Inaugural-Dissertation

zur Erlangung der Doktorwürde der
Naturwissenschaftlich-Mathematischen Gesamtfakultät der
Ruprecht-Karls-Universität Heidelberg

vorgelegt von

Ulrich Schmitt

geboren am 24.12.1985

in Köln

Tag der mündlichen Prüfung: ______________

Towards a Twist Conjecture in Non-Commutative Iwasawa Theory

Gutachter: Prof. Dr. Otmar Venjakob

Abstract

In this thesis we study three conjectures of Kato. The first one concerns p-adic Lie extensions $F_\infty/\mathbb{Q}$ containing the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{cyc}$ and the existence of an element $L_{p,u} \in K_1(\mathbb{Z}_p[[G(F_\infty/\mathbb{Q})]]_{S^*})$ depending on a global unit u. $L_{p,u}$ is required to map to a specified element under the connecting morphism ∂_{global} from K-theory and to satisfy a prescribed interpolation property. We state an analogous conjecture for imaginary quadratic number fields K and, under a torsion assumption, prove it for certain abelian CM elliptic curves cases.

The second conjecture is Kato's local main conjecture for p-adic Lie extensions $F'_\infty/\mathbb{Q}_p$ containing $\mathbb{Q}_p^{cyc}$ and concerns the existence of a element $\mathcal{E}_{p,u'} \in K_1(\widehat{\mathbb{Z}}_p^{ur}[[G(F'_\infty/\mathbb{Q}_p)]]_{\tilde{S}'^*})$ depending on a global unit u. $\mathcal{E}_{p,u'}$ is required to map to a specified element under ∂_{local} and to satisfy a prescribed interpolation property. In [Ven13], for certain abelian extensions an element $\mathcal{E}_{p,u'}$ is constructed and we prove that it satisfies the desired interpolation property.

Regarding the third conjecture, we prove the following for certain CM elliptic curves $E/\mathbb{Q}$ and good ordinary primes p. Up to an element $\Omega_{p,u,u'}$ reflecting a base change related to u and u', twists of $L_{p,u}$ and $\mathcal{E}_{p,u'}$ by representations related to E assemble to an element $\mathcal{L}_{p,u,E}$ that, up to an Euler factor, is a characteristic element of the dual Selmer group $\mathrm{Sel}(K(E[p^\infty]), T_pE^*(1))^\vee$ and that has an interpolation property related to that expected of a p-adic L-function of E.

Zusammenfassung

In dieser Arbeit werden drei Vermutungen von Kato untersucht, von denen die erste für eine p-adische Lie Erweiterung $F_\infty/\mathbb{Q}$ formuliert wird, die die zyklotomische $\mathbb{Z}_p$-Erweiterung $\mathbb{Q}^{cyc}$ enthält. Es wird die Existenz eines von einer globalen Einheit u abhängigen Elementes $L_{p,u} \in K_1(\mathbb{Z}_p[[G(F_\infty/\mathbb{Q})]]_{S^*})$ vermutet, das einerseits Urbild eines gewissen Elementes unter dem Verbindungshomomorphismus ∂_{global} aus der K-Theorie ist und andererseits eine vorgegebene Interpolationseigenschaft besitzt. Wir formulieren ein Analogon der Vermutung für quadratisch imaginäre Zahlkörper K und beweisen dieses - unter einer Torsionsannahme - für abelsche Erweiterungen $K(E[p^\infty])/K$ für eine bestimmte Klasse von CM elliptischen Kurven E.

Die zweite Vermutung betrifft eine p-adische Lie Erweiterung $F'_\infty/\mathbb{Q}_p$, die $\mathbb{Q}_p^{cyc}$ enthält. Es wird die Existenz eines Elementes $\mathcal{E}_{p,u'} \in K_1(\widehat{\mathbb{Z}}_p^{ur}[[G(F'_\infty/\mathbb{Q}_p)]]_{\tilde{S}'^*})$ vermutet, das von einer lokalen Einheit u' abhängt, wiederum eine bestimmte Interpolationseigenschaft besitzt und unter ∂_{local} auf ein gewisses Element abbildet. In [Ven13] wird für gewisse abelsche Erweiterungen ein Element $\mathcal{E}_{p,u'}$ konstruiert, für das wir das gewünschte Interpolationsverhalten nachweisen.

Bezüglich der dritten Vermutung beweisen wir Folgendes für gewisse CM elliptische Kurven $E/\mathbb{Q}$ und gute, ordinäre Primstellen p. Wir betrachten von E induzierte Twists von $L_{p,u}$ und $\mathcal{E}_{p,u'}$ und definieren ein Element $\Omega_{p,u,u'}$, das einen Basiswechsel beschreibt, der von u und u' abhängt. Mittels dieser Twists und $\Omega_{u,u',p}$ definieren wir $\mathcal{L}_{p,u,E}$, das einerseits, bis auf einen Eulerfaktor, ein charakteristisches Element des Duals $\mathrm{Sel}(K(E[p^\infty]), T_pE^*(1))^\vee$ der Selmer Gruppe ist und andererseits eine Interpolationseigenschaft besitzt, die in engem Zusammenhang zu der steht, die von einer p-adischen L-Funktion von E erwartet wird.

Danksagung

Besonderer Dank gilt meinem Betreuer Prof. Dr. O. Venjakob für seinen Zuspruch, seine Kritik und seine kontinuierliche Unterstützung. Für viele Erklärungen und Diskussionen möchte ich mich ganz herzlich bei Dr. M. Witte bedanken, der sich stets für mich Zeit genommen hat. Für mathematische Erläuterungen bedanke ich mich ebenfalls bei Dr. T. Bouganis, Prof. Dr. K. Wingberg und Prof. Dr. J. Stix. Darüber hinaus danke ich Prof. Dr. W. Bley, Dr. G. Zábrádi, Prof. Dr. M. Flach and Dr. K. Ardakov für Erklärungen von Teilen ihrer Arbeiten.

Ganz besonders möchte ich mich auch für die organisatorische und stets freundliche Unterstützung bei Frau B. Schmoetten-Jonas bedanken.

Dank gebührt auch der *Studienstiftung des deutschen Volkes*, die mein Promotionsvorhaben finanziell und ideell unterstützt hat. Für finanzielle Unterstützung bin ich auch dem *European Research Grant* durch die Förderung des Projektes *IWASAWA: Iwasawa Theory of p-adic Lie Extensions* verbunden.

Mein freundschaftlicher Dank gilt meinen Bürokollegen Dr. M. Sigl, Dr. J. to Baben und Dr. M. Spiegel, die das mathematische Institut durch ihre Aufgeschlossenheit und ihre vielfältigen Interessen bereichert haben.

Contents

Introduction **i**

Notation and Conventions **xiii**

1 Some K-theory **1**
- 1.1 Twist Operators on K_1- and K_0-groups . . . 2
  - 1.1.1 Technical background . . . 2
  - 1.1.2 Twist operators on K_1 of localized Iwasawa algebras . . . 6
  - 1.1.3 Fukaya and Kato's $K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$ . . . 9
  - 1.1.4 K_0 and the connecting homomorphism . . . 13
- 1.2 Finitely generated $\mathbb{Z}_p$-modules and K_0-groups . . . 15
  - 1.2.1 Setting . . . 15
  - 1.2.2 Main results . . . 16

2 Global Conjecture **21**
- 2.1 Introduction . . . 21
- 2.2 Setting . . . 21
- 2.3 Statement of the Global Conjecture . . . 23
- 2.4 The CM case . . . 25
  - 2.4.1 Notation . . . 26
  - 2.4.2 Global and semi-local units . . . 27
  - 2.4.3 Elliptic units . . . 29
  - 2.4.4 The formal group $\hat{E}$ and Coleman's theorem in a semi-local framework . . . 43
  - 2.4.5 Triviality of the annihilator $\mathrm{Ann}_{\Lambda(G,\hat{\mathbb{Z}}_p^{ur})}(\lambda)$ . . . 54
  - 2.4.6 Elliptic units continued . . . 59
  - 2.4.7 Relations in $K_0(S\text{–tor})$ . . . 63
  - 2.4.8 Commutative main theorem . . . 67

3 Local Main Conjecture **75**
- 3.1 Setting . . . 75
- 3.2 Statement of the Local Main Conjecture . . . 78

3.3 Interpolation Property . . . 78
3.3.1 Coleman map . . . 79
3.3.2 Definition of $\mathcal{E}_{p,u'}$ . . . 83
3.3.3 Local constants and p-adic regulators . . . 83
3.3.4 The values of $\mathcal{E}_{u'}$ at Artin characters . . . 85

4 Selmer Groups of p-adic Galois Representations 91
4.1 Definition . . . 91
4.2 Connection with the sequence of Poitou-Tate . . . 92
4.3 Tate Module of an abelian variety . . . 95
4.3.1 First local cohomology groups for $\nu \in \Sigma_f \setminus \Sigma_p$ . . . 97
4.3.2 First local cohomology groups for $\nu \in \Sigma_p$ . . . 100
4.3.3 Second local cohomology groups . . . 103
4.3.4 First global cohomology groups . . . 104
4.3.5 Vanishing of $\varprojlim_n H^1_f(G_{n,\Sigma}, T_pE)$ for $E/\mathbb{Q}$ with CM and good ordinary reduction at split p . . . 104
4.3.6 Second global cohomology group . . . 109

5 The element $\Omega_{p,u,u'}$ 111
5.1 Setting . . . 111
5.2 Choices of u and u' . . . 113
5.2.1 Local Case . . . 114
5.2.2 Global Case . . . 114
5.3 Definition . . . 115
5.3.1 Global contribution . . . 115
5.3.2 Local contribution . . . 116
5.4 Relations in $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$ . . . 118

6 Twist conjecture for Elliptic Curves $E/\mathbb{Q}$ with CM 119
6.1 Setting . . . 120
6.2 Main theorems . . . 122

A Appendix 131
A.1 Some Galois Isomorphisms . . . 131
A.2 Non-degenerate and perfect Pairings . . . 133
A.2.1 Weil pairing . . . 133
A.2.2 $\mathbb{Q}_p/\mathbb{Z}_p$-valued pairings . . . 134
A.3 Galois Cohomology . . . 136
A.3.1 Functoriality of local Tate duality . . . 137
A.3.2 Connection with étale Cohomology and the Kummer sequence . . . 138
A.3.3 Tensor products and cohomology . . . 139

A.3.4 Kummer sequence 147
A.4 The sequence of Poitou-Tate 150
A.4.1 Definition 150
A.4.2 Functoriality 151
A.5 Σ-units and Σ-ideal class groups 159
A.6 Elliptic curves with complex multiplication 160
A.6.1 Fields generated by division points 161
A.6.2 Größencharacters and conductors 166
A.6.3 Curves defined over $\mathbb{Q}$ 166
A.6.4 The Tate modules $T_pE, T_\pi E$ and $T_{\bar\pi}E$ 169
A.7 Modules over the completed group ring 172
A.8 Ore sets over complete DVRs 174
A.8.1 Characterization 175
A.8.2 Functorial properties 179
A.9 The Iwasawa algebra $\Lambda(\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times)$ and its modules 186
A.9.1 The Ore Set S and some of its elements 187

Bibliography **200**

Introduction

We begin this introduction by giving a brief summary of the development of a select few topics from Iwasawa theory in order to recall some of the context of this thesis. Most facts about the historical development are taken from the more detailed and expertly written accounts by J. Coates and R. Sujatha [CS06], K. Kato [Kat07] and R. Greenberg [Gre01b]. Afterwards, we summarize the contents and main results of this thesis.

Historical Development

In the middle of the 19th century E. E. Kummer made several remarkable discoveries including what is nowadays called *Kummer's criterion for the irregularity of primes* and *Kummer's congruence* ([CS10], Theorems 1.1.2 and 1.1.3), compare [Kum75] for Kummer's original work and some of his correspondence and the review [Maz77] for a concise summary. The criterion for the irregularity of a prime p establishes a connection between special values of the Riemann zeta function $\zeta(s)$ and the ideal class group $Cl(\mathbb{Q}(\mu_p))$ of $\mathbb{Q}(\mu_p)$, the number field obtained by adjoining μ_p to $\mathbb{Q}$, where μ_{p^k}, $k \geq 1$, denotes the group of p^k-th roots of unity. It says that a prime p is irregular, i.e., it divides the order $\#Cl(\mathbb{Q}(\mu_p))$ of $Cl(\mathbb{Q}(\mu_p))$, if and only if it divides the numerator of at least one of $\zeta(-1), \zeta(-3), \ldots, \zeta(4-p)$.

In 1964, T. Kubota and H.-W. Leopoldt [KL64] proved the existence of a p-adic analogue ζ_p of the Riemann zeta function that interpolates special values of $\zeta(s)$. Five years later, K. Iwasawa [Iwa69] gave a different description of ζ_p in terms of power series in one indeterminate T, which enabled an interpretation of ζ_p in terms of the Iwasawa algebra $\Lambda(G) = \varprojlim_U \mathbb{Z}_p[G/U]$, where U runs through all open normal subgroups of G and $G = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q})$ is the Galois group of the maximal real subfield $\mathbb{Q}(\mu_{p^\infty})^+$ of $\mathbb{Q}(\mu_{p^\infty}) = \bigcup_n \mathbb{Q}(\mu_{p^n})$ over $\mathbb{Q}$. It is this construction of ζ_p and results from K. Iwasawa's paper [Iwa64], which led to *Iwasawa's Theorem* as stated in [CS06]. One should note that in loc. cit. the existence of ζ_p is proved by different means than used in [Iwa69]. In fact, it is shown that ζ_p can be expressed as the image of a compatible system of cyclotomic units under a map $\tilde{\mathcal{L}}$ involving R. F. Coleman's [Col79] interpolating power series and an integral logarithm [CW78]. In order to state Iwasawa's theorem let us write U_n for the principal units of $\mathbb{Q}_p(\mu_{p^n})^+$ and C_n, $n \geq 1$, for the subgroup of cyclotomic units as defined in loc. cit. Setting $U_\infty = \varprojlim_n U_n$ and $C_\infty = \varprojlim_n C_n$ where the limits are taken with respect to norm maps and writing $I(G) = \ker(\Lambda(G) \xrightarrow{\text{aug}} \mathbb{Z}_p)$ for the augmentation ideal we can formulate the following theorem.

Theorem (Iwasawa's Theorem, see ([CS06], Theorem 1.5.1)). *There is a canonical isomorphism*

$$U_\infty/C_\infty \cong \Lambda(G)\big/(I(G)\cdot\zeta_p)$$

of $\Lambda(G)$-modules.

Via class field theory U_∞/C_∞ is closely connected to the Galois group X_∞ of the maximal abelian p-extension of $\mathbb{Q}(\mu_{p^\infty})^+$ which is unramified outside the unique prime above p of $\mathbb{Q}(\mu_{p^\infty})^+$ over $\mathbb{Q}(\mu_{p^\infty})^+$. It was proven by K. Iwasawa [Iwa73] that X_∞ is finitely generated and torsion as a $\Lambda(G)$-module and that to such modules one can associate a characterictic ideal $\mathrm{char}_{\Lambda(G)}(X_\infty)$, an arithmetic invariant which, by definition, is a principal ideal in $\Lambda(G)$, see [CS06] for details. The natural question about generators of $\mathrm{char}_{\Lambda(G)}(X_\infty)$ was (initially conjecturally) answered by the *cyclotomic main conjecture.*

Theorem (Cyclotomic Main Conejcture). *We have an equality*

$$\mathrm{char}_{\Lambda(G)}(X_\infty) = I(G)\cdot\zeta_p. \qquad (\mathrm{MC}(\mathbb{G}_m, \mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}))$$

of ideals in $\Lambda(G)$.

The augmentation ideal appears in the equation $(\mathrm{MC}(\mathbb{G}_m, \mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}))$ for the following reason. Let us write $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$. ζ_p, by definition, is the image in $\mathrm{Quot}(\Lambda(G))$ of an element of the form $\lambda(e)/(\sigma_e - 1)$ in $\mathrm{Quot}(\Lambda(\mathcal{G}))$, where $\lambda(e) \in \Lambda(\mathcal{G})$ is the image of a a cyclotomic unit associated to an integer e under the map $\tilde{\mathcal{L}}$ mentioned above and $\sigma_e - 1$ is a generator of $I(\mathcal{G})$ such that the quotient $\lambda(e)/(\sigma_e - 1)$ is independent of e. Therefore, while ζ_p is only a pseudo-measure, any element of the form $x\cdot\zeta_p$, where $x \in I(G)$, belongs to $\Lambda(G)$.

As remarked by J. Coates and R. Sujatha (loc. cit., p. 8f) K. Iwasawa's work [Iwa64] can be considered as the *"genesis of the main conjecture"*. The conjecture $(\mathrm{MC}(\mathbb{G}_m, \mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}))$ was first proven by B. Mazur and A. Wiles [MW84]. A different proof was given by K. Rubin in the appendix of [Lan90] using V. Kolyvagin's [Kol90] and F. Thaine's [Tha88] Euler systems. For an exposition of the Iwasawa main conjecture for more general number fields we refer to the book [NSW08] by J. Neukirch, A. Schmidt and K. Wingberg, which also contains several explanations of the analogy between the number field and the function field case.

