(M, \mu_n)$. It also acts as 1 on $\mathrm{Gal}(HE/E)$, so $E(\sqrt[n]{M}) \cap HE = E$. Since $H \cap E = F$, it follows that $E(\sqrt[n]{M}) \cap H = F$.

Since $\mu_n \cap F = \{1\}$, we have $\hat{H}^0(\mathrm{Gal}(E/F), \mu_n) = 0$ and therefore $H^1(\mathrm{Gal}(E/F), \mu_n) = 0$ as $\mathrm{Gal}(E/F)$ is cyclic. The natural map $F^\times/F^{\times n} \to E^\times/E^{\times n}$ is therefore an injection, and we see that the injection

$$\mathrm{Gal}(E(\sqrt[n]{M})/E) \to \mathrm{Hom}(M, \mu_n)$$

is in fact an isomorphism.

Fix a primitive nth root of unity ζ_n, and define a homomorphism $\iota\colon (\mathbb{Z}/n\mathbb{Z})[\Delta] \to \mu_n$ on group elements by $\iota(1) = \zeta_n$ and $\iota(\delta) = 1$ for $\delta \neq 1$. The homomorphism $\iota \circ \theta\colon M \to \mu_n$ corresponds to an

element $\tau \in \mathrm{Gal}(E(\sqrt[n]{M})/E)$ satisfying

$$\frac{\tau(\sqrt[n]{x})}{\sqrt[n]{x}} = \iota \circ \theta(x)$$

for all $x \in M$.

By what we have shown, restriction maps define an isomorphism

$$\mathrm{Gal}(HE(\sqrt[n]{M})/F) \cong \mathrm{Gal}(H/F) \times \mathrm{Gal}(E/F) \times \mathrm{Gal}(E(\sqrt[n]{M})/E).$$

So, we may choose $\sigma \in \mathrm{Gal}(HE(\sqrt[n]{M})/F)$ such that $\sigma|_{E(\sqrt[n]{M})} = \tau$ and $\sigma|_H$ corresponds to $\mathfrak{c} \in A_F$ via the Artin isomorphism. By the Čebotarev density theorem, there exist infinitely many primes ℓ that are unramified in $E(\sqrt[n]{M})$ and for which the Frobenius φ_ℓ at ℓ has the same conjugacy class as σ in $\mathrm{Gal}(HE(\sqrt[n]{M})/\mathbb{Q})$.

Now fix such a prime ℓ, and let $\mathfrak{l}$ be a prime lying over it. Here then are its most easily derived properties. Since $\sigma|_F = 1$, the prime $\mathfrak{l}$ has degree 1, or in other words $\ell \in \mathscr{P}$. Since $\sigma|_H$ corresponds to $\mathfrak{c}$, we have $\mathfrak{l} \in \mathfrak{c}$. Since $\sigma|_E = 1$, the prime $\mathfrak{l}$ splits in E/F, so $\ell \in \mathscr{P}_n$. Since ℓ is unramified in the Galois extension $E(\sqrt[n]{M})$ of $\mathbb{Q}$, we have $[x]_\ell = 0$ for all $x \in M$.

The component of $\pi_\ell(x) \in I_\ell/nI_\ell$ as $\mathfrak{l}$ is trivial if and only if x is an nth power modulo $\mathfrak{l}$, as in Remark 6.4.10. On the other hand, $\theta(x)\mathfrak{l} \in I_\ell/nI_\ell$ is trivial if and only if $\iota \circ \theta(x) = 1$, so if and only if $\tau|$ fixes $\sqrt[n]{x}$, and then if and only if $\varphi_\mathfrak{l}$ fixes $\sqrt[n]{x}$, and then finally if and only if x is an nth power modulo $\mathfrak{l}$. Thus, there exists a $u \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that the $\mathfrak{l}$-component of $\pi_\ell(x)$ and $u\theta(x)\mathfrak{l}$ agree for all $x \in M$. The map

$$\pi_\ell(x) - u\theta(x)\mathfrak{l} \colon M \to \bigoplus_{\substack{\mathfrak{l}' \mid \ell \\ \mathfrak{l} \neq \mathfrak{l}'}} (\mathbb{Z}/n\mathbb{Z})\mathfrak{l} \subset I_\ell/nI_\ell$$

is Δ-equivariant as the difference of Δ-equivariant maps, so its image is $\mathbb{Z}/n\mathbb{Z}[\Delta]$-stable, but its image also lies in a subgroup of I_ℓ/nI_ℓ containing no nontrivial $\mathbb{Z}/n\mathbb{Z}[\Delta]$-submodule, as Δ acts transitively on the primes of F over ℓ. It follows that $\pi_\ell(x) = u\theta(x)\mathfrak{l}$ for all $x \in M$. □

Recall that $\mathscr{E}_F = E_F \otimes_\mathbb{Z} \mathbb{Z}_p$, and set $\mathscr{C}_F = C_F \otimes_\mathbb{Z} \mathbb{Z}_p$.

LEMMA 6.4.13. *Suppose that $\chi \colon \Delta \to \mathscr{O}_\chi^\times$ is a p-adic character of Δ. Extending χ to a primitive Dirichlet character, if $1 - \chi(\ell) \in \mathscr{O}_\chi^\times$ for all $\ell \mid m$, then $e_\chi(1 - \zeta_m)$ generates $\mathscr{C}_F^{(\chi)}$ as an $\mathscr{O}_\chi$-module.*

PROOF. Let $\zeta_d = \zeta_m^{m/d}$ for d dividing m. The group $\mathscr{C}_F$ is the intersection with $\mathscr{E}_F$ of the $\mathbb{Z}_p[\Delta]$-module generated by the elements $1 - \zeta_d$ for d dividing m. Since the norm from $\mathbb{Q}(\zeta_d)$ to $\mathbb{Q}(\zeta_e)$ for e dividing d of the element $1 - \zeta_d$ is $1 - \zeta_e$ so long as every prime dividing d also divides e, we can reduce this generating set to the set of $1 - \zeta_d$ with $(d, \frac{m}{d}) = 1$. In general, if $\ell_1, \ldots, \ell_k$ are the primes dividing d but not e, then the norm of $1 - \zeta_d$ is the application of $(1 - \varphi_{\ell_1}^{-1}) \cdots (1 - \varphi_{\ell_k}^{-1})$ to $1 - \zeta_e$.

Projecting to the χ-isotypical quotient, we have that it becomes the multiple of the image of $1-\zeta_e$ by $(1-\chi(\ell_1)^{-1})\cdots(1-\chi(\ell_k)^{-1})$, which is a unit by assumption. □

We may now bound the orders of eigenspaces of even eigenspaces of p-parts of class groups. The proof of the following result using Euler systems is due to Kolyvagin. We suppose that m is divisible by 4 if it is even.

THEOREM 6.4.14. *Suppose that $p\nmid|\Delta|$, and let χ be a primitive finite order p-adic character of Δ. Then the order of $A_F^{(\chi)}$ divides the order of $(\mathscr{E}_F/\mathscr{C}_F)^{(\chi)}$.*

PROOF. Let $\mathscr{O}$ be the $\mathbb{Z}_p$-algebra generated by the image of χ, and let f be its residue degree. Let $a_\chi=|A_F^{(\chi)}|^{1/f}$ and $q_\chi=|(\mathscr{E}_F/\mathscr{C}_F)^{(\chi)}|^{1/f}$, and set $n=a_\chi q_\chi$. Let $\mathfrak{c}_1,\dots,\mathfrak{c}_q$ be ideal classes generating $A_F^{(\chi)}$ as an $\mathscr{O}$-module.