The $\Lambda(G)$-module X_∞ is closely related to the inductive limit $\varinjlim_n \big(Cl(\mathbb{Q}(\mu_{p^n}))\{p\}\big)$ of the p-primary parts of the ideal class groups $Cl(\mathbb{Q}(\mu_{p^n}))$ of $\mathbb{Q}(\mu_{p^n})$ via multiplicative Kummer theory, see (loc. cit., (1.22)). From this viewpoint, the main conjecture $(\mathrm{MC}(\mathbb{G}_m, \mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}))$ constitutes a connection between the p-adic analogue ζ_p of the Riemann zeta function and the Galois module structure of the inductive limit of the ideal class groups associated to the tower $\mathbb{Q}(\mu_{p^n})$, $n \geq 1$.

From a historical point of view, one of the key new features of Iwasawa theory is the focus on the action of the Galois group G on arithmetic objects. K. Kato ([Kat07], p. 338) phrases it as

> *"Compared with Kummer's criterion and class number formula, Iwasawa theory is finer in the point that it describes not only the class number, i.e. the order of the ideal class group, but also the action of the Galois group on the ideal class group. In fact, one could even say that the aim of Iwasawa theory is to describe Galois actions on arithmetic objects in terms of zeta values."*

This description of Iwasawa theory is substantiated by the array of Iwasawa main conjectures that have been formulated and studied over the past 60 years. In several abelian cases and in a few non-abelian settings main conjectures have been proven. Among the most notable, A. Wiles [Wil90] proved the main conjecture for totally real base fields and K. Rubin [Rub91] proved certain cases of (one- and two- variable) main conjectures for quadratic imaginary fields (versions without p-adic L-function). M. Kakde [Kak11], [Kak13] proved a non-commutative main conjecture for (certain) p-adic Lie extensions of a totally real base field.

K. Rubin's main conjecture for quadratic imaginary base field has applications to the Iwasawa theory of elliptic curves, which was initiated by B. Mazur [Maz72], [MSD74] for cyclotomic extensions. In loc. cit. B. Mazur and P. Swinnerton-Dyer constructed a p-adic L-function $L_p(E)$ for an odd prime p and a (modular) elliptic curve $E/\mathbb{Q}$ which has good ordinary reduction at p. $L_p(E)$ is characterized by interpolating (up to a period and local term) the value at 1 of the twisted Hasse-Weil L-series $L(z, E, \chi)$, where χ is a Dirichlet character of p-power conductor regarded as a character of $\mathcal{G}$ via the cyclotomic character, see [Gre01b] for a more detailed discussion. In the Iwasawa theory of elliptic curves curves the Galois group X_∞ is replaced by the Pontryagin dual $\mathrm{Sel}(E/\mathbb{Q}(\mu_{p^\infty}))^\vee := \mathrm{Hom}(\varinjlim_n \mathrm{Sel}(E/\mathbb{Q}(\mu_{p^n})), \mathbb{Q}_p/\mathbb{Z}_p)$ of the direct limit $\varinjlim_n \mathrm{Sel}(E/\mathbb{Q}(\mu_{p^n}))$ of Selmer groups, which, for a general number field F fit into an exact sequence induced by the Kummer map

$$0 \to E(F) \otimes \mathbb{Q}/\mathbb{Z} \to \mathrm{Sel}(E/F) \to Ш(E/K) \to 0,$$

where $Ш(E/K) \subset H^1(G_F, E(\bar{F}))$ is the Tate-Šafarevič group and $\mathrm{Sel}(E/F)$ is a subgroup of $H^1(G_F, E(\bar{F})_{\mathrm{tor}})$, see [Gre01a] for a detailed discussion of these groups. K. Kato [Kat04] proved that $\mathrm{Sel}(E/\mathbb{Q}(\mu_{p^\infty}))^\vee$ is $\Lambda(\mathcal{G})$-torsion and the Iwasawa main conjecture now states

Conjecture. *We have an equality*

$$\mathrm{char}_{\Lambda(\mathcal{G})}(\mathrm{Sel}(E/\mathbb{Q}(\mu_{p^\infty}))^\vee) = \Lambda(\mathcal{G}) L_p(E), \qquad (\mathrm{MC}(E, \mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}))$$

of ideals in $\Lambda(\mathcal{G})$.

Note the analogy to the cyclotomic main conjecture $(\mathrm{MC}(\mathbb{G}_m, \mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}))$. In [Kat07], K. Kato gives a list of cases in which this conjecture is proven, which includes C. Skinner's and E. Urban's work [SU] on elliptic modular forms.

Up to this point we have considered the cyclotomic Galois extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$, which was Iwasawa's starting point and can be considered as the extension obtained by adjoining the p-power torsion points of the multiplicative formal group $\mathbb{G}_m$ to $\mathbb{Q}$. There are, however, numerous other interesting Galois extensions arising, for example, from geometric objects such as abelian varieties A over number fields F. Adjoining to F the coordinates of all p-power division points of A one obtains a p-adic Lie extension $F(A[p^\infty])/F$ which coincides with the trivializing extension of the action of G_F on the p-adic Tate-module $T_pA = \varprojlim_n E(\bar{F})[p^n]$ of A. The existence of p-adic L-functions in these cases is mostly conjectural and since, in general, the extensions $F(A[p^\infty])/F$ are non-abelian, one no longer has the notion of principal characteristic ideal at disposal. A suitable analogue for non-commutative settings has been developed by O. Venjakob [Ven03] in terms of K-theory and used in [CFK⁺05] to formulate a main conjecture for elliptic curves over a large class of p-adic Lie extensions, compare the beginning of chapter 1 for a discussion. One should mention that proven non-commutative main conjectures are scarce, M. Kakde's result mentioned above being one of the few examples.

Historically, elliptic curves E over a quadratic imaginary number field K with complex multiplication (CM) by $\mathcal{O}_K$ were among the examples studied first. To have complex multiplication means that the endomorphism ring $\mathrm{End}_{\bar{K}}(E)$ of E is equal to $\mathcal{O}_K$, i.e., strictly bigger than $\mathbb{Z}$. These CM-cases are in some sense the most simple cases after $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$ since the Galois group $G(K(E[p^\infty])/K)$ is also abelian and contains an open subgroup (the Galois group of the composite of all $\mathbb{Z}_p$-extensions of K over K) isomorphic to $\mathbb{Z}_p^2$. For split primes p, K. Rubin's [Rub91] two variable main conjecture and R. I. Yager's [Yag82] results on M. Katz' [Kat76] p-adic L-function(s) combined, imply the main conjecture in this case. It was shown by T. Bouganis and O. Venjakob [BV10] that these results also imply the main conjecture for the non-abelian p-adic Lie extension $K(E[p^\infty])/\mathbb{Q}$ adding to the short list of proven non-commutative cases.

The cyclotomic units that were used above are, in the CM setting, replaced by elliptic units. Especially the p-adic L-function is now obtained from a compatible system of elliptic units in the tower $K(E[p^n])_n$, $n \geq 1$ (and the Coleman map). R. I. Yager's main result ([Yag82], Theorem 1) is completely analogous to *Iwasawa's Theorem* from the cyclotomic theory above. It states that the p-adic L-function of M. Katz is a generator of the characteristic ideal of the quotient of the (respective projective limits of) principal semi-local units and the elliptic units for the tower $K(E[p^n])_n$, $n \geq 1$.

We want to end this historical account by noting that several generalizations of Iwasawa theory have been proposed and developed. For example, R. Greenberg and P. Schneider have formulated an Iwasawa theory for p-adic representations [Gre89] and, more generally, for motives [Sch89], [Gre94]. Moreover, non-commutative Iwasawa main conjectures as in [CFK⁺05] and for more general motives (with good ordinary reduction above p) are nowadays also studied in the context of equivariant Tamagawa number conjectures. The compatibility of the two conjectures was shown in [FK06].

Content and Results of the Thesis

In this thesis three conjectures are studied that were stated by K. Kato during a talk he gave in Cambridge on the occasion of J. Coates' sixtieth birthday. As was explained in the historical account above, the search for p-adic L-functions and their relation to arithmetic objects such as ideal class groups and Selmer groups has been central to Iwasawa theory. K. KATO's three conjectures are concerned with the possibility of expressing p-adic L-functions of motives by twisting certain universal local and global elements. We note that T. FUKAYA and K. KATO [FK06] expect twisting principles to hold in much greater generality in the context of (global and local) non-commutative Tamagawa number conjectures.

Before discussing the three conjectures in more detail, let us note that the first two conjectures about the universal elements are stated independently of any motive and depend just on a global, resp., local p-adic Lie extension F_∞/F. Moreover, while we state the conjectures in full generality, our results only concern certain special cases. In fact, we focus mainly on the case which arises from the study of an elliptic curve over $\mathbb{Q}$ with complex multiplication by the ring of integers $\mathcal{O}_K$ of a quadratic imaginary number field K, building on K. RUBIN's [Rub91] two variable main conjecture and K. KATO's [Kat] and O. VENJAKOB's [Ven13] work on (commutative) local ϵ-isomorphisms. Let us describe the conjectures.

The first conjecture is of global nature and will be studied in chapter 2. Let us fix a prime p and a compact p-adic Lie extension $F_\infty/\mathbb{Q}$ containing $\mathbb{Q}(\mu_{p^\infty})$, where μ_{p^∞} denotes the group of all p-power roots of unity. Moreover, we assume that $F_\infty = \bigcup_{n\geq 1} F_n$, where

$$\dots F_{n-1} \subseteq F_n \subseteq F_{n+1} \dots$$

is a tower of finite Galois extensions F_n of $\mathbb{Q}$. We write $\mathcal{G} = \mathrm{Gal}(F_\infty/\mathbb{Q})$ and $\mathcal{H} = G(F_\infty/\mathbb{Q}^{cyc})$, where $\mathbb{Q}^{cyc}$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, such that

$$\mathcal{G}/\mathcal{H} \cong \mathbb{Z}_p.$$

Then, we write $\mathcal{S}$ and $\mathcal{S}^*$ for the canonical left and right Ore sets of the Iwasawa algebra $\Lambda(\mathcal{G})$ from [CFK+05] associated to $\mathcal{H}$, see also the beginning of section 2.3 for a definition. Moreover, let Σ be the set of primes of $\mathbb{Q}$ consisting of the archimedean prime ν_∞ of $\mathbb{Q}$, the prime (p) and those primes that ramify in $F_\infty/\mathbb{Q}$ and assume that Σ is finite. The first conjecture predicts the existence of a universal element

$$L_{p,u} \in K_1(\Lambda(\mathcal{G})_{\mathcal{S}^*}).$$

This universal element $L_{p,u}$ depends on a global unit $u \in \varprojlim_n (\mathcal{O}_{F_n}^\times \otimes \mathbb{Z}_p)$ which is a $\Lambda(\mathcal{G})_S$-generator of $S^{-1}(\varprojlim_n (\mathcal{O}_{F_n}^\times \otimes \mathbb{Z}_p))$ (in general, such a unit is only conjectured to exist). $L_{p,u}$ is characterized by two properties. Firstly, it is supposed to satisfy an interpolation property (how to evaluate elements of $K_1(\Lambda(\mathcal{G})_{\mathcal{S}^*})$ at Artin representations is explained in [CFK+05]): its values at Artin representations ρ are supposed to interpolate the leading coefficient of the Artin L-function $L_\Sigma(\rho, s)$ of ρ divided by a regulator $R(u,\rho)$ depending on ρ and u, i.e.,

$$L_{p,u}(\rho) = \lim_{s\to 0} \frac{s^{-r_\Sigma(\rho)} L_\Sigma(\rho, s)}{R(u,\rho)}, \qquad (L_{p,u}\text{-values})$$

where $r_\Sigma(\rho)$ is the order of vanishing of $L_{\Sigma_f}(\rho, s)$ at $s = 0$. Note that this formula is reminiscent of the class number formula for number fields.

Secondly, $L_{p,u}$ is supposed to map to a prescribed element under the connecting homomorphism $\partial : K_1(\Lambda(\mathcal{G})_{\mathcal{S}^*}) \longrightarrow K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$ from K-theory, where $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$ denotes the category of finitely generated $\mathcal{G}$-modules that are $\mathcal{S}^*$-torsion. To be more concrete, let us define

$$\mathbb{H}^m_\Sigma := \varprojlim_n H^m_{\text{ét}}\big(\mathcal{O}_{F_n}[\frac{1}{\Sigma_f}], \mathbb{Z}_p(1)\big) \cong \varprojlim_n H^m\big(G_\Sigma(F_n), \mathbb{Z}_p(1)\big)$$

for $m \geq 1$ and note that these groups vanish for $m \geq 3$ since $cd_p G_\Sigma(F_n) \leq 2$ for any F_n, where we also write Σ for the primes of F_n above Σ. The Kummer sequence gives an isomorphism $\varprojlim_n(\mathcal{O}^\times_{F_n,\Sigma} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \xrightarrow{\sim} \mathbb{H}^1_\Sigma$ so that we can consider the image of u in $\mathbb{H}^1_\Sigma$. The idea is to consider $\mathbb{H}^1_\Sigma$ and $\mathbb{H}^2_\Sigma$ as *universal* Iwasawa modules attached to the extension $F_\infty/\mathbb{Q}$. Now, the second defining property of $L_{p,u}$ is given by

$$\partial(L_{p,u}) = [\mathbb{H}^2_\Sigma] - [\mathbb{H}^1_\Sigma/\Lambda(\mathcal{G})u]. \qquad (\partial\text{-image } L_{p,u})$$

While K. Kato formulated the global conjecture for the base field $\mathbb{Q}$ and, in general, non-abelian extensions $F_\infty/\mathbb{Q}$, we formulate an analogue of the conjecture for a quadratic imaginary base field K and prove it in the following commutative setting

(i) there exists an elliptic curve E/K with complex multiplication by the ring of integers $\mathcal{O}_K$ and conductor divisible by one prime of K only,

(ii) K_∞/K, where $K_\infty = K(E[p^\infty])$ is the field obtained by adjoining all coordinates of p-power division points of E to K for some prime $p \neq 2,3$ above which E has good ordinary reduction,

under the assumption that $\varprojlim_{k,n} Cl(K_{k,n})\{p\}$ is S^*-torsion, where we write $K_{k,n} = K(E[\pi^n\bar{\pi}^k])$, $k,n \geq 0$, for two generators π and $\bar{\pi}$ of the distinct primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ of K above p (p splits in K by assumption (ii)). $Cl(K_{k,n})\{p\}$ denotes the p-primary part of the ideal class group of $K_{k,n}$ and S^* denotes the canonical Ore set in $\Lambda(G)$, where we write G for the abelian p-adic Lie group $G(K_\infty/K)$.

It is more than likely that K. Kato knew (or at least expected) that an analogous conjecture holds in this abelian setting when he formulated the conjecture for the base field $\mathbb{Q}$. As for the generality of the above setting we note that all elliptic curves defined over $\mathbb{Q}$ that are listed in Appendix A, §3 of J. Silverman's book [Sil99] satisfy the assumptions (i) and (ii) (and, in fact, all assumptions of the cases in which we prove the local conjecture and the twist conjecture discussed below).

It turns out that under the just mentioned torsion assumption one can choose u to be a sequence of norm-compatible elliptic units $u = u(\mathfrak{q})$ in the tower $K_{k,n}$, $k,n \geq 1$, depending on an auxiliary ideal $\mathfrak{q}$ of $\mathcal{O}_K$ which is unramified in K_∞/K. The universal element $L_{p,u}$ is then given by $\frac{1}{(N\mathfrak{q}-\text{Frob}_\mathfrak{q})}$ which we show belongs to $\Lambda(G)^\times_S$, where $N\mathfrak{q}$ is the norm of the ideal $\mathfrak{q}$ and $\text{Frob}_\mathfrak{q}$ denotes the arithmetic Frobenius in $G(K_\infty/K)$. In [dS87], the element $\frac{1}{(N\mathfrak{q}-\text{Frob}_\mathfrak{q})}$ is used to make the p-adic L-function corresponding to $u(\mathfrak{q})$ (under the Coleman map for the formal group $\hat{E}$ and the integral logarithm) independent of the choice of $\mathfrak{q}$, just as the term $\sigma_e - 1$ appearing in the definition of ζ_p makes ζ_p independent of e, which we discussed in the paragraph after the cyclotomic main conjecture $(\mathrm{MC}(\mathbb{G}_m, \mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}))$.

Commutative Main Theorem (see Theorem 2.4.41). *Let the setting be as in (i) and (ii) above, assume that* $\varprojlim_{k,n} Cl(K_{k,n})\{p\}$ *is* S^**-torsion and write* $x_\mathfrak{q} = N\mathfrak{q} - \mathrm{Frob}_\mathfrak{q}$. *Then, under the connecting homomorphism* ∂, *the class* $[1/x_\mathfrak{q}] \in K_1(\Lambda(G)_{S^*})$ *of the element* $\frac{1}{x_\mathfrak{q}} \in \Lambda(G)_S^\times$ *maps to*

$$\partial\big([1/x_\mathfrak{q}]\big) = -[\Lambda(G)/\Lambda(G)x_\mathfrak{q}] = [\mathbb{H}^2_\Sigma] - [\mathbb{H}^1_\Sigma/\Lambda(G)u(\mathfrak{q})] \quad \text{in} \quad K_0(\mathfrak{M}_H(G)).$$

Moreover, $\frac{1}{x_\mathfrak{q}} = \frac{1}{(N\mathfrak{q} - \mathrm{Frob}_\mathfrak{q})}$ *satisfies the following interpolation property. Let* χ *be a complex Artin character* $\chi : G_K \longrightarrow \mathbb{C}^\times$ *such that the fixed field of the kernel is equal to* $\bar{K}^{\ker(\chi)} = K_{k,n}$, $k, n \geq 1$. *Then, we have (Kronecker's second limit formula)*

$$\frac{d}{ds} L_{\Sigma_f}(\chi, s)\,|_{s=0} = -\frac{1}{N\mathfrak{q} - \chi(\mathrm{Frob}_\mathfrak{q})} \cdot \frac{1}{12\omega_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}} \cdot \sum_{\sigma \in G(K_{k,n}/K)} \log|\,\sigma(e_{k,n}(\mathfrak{q}))\,|^2\,\chi(\sigma),$$

where $e_{k,n}(\mathfrak{q}) \in \mathcal{O}^\times_{K_{k,n}}$ *so that the image of* $(e_{k',n'}(\mathfrak{q}))_{k',n'}$ *in* $\varprojlim_{k,n}(\mathcal{O}^\times_{K_{k,n}} \otimes \mathbb{Z}_p)$ *coincides with* $u(\mathfrak{q})$ *and* $\omega_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}$ *denotes the number of roots of unity in* K *congruent to* 1 *modulo* $\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$, *where* $\mathfrak{f}$ *is the conductor of the Größencharacter* ψ_E *attached to* E/K.

Let us remark that for the interpolation property little work is needed as it is just a slight restatement of L. Kronecker's classical *second limit formula*. As for the determination of the image of $[1/x_\mathfrak{q}]$ under ∂, there are two main ingredients besides a vanishing result for finitely generated $\mathbb{Z}_p$-modules in $K_0(\mathfrak{M}_H(G))$ (which we derive in chapter 1 from results of G. Zábrádi [Zá10] and K. Ardakov and S. Wadsley [AW06], [AW08]) and the fact that the image of $u(\mathfrak{q})$ under the semi-local version of the Coleman map for $\hat{E}$ is not a zero-divisor in the Iwasawa algebra (which we prove in subsection 2.4.5). On the one hand, we use K. Rubin's result [Rub91] on the two variable main conjecture. On the other hand, we carefully compare K. Rubin's elliptic units $\mathcal{C}_\infty$ (which satisfy the analytic class number formula needed for the main result in loc. cit.) and the smaller group $\mathcal{D}_\infty$ considered by R. I. Yager [Yag82]. Strictly speaking, this comparison is needed in order to derive the two variable main conjecture in the CM case from K. Rubin's and R. I. Yager's work. Under assumption (i) from above, i.e., that the conductor $\mathfrak{f}$ of E is a prime power $\mathfrak{f} = \mathfrak{l}^r$ for some prime $\mathfrak{l}$ of K, we prove

Theorem (see Theorem 2.4.33). *In* $K_0(\mathfrak{M}_H(G))$ *we have an equality*

$$[\mathcal{C}_\infty/\mathcal{D}_\infty] = [\Lambda(G/D_\mathfrak{l})],$$

where we write $D_\mathfrak{l}$ *for the decomposition group of* $\mathfrak{l}$ *in* G.

Next, we discuss the second of K. KATO's conjectures, which is of local nature and will be studied in chapter 3. For a fixed prime p, we let F'_∞ be a p-adic Lie extension of $\mathbb{Q}_p$ containing $\mathbb{Q}_p(\mu_{p^\infty})$. We write $\mathcal{G}' = \mathrm{Gal}(F'_\infty/\mathbb{Q}_p)$ and $\mathcal{H}' = \mathrm{Gal}(F'_\infty/\mathbb{Q}_p^{cyc})$. Later, in the CM setting considered above, we will be interested in the case $F'_\infty = K_{\infty,\bar{\nu}}$ such that $\mathcal{G}' = G_{\bar{\nu}}$ is the decomposition group in G of a place $\bar{\nu}$ of K_∞ above p. Let us write $\widehat{\mathbb{Z}}_p^{ur}$ for the ring of Witt vectors $W(\bar{\mathbb{F}}_p)$ of a fixed algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$. Moreover, we write $\mathcal{S}'^*$ and $\tilde{\mathcal{S}}'^*$ for the canonical Ore sets in $\Lambda(\mathcal{G}')$ and $\widehat{\mathbb{Z}}_p^{ur}[[\mathcal{G}']]$, respectively.

The local conjecture predicts the existence of a universal *local constant-like* element

$$\mathcal{E}_{p,u'} \in K_1(\widehat{\mathbb{Z}}_p^{ur}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*})$$

depending on a local $\Lambda(\mathcal{G}')_{\mathcal{S}'}$-generator u' of $\mathcal{U}'(F'_\infty)_{\mathcal{S}'}$ belonging to $\mathcal{U}'(F'_\infty) = \varprojlim_{L,m} \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^{p^m}$, where the limit is taken over all finite subextensions $L/\mathbb{Q}_p$ of $F'_\infty/\mathbb{Q}_p$, with respect to norm maps, and all $m \in \mathbb{N}$. The element $\mathcal{E}_{p,u'}$, similar to $L_{p,u}$ above, is characterized by an interpolation property and by the requirement to map to a prescribed element under the connecting homomorphism $\partial : K_1(\widehat{\mathbb{Z}}_p^{ur}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*}) \to K_0(\mathfrak{M}_{\widehat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}'}(\mathcal{G}'))$ from K-theory, where $\mathfrak{M}_{\widehat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}'}(\mathcal{G}')$ denotes the category of finitely generated $\widehat{\mathbb{Z}}_p^{ur}[[\mathcal{G}']]$-modules that are $\tilde{\mathcal{S}}'^*$-torsion. In order to state the conjecture let us define the local universal cohomology groups

$$\mathbb{H}^m_{\mathrm{loc}} = \varprojlim_{L'} H^m(L', \mathbb{Z}_p(1))$$

for $m \geq 1$, where L' ranges through the finite subextensions of $F'_\infty/\mathbb{Q}_p$, and note that $\mathbb{H}^m_{\mathrm{loc}} = 0$ for $m \geq 3$ since $cd_p(G_{L'}) = 2$. We note that Kummer theory gives a map $\mathcal{U}'(F'_\infty) \longrightarrow \mathbb{H}^1_{\mathrm{loc}}$.

Local Main Conjecture. *There exists $\mathcal{E}_{p,u'} \in K_1(\widehat{\mathbb{Z}}_p^{ur}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*})$ such that for any Artin representation $\rho : \mathcal{G}' \longrightarrow \mathrm{Aut}_{\mathbb{C}_p}(V)$,*

$$\mathcal{E}_{p,u'}(\rho) = \frac{\epsilon_p(\rho)}{R_p(u',\rho)} \qquad (\mathcal{E}_{p,u'}\text{-values})$$

whenever $R_p(u',\rho) \neq 0$, where $\epsilon_p(\rho) = \epsilon_p(V)$ is the local constant attached to V and $R_p(u',\rho)$ is a p-adic regulator associated to ρ and u'. Moreover, the image of $\mathcal{E}_{p,u'}$ under the connecting homomorphism from K-theory is given by

$$\partial(\mathcal{E}_{p,u'}) = \left[\widehat{\mathbb{Z}}_p^{ur}\hat{\otimes}_{\mathbb{Z}_p}\mathbb{H}^2_{\mathrm{loc}}\right] - \left[\widehat{\mathbb{Z}}_p^{ur}\hat{\otimes}_{\mathbb{Z}_p}\left(\mathbb{H}^1_{\mathrm{loc}}/\Lambda(\mathcal{G}')u'\right)\right] \quad \text{in} \quad K_0(\mathfrak{M}_{\widehat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}'}(\mathcal{G}')). \qquad (\partial\text{-image } \mathcal{E}_{p,u'})$$

Based on the existence of an ϵ-isomorphism $\epsilon'_{\Lambda(G)}(\mathbb{T}_{un})$, O. VENJAKOB [Ven13] constructs an element $\mathcal{E}_{p,u'}$ satisfying (∂-image $\mathcal{E}_{p,u'}$) for abelian p-adic Lie extensions $F'_\infty/\mathbb{Q}_p$ of the form $F'_\infty = K'(\mu_{p^\infty})$, where K' is an infinite unramified extension of $\mathbb{Q}_p$. Moreover, in this setting a local $\Lambda(\mathcal{G}')_{\mathcal{S}'}$-generator u' of $\mathcal{U}'(F'_\infty)_{\mathcal{S}'}$ exists. We will prove that for $F'_\infty = K'(\mu_{p^\infty})$ O. VENJAKOB's element $\mathcal{E}_{p,u'}$ (multiplied by -1) has the desired interpolation property ($\mathcal{E}_{p,u'}$-values) for Artin characters. Since $\mathcal{E}_{p,u'}$, or rather $\mathcal{E}_{p,u'}^{-1}$ actually belongs to $\widehat{\mathbb{Z}}_p^{ur}[[\mathcal{G}']] \cap (\widehat{\mathbb{Z}}_p^{ur}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*})^\times$ we may consider $\mathcal{E}_{p,u'}^{-1}$ as a $\widehat{\mathbb{Z}}_p^{ur}$-valued measure on $\mathcal{G}'$. Our main result towards the local conjecture is

Theorem (see Theorem 3.3.7). *Let F'_∞ be of the form $K'(\mu_{p^\infty})$ as above. Then, for an Artin character $\chi : \mathcal{G}' \longrightarrow \mathbb{C}_p^\times$ we always have*

$$\Big(\int_{\mathcal{G}'} \chi \; d(\mathcal{E}_{p,u'}^{-1}) \Big) \cdot \varepsilon_p(\chi, \psi_{\epsilon^{-1}}, dx) = -R_p(u', \chi),$$

regardless of whether $R_p(u', \chi) \neq 0$.

It follows that $-\mathcal{E}_{p,u'}$ (O. Venjakob's element multiplied by -1) has the interpolation property ($\mathcal{E}_{p,u'}$-values). Note that multiplying by -1 does not change the image of $\mathcal{E}_{p,u'}$ under ∂. The proof of this interpolation property is a rather lengthy computation unwinding the definition of $\mathcal{E}_{p,u'}^{-1}$, which involves the Coleman map for $\mathbb{G}_m$ and the integral logarithm, and using the fact that the local constans $\varepsilon_p(\chi, \psi_{\epsilon^{-1}}, dx)$ can be expressed as Gauß sums. The use of R. F. Coleman's machinery for the formal group $\mathbb{G}_m$ is the reason why we have to introduce $\widehat{\mathbb{Z}}_p^{ur}$-coefficients.

The third of K. Kato's conjectures, which will be studied in chapter 6, brings together the elements $L_{p,u} = \frac{1}{(N\mathfrak{q} - \mathrm{Frob}_\mathfrak{q})} \in K_1(\Lambda(G)_{S^*})$ from the commutative main theorem and $\mathcal{E}_{p,u'} \in K_1(\widehat{\mathbb{Z}}_p^{ur}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*})$ from the local main conjecture. In fact, let $E/\mathbb{Q}$ be one of the elliptic curves from ([Sil99], Appendix A, §3) with complex multiplication by $\mathcal{O}_K$, K quadratic imaginary (these curves have bad reduction at one prime (l) only and this prime ramifies in $K/\mathbb{Q}$). As before, we set $K_\infty = K(E[p^\infty])$ for some prime p at which E has good ordinary reduction, which implies that p splits in K into disctinct primes $\mathfrak{p} = (\pi)$ and $\bar{\mathfrak{p}} = (\bar{\pi})$.

Let us write $\mathcal{G}$ for the non-abelian Galois group $G(K_\infty/\mathbb{Q})$ and $\mathcal{H} = G(K_\infty/\mathbb{Q}^{cyc})$. Moreover, we fix some prime $\bar{\nu}$ of K_∞ above $\mathfrak{p}$ and consider the extension $K_{\infty,\bar{\nu}}/\mathbb{Q}_p$ which is abelian (since p splits) and of the form $K'(\mu_{p^\infty})$ for some infinite unramified extension $K'/\mathbb{Q}_p$, in fact, one can take $K' = \bigcup_k K_\mathfrak{p}(E[\bar{\pi}^k])$ which follows from the Weil pairing. In particular, the local main conjecture holds for $\mathcal{G}' = G(K_{\infty,\bar{\nu}}/\mathbb{Q}_p)$, i.e., $\mathcal{E}_{p,u'}$ exists. The Galois groups we consider are related as follows

$$\mathcal{G}' \subset G \subset \mathcal{G},$$

where $\mathcal{G}'$ and G are abelian and $\mathcal{G}$ is non-abelian.

In chapter 1, based on work from [Ven03], we define twist operators $\tau_{E_{\bar{\pi}}(-1)}$ on $K_1(\Lambda(G)_{S^*})$ and $\tau_{E/\hat{E}(-1)}$ on $K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*})$ which are induced by the G-module $T_{\bar{\pi}}E(-1)$ and the $\mathcal{G}'$-module $(T_pE/T_p\hat{E})(-1)$, respectively, where (-1) denotes the -1-th Tate twist, $T_{\bar{\pi}}E = \varprojlim_n E[\bar{\pi}^n]$ and $T_p\hat{E} = \varprojlim_n \hat{E}[p^n]$. In particular, we are interested in the elements

$$\tau_{E_{\bar{\pi}}(-1)}(L_{p,u}) \in K_1(\Lambda(G)_{S^*}), \quad \tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'}) \in K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*}).$$

In section A.4 we recall that the modules $\mathbb{H}^1_\Sigma$, $\mathbb{H}^2_\Sigma$, $\mathbb{H}^1_{\mathrm{loc}}$ and $\mathbb{H}^2_{\mathrm{loc}}$ appear in the sequence of G. Poitou [Poi67] and J. Tate [Tat63] for the module $\mathbb{Z}_p(1)$. Using a result of T. Fukaya and K. Kato (about cases when tensoring commutes with taking cohomology), we then show that tensoring these modules by $T_{\bar{\pi}}E(-1)$ and $(T_pE/T_p\hat{E})(-1)$, respectively, and passing to the induced $\mathcal{G}$-modules, the resulting modules are related to the Pontryagin dual of the Selmer group

$$\mathrm{Sel}(K_\infty, T_pE^*(1))^\vee$$

through the Poitou-Tate sequence for T_pE. Here, T_pE^* denotes the $\mathbb{Z}_p$-dual representation of T_pE. The dual Selmer group is introduced in chapter 4, where we also study its relationship to the Poitou-Tate sequence. One of the noteworthy results of this chapter is the vanishing of $\varprojlim_n H^1_f(G_\Sigma(K(E[p^n])), T_pE)$, where H^1_f denotes the finite part of cohomology, which we prove in subsection 4.3.5 (similar results appear in the literature for the cyclotomic $\mathbb{Z}_p$-extension, e.g., in [Kat04]). In order to derive relations in $K_0(\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}}(\mathcal{G}))$ from the Poitou-Tate sequence for T_pE we have to introduce the quotients

$$\mathbb{H}^1_{\mathrm{loc}}/\Lambda(\mathcal{G}')u' \quad \text{and} \quad \mathbb{H}^1_\Sigma/\Lambda(G)u(\mathfrak{q})$$

which belong to $\mathfrak{M}_{\mathcal{H}'}(\mathcal{G}')$ and $\mathfrak{M}_H(G)$, respectively, while $\mathbb{H}^1_{\mathrm{loc}}$ and $\mathbb{H}^1_\Sigma$ do not.

This aim motivates the definition of $\Omega_{p,u,u'} \in \Lambda(\mathcal{G})^\times_{S^*}$ in chapter 5, which, by definition is a base change between two generators determined by u and u', respectively, of

$$\left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T_pE/T_p\hat{E}(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}}\right)\right)_{\mathcal{S}^*},$$

which is a free $\Lambda(\mathcal{G})_{\mathcal{S}^*}$-module of rank 1. It turns out that there is a canonical way to define $\Omega_{p,u,u'}$ so that it is independent of chosen bases of $T_{\bar{\pi}}E(-1)$ and $T_pE/T_p\hat{E}(-1)$. Finally, we may define

$$\mathcal{L}_{p,u,E} \coloneqq \frac{\tau_{E_{\bar{\pi}}(-1)}(L_{p,u})}{\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})} \cdot \Omega_{p,u,u'} \in K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*}),$$

where $\tilde{\mathcal{S}}^*$ is a canonical Ore set in $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]$ and for which we note that there are canonical maps between K_1-groups $K_1(\Lambda(G)_{S^*}) \to K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*})$ and $K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*}) \to K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*})$. Let us write $\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}}(\mathcal{G})$ for the category of finitely generated $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]$-modules which are $\tilde{\mathcal{S}}^*$-torsion. Our main theorems are the following.