Set $\delta_r=e_\chi\kappa_r$ for $r\in\mathscr{P}_n$. Primitivity and the fact that $p\nmid|\Delta|$ imply, by Lemma 6.4.13, that $\mathscr{C}_F^{(\chi)}$ is free of rank 1 over $\mathscr{O}_\chi$, generated by $\delta_1=e_\chi\alpha_1=e_\chi(\zeta_m-1)^2$. Then q_χ is the maximal integer t_0 such that $\delta_1\in(F^{\times t_0}/F^{\times n})^{(\chi)}$.

Let $1\le i\le g$, and suppose that for each $1\le j<i$, we have found primes $\mathfrak{l}_j\in\mathfrak{c}_j$ lying over primes $\ell_j\in\mathscr{P}_n$ such that for $r_j=\prod_{h=1}^j\ell_h$ and $t_j\le n$ the largest power of p such that

$$\delta_{r_j}\in(F^{\times t_j}/F^{\times n})^{(\chi)},$$

one has $t_j\mid t_{j-1}$ and

$$\frac{t_{j-1}}{t_j}\mathfrak{c}_j\in\mathscr{O}(\mathfrak{c}_1,\dots,\mathfrak{c}_{j-1}). \tag{6.4.1}$$

We look for $\mathfrak{l}_i$ with the same properties.

Let M_i be the $\mathscr{O}$-submodule of $F^\times/F^{\times n}$ generated by $\delta_{r_{i-1}}$. Define

$$\theta_i\colon M_i\to((\mathbb{Z}/n\mathbb{Z})[\Delta])^{(\chi)},\qquad \theta_i(\delta_{r_{i-1}})=t_{i-1}e_\chi.$$

By Proposition 6.4.12, there exists a prime $\mathfrak{l}_i\in\mathfrak{c}_i$ over some $\ell_i\in\mathscr{P}_n$ and satisfying $[\delta_{r_{i-1}}]_{\ell_i}=0$ and

$$\pi_{\ell_i}(\delta_{r_{i-1}})=u_it_{i-1}e_\chi\mathfrak{l}_i$$

for some $u_i\in(\mathbb{Z}/n\mathbb{Z})^\times$. Now let $r_i=\prod_{j=1}^i\ell_j$ and $t_i\le n$ be the largest power of p such that $\delta_{r_i}\in F^{\times t_i}/F^{\times n}$.

We have by Proposition 6.4.11 that

$$[\delta_{r_i}]_{\ell_i}=\pi_{\ell_i}(\delta_{r_{i-1}})=u_it_{i-1}e_\chi\mathfrak{l}_i \tag{6.4.2}$$

in I_{ℓ_i}/nI_{ℓ_i}. Since $\delta_{r_i}\in F^{\times t_i}/F^{\times n}$, this forces $t_i\mid t_{i-1}$. In particular, t_i divides $t_0=q_\chi$, and therefore $a_\chi=\frac{n}{q_\chi}$ divides $\frac{n}{t_i}$.

Proposition 6.4.11 also tells us that $[\delta_{r_i}]_\ell = 0$ unless $\ell \mid r_i$. Thus δ_{ℓ_i} has a t_ith root in $F^\times$ and nonzero valuation modulo n only at primes dividing $\ell_1, \dots, \ell_i$. It follows that $\frac{1}{t_i}[\delta_{r_i}]_{\ell_i}$ has trivial image in the quotient of $A_F^{(\chi)}$ by the $\mathscr{O}$-span of the classes $\mathfrak{c}_1, \dots, \mathfrak{c}_{i-1}$ of $\mathfrak{l}_1, \dots, \mathfrak{l}_{i-1}$. Moreover, we have by (6.4.2) that

$$\frac{1}{t_i}[\delta_{r_i}]_{\ell_i} \equiv u_i \frac{t_{i-1}}{t_i} e_\chi \mathfrak{l}_i \bmod \frac{n}{t_i} I_{\ell_i},$$

This implies that $\frac{t_{i-1}}{t_i}\mathfrak{c}_i \in \mathscr{O}(\mathfrak{c}_1, \dots, \mathfrak{c}_{i-1})$, completing the recursion.

Multiplying together (6.4.1) for $1 \le j \le g$ gives that a_χ divides

$$\prod_{i=1}^{g} \frac{t_{i-1}}{t_i} = \frac{q_\chi}{t_g},$$

which clearly divides q_χ. □

6.5. The main conjecture via Euler systems

Let p be an odd prime. Let m be a positive integer not divisible by p and divisible by 4 if m is even. Set $F = \mathbb{Q}(\mu_{mp})$, and let $F_n = \mathbb{Q}(\mu_{mp^n})$ for $n \ge 1$ and $F_\infty = \bigcup_{n=1}^\infty F_n$. Let $\Gamma(n) = \Gamma^{p^{n-1}} = \mathrm{Gal}(F_\infty/F_n)$ and $\Gamma_n = \mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^{n-1}\mathbb{Z}$. Let $\chi\colon (\mathbb{Z}/mp\mathbb{Z})^\times \to \mathscr{O}^\times$ be an even character of order prime to p, where $\mathscr{O} = \mathscr{O}_\chi$, which we also view as a primitive $\mathscr{O}$-valued Dirichlet character. Set $\Lambda = \mathscr{O}[\![\Gamma]\!]$ and $\Lambda_n = \mathscr{O}[\Gamma_n]$. We make a usual choice of identification of Λ with $\mathscr{O}[\![T]\!]$.

LEMMA 6.5.1.

a. The restriction map $(\mathfrak{X}_\infty)^{(\chi)}_{\Gamma(n)} \to \mathfrak{X}_n^{(\chi)}$ is an isomorphism.

b. The restriction map $(X_\infty)^{(\chi)}_{\Gamma(n)} \to X_n^{(\chi)}$ has trivial kernel unless $\chi(p) = 1$ and $\chi \ne 1$, in which case it is isomorphic to $\mathscr{O}$. It has trivial cokernel unless $\chi = 1$, in which case it is a finite quotient of Γ_n that is zero for sufficiently large n.

c. The inverse limit of norm maps $(\mathscr{U}_\infty)^{(\chi)}_{\Gamma(n)} \to \mathscr{U}_n^{(\chi)}$ is an injection unless $\chi\omega^{-1}(p) = 1$ and a surjection unless $\chi(p) = 1$.

d. The inverse limit of norm maps $(\mathscr{C}_\infty)^{(\chi)}_{\Gamma(n)} \to \mathscr{C}_n^{(\chi)}$ is an injection which is an isomorphism if $\chi(p) \ne 1$.

Note that if M is a finitely generated Λ-module such that M_Γ is finite, then it is torsion and T does not divide its characteristic ideal, so M^Γ is finite as well, and in particular M^Γ is contained in the maximal finite submodule M_{fin} of M.