Twist Theorem (see theorem 6.2.3). *Assume that* $\mathrm{Sel}(K_\infty, T_pE^*(1))^\vee$ *is* $\mathcal{S}^*$*-torsion. Then, up to a twisted Euler factor,* $\mathcal{L}_{p,u,E}$ *is a characteristic element of* $\hat{\mathbb{Z}}_p^{\mathrm{ur}}\hat{\otimes}_{\mathbb{Z}_p}\mathrm{Sel}(K_\infty, T_pE^*(1))^\vee$*, i.e., we have*

$$\partial(\mathcal{L}_{p,u,E}) = [\hat{\mathbb{Z}}_p^{\mathrm{ur}}\hat{\otimes}_{\mathbb{Z}_p}\mathrm{Sel}(K_\infty, T_pE^*(1))^\vee] + [\hat{\mathbb{Z}}_p^{\mathrm{ur}}\hat{\otimes}_{\mathbb{Z}_p}\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_{\nu_l}} T_pE(-1)] \quad \text{in} \quad K_0(\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}}(\mathcal{G})),$$

where l *is the unique prime at which* $E/\mathbb{Q}$ *has bad reduction and* $\mathcal{G}_{\nu_l}$ *is the decomposition group of some place of* K_∞ *above* l*.*

In order to determine the interpolation property of $\mathcal{L}_{p,u,E}$ we then first prove

Theorem (see theorem 6.2.5). *The element* $\frac{\Omega_{p,u,u'}}{\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})}$ *is equal to the* $\tau_{E_{\bar{\pi}}(-1)}$*-twist of the image of* u *under the semi-local version of the Coleman map for* $\mathbb{G}_m$*, i.e.,*

$$\frac{\Omega_{p,u,u'}}{\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})} = \tau_{E_{\bar{\pi}}(-1)}\Big(\sum_{\sigma \in G/\mathcal{G}'} \sigma \cdot \big(-\mathcal{L}_{\epsilon^{-1}}(loc_{\bar{\nu}}(\sigma^{-1}u))\big)\Big) \qquad \text{in} \qquad \big(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]\big)_{\mathcal{S}^*},$$

which shows that the left side does not depend on u'*. In particular,* $\mathcal{L}_{p,u,E}$ *is independent of* u'*.*

From this theorem we conclude that $\mathcal{L}_{p,u,E}$ is just a different guise of a well-known element studied in [dS87] for which an interpolation formula exists. In fact, we have the following

Corollary (see corollary 6.2.6). *We have an equality of elements in* $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\mathcal{S}^*}$

$$\mathcal{L}_{p,u,E} = \tau_{\psi^{-1}}(\lambda),$$

where $\tau_{\psi^{-1}}(\lambda)$ *denotes the twist of de Shalit's element* $\lambda \in \Lambda(G)$ *(from definition 2.4.24) by the* G*-module* $(T_\pi E)^*$*. The action of* G *on* $(T_\pi E)^*$ *is given by* ψ^{-1}*. For an Artin character* χ *of* $\mathcal{G}$ *we have*

$$\frac{1}{\Omega_p} \cdot \int_G \mathrm{Res}_G^{\mathcal{G}} \chi \, d\mathcal{L}_{p,u,E} = \frac{1}{\Omega} \cdot G\big(\psi \cdot \mathrm{Res}\chi\big) \cdot \Big(1 - \frac{(\psi \cdot \mathrm{Res}\chi)(\mathfrak{p})}{p}\Big) \cdot L_{\mathfrak{f}\bar{\mathfrak{p}}}((\psi \cdot \mathrm{Res}\chi)^{-1}, 0), \quad (0.0.1)$$

where $\psi = \psi_E$ *is the Größencharacter of* E/K *and we refer to ([dS87], p. 80) for the definition of* $G\big(\psi \cdot \mathrm{Res}\chi\big)$ *which is related to a local constant. In the expression* $(\psi \cdot \mathrm{Res}\chi)(\mathfrak{p})$ *we consider* $\psi \cdot \mathrm{Res}\chi$ *as a map on ideals of* K *prime to* $\mathfrak{f}$*.* Ω *is a complex period and* Ω_p *is a* p*-adic period determining an isomorphism of formal group* $\mathbb{G}_m \cong \hat{E}$*.*

Notation and Conventions

(i) Unless stated otherwise, group actions are assumed to be left-actions and modules over any ring are assumed to be left-modules.

(ii) If G is a profinite group and $\mathcal{O}_L$ is the ring of integers of a finite extension L of $\mathbb{Q}_p$, then we assume all $\mathcal{O}_L[[G]]$-modules to be Hausdorff topological $\mathcal{O}_L[[G]]$-modules. In particular, the G-action is continuous implying that for compact modules M and discrete modules D we have

$$M \cong \varprojlim_U M_U \qquad \text{and} \qquad D = \bigcup_U D^U,$$

where U runs through the open normal subgroups of G and the M_U denote the U-coinvariants while the D^U denote the U-invariants.

(iii) Let G be a group and H a subgroup of G. For a module A with an action of H we write

$$\mathrm{Ind}_G^H A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A \qquad \text{and} \qquad \mathrm{Coind}_G^H A = \mathrm{Map}_H(G, A),$$

for the induced and the coinduced module, which are left- and right adjoint to the forgetful functor G−Mod → H−Mod, respectively. If G is a profinite group, H a closed subgroup of G and M a compact $\mathbb{Z}_p[[H]]$-module, then we write

$$\text{c–Ind}_G^H A = \mathbb{Z}_p[[G]] \hat{\otimes}_{\mathbb{Z}_p[[H]]} M \tag{0.0.2}$$

for the compact induction of M from the closed subgroup H to G.

(iv) For a profinite group G and a topological finitely generated (free) $\mathbb{Z}_p$-module T with a continuous $\mathbb{Z}_p$-linear action of G we write

$$T^* = \mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p)$$

for the $\mathbb{Z}_p$-dual representation, where $g \in G$ acts on $f \in T^*$ by $(g.f)(t) := f(g^{-1}t)$, $t \in T$. For a compact module like T we write

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

for the Pontryagin dual, the discrete module of continuous homomorphisms from T to the discrete module $\mathbb{Q}_p/\mathbb{Z}_p$. If T is endowed with an action of G as above, then we define an action on $T^\vee$ by $(g.f)(t) := f(g^{-1}t)$, $g \in G$, $f \in T^\vee$, $t \in T$. For a discrete $\mathbb{Z}_p$-module D we define $D^\vee$ similarly

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

where the second equation holds since D is discrete. As before, if D carries a $\mathbb{Z}_p$-linear action of G, then so does $D^\vee$.

(v) For any ring R, an R-module M and a right and left denominator set S of R we will R_S for the ring localized at S and M_S for the usual localized R_S-module. Sometimes we also write $S^{-1}R$ and $S^{-1}M$ for the localizations R_S and M_S, respectively.

Chapter 1

Some K-theory

In classical commutative Iwasawa theory one uses the notion of *pseudo-isomorphism* in order to define principal characteristic ideals attached to (torsion) Iwasawa modules M, see, e.g., [Rub91] and [Was97]. Generators of the characteristic ideals attached to M are called characteristic elements of M and the search for characteristic elements of certain Iwasawa modules prompted the formulation of several well-known main conjectures. As is explained in [CFK$^+$05], in general, in non-commutative Iwasawa theory the structure theory from the commutative setting is no longer at our disposal.

For Iwasawa algebras of (non-abelian) p-adic Lie groups G containing a closed normal subgroup H such that $G/H \cong \mathbb{Z}_p$ an alternative approach has been developed in [Ven03] and [CFK$^+$05]. Instead of defining characteristic ideals one considers classes of modules in the Grothendieck group $K_0(\mathfrak{M}_H(G))$ of the category $\mathfrak{M}_H(G)$ of finitely generated $\Lambda(G)$-modules M that are S^*-torsion (see (A.8.2) for a definition of S^*), the hope being that arithmetically interesing $\Lambda(G)$-torsion modules belong to this category. Moreover, an element of $K_1(\Lambda(G)_{S^*})$ is called a characteristic element of a module M belonging to $\mathfrak{M}_H(G)$ if it maps to $[M] \in K_0(\mathfrak{M}_H(G))$ under the connecting homomorphism

$$\partial : K_1(\Lambda(G)_{S^*}) \longrightarrow K_0(\mathfrak{M}_H(G))$$

from K-theory. We refer to [Ven03] for a discussion that this appoach is an adequate alternative to the classical one used in commutative Iwasawa theory.

In section 1.1 of this chapter we introduce twist operators on the above K-groups building on results of ([Ven03], chapter 7), but working with more general discrete valuation rings $\mathcal{O}$ than $\mathbb{Z}_p$ since we will later also be interested in results over $\hat{\mathbb{Z}}_p^{ur}$. The twist operators are defined in such a way that they are compatible with the map ∂ and with extensions of scalars from $\mathbb{Z}_p$ to $\hat{\mathbb{Z}}_p^{ur}$ coefficients.

In section 1.2, building on results of Zábrádi [Z1́0] and Ardakov and Wadsley [AW06], [AW08], we will show in corollary 1.2.3 that for certain pairs $H \subset G$ the classes of finitely generated $\mathbb{Z}_p$-modules vanish in $K_0(\mathfrak{M}_H(G))$.

1.1 Twist Operators on K_1- and K_0-groups

In this section we will define twist operators on K_1-groups of certain localized Iwasawa algebras and also give compatible definitions for alternative descriptions of the K_1-groups. We twist with respect to continuous representations

$$\rho : G \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T),$$

where G is a p-adic Lie group containing a closed subgroup H such that $G/H \cong \mathbb{Z}_p$ and T is a free $\mathbb{Z}_p$-module of finite rank.

With a view to the algebraic side of the main conjectures from Iwasawa theory we want to determine how twisting affects the image of an element under the connecting homomorphism from K-theory. As we will see in lemma 1.1.20 twisting on the K_1-side corresponds to tensoring and passing to the diagonal action on the K_0-side. This result will then be used in the next chapter in the proof of the twist conjecture for the p-adic L-function of an elliptic curve with CM.

1.1.1 Technical background

In this section we prove some lemmata for $\mathbb{Z}_p[[G]]$- and $\hat{\mathbb{Z}}_p^{ur}[[G]]$-modules that we need in order to define twist operators on K-groups. Let us begin with $\mathbb{Z}_p[[G]]$-modules. Let G be a profinite group and let $\mathcal{O} = \mathcal{O}_L$ be the ring of integers of a finite extension L of $\mathbb{Q}_p$. We write $\Lambda(G) = \Lambda_{\mathcal{O}}(G)$ for the Iwasawa algebra with coefficients in $\mathcal{O}$ and consider continuous representations

$$\rho : G \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T),$$

where T is a finitely generated $\mathcal{O}$-module, free of rank r. We fix an $\mathcal{O}$-basis of T, i.e., an $\mathcal{O}$-linear isomorphism

$$\phi_T : T \cong \mathcal{O}^r,$$

where we consider the elements of $\mathcal{O}^r$ as column vectors. In the following, for any finitely generated left $\Lambda(G)$-module M, unless specified otherwise, we always consider the left action of $\Lambda(G)$ on $T \otimes_{\mathcal{O}} M$ induced by $g.(t \otimes m) := (\rho(g)(t)) \otimes gm$ for $g \in G, t \in T, m \in M$. We will call this the diagonal action. For $\rho(g)(t)$ we simply write $g.t$, for any $g \in G$, $t \in T$.

We will need the following Lemma.

Lemma 1.1.1. *For any choice of $\phi : T \cong \mathcal{O}^r$ we have a canonical isomorphism of left $\Lambda(G)$-modules*

$$T \otimes_{\mathcal{O}} \Lambda(G) \xrightarrow{\sim} \Lambda(G)^r,$$

with respect to the diagonal $\Lambda(G)$-action on the left and the canonical $\Lambda(G)$-action on the right. The isomorphism is induced by mapping $t \otimes g$ to $\phi\big(g^{-1}.t\big)g$, where $g \in G$, $t \in T$. Here we consider the elements of $\Lambda(G)^r$ as column vectors.

Proof. This lemma is quoted from ([Ven03], Lemma 7.2), but note that we use the canonical isomorphism

$$T \otimes_{\mathcal{O}} \Lambda(G) \cong \Lambda(G) \otimes_{\mathcal{O}} T,$$

which is $\Lambda(G)$-linear with respect to the diagonal actions on both sides. □

Next we turn to $\hat{\mathbb{Z}}_p^{ur}[[G]]$-modules. As above, let G be a profinite group. The aim of the rest of this subsection is threefold. First, we want to show that the tensor product of a finitely generated pseudo-compact $\hat{\mathbb{Z}}_p^{ur}[[G]]$-module with a free $\mathbb{Z}_p$-module of finite rank naturally has a $\hat{\mathbb{Z}}_p^{ur}[[G]]$-action induced by the diagonal G-action (as in the $\mathbb{Z}_p[[G]]$-case), see lemma 1.1.4. Then, we show that a $\hat{\mathbb{Z}}_p^{ur}$-version of lemma 1.1.1 holds, see lemma 1.1.5. Lastly, we will prove that twisting commutes with extension of scalars from $\mathbb{Z}_p[[G]]$- to $\hat{\mathbb{Z}}_p^{ur}[[G]]$-modules, see corollary 1.1.7. For the notion of pseudo-compact modules over topological rings we refer to [Wit03] and note that being pseudo-compact is not an intrinsic topological property of the module but a relative property with respect to the ring. For example, $\hat{\mathbb{Z}}_p^{ur}$ is pseudo-compact as a $\hat{\mathbb{Z}}_p^{ur}$-module, but not as a $\mathbb{Z}_p$-module.

We write $\tilde{\Lambda}(G) = \Lambda(G)\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur}$. For any open (or closed) subgroup U of G we write $\tilde{I}(U)$ for the kernel of the augmentation map $\tilde{\Lambda}(U) \twoheadrightarrow \hat{\mathbb{Z}}_p^{ur}$.

Remark 1.1.2. (i) Underlying all of what follows in this subsection is the fact that the two-sided ideals of $\tilde{\Lambda}(G)$ of the form

$$(p^n\tilde{\Lambda}(G) + \tilde{I}(U)), \qquad n \geq 1, U \text{ open and normal in } G,$$

generate the topology of $\tilde{\Lambda}(G)$ and that the modules

$$\tilde{\Lambda}(G)/(p^n\tilde{\Lambda}(G) + \tilde{I}(U)) \cong \hat{\mathbb{Z}}_p^{ur}/p^n[G/U]$$

for open and normal U in G and $n \geq 1$, are discrete and of finite length as $\hat{\mathbb{Z}}_p^{ur}$-modules, compare ([Sch11], Chapter IV, §19).

(ii) All topological rings that we will consider, i.e., $\mathbb{Z}_p$, $\hat{\mathbb{Z}}_p^{ur}$, $\mathbb{Z}_p[[G]]$ and $\hat{\mathbb{Z}}_p^{ur}[[G]]$, are pseudo-compact as right- and left-modules over themselves.

(iii) Note that (as in the case of $\Lambda(G)$-modules) any $\tilde{\Lambda}(G)$-linear map $M \to N$ between modules M, N equipped with the topologies induced by the submodules $\{p^nM + \tilde{I}(U)M\}_{n,U}$ and $\{p^nN + \tilde{I}(U)N\}_{n,U}$, respectively, where n ranges through $\mathbb{N}_{\geq 1}$ and U through the open normal subgroups of G, is continuous.

In our setting, proposition A.7.2 says the following.

Proposition 1.1.3. *Let G be a profinite group. The topology of any finitely generated pseudo-compact $\tilde{\Lambda}(G)$-module M coincides with the topology induced by the submodules $\{p^nM + \tilde{I}(U)M\}_{n,U}$, where n ranges through $\mathbb{N}_{\geq 1}$ and U through the open normal subgroups of G.*

Using proposition 1.1.3 we can prove the following lemma. We remark that for a finitely generated pseudo-compact $\tilde{\Lambda}(G)$-module M, the submodules $\{p^nM + \tilde{I}(U)M\}_{n,U}$, considered as $\mathbb{Z}_p$-submodules, form a cofinal system among all open $\mathbb{Z}_p$-submodules of M, simply because the $\{p^nM + \tilde{I}(U)M\}_{n,U}$ form a fundamental system of open neighbourhoods of 0.