PROPOSITION 6.5.2. *Suppose that $\chi(p) \ne 1$ and $\chi\omega^{-1}(p) \ne 1$. Then there exists an open ideal $\mathfrak{a}$ of Λ that annihilates both the kernel and cokernel of the inverse limit of norm maps $N_n\colon (\mathscr{E}_\infty)^{(\chi)}_{\Gamma_n} \to \mathscr{E}_n^{(\chi)}$.*

PROOF. Consider the following two commutative diagrams with top rows arising from taking the $\Gamma(n)$-homology of Proposition 3.3.6 (noting Theorem 3.3.4) and the bottom rows coming from Theorem 1.5.4 (noting Theorem 1.5.21):

$$\begin{array}{ccccccccc}
(X_\infty^{(\chi)})^{\Gamma(n)} & \longrightarrow & (\mathscr{U}_\infty^{(\chi)}/\mathscr{E}_\infty^{(\chi)})_{\Gamma(n)} & \longrightarrow & (\mathfrak{X}_\infty^{(\chi)})_{\Gamma(n)} & \longrightarrow & (X_\infty^{(\chi)})_{\Gamma(n)} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_n} & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \wr} & & \\
0 & \longrightarrow & \mathscr{U}_n^{(\chi)}/\mathscr{E}_n^{(\chi)} & \longrightarrow & \mathfrak{X}_n^{(\chi)} & \longrightarrow & A_n^{(\chi)} & \longrightarrow & 0
\end{array}$$

and

$$\begin{array}{ccccccccc}
(\mathscr{U}_\infty^{(\chi)}/\mathscr{E}_\infty^{(\chi)})^{\Gamma(n)} & \longrightarrow & (\mathscr{E}_\infty^{(\chi)})_{\Gamma(n)} & \longrightarrow & (\mathscr{U}_\infty^{(\chi)})_{\Gamma(n)} & \longrightarrow & (\mathscr{U}_\infty^{(\chi)}/\mathscr{E}_\infty^{(\chi)})_{\Gamma(n)} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle N_n} & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \pi_n} & & \\
0 & \longrightarrow & \mathscr{E}_n^{(\chi)} & \longrightarrow & \mathscr{U}_n^{(\chi)} & \longrightarrow & \mathscr{U}_n^{(\chi)}/\mathscr{E}_n^{(\chi)} & \longrightarrow & 0.
\end{array}$$

By Lemma 6.5.1 and our assumption that $\chi(p) \neq 1$, we have that the rightmost two vertical arrows in the first diagram and the middle vertical arrow in the second diagram are isomorphisms. In particular, we have exact sequences

$$(X_\infty^{(\chi)})^{\Gamma(n)} \to (\mathscr{U}_\infty^{(\chi)}/\mathscr{E}_\infty^{(\chi)})_{\Gamma(n)} \xrightarrow{\pi_n} \mathscr{U}_n^{(\chi)}/\mathscr{E}_n^{(\chi)} \to 0. \tag{6.5.1}$$

and

$$(\mathscr{U}_\infty^{(\chi)}/\mathscr{E}_\infty^{(\chi)})^{\Gamma(n)} \to (\mathscr{E}_\infty^{(\chi)})_{\Gamma(n)} \xrightarrow{N_n} \mathscr{E}_n^{(\chi)} \to \ker \pi_n \to 0. \tag{6.5.2}$$

Since $(X_\infty^{(\chi)})_{\Gamma(n)} \cong A_n^{(\chi)}$ is finite, so is $(X_\infty^{(\chi)})^{\Gamma(n)}$, and being contained in the maximal finite Λ-submodule of $X_n^{(\chi)}$, it has order bounded independent of n. By (6.5.1) and (6.5.2), we then have that $\operatorname{coker} N_n \cong \ker \pi_n$ also has bounded order. The group $\mathfrak{X}_n^{(\chi)} \cong (\mathfrak{X}_\infty^{(\chi)})_{\Gamma(n)}$ is finite by our assumption on χ and the theorem of Ferrero-Greenberg, so its subgroup $\mathscr{U}_n^{(\chi)}/\mathscr{E}_n^{(\chi)}$ is finite as well. Equation (6.5.1) then also yields that $(\mathscr{U}_\infty^{(\chi)}/\mathscr{E}_\infty^{(\chi)})_{\Gamma(n)}$ is finite, so $\ker N_n \cong (\mathscr{U}_\infty^{(\chi)}/\mathscr{E}_\infty^{(\chi)})^{\Gamma(n)}$ is finite of order bounded in n by the order of the maximal finite submodule of $\mathscr{U}_\infty^{(\chi)}/\mathscr{E}_\infty^{(\chi)}$ (which is in fact trivial). Letting $\mathfrak{a}$ be the annihilator of $(X_\infty^{(\chi)})_{\mathrm{fin}} \oplus (\mathscr{U}_\infty^{(\chi)}/\mathscr{E}_\infty^{(\chi)})_{\mathrm{fin}}$, we are done. □

Let h_χ denote a characteristic power series of $\mathfrak{X}_\infty^{(\chi)}$, and let j_χ denote a characteristic power series of $\mathscr{E}_\infty^{(\chi)}/\mathscr{C}_\infty^{(\chi)}$.

PROPOSITION 6.5.3. *Suppose that $\chi(p) \neq 1$. Then there exists an open ideal $\mathfrak{a}$ of Λ such that for all $\lambda \in \mathfrak{a}$ and $n \geq 1$, there exists a Λ_n-module homomorphism $\theta_{n,\lambda} : \mathscr{E}_n^{(\chi)} \to \Lambda_n$ such that*

$$\theta_{n,\lambda}(\mathscr{C}_\infty^{(\chi)}) = \lambda\, j_\chi \Lambda_n.$$

PROOF. Under our assumption that $\chi(p) \neq 1$, we have $\mathscr{U}_\infty^{(\chi)} \cong \Lambda$ via the product of Coleman maps by Corollary 6.1.2. Consequently, its submodule $\mathscr{E}_\infty^{(\chi)}$ is torsion-free of rank one. In particular, there exists an injective pseudo-isomorphism $\theta\colon \mathscr{E}_\infty^{(\chi)} \to \Lambda$. By Proposition 6.1.5, the Λ-module $\mathscr{C}_\infty^{(\chi)}$ is cyclic, so

$$\theta(\mathscr{C}_\infty^{(\chi)}) = \mathrm{char}_{\Lambda_\chi}(\Lambda_\chi/\theta(\mathscr{C}_\infty^{(\chi)})) = \mathrm{char}_{\Lambda_\chi}(\mathscr{E}_\infty^{(\chi)}/\mathscr{C}_\infty^{(\chi)}) = (j_\chi).$$

Now let $\mathfrak{a}$ be as in Proposition 6.5.2. Let $\theta_n\colon (\mathscr{E}_\infty^{(\chi)})_{\Gamma(n)} \to \Lambda_n$ be the map induced by θ. For any $\lambda \in \mathfrak{a}$ and $u \in \mathscr{E}_n^{(\chi)}$, we let $\theta_{n,\lambda}(u)$ be $\theta_n(v)$ for any v with $N_n(v) = \lambda u$, which exists since λ annihilates $\mathrm{coker} N_n$ and is unique since θ_n is necessarily trivial on the finite kernel of N_n. The result then follows by definition of $\theta_{n,\lambda}$. □

LEMMA 6.5.4. *Suppose that $\chi(p) \neq 1$. Let f_i with $1 \leq i \leq g$ be such that $X_\infty^{(\chi)} \simeq \prod_{i=1}^g \Lambda/(f_i)$. Then there exists an open ideal $\mathfrak{b}$ of Λ such that, for each $n \geq 1$, there exist elements $\mathfrak{c}_1, \ldots, \mathfrak{c}_g$ of $A_n^{(\chi)}$ such that the annihilator $\mathrm{Ann}(\mathfrak{c}_i)$ of each $\mathfrak{c}_i$ as an element of the Λ_n-module $A_n^{(\chi)}/\Lambda_n(\mathfrak{c}_1, \ldots, \mathfrak{c}_{i-1})$ satisfies $\mathfrak{b}\,\mathrm{Ann}(\mathfrak{c}_i) \subseteq f_i\Lambda_n$.*

PROOF. By the given pseudo-isomorphism, there exists an exact sequence

$$0 \to \bigoplus_{i=1}^g \Lambda/(f_i) \to X_\infty^{(\chi)} \to Q \to 0$$

with Q finite. Taking Γ_n-homology and noting that $(X_\infty^{(\chi)})_{\Gamma(n)} \cong A_n^{(\chi)}$ by assumption, we obtain an exact sequence

$$Q^{\Gamma(n)} \to \bigoplus_{i=1}^g \Lambda_n/f_i\Lambda_n \to A_n^{(\chi)} \to Q_{\Gamma(n)} \to 0. \tag{6.5.3}$$

Let $\mathfrak{b}$ be the Λ-annihilator of Q. Let $\mathfrak{c}_i$ be the image of the generator e_i of the ith summand $\Lambda_n/f_i\Lambda_n$ in $A_n^{(\chi)}$.

If $x \in \Lambda_n$ is such that $x \cdot \mathfrak{c}_i \in \Lambda_n(\mathfrak{c}_1, \ldots, \mathfrak{c}_n)$, then we have xe_i is in the sum of the image of $Q^{\Gamma(n)}$ and $\bigoplus_{j\neq i}\Lambda_n/f_j\Lambda_n$ in $\bigoplus_{j=1}^g \Lambda_n/f_j\Lambda_n$ by (6.5.3). Since $\mathfrak{b}$ annhilates Q, any $\lambda \in \mathfrak{b}$ satisfies $\lambda x e_i \in \bigoplus_{j\neq i}\Lambda_n/f_j\Lambda_n$, but $\lambda x e_i$ is clearly in the ith summand, so $\lambda x e_i = 0$. In other words, $\mathfrak{b}\,\mathrm{Ann}(\mathfrak{c}_i) \subseteq f_i\Lambda_n$. □

Let us now work over F_n^+.

LEMMA 6.5.5. *Let $r \in \mathscr{P}_m$ for a power m of p, let ℓ be a prime divisor of r, and let $\mathfrak{q}$ be a prime of F_n^+ over ℓ. Let B be the subgroup of A_n^+ generated by the primes dividing $\frac{r}{\ell}$. Let $\mathfrak{c} = e_\chi[\mathfrak{q}] \in A_n^{(\chi)}$. Let $\delta_r = e_\chi \kappa_r$, and let $M = \Lambda_n\delta_r \subseteq (F^\times/F^{\times m})^{(\chi)}$. Suppose that we can choose*

$$m \geq |A_n^{(\chi)}| \cdot |(I_\ell/mI_\ell)^{(\chi)}/\Lambda_n[\delta_r]_\ell|.$$

Let $I \subseteq \Lambda_n$ denote the annihilator of the image of $\mathfrak{c}$ in A_n^+/B. Suppose also that $\lambda, f \in \Lambda_n$ are such that

$$\lambda I \subset f\Lambda_n, \quad \textit{and} \quad \Lambda_n/f\Lambda_n \textit{ is finite}.$$

Then there exists a Λ_n-module homomorphism

$$\theta : M \to (\Lambda_n/m\Lambda_n)^{(\chi)}$$

such that for

$$\eta : F^\times/F^{\times n} \to \Lambda_n/m\Lambda_n, \qquad \eta(x)\mathfrak{q} = \pi_\ell(x),$$

we have

$$\theta(\delta_r) = \lambda\eta(\delta_r).$$

PROOF. By assumption, we have $m \cdot A_n^{(\chi)} = 0$. Define $\tilde{\eta} : F_n^\times \to \Lambda_n$ by $\tilde{\eta}(x)\mathfrak{q} = (x)_\ell$, where $(x)_\ell$ denotes the image of (x) in I_ℓ so that $\tilde{\eta}$ lifts η. Let $\tilde{\delta}_r \in F_n^\times$ be a lift of δ_r. Then $(\tilde{\delta}_r)$ is a multiple of m at primes not dividing r, so its image in A_n^+/B is $\eta(\delta_r)\mathfrak{q}$, but also zero as the image of a principal ideal. Thus $\eta(\delta_r) \in I$, and so $\lambda\tilde{\eta}(\tilde{\delta}_r) \in f\Lambda_n$ by assumption. Since $\Lambda_n/f\Lambda_n$ is finite, we may set

$$\alpha = \frac{\lambda\tilde{\eta}(\tilde{\delta}_r)}{f} \in \Lambda_n.$$

We define θ as in the lemma as the unique Λ_n-module homomorphism with $\theta(\delta_r) = \alpha$, if it exists. If $a \in \Lambda_n$ is such that $a\delta_r = 0$, then $[a\delta_r]_\ell = 0$. For $h = |A_n^{(\chi)}|$, we have

$$\frac{m}{h} \cdot (I_\ell/mI_\ell)^{(\chi)} \subseteq \Lambda_n[\delta_r]_\ell,$$

so we must have $a \in h\Lambda_n$. Writing $a\tilde{\delta}_r = x^m$ for some $x \in F_n^\times$, we have $e_\chi[x]_\ell = [\frac{1}{m}a\tilde{\delta}_r]_\ell$, and (x) has valuation a multiple of h at primes not dividing r. Since $h \cdot A_n^{(\chi)} = 0$, the element $\frac{1}{m}(a\tilde{\delta}_r)_\ell$ has trivial image in $A_n^{(\chi)}/B$. In other words, $\frac{1}{m}\tilde{\eta}(a\tilde{\delta}_r) \cdot \mathfrak{c} \in B$. Then

$$a\alpha f = a\lambda\tilde{\eta}(\tilde{\delta}_r) \in mf\Lambda_n,$$

so θ is 0 on $a\delta_r$. Therefore, θ is well-defined. □

We now come to our proof of a divisibility in the main conjecture. For now, the proof is omitted.

THEOREM 6.5.6. *If $\chi(p) \neq 1$ and $\chi\omega^{-1}(p) \neq 1$, then* $\mathrm{char}(X_\infty^{(\chi)})$ *divides* $\mathrm{char}(\mathscr{E}_\infty^{(\chi)}/\mathscr{C}_\infty^{(\chi)})$.

6.6. Geometry of modular curves

The original approach of Mazur and Wiles to the main conjecture was a heavily involved study of Galois actions on the cohomology of modular curves, inspired by the work of Ribet in his proof of the converse to Herbrand's theorem, which looked at the Galois representations attached to a newform satisfying a mod p congruence with an Eisenstein series. The work of Wiles was a significant refinement, and in some sense simplification, of the work of Mazur-Wiles that employed Hida theory and Galois representations constructed out of pseudo-representations to complete the proof of the more general main conjecture over totally real extensions of $\mathbb{Q}$. Back in the setting of the main conjecture over $\mathbb{Q}$, a further simplification of Wiles' work can be found in the work of Masami Ohta (for primes $p \geq 5$). In this setting, the Galois representations that Wiles constructs are quotients of inverse limits of cohomology groups of modular curves, so one can study cohomology directly. It is this approach that we will attempt to roughly sketch here. For this, we will have to assume substantially more background than earlier in these notes, so we will try to focus on ideas to compensate for this.