Lemma 1.1.4. *Let T be a free $\mathbb{Z}_p$-module of finite rank $r \geq 1$ with a continuous $\mathbb{Z}_p$-linear G-action and let M be a finitely generated pseudo-compact $\tilde{\Lambda}(G)$-module. Then, we have an isomorphism*

$$T \otimes_{\mathbb{Z}_p} M \cong T \hat{\otimes}_{\mathbb{Z}_p} M$$

induced by the natural map $T \otimes_{\mathbb{Z}_p} M \to T\hat{\otimes}_{\mathbb{Z}_p} M$. In particular, one can extend the diagonal G-action on $T \otimes_{\mathbb{Z}_p} M$, i.e., $g.(t \otimes m) := (g.t) \otimes (g.m)$, $g \in G$, $t \in T$, $m \in M$, to an action of $\hat{\mathbb{Z}}_p^{ur}[[G]]$.

Proof. In the following we will consider pairs (n, U) such that $n \in \mathbb{N}_{\geq 1}$ and U is an open and normal subgroup of G acting trivially on T/p^n. Such pairs (n, U) form a cofinal subsystem of all pairs (n, U) without any restriction on the open and normal U. Fixing an isomorphism $\phi_T : T \cong \mathbb{Z}_p^r$, we have

$$\begin{aligned} T\hat{\otimes}_{\mathbb{Z}_p} M &\overset{\text{def}}{=} \varprojlim_{n,U} \left(T/p^n \otimes_{\mathbb{Z}_p} M \big/ (p^nM + \tilde{I}(U)M)\right) \\ &\cong \varprojlim_{n,U} \left(T \otimes_{\mathbb{Z}_p} M \big/ (p^nM + \tilde{I}(U)M)\right) \\ &\cong \varprojlim_{n,U} \left(\mathbb{Z}_p^r \otimes_{\mathbb{Z}_p} M \big/ (p^nM + \tilde{I}(U)M)\right) \\ &\cong \varprojlim_{n,U} \left(\left(M \big/ (p^nM + \tilde{I}(U)M)\right)^r\right) \\ &\cong M^r \\ &\cong \mathbb{Z}_p^r \otimes_{\mathbb{Z}_p} M \\ &\cong T \otimes_{\mathbb{Z}_p} M. \end{aligned} \tag{1.1.1}$$

But the module $\varprojlim_{n,U} \left(T/p^n \otimes_{\mathbb{Z}_p} M \big/ (p^nM + \tilde{I}(U)M)\right)$ carries a natural action of $\hat{\mathbb{Z}}_p^{ur}[[G]]$ induced by the action of $\hat{\mathbb{Z}}_p^{ur}/p^n[G/U]$ on $T/p^n \otimes_{\mathbb{Z}_p} M \big/ (p^nM + \tilde{I}(U)M)$, which, in turn, is induced by the diagonal action of G/U. ◻

Next, we state a $\hat{\mathbb{Z}}_p^{ur}$-version of lemma 1.1.1

Lemma 1.1.5. *For any choice of $\phi : T \cong \mathbb{Z}_p^r$ we have a canonical isomorphism of left $\tilde{\Lambda}(G)$-modules*

$$T \otimes_{\mathbb{Z}_p} \tilde{\Lambda}(G) \xrightarrow{\sim} \tilde{\Lambda}(G)^r,$$

with respect to the diagonal $\tilde{\Lambda}(G)$-action on the left (see lemma 1.1.4) and the canonical $\tilde{\Lambda}(G)$-action on the right. The isomorphism is induced by mapping $t \otimes g$ to $\phi\big(g^{-1}.t\big)g$, where $g \in G$, $t \in T$. Here we consider the elements of $\tilde{\Lambda}(G)^r$ as column vectors.

Proof. One can copy the proof of lemma 1.1.1, see ([Ven03], Lemma 7.2), using that for pairs (U,n), where $n \geq 1$ is an integer and U is an open normal subgroup of G such that U acts trivially on T/p^n, the isomorphism

$$T/p^n \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G/U] \cong \mathbb{Z}_p^r/p^n \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G/U], \quad \bar{t} \otimes \bar{g} \longmapsto \overline{\phi(g^{-1}.t)} \otimes \bar{g},$$

induces an isomorphism

$$T/p^n \otimes_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur}[G/U] \cong \mathbb{Z}_p^r/p^n \otimes_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur}[G/U],$$

by tensoring with $- \otimes_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur}$. The only point that needs special attention is the isomorphism

$$T \otimes_{\mathbb{Z}_p} \tilde{\Lambda}(G) \cong T \hat{\otimes}_{\mathbb{Z}_p} \tilde{\Lambda}(G),$$

which holds by lemma 1.1.4. □

We now prove the fact that twisting commutes with extension of scalars $\tilde{\Lambda}(G) \otimes_{\Lambda(G)} -$ for finitely presented $\Lambda(G)$-modules. For any open or closed subgroup U of G let us write $I(U)$ for the kernel of the augmentation map $\Lambda(U) \twoheadrightarrow \mathbb{Z}_p$.

Remark 1.1.6. (i) Let M be a finitely presented $\Lambda(G)$-module. Then, as in remark A.8.18, one can show that

$$\tilde{\Lambda}(G) \otimes_{\Lambda(G)} M \cong \hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} M.$$

(ii) If M is finitely generated as a $\Lambda(G)$-module, then $\hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} M$ is finitely generated and pseudo-compact as a $\tilde{\Lambda}(G)$-module. Indeed, if M is finitely generated over $\Lambda(G)$, then it is compact and its topology is generated by the submodules $\{p^n M + I(U)M\}_{n\geq 1, U}$, U open and normal in G, see ([NSW08], (5.2.17) Proposition (ii)). By ([Wit03], Proposition 1.10), $\hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} -$ is right exact on compact $\mathbb{Z}_p$-modules showing that $\hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} M$ is certainly finitely generated as a $\tilde{\Lambda}(G)$-module. Moreover, by definition, we have

$$\hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} M = \varprojlim_{n,U} \left(\hat{\mathbb{Z}}_p^{ur}/p^n \otimes_{\mathbb{Z}_p} M/(p^n M + I(U)M) \right)$$

and $\hat{\mathbb{Z}}_p^{ur}/p^n \otimes_{\mathbb{Z}_p} M/(p^n M + I(U)M)$ is of finite length even as a $\hat{\mathbb{Z}}_p^{ur}$-module (since $M/(p^n M + I(U)M)$ is finitely generated as a $\mathbb{Z}_p$-module), so it is certainly of finite length as a $\tilde{\Lambda}(G)$-module.

If $\tilde{M}$ is a finitely generated pseudo-compact $\tilde{\Lambda}(G)$-module and T a free $\mathbb{Z}_p$-module of rank r with continuous action of G, then we equip $T \otimes_{\mathbb{Z}_p} \tilde{M}$ with the $\tilde{\Lambda}(G)$-action induced by the diagonal action of G, i.e., $g.(t \otimes \tilde{m}) := (g.t) \otimes (g\tilde{m})$, for $g \in G, t \in T, \tilde{m} \in \tilde{M}$, compare lemma 1.1.4.

Corollary 1.1.7. *Let M be a finitely presented $\Lambda(G)$-module. Then, we have an isomorphism*

$$\tilde{\Lambda}(G) \otimes_{\Lambda(G)} (T \otimes_{\mathbb{Z}_p} M) \cong T \otimes_{\mathbb{Z}_p} (\tilde{\Lambda}(G) \otimes_{\Lambda(G)} M)$$

of $\tilde{\Lambda}(G)$-modules, mapping $\tilde{\lambda} \otimes (t \otimes m)$ to $\tilde{\lambda}\big(t \otimes (1 \otimes m)\big)$, where $\tilde{\lambda} \in \tilde{\Lambda}, t \in T, m \in M$.

Proof. Recall that for finitely generated $\Lambda(G)$-modules N the original topology coincides with that induced by the submodules $\{p^n N + I(U)N\}_{n,U}$ where U is open and normal in G by ([NSW08], (5.2.17) Proposition). Therefore, any $\Lambda(G)$-homomorphism between finitely generated $\Lambda(G)$-modules is continuous. Now, one can show that there always is a map

$$\tilde{\Lambda}(G) \otimes_{\Lambda(G)} (T \otimes_{\mathbb{Z}_p} M) \longrightarrow T \otimes_{\mathbb{Z}_p} (\tilde{\Lambda}(G) \otimes_{\Lambda(G)} M)$$

as in the statement of the corollary and that it is functorial with respect to continuous (hence, any) morphism $M \to N$ of finitely generated $\Lambda(G)$-modules. By our assumption that M is finitely presented, the right exactness of the usual tensor product and the five lemma, it is sufficient to prove the corollary for $M = \Lambda(G)^k$ for any $k \geq 1$. But in this case, by lemmata 1.1.1 and 1.1.5 (recall the isomorphism in lemma 1.1.5 is induced by the one from lemma 1.1.1) we have

$$\begin{aligned}
\tilde{\Lambda}(G) \otimes_{\Lambda(G)} (T \otimes_{\mathbb{Z}_p} \Lambda(G)^k) &\cong \tilde{\Lambda}(G) \otimes_{\Lambda(G)} (T \otimes_{\mathbb{Z}_p} \Lambda(G))^k \\
&\cong \tilde{\Lambda}(G) \otimes_{\Lambda(G)} \Lambda(G)^{rk} \\
&\cong \tilde{\Lambda}(G)^{rk} \\
&\cong (T \otimes_{\mathbb{Z}_p} \tilde{\Lambda}(G))^k \\
&\cong T \otimes_{\mathbb{Z}_p} (\tilde{\Lambda}(G) \otimes_{\Lambda(G)} \Lambda(G)^k),
\end{aligned}$$

which concludes the proof. □

1.1.2 Twist operators on K_1 of localized Iwasawa algebras

For a unital ring R we define $GL(R)$ to be the inductive limit $GL(R) := \varinjlim_n GL_n(R)$, where $GL_n(R)$ is embedded into $GL_{n+1}(R)$ by

$$GL_n(R) \ni \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \longmapsto \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n,1} & \cdots & a_{n,n} & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in GL_{n+1}(R).$$

Similarly, we define the subgroup of elementary matrices $E(R) := \varinjlim_n E_n(R)$, which is equal to the commutator subgroup $[GL(R), GL(R)]$ of $GL(R)$, see ([Ros94], 2.1.4. Proposition (Whitehead's Lemma)). We then set

$$K_1(R) = GL(R)/E(R),$$

which is the definition of first K-group found in loc. cit. We see that $K_1(R)$ is the abelianization of $GL(R)$.

Now, let G be a p-adic Lie group.

Remark 1.1.8. Both Iwasawa algebras $\Lambda(G) = \mathcal{O}_L[[G]]$, for some finite extension L of $\mathbb{Q}_p$, and $\tilde{\Lambda}(G) = \hat{\mathbb{Z}}_p^{ur}[[G]]$ are now Noetherian as was proven by Lazard [Laz65]. This implies that any finitely generated abstract $\tilde{\Lambda}(G)$-module M becomes pseudo-compact with respect to the topology induced by the submodules $\{p^n M + \tilde{I}(U)M\}_{n,U}$, where n ranges through $\mathbb{N}_{\geq 1}$ and U through the open normal subgroups of G. Indeed, for any such module we can now find a finite presentation

$$\tilde{\Lambda}(G)^n \xrightarrow{\varphi} \tilde{\Lambda}(G)^k \to M \to 0,$$

and the statement follows from the proof found in ([Gab62], Chapitre IV, §3, Théorème 3) of the fact that the category of pseudo-compact $\tilde{\Lambda}(G)$-modules is abelian. In short, since $\ker(\varphi)$ is closed one can show that $\tilde{\Lambda}(G)^n/\ker(\varphi)$, equipped with the quotient topology, is pseudo-compact. Identifying $\tilde{\Lambda}(G)^n/\ker(\varphi)$ with the image $\mathrm{im}(\varphi)$ of φ one then shows that the quotient topology on $\mathrm{im}(\varphi)$ coincides with the subspace topology induced by $\tilde{\Lambda}(G)^k$. In particular, $\mathrm{im}(\varphi)$ must then be a closed submodule of $\tilde{\Lambda}(G)^k$ since $\tilde{\Lambda}(G)^n/\ker(\varphi)$ is complete. Since $\mathrm{im}(\varphi)$ is closed in $\tilde{\Lambda}(G)^k$, it follows that $\tilde{\Lambda}(G)^k/\mathrm{im}(\varphi)$ is pseudo-compact with respect to the quotient topology. That the latter module carries the topology as claimed was shown in proposition 1.1.3.

Henceforth we shall assume that G contains a closed normal subgroup H such that

$$G/H = \Gamma \cong \mathbb{Z}_p.$$

Moreover, in the following $\mathcal{O}$ will stand for either

$$\mathcal{O} = \mathbb{Z}_p \qquad \text{or} \qquad \mathcal{O} = \hat{\mathbb{Z}}_p^{ur}$$

and we will write $\Lambda_{\mathcal{O}}(G) = \mathcal{O}[[G]]$ for the Iwasawa algebra with coefficients in $\mathcal{O}$. We write S and S^* for the two Ore sets of $\Lambda_{\mathcal{O}}(G)$ as defined in (A.8.1) and (A.8.2).

Now, let $\rho : G \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T)$ be a continuous $\mathbb{Z}_p$-linear representation, where T is a free $\mathbb{Z}_p$-module of finite rank r. We fix an isomorphism

$$\phi_T : T \cong \mathbb{Z}_p^r, \tag{1.1.2}$$

which is equivalent to choosing a $\mathbb{Z}_p$-basis of T, and for any $g \in G$ we shall denote by

$$\rho_{\phi_T}(g) \ \in \ M_r(\mathbb{Z}_p)$$

the $(r \times r)$-matrix with coefficients in $\mathbb{Z}_p$ associated to $\phi_T \circ \rho(g) \circ \phi_T^{-1}$ and the standard basis of $\mathbb{Z}_p^r$. For any matrix A let us write A^{t} for the transpose of A. Consider the homomorphism

$$G \longrightarrow \Big(M_r\big(\Lambda_{\mathcal{O}}(G)\big)\Big)^{\times}, \qquad g \longmapsto (\rho_{\phi_T}(g^{-1}))^{\mathrm{t}} g,$$

which induces an $\mathcal{O}$-algebra map

$$\tau_\rho : \Lambda_{\mathcal{O}}(G) \longrightarrow M_r\big(\Lambda_{\mathcal{O}}(G)\big).$$

We want to show that τ_ρ extends to the localized Iwasawa algebra, which will enable us to define the twist operator τ_ρ on $K_1(\Lambda_{\mathcal{O}}(G)_{S^*})$.

Proposition 1.1.9. *The homorphism τ_ρ extends to a ring homomorphism*

$$\tau_\rho : \Lambda_{\mathcal{O}}(G)_{S^*} \longrightarrow M_r\big(\Lambda_{\mathcal{O}}(G)_{S^*}\big).$$

Proof. The proof uses similar arguments as the proof of Lemma 7.6 in [Ven03]. First we note that $\tau_\rho(p) = p \cdot \mathrm{id}$, so it suffices to show that τ_ρ extends to a ring homomorphism $\tau_\rho : \Lambda_{\mathcal{O}}(G)_S \longrightarrow M_r\big(\Lambda_{\mathcal{O}}(G)_S\big)$. Let s be any element of S. Since s is a non-zero divisor in $\Lambda_{\mathcal{O}}(G)$ by theorem A.8.4, multiplication with s from the right induces an exact sequence of left $\Lambda_{\mathcal{O}}(G)$-modules

$$0 \longrightarrow \Lambda_{\mathcal{O}}(G) \xrightarrow{\cdot s} \Lambda_{\mathcal{O}}(G) \longrightarrow \Lambda_{\mathcal{O}}(G)/\Lambda_{\mathcal{O}}(G)s \longrightarrow 0.$$

Applying the exact functor $T \otimes_{\mathbb{Z}_p} -$ we get an exact sequence

$$0 \longrightarrow T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G) \xrightarrow{\mathrm{id}_T \otimes \cdot s} T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G) \longrightarrow T \otimes_{\mathbb{Z}_p} (\Lambda_{\mathcal{O}}(G)/\Lambda_{\mathcal{O}}(G)s) \longrightarrow 0,$$

which is an exact sequence of right $\Lambda_{\mathcal{O}}(G)$-modules with respect to the diagonal $\Lambda_{\mathcal{O}}(G)$-actions. By lemma 1.1.11, which we prove below, this sequence induces an exact sequence

$$0 \longrightarrow \Lambda_{\mathcal{O}}(G)^r \xrightarrow{\cdot \tau_\rho(s)} \Lambda_{\mathcal{O}}(G)^r \longrightarrow T \otimes_{\mathbb{Z}_p} (\Lambda_{\mathcal{O}}(G)/\Lambda_{\mathcal{O}}(G)s) \longrightarrow 0, \tag{1.1.3}$$

where we view $\Lambda_{\mathcal{O}}(G)^r$ as a set of row vectors and $\cdot\tau_\rho(s)$ denotes multiplication with $\tau_\rho(s)$ from the right. By lemmata 1.1.1 and 1.1.5 we know that $T \otimes_{\mathbb{Z}_p} (\Lambda_{\mathcal{O}}(G)/\Lambda_{\mathcal{O}}(G)s)$ is finitely generated as a $\Lambda_{\mathcal{O}}(H)$-module and, hence, that it is S-torsion by proposition A.8.3. Since localizing by S is an exact functor, (1.1.3) gives the desired isomorphism $\cdot\tau_\rho(s) : \Lambda_{\mathcal{O}}(G)_S^r \xrightarrow{\cong} \Lambda_{\mathcal{O}}(G)_S^r$, i.e., $\tau_\rho(s)$ belongs to $GL_r\big(\Lambda_{\mathcal{O}}(G)_S\big)$. The universal property of localization implies that τ_ρ extends to the localized Iwasawa algebra. □

Using the fact ([Lam99], §17B, (17.20) Theorem) that $\Lambda_{\mathcal{O}}(G)_{S^*}$ and $M_r\big(\Lambda_{\mathcal{O}}(G)_{S^*}\big)$, $r \geq 1$, are Morita-equivalent and the Morita invariance of K_1 ([Wei13], III §1, Proposition 1.6.4), we immediately get the following result.