For a given level $N \geq 4$, the modular curve $X_1(N)$ may be defined as a scheme over $\mathbb{Z}$. Over, $\mathbb{Z}[\frac{1}{N}]$, it is a compactification of the fine moduli scheme $Y_1(N)$ that represents the functor that to a $\mathbb{Z}[\frac{1}{N}]$-scheme S associates the set of pairs (E,P), where E is an elliptic curve over S and P is a point of order N generating a subgroup scheme of $E_{/S}$ isomorphic to $(\mathbb{Z}/N\mathbb{Z})_{/S}$. If we consider the base change $\overline{X_1(N)}$ of $X_1(N)$ to $\overline{\mathbb{Q}}$, then its p-adic étale cohomology group $\mathscr{T}_N = H^1_{\text{ét}}(\overline{X_1(N)}, \mathbb{Q}_p(1))$ has a continuous action of $G_{\mathbb{Q}}$ that is unramified outside of the primes over N and ∞.

There is also an action on cohomology of Hecke operators given by correspondences. To describe this, we remark that a choice of embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ gives rise to an isomorphism

$$\mathscr{T}_N \xrightarrow{\sim} H^1(X_1(N)(\mathbb{C}), \mathbb{Z}_p)$$

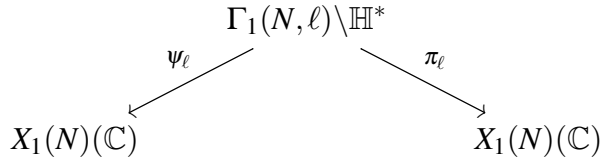
of $\mathbb{Q}_p$-vector spaces, where the right-hand side is singular cohomology. This isomorphism commutes with the actions of Hecke operators, so we can describe them on the right side. Recall that $X_1(N)(\mathbb{C})$ is a quotient of the union $\mathbb{H}^*$ of the upper-half place $\mathbb{H}$ and $\mathbb{Q} \cup \{\infty\}$ by the congruence subgroup

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid (c,d) \equiv (0,1) \bmod N \right\}.$$

For a prime ℓ, set

$$\Gamma_1(N,\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \mid c \equiv 0 \bmod \ell \right\}.$$

Consider the diagram



where ψ_ℓ is induced by multiplication by ℓ on $\mathbb{H}^*$ and π_ℓ is induced by the identity. This gives rise to two correspondences on $H^1(X_1(N)(\mathbb{C}),\mathbb{Z}_p)$ which are in a sense dual: we take the dual correspondence $T^*(\ell)$ given by pullback by ψ_ℓ followed by pushforward by π_ℓ. (The usual Hecke correspondence $T(\ell)$ is given instead by $(\psi_\ell)_*\pi_\ell^*$.) We also have dual diamond operators $\langle j\rangle^*$ for $j \in (\mathbb{Z}/N\mathbb{Z})^\times$ (inverse to the usual ones) that are the automorphisms induced by the maps on $Y_1(N)$ given by $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $d \equiv j^{-1} \bmod N$. We let $\mathfrak{h}(N)$ denote the Hecke algebra of endomorphisms of $H^1(X_1(N)(\mathbb{C}),\mathbb{Z}_p)$ generated by these dual correspondences and diamond operators. Back on étale cohomology, the Galois and Hecke actions commute.

If $N \mid M$, then we have trace maps $\mathrm{Tr}\colon \mathscr{T}_M \to \mathscr{T}_N$ given on singular cohomology by summing over $\Gamma_1(N)/\Gamma_1(M)$-conjugates (upon pullback to $\mathscr{T}_M$ via the injective map induced by the identity on $\mathbb{H}$). One key reason for our use of dual Hecke operators is that the trace map commutes with their actions. In particular, if we consider a tower of modular curves $X_1(Np^n)$ for a fixed $N \geq 1$ not divisible by p and $n \geq 1$, then we have an inverse limit of cohomology groups $\varprojlim_n \mathscr{T}_{mp^n}$ under trace maps. Of particular interest to us is the $T^*(p)$-ordinary part $\mathscr{T} = \varprojlim_n \mathscr{T}_{mp^n}^{\mathrm{ord}}$ of H: it is the maximal direct summand of H on which $T^*(p)$ acts invertibly. The ordinary part $\mathfrak{h}^* = \varprojlim_n \mathfrak{h}(mp^n)^{\mathrm{ord}}$ inverse limit of Hecke algebras acting on $\mathscr{T}$. This Hecke algebra $\mathfrak{h}^*$ is known as Hida's ordinary (dual, cuspidal) $\mathbb{Z}_p$-Hecke algebra of tame level m.

One of the key properties of Hida's ordinary Hecke algebra $\mathfrak{h}$ is it nicely encapsulates the structure of ordinary parts of cuspidal Hecke algebras of all weights and levels. The Hecke algebra is free of finite rank over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![T]\!]$, where $T = \langle 1+p\rangle^* - 1$. If for $k \geq 2$ and $n \geq 1$, the ordinary part of the weight k, level Np^n Hecke algebra that acts on $H^1(X_1(mp^n)(\mathbb{C}),\mathrm{Sym}^{k-1}(\mathbb{Z}_p^2))^{\mathrm{ord}}$, is isomorphic to $\mathfrak{h}/((1+T)^{p^n} - (1+p)^{p^n(k-2)})$. Moreover, the latter cohomology group is isomorphic to the quotient of the free of finite rank Λ-module $\mathscr{T}$ by the action of $(1+T)^{p^n} - (1+p)^{p^n(k-2)}$.

It is perhaps more typical to speak of Hida's Hecke algebra as acting on the space of ordinary Λ-adic cusp forms via the usual (not dual) action of Hecke operators. (The algebras of usual and dual Hecke algebras are isomorphic via the map that takes a Hecke operator to the corresponding dual operator.) For this, one has the theory of Λ-adic modular forms, which are q-expansions with coefficients in Λ that specialize upon plugging in $(1+p)^{k-2} - 1$ for T to weight k cusp forms for each (or, equivalently, all but finitely many) $k \geq 2$. For an eigenform to be $T(p)$-ordinary means that its pth Fourier coefficient is a unit. Again, we have the same sort of good control when we specialize

at various weights and levels. Let us denote the $\mathfrak{h}$-module of Λ-adic cusp forms by $\mathscr{S}$. Hida proved that the pairing $\mathfrak{h} \times \mathscr{S} \to \Lambda$ of Λ-modules that takes (T, f) to the q-coefficient of Tf is perfect, so $\mathfrak{h} \cong \mathrm{Hom}_\Lambda(\mathscr{S}, \Lambda)$ and $\mathscr{S} \cong \mathrm{Hom}_\Lambda(\mathfrak{h}, \Lambda)$. Moreover, $\mathscr{S} \otimes_\Lambda \mathscr{Q}$, where $\mathscr{Q}$ is the quotient field of Λ, is free of rank one over $\mathfrak{h} \otimes_\Lambda \mathscr{Q}$.