Corollary 1.1.10. *The homomorphism τ_ρ induces an operator τ_ρ on $K_1(\Lambda_{\mathcal{O}}(G)_{S^*})$.*

It remains to prove the lemma that we used in the proof of proposition 1.1.9. We note that τ_ρ induces a ring homomorphism

$$M_k(\Lambda_{\mathcal{O}}(G)) \longrightarrow M_k(M_r(\Lambda_{\mathcal{O}}(G))),$$

which, by abuse of notation, we also denote by τ_ρ.

Lemma 1.1.11. *For any $k \times k$-matrix $A \in M_k(\Lambda_{\mathcal{O}}(G))$, $k \geq 1$, we have a commutative diagram of left $\Lambda_{\mathcal{O}}(G)$-modules*

$$\begin{array}{ccc} T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^k & \xrightarrow{\mathrm{id}_T \otimes \cdot A} & T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^k \\ \downarrow \cong & & \downarrow \cong \\ (\Lambda_{\mathcal{O}}(G)^r)^k & \xrightarrow{\cdot \tau_\rho(A)} & (\Lambda_{\mathcal{O}}(G)^r)^k, \end{array}$$

where we consider $\Lambda_{\mathcal{O}}(G)^k$ and $(\Lambda_{\mathcal{O}}(G)^r)^k$ as modules of row vectors and the vertical maps are the composite of the natural map $T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^k \cong (T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G))^k$ and the maps induced from lemmata 1.1.1 and 1.1.5 (for which, of course, we use the fixed ϕ_T) and the transpose map

$$(\Lambda_{\mathcal{O}}(G)^r, \text{column vectors}) \to (\Lambda_{\mathcal{O}}(G)^r, \text{row vectors}), v \mapsto v^{\mathrm{t}}.$$

Moreover, $\cdot\tau_\rho(A)$ denotes multiplication with $\tau_\rho(A)$ from the right.

Proof. Using that any matrix $A = (a_{i,j})_{1 \leq i,j \leq k}$ can be written as $A = \sum_{1 \leq i,j \leq k} A_{i,j}$, where $A_{i,j}$ is the matrix that has entries equal to zero everywhere except for its (i,j)-th entry, which is given by $a_{i,j}$, and by linearity of the involved maps, one easily reduces to the case $k = 1$. In this case, first consider an element $A = h$ belonging to G. Then, for an element of the form $t' \otimes g \in T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)$ with $g \in G$ we have

$$\begin{aligned} \Big(\phi_T\big(\rho((gh)^{-1})(t')\big)\Big)^{\mathrm{t}} gh &= \Big(\phi_T\big(\rho(h^{-1})\big(\rho(g^{-1})(t')\big)\big)\Big)^{\mathrm{t}} gh \\ &= \Big(\rho_{\phi_T}(h^{-1}) \cdot \phi_T\big(\rho(g^{-1})(t')\big)\Big)^{\mathrm{t}} gh \\ &= \Big(\phi_T\big(\rho(g^{-1})(t')\big)\Big)^{\mathrm{t}} \cdot \Big(\rho_{\phi_T}(h^{-1})\Big)^{\mathrm{t}} gh \\ &= \Big(\phi_T\big(\rho(g^{-1})(t')\big)\Big)^{\mathrm{t}} g \cdot \tau_\rho(h), \end{aligned}$$

which, by continuity, shows that the diagram commutes for all elements of $T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)$ and for h belonging to G. The universal property of the Iwasawa algebra then implies that it commutes for arbitrary $A \in \Lambda_{\mathcal{O}}(G)$. □

1.1.3 Fukaya and Kato's $K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$

There is a another description of $K_1(\Lambda_{\mathcal{O}}(G)_{S^*})$. We refer the reader to ([FK06], section 1.3) for the definition of the localized K_1-group $K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$, where Σ, in our case, denotes the category of bounded complexes of finitely generated projective $\Lambda_{\mathcal{O}}(G)$-modules, the cohomology groups of which are S^*-torsion. Fukaya and Kato prove the following proposition ([FK06], Proposition 1.3.7).

Proposition 1.1.12. *There is an isomorphism*

$$K_1(\Lambda_{\mathcal{O}}(G), \Sigma) \cong K_1(\Lambda_{\mathcal{O}}(G)_{S^*}). \tag{1.1.4}$$

Fukaya and Kato give an explicit desciption of this isomorphism and its inverse. A representative of an element λ in $K_1(\Lambda_{\mathcal{O}}(G)_S)$, can be written as A/s, where $A \in M_n(\Lambda_{\mathcal{O}}(G)) \cap GL_n(\Lambda_{\mathcal{O}}(G)_{S^*})$ and $s \in S^*$. The inverse of (1.1.4) is given by

$$\lambda \longmapsto [[\Lambda_{\mathcal{O}}(G)^n \xrightarrow{\cdot A} \Lambda_{\mathcal{O}}(G)^n], \mathrm{id}] \cdot [[\Lambda_{\mathcal{O}}(G)^n \xrightarrow{\cdot s \cdot \mathrm{id}} \Lambda_{\mathcal{O}}(G)^n], \mathrm{id}]^{-1},$$

where we consider $\Lambda_{\mathcal{O}}(G)^n$ as the set of row vectors, matrix multiplication is from the right and the complexes are concentrated in degrees 0 and 1.

Remark 1.1.13. Note that for $A \in M_n(\Lambda_{\mathcal{O}}(G)) \cap GL_n(\Lambda_{\mathcal{O}}(G)_{S^*})$ the map $\Lambda_{\mathcal{O}}(G)^n \xrightarrow{\cdot A} \Lambda_{\mathcal{O}}(G)^n$ has S^*-torsion kernel and cokernel. Hence, $[\Lambda_{\mathcal{O}}(G)^n \xrightarrow{\cdot A} \Lambda_{\mathcal{O}}(G)^n]$ belongs to Σ.

Next, we want to define a twist operator on $K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$ and show that with respect to the isomorphism (1.1.4) it is compatible with the twist operator on $K_1(\Lambda_{\mathcal{O}}(G)_{S^*})$.

First of all, let $C^\bullet = \dots C^{i-1} \to C^i \to C^{i+1} \dots$ be an element of Σ. We want to show that $T \otimes_{\mathbb{Z}_p} C^\bullet$ defined by $\dots T \otimes_{\mathbb{Z}_p} C^{i-1} \to T \otimes_{\mathbb{Z}_p} C^i \to T \otimes_{\mathbb{Z}_p} C^{i+1} \dots$ also belongs to Σ, where, on the tensor products, we consider the diagonal action. This follows from two observations. If P is a finitely generated, projective $\Lambda_{\mathcal{O}}(G)$-module, such that $P \oplus Q \cong \Lambda_{\mathcal{O}}(G)^d$ for some $\Lambda_{\mathcal{O}}(G)$-module Q, then with respect to the diagonal $\Lambda_{\mathcal{O}}(G)$-actions on each tensor product

$$\left(T \otimes_{\mathbb{Z}_p} P\right) \oplus \left(T \otimes_{\mathbb{Z}_p} Q\right) \cong T \otimes_{\mathbb{Z}_p} (P \oplus Q) \cong T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^d \cong \left(T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)\right)^d, \tag{1.1.5}$$

from which it follows by lemmata 1.1.1 and 1.1.5 that $T \otimes_{\mathbb{Z}_p} P$ with the diagonal action is also finitely generated and projective. On the other hand, we have the following

Lemma 1.1.14. *If M is finitely generated over $\Lambda_{\mathcal{O}}(G)$ and S^*-torsion, then so is $T \otimes_{\mathbb{Z}_p} M$ equipped with the diagonal G-action.*

Proof. M is S^*-torsion if and only if $M/(M(p))$ is S-torsion (where $M(p)$ denotes the p-primary torsion part of M) and a finitely generated $\Lambda_{\mathcal{O}}(G)$-module is S-torsion if and only if it is finitely generated over $\Lambda_{\mathcal{O}}(H)$ by proposition A.8.3. Let us prove that $(T \otimes_{\mathbb{Z}_p} M)/\big((T \otimes_{\mathbb{Z}_p} M)(p)\big)$ is finitely generated over $\Lambda_{\mathcal{O}}(H)$. Choose a surjection $\Lambda_{\mathcal{O}}(H)^k \twoheadrightarrow M/(M(p))$ which induces a surjection $\left(T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(H)\right)^k \cong T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(H)^k \twoheadrightarrow T \otimes_{\mathbb{Z}_p} \big(M/(M(p))\big)$. By lemmata 1.1.1 and 1.1.5 we have $\left(T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(H)\right)^k \cong \Lambda_{\mathcal{O}}(H)^{rk}$, so $T \otimes_{\mathbb{Z}_p} \big(M/(M(p))\big)$ is finitely generated over $\Lambda_{\mathcal{O}}(H)$. Now, we only have to note that we have a surjection $T \otimes_{\mathbb{Z}_p} \big(M/(M(p))\big) \twoheadrightarrow (T \otimes_{\mathbb{Z}_p} M)/\big((T \otimes_{\mathbb{Z}_p} M)(p)\big)$, which concludes the proof. □

Together, these observations and the exactness of $T \otimes_{\mathbb{Z}_p} -$ imply that

$$C^\bullet \longmapsto T \otimes_{\mathbb{Z}_p} C^\bullet$$

defines a functor from Σ to itself. For a morphism f between complexes, the functor is defined by extending f to $\mathrm{id}_T \otimes f$, of course.

Now, given an element $[C^\bullet, a]$ of $K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$, by definition of the morphisms in the determinant category $\mathcal{C}_{\Lambda_{\mathcal{O}}(G)}$ given in ([FK06], §1.2.1), the isomorphism $a : \mathrm{Det}_{\Lambda_{\mathcal{O}}(G)}(0) \longrightarrow \mathrm{Det}_{\Lambda_{\mathcal{O}}(G)}(C^\bullet)$ canonically induces an isomorphism $\mathrm{id}_T \otimes a : \mathrm{Det}_{\Lambda_{\mathcal{O}}(G)}(0) \longrightarrow \mathrm{Det}_{\Lambda_{\mathcal{O}}(G)}(T \otimes_{\mathbb{Z}_p} C^\bullet)$. Now we define our twist operator on $K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$ and afterwards remark that this definition can be extended to more general modules, see remark 1.1.16 (ii).

Definition 1.1.15 (Twist operator on $K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$). *We define the operator*

$$\sigma_\rho : K_1(\Lambda_{\mathcal{O}}(G), \Sigma) \longrightarrow K_1(\Lambda_{\mathcal{O}}(G), \Sigma), \qquad [C^\bullet, a] \longmapsto [T \otimes_{\mathbb{Z}_p} C^\bullet, \mathrm{id}_T \otimes a].$$

Remark 1.1.16. (i) It is a straighforward exercise to check that this operator is well-defined (as in the case when proving that the functor $Y \otimes_{\Lambda_{\mathcal{O}}(G)} -$ below in (ii) for general finitely generated projective Y is well-defined); most of the relations in $K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$ can be shown to be respected by the fact that T is free as a $\mathbb{Z}_p$-module.

(ii) A more conceptual approach than the one used in definition 1.1.15 would be to consider the $(\Lambda_{\mathcal{O}}(G), \Lambda_{\mathcal{O}}(G))$-bimodule $Y := \Lambda_{\mathcal{O}}(G) \otimes_{\mathbb{Z}_p} T$, where the left $\Lambda_{\mathcal{O}}(G)$-module structure is given by the action on the $\Lambda_{\mathcal{O}}(G)$-factor and the right $\Lambda_{\mathcal{O}}(G)$-module structure is induced by the diagonal G-action from the right given by $(\lambda \otimes t).g := (\lambda \cdot g) \otimes g^{-1}.t$, $\lambda \in \Lambda_{\mathcal{O}}(G), t \in T, g \in G$. Y is finitely generated and free as a left $\Lambda_{\mathcal{O}}(G)$-module. In particular, it is projective as a left $\Lambda_{\mathcal{O}}(G)$-module and for such bimodules there is functor between the determinant categories

$$Y \otimes_{\Lambda_{\mathcal{O}}(G)} - : \mathcal{C}_{\Lambda_{\mathcal{O}}(G)} \longrightarrow \mathcal{C}_{\Lambda_{\mathcal{O}}(G)}, \qquad (P, Q) \longmapsto (Y \otimes_{\Lambda_{\mathcal{O}}(G)} P, Y \otimes_{\Lambda_{\mathcal{O}}(G)} Q),$$

see ([FK06], §1.2.5). For $\mathcal{O} = \mathbb{Z}_p$ and any finitely generated left $\Lambda_{\mathcal{O}}(G)$-module P there is a natural isomorphism

$$(\Lambda_{\mathcal{O}}(G) \otimes_{\mathbb{Z}_p} T) \otimes_{\Lambda_{\mathcal{O}}(G)} P \xrightarrow{\sim} T \otimes_{\mathbb{Z}_p} P$$

given in lemma A.3.11 (the proof there works for a general p-adic Lie group G), which shows that naturally

$$Y \otimes_{\Lambda_{\mathcal{O}}(G)} C^\bullet \cong T \otimes_{\mathbb{Z}_p} C^\bullet \qquad \text{and} \qquad Y \otimes_{\Lambda_{\mathcal{O}}(G)} \mathrm{Det}_{\Lambda_{\mathcal{O}}(G)}(C^\bullet) \cong \mathrm{Det}_{\Lambda_{\mathcal{O}}(G)}(T \otimes_{\mathbb{Z}_p} C^\bullet)$$

for any $C^\bullet$ in Σ. We conclude that the operator

$$[C^\bullet, a] \longmapsto [Y \otimes_{\Lambda_{\mathcal{O}}(G)} C^\bullet, Y \otimes_{\Lambda_{\mathcal{O}}(G)} a]$$

coincides with σ_ρ.

The following lemma shows that definition 1.1.15 of σ_ρ, via the isomorphism from (1.1.4), is compatible with τ_ρ.

Lemma 1.1.17. *The following diagram commutes*

$$\begin{array}{ccc} K_1(\Lambda_{\mathcal{O}}(G)_{S^*}) & \xrightarrow{\tau_\rho} & K_1(\Lambda_{\mathcal{O}}(G)_{S^*}) \\ \downarrow \cong & & \downarrow \cong \\ K_1(\Lambda_{\mathcal{O}}(G),\Sigma) & \xrightarrow{\sigma_\rho} & K_1(\Lambda_{\mathcal{O}}(G),\Sigma) \end{array} \tag{1.1.6}$$

where the vertical maps are the isomorphisms from proposition 1.1.12.

Proof. Let B be an element of $M_k(\Lambda_{\mathcal{O}}(G)) \cap GL_k(\Lambda_{\mathcal{O}}(G)_{S^*})$ for some $k \geq 1$. The statement of the lemma immediately follows from the commutative diagram

$$\begin{array}{ccc} T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^k & \xrightarrow{\mathrm{id}_T \otimes \cdot B} & T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^k \\ \downarrow \cong & & \downarrow \cong \\ (\Lambda_{\mathcal{O}}(G)^r)^k & \xrightarrow{\cdot \tau_\rho(B)} & (\Lambda_{\mathcal{O}}(G)^r)^k, \end{array} \tag{1.1.7}$$

from lemma 1.1.11. In fact, first note that as complexes concentrated in degrees 0 and 1 the upper and the lower row of diagram (1.1.7) belong to Σ, compare remark 1.1.13.