One sees that $\mathscr{T}$ fits in an exact sequence of $\mathbb{Z}_p[\![G_{\mathbb{Q}_p}]\!]$-modules of the form

$$0 \to \mathscr{T}_{\mathrm{sub}} \to \mathscr{T} \to \mathscr{T}_{\mathrm{quo}} \to 0,$$

where $\mathscr{T}_{\mathrm{quo}}$ has unramified action and is noncanonically isomorphic to the space of ordinary Λ-adic cusp forms via an isomorphism that switches dual and usual Hecke actions. The key point here is that for the Galois representation $\mathscr{T}$ to be ordinary for $T^*(p)$ means also to be ordinary in the sense of p-adic Hodge theory, which insures that it has a filtration of the above form. The Hecke operator $T^*(p)$ acts as the Frobenius φ_p on $\mathscr{T}_{\mathrm{quo}}$. The characteristic polynomial of the Frobenius φ_ℓ for $\ell \nmid mp$ acting on the rank two module $\mathscr{T} \otimes_\Lambda \mathscr{Q}$ is an $\mathfrak{h} \otimes_\Lambda \mathscr{Q}$-representation with $T^*(p)$-action given by $x^2 - T^*(\ell)x + \ell\langle\ell\rangle^*$. One might roughly think of $\mathscr{T}$ as encapsulating all of the p-adic Galois representations attached to ordinary cusp forms of tame level (dividing) m at once.

A version of Poincaré duality, modified to be compatible with the inverse limit, sets up a perfect pairing of Λ-modules $(\ ,\ ) \colon \mathscr{T} \times \mathscr{T} \to \Lambda$ such that $(Tx, y) = (x, Ty)$ for $x, y \in \mathscr{T}$ and $T \in \mathfrak{h}$, and this induces a perfect pairing $\mathscr{T}_{\mathrm{sub}} \times \mathscr{T}_{\mathrm{quo}} \to \Lambda$. From this and the duality between Hida's Hecke algebra and ordinary Λ-adic cusp forms, we see that $\mathscr{T}_{\mathrm{sub}} \cong \mathfrak{h}$. We remark that we may lift $\mathscr{T}_{\mathrm{quo}} \otimes_\Lambda \mathscr{Q}$ to a subspace of $\mathscr{T} \otimes_\Lambda \mathscr{Q}$ complementary to $\mathscr{T}_{\mathrm{sub}} \otimes_\Lambda \mathscr{Q}$. We would preferably lift $\mathscr{T}_{\mathrm{quo}}$ itself, but it is not clear one can do this if $\theta\omega^{-1}(p) = 1$. However, we can get away with something close in all eigenspaces using the action of a chosen element ν of the inertia group I_p at p with $\nu(\zeta_{p^n}) = \zeta_{p^n}^{1+p}$ for all n. Set $u = (1+T)(1+p)$ and $\Lambda' = \Lambda[(u-1)^{-1}]$. We declare $\mathscr{T}^+$ to be the $\mathfrak{h} \otimes_\Lambda \Lambda'$-submodule fixed by ν. This clearly works, as the determinant in $\mathscr{Q}^\times$ of the action of ν is u, but ν acts trivially on the quotient $\mathscr{T}_{\mathrm{quo}} \otimes_\Lambda \Lambda'$. We set $\mathscr{T}^- = \mathscr{T}_{\mathrm{sub}} \otimes_\Lambda \Lambda'$.

By picking an ordered basis of $\mathscr{T} \otimes_\Lambda \mathscr{Q}$ from $\mathscr{T}^-$ and $\mathscr{T}^+$, respectively, we see that the Galois representation

$$\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathfrak{h} \otimes_\Lambda \mathscr{Q}), \qquad \rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is upper-triangular on $G_{\mathbb{Q}_p}$ and has the form

$$\rho|_{I_p} = \begin{pmatrix} \det\rho & b \\ 0 & 1 \end{pmatrix}$$

on the inertia subgroup I_p. We are particularly interested in the map c.

Let I denote the ideal of $\mathfrak{h}$ generated by all $T^*(\ell) - 1 - \ell\langle\ell\rangle^*$ for primes $\ell \nmid mp$ and $T^*(\ell) - 1$ for primes $\ell \mid mp$, and fix an even p-adic character θ of $(\mathbb{Z}/mp\mathbb{Z})^\times$ of conductor m or mp. Set $\chi = \theta\omega^2$.

The image I_θ of I in $\mathfrak{h}^{(\theta)}$ (which corresponds to the θ^{-1}-eigenspace of the usual non-cuspidal Hecke algebra acting on the space Λ-adic cuspidal modular forms) is the image of the ideal of the Hecke algebra acting on Λ-adic modular forms that is the annihilator of the Λ-adic Eisenstein series

$$G_{\theta^{-1}} = \frac{1}{2} g_\chi^0 + \sum_{n=1}^{\infty} \sum_{\substack{d|n \\ (d,mp)=1}} d\theta^{-1}(d)\langle \kappa(d)\rangle q^n,$$

where $\kappa(d)$ is the projection of $d \in \mathbb{Z}_{p,m}^\times$ into $1+p\mathbb{Z}_p$. Here $g_\chi^0 = g_\chi$ if $\theta\omega(p) \neq 1$ and $g_\chi^0 = (T-p)^{-1} g_\chi$ otherwise.

The quotient $(\mathfrak{h}/I)^{(\theta)}$ measures, in a sense, the failure of the above Eisenstein series $G_{\theta^{-1}}$ to be a cusp form. This Eisenstein series induces map from Hida's full modular Hecke algebra $\mathfrak{H}$ acting on the space of Λ-adic modular forms to $\Lambda_{\theta^{-1}}$, taking $T(\ell)$ to the corresponding Fourier coefficient, and its kernel is the Eisenstein ideal in the θ^{-1}-eigenspace of this Hecke algebra. On the dual cuspidal Hecke algebra $\mathfrak{h}^{(\theta)}$, this yields a surjection $(\mathfrak{h}/I)^{(\theta)} \to \Lambda_\theta/\iota(g_\chi^0)$ since $G_{\theta^{-1}}$ becomes a cusp form when reduced modulo its constant term. In fact, this surjection is an isomorphism for $\theta \neq \omega^2$, though we shall not require it in our proof.

Now suppose that $f_\chi \notin (\Lambda_\chi[T^{-1}])^\times$. Note that T divides f_χ if and only if $\chi\omega^{-1}(p) = \theta\omega(p) = 1$. (Recall that $f_\chi((1+p)^s - 1) = L_p(\chi, s)$ for all $s \in \mathbb{Z}_p$.). By the result of Ferrero and Greenberg, T exactly divides f_χ in the "exceptional" case that $\chi\omega^{-1}(p) = 1$, and $T \nmid f_\chi$ for non-exceptional χ.

We shall be interested in the θ-eigenspaces (under the action of diamond operators) of our Galois representation ρ that is defined by $\mathscr{T}^{(\theta)} \otimes_\Lambda \mathscr{Q}$, so we view ρ as taking values in $\mathrm{GL}_2(\mathfrak{h}^{(\theta)} \otimes_\Lambda \mathscr{Q})$ by projection.

LEMMA 6.6.1. *For $\sigma, \tau \in G_\mathbb{Q}$, the elements $a(\sigma) - \det\rho(\sigma)$, $d(\sigma) - 1$, and $b(\sigma)c(\tau)$ of $\mathfrak{h}^{(\theta)} \otimes_\Lambda \mathscr{Q}$ are all contained in $I_\theta \subset \mathfrak{h}^{(\theta)}$.*

PROOF. Note that $\mathfrak{h} = \mathrm{End}_\mathfrak{h}(\mathfrak{h}) = \mathrm{End}_\mathfrak{h}(\mathscr{S})$, so a and d take values in $\mathfrak{h}$, and moreover $b(\sigma)c(\tau) \in \mathfrak{h}$ for all $\sigma, \tau \in G_\mathbb{Q}$ since compositions of elements in $\mathrm{Hom}_\mathfrak{h}(\mathscr{S}, \mathfrak{h})$ and $\mathrm{Hom}_\mathfrak{h}(\mathfrak{h}, \mathscr{S})$ lie in one of the aforementioned endomorphism groups.

It suffices to show the containments in question on Frobenius elements φ_ℓ (or their "geometric" inverses) at $\ell \mid Np$ by the Čebotarev density theorem. One has that

$$a(\varphi_\ell^{-1}) + d(\varphi_\ell^{-1}) = \ell^{-1}T(\ell) = \ell^{-1}\langle\ell\rangle T^*(\ell) \equiv 1 + \ell^{-1}\langle\ell\rangle \bmod I_\theta.$$

Since $\det\rho(\varphi_\ell^{-1}) = \ell^{-1}\langle\ell\rangle$ for all ℓ, we therefore have

$$a(\sigma) + d(\sigma) \equiv 1 + \det\rho(\sigma) \bmod I_\theta$$

for all $\sigma \in G_{\mathbb{Q}}$. The element ν used to lift $\mathscr{T}_{\mathrm{quo}}$ satisfies

$$\rho(\nu) = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix},$$

where $u = (1+p)(T+1)$. Taking the trace of $\rho(\nu\sigma)$, we see that

$$ua(\sigma) + d(\sigma) \equiv 1 + u \det\rho(\sigma) \bmod I_\theta,$$

again for all σ. It follows that $a(\sigma) - \det\rho(\sigma) \in I_\theta$ and $d(\sigma) - 1 \in I_\theta$.

Now consider $\sigma, \tau \in G_{\mathbb{Q}}$ and note that $a(\sigma\tau) = a(\sigma)a(\tau) + b(\sigma)c(\tau)$. Thus we have

$$b(\sigma)c(\tau) = (a(\sigma\tau) - \det\rho(\sigma\tau)) - (a(\sigma)a(\tau) - \det\rho(\sigma)\cdot\det\rho(\tau)) \in I_\theta.$$

□

Let B (resp., C) denote the $\mathfrak{h}\otimes_\Lambda\Lambda'$-submodules of $\mathfrak{h}^{(\theta)}\otimes_\Lambda\mathscr{Q}$ generated by the elements $b(\sigma)$ (resp., $c(\sigma)$) with $\sigma \in G_{\mathbb{Q}}$. The $\mathfrak{h}$-module BC of sums of products is an ideal of $\mathfrak{h}^{(\theta)}$ contained in I_θ.

LEMMA 6.6.2. *The ideal BC of $\mathfrak{h}^{(\theta)}\otimes_\Lambda\Lambda'$ is a faithful $\mathfrak{h}^{(\theta)}$-module.*

PROOF. The map $\delta\colon G_{\mathbb{Q}} \to (\mathfrak{h}/BC)^\times$ induced by $\sigma \mapsto d(\sigma)$ is a homomorphism that is unramified outside of the primes over m. It is then at most tamely ramified at these primes, so by class field theory the map factors through a quotient of $\prod_{\ell|m}\mathbb{Z}_\ell^\times$. Since the pro-abelian group $(\mathfrak{h}/BC)^\times$ has finite prime-to-p part and the group $\prod_{\ell|m}\mathbb{Z}_\ell^\times$ has finite p-part, we see that the image of δ is finite

For $\ell \nmid mp$, we have

$$\begin{aligned}\ell^{-1}\langle\ell\rangle(T^*(\ell) - 1 - \ell\langle\ell\rangle^*) &= a(\varphi_\ell^{-1}) + d(\varphi_\ell^{-1}) - \det\rho(\varphi_\ell^{-1}) - 1 \\ &= -(a(\varphi_\ell^{-1}) - 1)(d(\varphi_\ell^{-1}) - 1) + b(\varphi_\ell^{-1})c(\varphi_\ell^{-1}),\end{aligned}$$

By the Čebotarev density theorem, we can find infinitely many primes $\ell \nmid mp$ such that $d(\varphi_\ell^{-1}) - 1 \in BC$. For such an ℓ, we have then $T^*(\ell) - 1 - \ell\langle\ell\rangle^* \in BC$. This element is not a zero divisor in $\mathfrak{h}^{(\theta)}$ (as it does not annihilate any ordinary Λ-adic cuspidal eigenform with character θ^{-1}, which we do not verify here), so the annihilator of BC in $\mathfrak{h}^{(\theta)}$ is trivial. □

We have the following corollary.

COROLLARY 6.6.3. *The $\mathfrak{h}^{(\theta)}\otimes_\Lambda\Lambda'$-modules B and C are faithful.*

Let $F = \mathbb{Q}(\mu_{mp})$, and let F_∞ be its cyclotomic $\mathbb{Z}_p$-extension.

PROPOSITION 6.6.4. *The map $\bar{c}\colon G_{\mathbb{Q}} \to C/I_\theta C$ induced by c restricts to a homomorphism on G_{F_∞} with the same image as $\bar{c}$ and which factors through $X_\infty^{(\omega\chi^{-1})}$*

PROOF. For $\sigma, \tau \in G_{\mathbb{Q}}$, we have that

$$c(\sigma\tau) = a(\tau)c(\sigma) + c(\tau)d(\sigma) \equiv \det\rho(\tau)c(\sigma) + c(\tau) \bmod I_\theta.$$

Since $\det\rho$ factors through $\mathrm{Gal}(F_\infty/\mathbb{Q})$, we see that $\bar{c}$ is a homomorphism, and it factors through X_∞ since $c|_{I_p} = 0$.

For $\sigma_j \in \mathrm{Gal}(F_\infty/\mathbb{Q})$ with $\sigma_j(\zeta_{mp^n}) = \zeta_{mp^n}^j$ for all n, where $j \in \mathbb{Z}_{p,m}^\times$, we have

$$\det\rho(\sigma_j) = j_p\langle j\rangle^* = \omega\theta(j)\kappa(j)\langle\kappa(j)\rangle^*.$$

In particular, for $j \in (\mathbb{Z}/mp\mathbb{Z})^\times$ and $\tau \in G_{F_\infty}$, we have

$$\bar{c}(\sigma_j\tau\sigma_j^{-1}) = \det\rho(\sigma_j)^{-1}\bar{c}(\tau) = (\omega\theta)^{-1}(j)\bar{c}(\tau) = \omega\chi^{-1}(j)\bar{c}(\tau).$$

Finally, letting $\sigma \in G_{\mathbb{Q}}$, the commutator $[\nu, \sigma]$ lies in G_{F_∞}, and we have

$$\bar{c}([\nu, \sigma]) = (u^{-1} - 1)\bar{c}(\sigma).$$

Since $u^{-1} - 1$ is a unit in Λ', we are done. □

Using the fact that C is a faithful $\mathfrak{h}^{(\theta)}$-module and the theory of Fitting ideals, one can show that the characteristic ideal of $C/I_\theta C$ as a module over the algebra Λ_θ of diamond operators is divisible by $g^0_{\omega^2\theta^{-1}}$. Since $X_\infty^{(\omega\chi^{-1})}$ maps surjectively to $C/I_\theta C$ via $\bar{c}$, we obtain the following theorem (upon application of the theorem of Ferrero and Greenberg to deal with exceptional zeros).