The upper and the lower row of diagram (1.1.7) are isomorphic as complexes. But isomorphic complexes with compatible trivializations are equal in $K_1(\Lambda_{\mathcal{O}}(G),\Sigma)$, compare section 1.3 on the localized K_1 in [FK06]. Hence, the following two images are the same. Let A/s, $A \in M_k(\Lambda_{\mathcal{O}}(G)) \cap GL_k(\Lambda_{\mathcal{O}}(G)_{S^*})$, $s \in S^*$, be a representative of an arbitrary element of $K_1(\Lambda_{\mathcal{O}}(G)_{S^*})$. Note that $A/s = A \cdot (\frac{1}{s} \cdot \mathrm{id}_k) = A \cdot (s \cdot \mathrm{id}_k)^{-1}$, where id_k is the $k \times k$-identity matrix, and that $s \cdot \mathrm{id}_k$ also belongs to $M_k(\Lambda_{\mathcal{O}}(G)) \cap GL_k(\Lambda_{\mathcal{O}}(G)_{S^*})$. On the one hand, under the top horizontal map from (1.1.6), the class of A/s maps to the class of $\tau_\rho(A) \cdot \tau_\rho(s \cdot \mathrm{id}_k)^{-1} \in GL_{rk}(\Lambda_{\mathcal{O}}(G)_{S^*})$, which maps to

$$[[\Lambda_{\mathcal{O}}(G)^{rk} \overset{\cdot \tau_\rho(A)}{\longrightarrow} \Lambda_{\mathcal{O}}(G)^{rk}], \mathrm{id}] \cdot [[\Lambda_{\mathcal{O}}(G)^{rk} \overset{\cdot \tau_\rho(s \cdot \mathrm{id}_k)}{\longrightarrow} \Lambda_{\mathcal{O}}(G)^{rk}], \mathrm{id}]^{-1} \text{ in } K_1(\Lambda_{\mathcal{O}}(G),\Sigma).$$

On the other hand, the class of A/s maps to

$$[[\Lambda_{\mathcal{O}}(G)^{k} \overset{\cdot A}{\longrightarrow} \Lambda_{\mathcal{O}}(G)^{k}], \mathrm{id}] \cdot [[\Lambda_{\mathcal{O}}(G)^{k} \overset{\cdot (s \cdot \mathrm{id}_k)}{\longrightarrow} \Lambda_{\mathcal{O}}(G)^{k}], \mathrm{id}]^{-1} \text{ in } K_1(\Lambda_{\mathcal{O}}(G),\Sigma),$$

which, under σ_ρ, maps to

$$[[T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^{k} \overset{\mathrm{id}_T \otimes \cdot A}{\longrightarrow} T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^{k}], \mathrm{id}] \cdot [[T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^{k} \overset{\mathrm{id}_T \otimes \cdot (s \cdot \mathrm{id}_k)}{\longrightarrow} T \otimes_{\mathbb{Z}_p} \Lambda_{\mathcal{O}}(G)^{k}], \mathrm{id}]^{-1},$$

which concludes the proof. □

1.1.4 K_0 and the connecting homomorphism

Let the setting be as in section 1.1.3. In ([FK06], Theorem 1.3.15) Fukaya and Kato define an exact sequence

$$K_1(\Lambda_{\mathcal{O}}(G)) \longrightarrow K_1(\Lambda_{\mathcal{O}}(G), \Sigma) \xrightarrow{\text{(ii)}} K_0(\Sigma) \longrightarrow K_0(\Lambda_{\mathcal{O}}(G)),$$

where (ii) is defined by $[C^\bullet, a] \longmapsto -[[C^\bullet]]$. For the precise definition of $K_0(\Sigma)$, which is the abelian group, written additively, generated by elements of Σ, subject to some relations, we refer to (loc. cit., Definition 1.3.14). We make the following

Definition 1.1.18. *Let $\mathcal{O}$ be a complete discrete valuation ring of characteristic* 0 *and of residue characteristic p. By $\mathfrak{M}_{\mathcal{O},H}(G)$ we denote the category of finitely generated $\mathcal{O}[[G]]$-modules that are S^*-torsion, where S^* denotes the Ore set defined in (A.8.1) and (A.8.2). If $\mathcal{O} = \mathbb{Z}_p$ we also write $\mathfrak{M}_H(G) = \mathfrak{M}_{\mathcal{O},H}(G)$.*

In case that G has no elements of order p, which we assume henceforth, it is important to note that we have an isomorphism

$$K_0(\Sigma) \xrightarrow{\sim} K_0(\mathfrak{M}_{\mathcal{O},H}(G)), \qquad [[C^\bullet]] \longmapsto \sum_i (-1)^i [H^i(C^\bullet)],$$

compare ([FK06], Section 4.3.3). We define a connecting homomorphism $\partial : K_1(\Lambda_{\mathcal{O}}(G)_{S^*}) \longrightarrow K_0(\mathfrak{M}_{\mathcal{O},H}(G))$ by the commutativity of the following diagram

$$\begin{array}{ccc} K_1(\Lambda_{\mathcal{O}}(G)_{S^*}) & \xrightarrow{\partial} & K_0(\mathfrak{M}_{\mathcal{O},H}(G)) \\ \downarrow \cong & & \uparrow \cong \\ K_1(\Lambda_{\mathcal{O}}(G), \Sigma) & \xrightarrow{\text{(ii)}} & K_0(\Sigma). \end{array}$$

Let us describe ∂ concretely. The class of $\lambda/s \in GL_n(\Lambda_{\mathcal{O}}(G)_{S^*})$, where $\lambda \in M_n(\Lambda_{\mathcal{O}}(G)) \cap GL_n(\Lambda_{\mathcal{O}}(G)_{S^*})$ and $s \in S^*$, maps to

$$[[\Lambda_{\mathcal{O}}(G)^n \xrightarrow{\lambda} \Lambda_{\mathcal{O}}(G)^n], \mathrm{id}] \cdot [[\Lambda_{\mathcal{O}}(G)^n \xrightarrow{s\cdot \mathrm{id}_n} \Lambda_{\mathcal{O}}(G)^n], \mathrm{id}]^{-1} \;\in\; K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$$

under the vertical isomorphism on the left, where we recall that the complexes are concentrated in degrees 0 and 1. Under (ii) this maps to

$$-[[\Lambda_{\mathcal{O}}(G)^n \xrightarrow{\lambda} \Lambda_{\mathcal{O}}(G)^n]] + [[\Lambda_{\mathcal{O}}(G)^n \xrightarrow{s\cdot \mathrm{id}_n} \Lambda_{\mathcal{O}}(G)^n]] \;\in\; K_0(\Sigma),$$

which, in turn, maps to

$$[\operatorname{coker}(\lambda)] - [\operatorname{coker}(s \cdot \mathrm{id}_n)] \;\in\; K_0(\mathfrak{M}_{\mathcal{O},H}(G)), \tag{1.1.8}$$

for which we note that multiplication from the right with both λ and $s\cdot \mathrm{id}_n$ has trivial kernel. In particular, for $\lambda/s \in \Lambda_{\mathcal{O}}(G)^{\times}_{S^*}$ we have

$$\partial([\lambda/s]) = [\Lambda_{\mathcal{O}}(G)/\lambda\Lambda_{\mathcal{O}}(G)] - [\Lambda_{\mathcal{O}}(G)/s\Lambda_{\mathcal{O}}(G)],$$

where we write $[\lambda/s]$ for the class of λ/s in $K_1(\Lambda_{\mathcal{O}}(G)_{S^*})$. For a representation $\rho : G \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T)$ we have defined an operator σ_ρ on $K_1(\Lambda_{\mathcal{O}}(G), \Sigma)$ in definition 1.1.15, which motivates the following

Definition 1.1.19 (Twist operator on $K_0(\Sigma)$). *We define an operator $\tilde{\sigma}_\rho$ on $K_0(\Sigma)$ by*

$$[[C^\bullet]] \longmapsto [[T \otimes_{\mathbb{Z}_p} C^\bullet]],$$

where $C^\bullet$ is a complex in Σ and $T \otimes_{\mathbb{Z}_p} C^\bullet$ is the complex which arises by tensoring each module C^i with $T \otimes_{\mathbb{Z}_p} -$ and passing to the diagonal $\Lambda_{\mathcal{O}}(G)$-action on $T \otimes_{\mathbb{Z}_p} C^i$.

It follows immediately from the definition of $K_0(\Sigma)$ that this is well-defined. Evidently, we have the following commutative diagram

$$\begin{array}{ccc} K_1(\Lambda_{\mathcal{O}}(G), \Sigma) & \xrightarrow{\text{(ii)}} & K_0(\Sigma) \\ \downarrow{\scriptstyle \sigma_\rho} & & \downarrow{\scriptstyle \tilde{\sigma}_\rho} \\ K_1(\Lambda_{\mathcal{O}}(G), \Sigma) & \xrightarrow{\text{(ii)}} & K_0(\Sigma). \end{array}$$

Lemma 1.1.20. *Assume that G has no elements of order p. Let $\rho : G \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T)$ be as above and consider a representative A/s, $A \in M_n(\Lambda_{\mathcal{O}}(G)) \cap GL_n(\Lambda_{\mathcal{O}}(G)_{S^*})$, $s \in S^*$, of an element in $K_1(\Lambda_{\mathcal{O}}(G)_{S^*})$. Then, we have*

$$\partial(\tau_\rho([A/s])) = [T \otimes_{\mathbb{Z}_p} \mathrm{coker}(\cdot A)] - [T \otimes_{\mathbb{Z}_p} \mathrm{coker}(\cdot(s\cdot \mathrm{id}_n))] \ \in \ K_0(\mathfrak{M}_{\mathcal{O},H}(G)).$$

Proof. Using that T is flat over $\mathbb{Z}_p$, this result can immediately be read off the following commutative diagram, which summarizes the content of this subsection and subsection 1.1.3

$$\begin{array}{ccccc} K_1(\Lambda_{\mathcal{O}}(G)_{S^*}) & \xrightarrow{\tau_\rho} & K_1(\Lambda_{\mathcal{O}}(G)_{S^*}) & \xrightarrow{\partial} & K_0(\mathfrak{M}_{\mathcal{O},H}(G)) \\ \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \cong} & & \uparrow{\scriptstyle \cong} \\ K_1(\Lambda_{\mathcal{O}}(G), \Sigma) & \xrightarrow{\sigma_\rho} & K_1(\Lambda_{\mathcal{O}}(G), \Sigma) & \xrightarrow{\text{(ii)}} & K_0(\Sigma). \end{array}$$

□

Comparing this result with (1.1.8), we see that twisting on K_1 indeed corresponds to tensoring with $T \otimes_{\mathbb{Z}_p} -$ and passing to the diagonal action on K_0 as stated at the beginning of section 1.1. Therefore, making the following definition is compatible with our previous definitions.

Definition 1.1.21 (Twist operator on $K_0(\mathfrak{M}_{\mathcal{O},H}(G))$). *We define a twist operator $\tilde{\tau}_\rho$ on $K_0(\mathfrak{M}_{\mathcal{O},H}(G))$ by*

$$\tilde{\tau}_\rho : K_0(\mathfrak{M}_{\mathcal{O},H}(G)) \longrightarrow K_0(\mathfrak{M}_{\mathcal{O},H}(G)), \qquad [M] \longmapsto [T \otimes_{\mathbb{Z}_p} M],$$

where the action of $\Lambda_{\mathcal{O}}(G)$ on $T \otimes_{\mathbb{Z}_p} M$ is induced by the diagonal G-action.

All in all, we have a commutative diagram

$$\begin{array}{ccc} K_1(\Lambda_{\mathcal{O}}(G)_{S^*}) & \xrightarrow{\partial} & K_0(\mathfrak{M}_{\mathcal{O},H}(G)) \\ \downarrow{\scriptstyle \tau_\rho} & & \downarrow{\scriptstyle T \otimes_{\mathbb{Z}_p} -} \\ K_1(\Lambda_{\mathcal{O}}(G)_{S^*}) & \xrightarrow{\partial} & K_0(\mathfrak{M}_{\mathcal{O},H}(G)). \end{array} \tag{1.1.9}$$

1.2 Finitely generated $\mathbb{Z}_p$-modules and K_0-groups

Let G be a p-adic Lie group and H a closed subgroup satisfying the conditions (i), (ii) and (iii) defined below in section 1.2.1. Our goal in this chapter is to show that the class $[M]$ of a module $M \in \mathfrak{M}_H(G)$, which is finitely generated as a $\mathbb{Z}_p$-module, vanishes in $K_0(\mathfrak{M}_H(G))$, that is,

$$[M] = 0 \ \in K_0(\mathfrak{M}_H(G)).$$

The proof we present for finitely generated free $\mathbb{Z}_p$-modules is due to Gergely Zábrádi, see ([Zĺ0], Lemma 4.1 and Proposition 4.2), who considered special groups H and G (in fact he considered the GL_2-case for elliptic curves without complex multiplication), but this proof can be adapted to work in the setting described in section 1.2.1. In contrast to Zábrádi, we then show that the general case of any finitely generated $\mathbb{Z}_p$-module, not necessarily free, follows from the case of free modules.

1.2.1 Setting

For any profinite group P, as before, we write $\Lambda(P)$ for the Iwasawa algebra of P with coefficients in $\mathbb{Z}_p$ and $\Omega(P)$ for the Iwasawa algebra $\varprojlim_U \mathbb{F}_p[P/U]$ with coeffiecients in $\mathbb{F}_p$.

In this chapter we consider a compact p-adic Lie group G and a closed normal subgroup H (which is automatically a compact p-adic Lie group, see [DdSMS03], 9.6 Theorem (i)) satisfying the following conditions

(i) $G \cong H \times \Gamma$, where $\Gamma \cong \mathbb{Z}_p$,

(ii) G, and therefore H, has no element of finite p-power order,

(iii) for all regular elements h in H, that is, for all elements h in H of finite order, the centralizer $C_H(h)$ of h in H has dimension greater or equal to 1 as p-adic Lie group.

For such H and G we recall the facts that all of the following rings

$$\Lambda(G), \Lambda(H), \Omega(G) \text{ and } \Omega(H)$$

are Noetherian and have finite global dimension, compare the paper ([AW06], 3.3 Proposition, p. 349) by Ardakov and Wadsley.

We recall that for the $\mathbb{F}_p$-algebra $\Omega(H)$ one can introduce the concept of Gelfand-Kirillov dimension, see ([MR87] chapter 8, p. 297ff). One considers a filtration defined by powers of the radical J of $\Omega(H)$ and then, for a finitely generated $\Omega(H)$-module M one defines

$$d(M) := GK(grM)$$

as the Gelfand-Kirillov dimension $GK(grM)$ of grM, which is a certain graded module associated to M and J. $GK(grM)$ is given by the growth rate $\gamma(f)$ of the function

$$f(n) = \dim_{\mathbb{F}_p} M/MJ^n,$$

see the survey article of Ardakov and Brown ([AB06], proof of 5.4. Proposition). We are not going to define what growth rate means - for a definition see ([MR87] chapter 8, p. 297ff) - but note that for a $\Omega(H)$-module M that is finitely generated as a $\mathbb{F}_p$-vector space, the function f is bounded by the dimension $\dim_{\mathbb{F}_p} M$, from which it immediately follows that the growth rate equals 0, i.e., we have $d(M) = 0$.

1.2.2 Main results

We have the following proposition due to Serre, see [Ser98b], which was generalized by Ardakov and Wadsley in [AW08].

Proposition 1.2.1. *Let H be a compact p-adic Lie group satisfying conditions* (ii) *and* (iii) *above and let M be a $\Omega(H)$-module which is finitely generated as a $\mathbb{F}_p$-vector space. Then, we have*

$$[M] = 0 \ \in G_0(\Omega(H)),$$

where $G_0(\Omega(H))$ denotes $K_0(\Omega(H)-\mathrm{mod})$, the 0-th K-group of the category $\Omega(H)$-mod of finitely generated $\Omega(H)$-modules.

Proof. Due to Serre, see [Ser98b] or as a special case of the more general result ([AW08], Theorem A) due to Ardakov and Wadsley, we know that under condition (iii) about the centralizers $C_H(h)$ for regular $h \in H$, the Euler characteristic $\chi(H, N)$ is given by

$$\chi(H, N) = 1$$

for all $\Omega(H)$-modules N which are finitely generated $\mathbb{F}_p$-vector spaces or, more generally, in the language of Ardakov and Wadsley, for all finitely generated $\Omega(H)$-modules N such that $d(N) < \dim C_H(h)$ for all regular $h \in H$. For a definition of the Euler characteristic see ([AW06], 4.5. Definition). Since $\Omega(H)$ is Noetherian and has finite global dimension we have an isomorphism

$$\gamma : G_0(\Omega(H)) \cong K_0(\Omega(H)),$$

which is known as the resolution theorem, see, for example, the books on K-theory by Srinivas ([Sri08], Theorem (4.6)) and Rosenberg ([Ros94], 3.1.13. Theorem). Ardakov and Wadsley give a formula for the map γ in ([AW06], 4.8. Proposition), which shows that

$$\gamma([M]) = 0 \quad \text{if} \quad \chi(H, M \otimes_{\mathbb{F}_p} V_i^*) = 1 \text{ for } i = 1, \ldots, s,$$

where $V_1, \ldots, V_s$ give a complete set of representatives for the isomorphism classes of simple $\Omega(H)$-modules. Since H is virtually pro-p, the V_i are all finite dimensional $\mathbb{F}_p$-vector spaces, see ([AW06], beginning of section 4.1.) and therefore $M \otimes_{\mathbb{F}_p} V_i^*$ are finite dimensional and the proposition follows from the result of Serre. □

Now, we are able to present the main result of this chapter, the proof of which is almost identical to Zábrádi's proof of ([Zí10], Lemma 4.1 and Proposition 4.2), who considered the GL_2-case.