THEOREM 6.6.5. *The ideal* (f_χ) *divides* $\mathrm{char}_{\Lambda_\chi} X_\infty^{(\omega\chi^{-1})}$.

APPENDIX A

Duality in Galois cohomology

Fix a prime p. For a field E, let G_E denote its absolute Galois group, i.e., the Galois group of its separable closure E^{sep} as an extension of E. Let μ_{p^∞} denote the group of all p-power roots of unity in E^{sep}.

Now let E be a nonarchimedean local field of characteristic not equal to p. Recall that its Brauer group $\mathrm{Br}(E) = H^2(G_{E,S}, (E^{\mathrm{sep}})^\times)$ is canonically isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ by class field theory. This has the following corollary.

LEMMA A.0.1. *We have an isomorphism*

$$H^2(G_E, \mathbb{Q}_p/\mathbb{Z}_p(1)) \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p.$$

PROOF. Of course, we may replace $\mathbb{Q}_p/\mathbb{Z}_p(1)$ by μ_{p^∞} in the statement, which in fact will make the isomorphism canonical. First, we remark that, since direct limits are exact, we have an isomorphism

$$H^2(G_E, \mu_{p^\infty}) \cong \varinjlim_n H^2(G_E, \mu_{p^n}).$$

Kummer theory sets up an exact sequence

$$0 \to H^2(G_E, \mu_{p^n}) \to \mathrm{Br}(E) \xrightarrow{p^n} \mathrm{Br}(E),$$

the left exactness following from Hilbert's theorem 90. Since the p^n torsion in $\mathrm{Br}(E)$ is canonically isomorphic to $1/p^n\mathbb{Z}/\mathbb{Z}$ and $\mathbb{Q}_p/\mathbb{Z}_p$ is the direct limit of the latter groups, we have the result. □

REMARK A.0.2. If T is a finite $\mathbb{Z}_p[G_E]$-module, then $H^i(G_E, T)$ is finite for every i.

THEOREM A.0.3 (Tate duality). *Let T be a finite $\mathbb{Z}_p[G_E]$-module. Then for $i \in \mathbb{Z}$ the cup product*

$$H^i(G_E, T) \times H^{2-i}(G_E, T^\vee(1)) \to H^2(G_E, \mathbb{Q}_p/\mathbb{Z}_p(1))$$

is nondegenerate, inducing an isomorphism

$$H^i(G_E, T) \cong H^{2-i}(G_E, T^\vee(1))^\vee.$$

REMARK A.0.4. In fact, we have, more generally, such a duality for compact $\mathbb{Z}_p$-modules T with continuous G_E-actions. Here, we must use continuous cohomology, i.e., the cohomology groups of the complex of continuous G_E-cochains with values in T. We will in general denote such cohomology groups using the same notation as the usual profinite cohomology groups.

Finally, let F denote a global field of characteristic not equal to p, and let S be a finite set of primes of F.

DEFINITION A.0.5. Let T be a finite $\mathbb{Z}_p[G_{F,S}]$-module. For $i \in \{1,2\}$, the ith Shafarevich-Tate group of T is

$$Ш^i(G_{F,S},T) = \ker\Big(H^i(G_{F,S},T) \xrightarrow{\Sigma \mathrm{Res}_v} \bigoplus_{v\in S} H^i(G_{F_v},T)\Big),$$

where the map Res_v is the compostion of restriction to a decomposition group at $v \in S$ in $G_{F,S}$ with inflation to the absolute Galois G_{F_v}.

The duality theorem is then as following

THEOREM A.0.6 (Poitou-Tate duality). *Let T be a finite $\mathbb{Z}_p[G_{F,S}]$-module. For $i \in \{1,2\}$, we have isomorphisms*

$$Ш^i(G_{F,S},T) \xrightarrow{\sim} Ш^{3-i}(G_{F,S},T^\vee(1))^\vee.$$

For $v \in S_\infty$ and any $i \in \mathbb{Z}$, we will use $H^i(G_{F_v},T)$ to denote the ith Tate cohomology group of T, by abuse of notation.

REMARK A.0.7. For $v \in S_\infty$, the cup product induces isomorphisms

$$H^i(G_{F_v},T) \xrightarrow{\sim} H^{2-i}(G_{F_v},T^\vee(1))^\vee$$

for all $i \in \mathbb{Z}$.

Combining Poitou-Tate duality with Tate duality, we obtain the following nine-term exact sequence.

THEOREM A.0.8 (Poitou-Tate sequence). *For a finite $\mathbb{Z}_p[G_{F,S}]$-module T, we have an exact sequence*

$$\begin{array}{l}
0 \longrightarrow H^0(G_{F,S},T) \longrightarrow \bigoplus_{v\in S} H^0(G_{F_v},T) \longrightarrow H^2(G_{F,S},T^\vee(1))^\vee \dashrightarrow \\
\dashrightarrow H^1(G_{F,S},T) \longrightarrow \bigoplus_{v\in S} H^1(G_{F_v},T) \longrightarrow H^1(G_{F,S},T^\vee(1))^\vee \dashrightarrow \\
\dashrightarrow H^2(G_{F,S},T) \longrightarrow \bigoplus_{v\in S} H^2(G_{F_v},T) \longrightarrow H^0(G_{F,S},T^\vee(1))^\vee \longrightarrow 0.
\end{array}$$

PROOF. We first define the maps in question. The maps

$$\mathrm{Res}_v \colon H^i(G_{F,S},T) \to H^i(G_{F_v},T)$$

are the compositions of the restriction maps from $G_{F,S}$ to a decomposition group above $v \in S$ with inflation to the absolute Galois group G_{F_v}. The maps

$$H^i(G_{F_v}, T) \to H^{2-i}(G_{F,S}, T^\vee(1))^\vee$$

are the compositions of the maps

$$H^i(G_{F_v}, T) \to H^{2-i}(G_{F_v}, T^\vee(1))^\vee$$

of Tate duality with the Pontryagin duals of the maps Res_v with for the module $T^\vee(1)$. Finally the maps

$$H^{3-i}(G_{F,S}, T^\vee(1))^\vee \to H^1(G_{F,S}, T)$$

are defined to be the natural maps that factor through the Poitou-Tate isomorphisms

$$Ш^{3-i}(G_{F,S}, T^\vee(1))^\vee \to Ш^i(G_{F,S}, T).$$

We briefly sketch the proof of exactness. Exactness at the first and last stages follows from injectivity of restriction on zeroth cohomology groups. Exactness at the local stages follows from global class field theory, which tells us that the image of $H^i(G_{F,S}, T)$ is the orthogonal complement of the image of $H^{2-i}(G_{F,S}, T^\vee(1))$ under the sum of local cup products. (We omit the argument, but see [**NSW**, Section 8.6].) Finally, exactness at the other four global stages follows directly from Poitou-Tate duality. □

REMARK A.0.9. As with Tate duality, we have Poitou-Tate duality and the Poitou-Tate sequence more generally for compact $\mathbb{Z}_p$-modules T with continuous $G_{F,S}$-actions.

Bibliography

[HS] Y. Hachimori and R. Sharifi, On the failure of pseudo-nulllity of Iwasawa modules, *J. Alg. Geom.* **14** (2005), 567–591.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Second Edition, Grundlehren der mathematischen Wissenschaften **323**, Springer, 2008.