Theorem 1.2.2. *Let G be a compact p-adic Lie group and H a closed normal subgroup of G such that the pair (G, H) satisfies the conditions (i), (ii) and (iii) from the beginning of this section. Moreover, let M be a $\Lambda(G)$-module that is finitely generated and free as a $\mathbb{Z}_p$-module. We then have*

$$[M] = 0 \quad \text{in} \quad K_0(\mathfrak{M}_H(G)).$$

Proof. We note that since p is contained in the radical of $\Lambda(H)$ we have an isomorphism

$$K_0(\Lambda(H)) \cong K_0(\Omega(H))$$

induced by sending the class $[P]$ of a finitely generated projective $\Lambda(H)$-module P to $[P/pP]$. Together with the two isomorphisms from the resolution theorem for $\Lambda(H)$ and $\Omega(H)$, respectively, we see that we have an isomorphism

$$G_0(\Omega(H)) \cong K_0(\Omega(H)) \cong K_0(\Lambda(H)) \cong G_0(\Lambda(H)), \tag{1.2.1}$$

mapping $[\mathbb{F}_p]$ in $G_0(\Omega(H))$ to $[\mathbb{Z}_p]$ in $G_0(\Lambda(H))$, which we show in lemma 1.2.5 below (this is not obvious as it might seem, since there is generally no map between $G_0(\Lambda(H))$ and $G_0(\Omega(H))$ induced by $\Lambda(H) \to \Omega(H)$ since $\Omega(H)$ is not flat as a $\Lambda(H)$-module).

Next, we have an exact functor

$$\mathcal{F} : \Lambda(H)\text{–mod} \longrightarrow \mathfrak{M}_H(G),$$

sending a finitely generated $\Lambda(H)$-module N to $\mathcal{F}(N) := N$ considered as a $\Lambda(G)$-module, where we extend the action of H to an action of G by simply letting Γ act trivially on N - recall that, by (i), G is given by the direct product $H \times \Gamma$. The functor $\mathcal{F}$ induces a map

$$\mathcal{F}_* : G_0(\Lambda(H)) \longrightarrow K_0(\mathfrak{M}_H(G)), \qquad [N] \longmapsto [N]. \tag{1.2.2}$$

Finally, we note that tensoring any N in $\mathfrak{M}_H(G)$ with the flat $\mathbb{Z}_p$-module M and passing to the diagonal G-action induces a map $K_0(\mathfrak{M}_H(G)) \to K_0(\mathfrak{M}_H(G))$, $[N] \mapsto [N \otimes_{\mathbb{Z}_p} M]$, which, composed with (1.2.2) and (1.2.1), yields

$$G_0(\Omega(H)) \cong G_0(\Lambda(H)) \xrightarrow{\mathcal{F}_*} K_0(\mathfrak{M}_H(G)) \xrightarrow{-\otimes_{\mathbb{Z}_p} M} K_0(\mathfrak{M}_H(G)),$$

mapping $[\mathbb{F}_p]$, $\mathbb{F}_p$ equipped with the trivial H-action, to $[M]$ since $\mathbb{Z}_p \otimes_{\mathbb{Z}_p} M \cong M$. But $[\mathbb{F}_p] = 0$ in $G_0(\Omega(H))$ by proposition 1.2.1. □

Before giving the proof of the lemma mentioned in the proof above, we derive the general case of the previous theorem for finitely generated, but not necessarily free $\mathbb{Z}_p$-modules and record a corollary about induced modules.

Corollary 1.2.3. *Let G be a compact p-adic Lie group and H a closed normal subgroup of G such that the pair (G,H) satisfies the conditions (i), (ii) and (iii) from the beginning of this section and let M be a $\Lambda(G)$-module that is finitely generated as a $\mathbb{Z}_p$-module. We then have*

$$[M] = 0 \quad \text{in} \quad K_0(\mathfrak{M}_H(G)).$$

Proof. We can reduce to the case that M is a finite module as follows. Let $T(M)$ be the torsion part of M which is finite of p-power order and consider the exact sequence

$$0 \longrightarrow T(M) \longrightarrow M \longrightarrow M/T(M) \longrightarrow 0, \tag{1.2.3}$$

of $\Lambda(G)$-modules. Note that $M/T(M)$ is finitely generated and free as a $\mathbb{Z}_p$-module. The exact sequence (1.2.3) and the previous theorem show that it is sufficient to prove that the class of $T(M)$ vanishes in $K_0(\mathfrak{M}_H(G))$.

From now on we assume that M is finite, given by $\{m_1, \dots m_r\}$. For each $i = 1, \dots, r$ denote by U_i some open normal subgroup of G that acts trivially on m_i and write U for the intersection $\cap_{i=1}^r U_i$, which is itself open and normal in G. Then $\Lambda(G)$ acts on M through $\mathbb{Z}_p[G/U]$ and we have an exact sequence of $\Lambda(G)$-modules

$$0 \longrightarrow N \longrightarrow \bigoplus_{i=1}^{r} \mathbb{Z}_p[G/U] \longrightarrow M \longrightarrow 0,$$

where N is, by definition, the kernel of the map to M. Since $\bigoplus_{i=1}^r \mathbb{Z}_p[G/U]$ is a finitely generated free $\mathbb{Z}_p$-module so is N and the exact sequence, in combination with the previous theorem, shows that $[M] = 0$ in $K_0(\mathfrak{M}_H(G))$. □

Sometimes one can use the previous corollary 1.2.3 to derive vanishing statements for induced modules of finitely generated $\mathbb{Z}_p$-modules and more general compact p-adic Lie groups $\mathcal{G}$.

Corollary 1.2.4. *Let $\mathcal{G}$ be a compact p-adic Lie group containing a closed normal subgroup $\mathcal{H}$ such that $\mathcal{G}/\mathcal{H} \cong \mathbb{Z}_p$. Moreover, assume that G is an open, not necessarily normal subgroup of $\mathcal{G}$, set $H := \mathcal{H} \cap G$ and assume that H and G satisfiy the conditions (i), (ii) and (iii) from the beginning of this section. For a $\Lambda(G)$-module M which is finitely generated as a $\mathbb{Z}_p$-module we then have*

$$[\mathrm{Ind}_{\mathcal{G}}^{G} M] = 0$$

in $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$.

Proof. By corollary A.8.16 we have an exact functor

$$\mathrm{Ind}_{\mathcal{G}}^{G} : \mathfrak{M}_H(G) \longrightarrow \mathfrak{M}_{\mathcal{H}}(\mathcal{G}), \quad N \longmapsto \mathrm{Ind}_{\mathcal{G}}^{G} N,$$

which induces a map

$$(\mathrm{Ind}_{\mathcal{G}}^{G})_* : K_0(\mathfrak{M}_H(G)) \longrightarrow K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$$

showing that, as the image of $[M] = 0$ in $K_0(\mathfrak{M}_H(G))$ (which holds by assumption),

$$[\mathrm{Ind}_{\mathcal{G}}^{G} M] = 0 \quad \text{in } K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G})),$$

for all finitely generated $\mathbb{Z}_p$-modules M with an action of $\Lambda(G)$. □

It remains to prove the following lemma, which Gergely Zábrádi explained to me.

Lemma 1.2.5. *Under the map from (1.2.1) $[\mathbb{F}_p]$ in $G_0(\Omega(H))$ maps to $[\mathbb{Z}_p]$ in $G_0(\Lambda(H))$.*

Proof. Let us consider a projective resolution

$$0 \to P^n \to \cdots \to P^0 \to \mathbb{Z}_p \to 0 \tag{1.2.4}$$

of $\mathbb{Z}_p$ as a $\Lambda(H)$-module, so that $[\mathbb{Z}_p]$ maps to $\sum_i (-1)^i [P^i]$ under the isomorphism

$$G_0(\Lambda(H)) \cong K_0(\Lambda(H)).$$

Moreover, $\sum_i (-1)^i [P^i]$ maps to $\sum_i (-1)^i [P^i/pP^i]$ in $G_0(\Omega(H))$, so we have to show that

$$\sum_i (-1)^i [P^i/pP^i] = [\mathbb{F}_p].$$

Now, since the P^i are all projective as $\Lambda(H)$-modules, they certainly are $\mathbb{Z}_p$-torsionfree and therefore flat as $\mathbb{Z}_p$-modules. This implies that for the right-exact functor $\mathbb{F}_p \otimes_{\mathbb{Z}_p} -$ the exact sequence (1.2.4) is an acyclic resolution of $\mathbb{Z}_p$ (this means $\mathrm{Tor}_k^{\mathbb{Z}_p}(\mathbb{F}_p, P^i) = 0,\ \forall i, k \geq 1$). Therefore, one can use (1.2.4) in order to compute $\mathrm{Tor}_i^{\mathbb{Z}_p}(\mathbb{F}_p, \mathbb{Z}_p)$, which is equal to 0 for all $i \geq 1$ since $\mathbb{Z}_p$ is flat as a $\mathbb{Z}_p$-module. It follows that tensoring (1.2.4) with $\mathbb{F}_p \otimes_{\mathbb{Z}_p} -$ yields an exact sequence

$$0 \to P^n/pP^n \to \cdots \to P^0/pP^0 \to \mathbb{F}_p \to 0, \tag{1.2.5}$$

regardless of the fact that $\mathbb{F}_p$ is not flat as a $\mathbb{Z}_p$-module. Now, (1.2.5) implies that we have the relation

$$\sum_i (-1)^i [P^i/pP^i] = [\mathbb{F}_p] \qquad \text{in} \qquad G_0(\Omega(H)),$$

which is what we wanted to show. $\square$

Chapter 2

Global Conjecture

2.1 Introduction

In this chapter we introduce the first of three conjectures stated by Kato during a talk he gave in Cambridge on the occasion of John Coates' sixtieth birthday. While Kato stated a global conjecture for a p-adic Lie extension $F_\infty/\mathbb{Q}$ (non-abelian, in general) of the base field $\mathbb{Q}$, we want to allow a number field F which is either quadratic imaginary or equal to $\mathbb{Q}$ as base field in the statement of the conjecture. We do this mainly because later on we will prove the conjecture in a commutative case with quadratic imaginary base field. In fact, we will prove the conjecture in theorem 2.4.41 for any extension K_∞/K such that

(i) K is a quadratic imaginary number field,

(ii) there exists an elliptic curve E/K with complex multiplication by the ring of integers $\mathcal{O}_K$ and conductor divisible by one prime of K only,

(iii) $K_\infty = K(E[p^\infty])$ is the field obtained by adjoining all coordinates of p-power division points of E to K for some prime $p \neq 2,3$ above which E has good ordinary reduction.

2.2 Setting

Let F be either a quadratic imaginary number field or equal to $\mathbb{Q}$, fix an algebraic closure $\bar{F}$ of F and an embedding $\bar{F} \hookrightarrow \mathbb{C}$ and let us fix a prime $p \in \mathbb{Z}$. Moreover, let F_∞/F, $F_\infty \subseteq \overline{F} \subseteq \mathbb{C}$, be a compact p-adic Lie extension containing $F(\mu_{p^\infty})$, where $\mu_{p^\infty} = \bigcup_{n\geq 1} \mu_{p^n}$ is the group of p-power roots of unity. If $p = 2$, then assume that F is totally imaginary. We write $\mathcal{G} = \mathrm{Gal}(F_\infty/F)$ and ι for the automorphism of F_∞ induced by complex conjugation on $\mathbb{C}$. Moreover, we write $(F_n)_{n\geq 0}$ for a familiy of finite Galois extensions of $F = F_0$ such that $F_\infty = \bigcup_{n\geq 0} F_n$. Let Σ be the set of primes of F consisting of the infinite prime ν_∞ of F, the primes of F above p and those primes that ramify in F_∞/F and assume that Σ is finite. Then, F_Σ, the maximal subextension of $\bar{F}/F$

that is unramified outside Σ, contains F_∞. We will write $G_\Sigma(F_n) = G(F_\Sigma/F_n)$, $n \geq 0$. Let us assume that there are only finitely many places of F_∞ above p, i.e., for each place ν of F above p the decomposition group $\mathcal{G}_\nu$ of some prime of F_∞ above ν has finite index in $\mathcal{G}$. We will write Σ_f for the non-archimedean primes in Σ and $\Sigma_\infty = \{\nu_\infty\}$, so that $\Sigma = \Sigma_f \cup \Sigma_\infty$.

Remark 2.2.1. These assumptions are satisfied in the case when F_∞ is the field obtained by adjoining to F the coordinates of p-power torsion points of an elliptic curve E/F with complex multiplication by $\mathcal{O}_K$, the ring of integers of a quadratic imaginary number field K, such that p splits in $\mathcal{O}_K$ and considering $\Sigma_f = \Sigma_{\text{bad}} \cup \{\nu \mid \nu \text{ divides } p\}$, where Σ_{bad} is the set of primes where F has bad reduction. The primes that ramify in F_∞/F are precisely the primes of bad reduction and the primes above p. Moreover, the primes above p are finitely decomposed.

We also write $\Sigma_n = \Sigma(F_n)$ (or Σ if it is clear from the context which F_n is under consideration) for the primes of F_n that lie above the primes in Σ and $\Sigma_{n,f} = \Sigma_f(F_n)$ (or Σ_f) for the finite places contained in $\Sigma(F_n)$.

In accordance with the literature, we will write $\mathcal{O}_{F_n}\big[\frac{1}{\Sigma_f}\big] = \mathcal{O}_{F_n,\Sigma}$ for the subring of F_n consisting of all $x \in F_n$ that are integral at all finite primes not in $\Sigma_f(F_n)$. We note that $\mathcal{O}_{F_n}\big[\frac{1}{\Sigma_f}\big]$ can be interpreted as a localisation of the Dedekind domain $\mathcal{O}_{F_n}$ at the multiplicatively closed set $\{(a_{\Sigma_f})^n \mid n \geq 0\}$ where a_{Σ_f} is an element of $\mathcal{O}_{F_n}$ such that $v_{\mathfrak{P}}(a_{\Sigma_f})$ is (greater or) equal to 1 precisely for all finite places $\mathfrak{P}$ of F_n contained in Σ_f and 0 for all other finite places. Such an element a_{Σ_f} exists by the finiteness of Σ as is shown by an argument stated in [Conb]: writing h_n for the class number of F_n, we know that the product $\prod_{\mathfrak{P}\in\Sigma_f}\mathfrak{P}^{h_n}$ is a principal ideal generated by an element a_{Σ_f} that has the required property. Since the localisation of a Dedekind domain is Dedekind again, we know that $\mathcal{O}_{F_n}\big[\frac{1}{\Sigma_f}\big]$ is Dedekind.

We define Iwasawa-modules

$$\mathbb{H}^m_\Sigma := \varprojlim_n H^m_{\text{ét}}\big(\mathcal{O}_{F_n}\big[\frac{1}{\Sigma_f}\big], \mathbb{Z}_p(1)\big) := \varprojlim_{n,k} H^m_{\text{ét}}\big(\operatorname{Spec}(\mathcal{O}_{F_n}\big[\frac{1}{\Sigma_f}\big]), (\mathbb{Z}_p/(p^k))(1)\big)$$

for $m \geq 0$, which we want to study in more detail. First we note that we can express these Iwasawa modules in terms of Galois cohomology of the Galois groups $G_\Sigma(F_n) = G(F_\Sigma/F_n)$, see section A.3. In fact, since the modules $(\mathbb{Z}_p/(p^k))(1)$ are finite and of order a power of p, the étale cohomology groups $H^m_{\text{ét}}\big(\operatorname{Spec}(\mathcal{O}_{F_n}\big[\frac{1}{\Sigma_f}\big]), (\mathbb{Z}_p/(p^k))(1)\big)$ coincide with the Galois cohomology groups

$$H^m(G_\Sigma(F_n), (\mathbb{Z}_p/(p^k))(1)),$$

see also ([FK06], section 1.6.3), and we get

$$\mathbb{H}^m_\Sigma \cong \varprojlim_n H^m(G_\Sigma(F_n), \mathbb{Z}_p(1)) \cong H^m(G_\Sigma(F), \Lambda(\mathcal{G})^\#(1)), \tag{2.2.1}$$

the isomorphisms being explained in section A.3. In section A.3.4 we recall that the Kummer sequence gives an isomorphism

$$\varprojlim_n(\mathcal{O}^\times_{F_n,\Sigma} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \xrightarrow{\sim} \mathbb{H}^1_\Sigma. \tag{2.2.2}$$

As in ([Ven00], p. 84) we define

$$X_{\mathrm{nr}} = \mathrm{Gal}(F_\infty^{ur,ab}(p)/F_\infty) \quad \text{and} \quad X_{\mathrm{cs}}^{\Sigma} = \mathrm{Gal}(F_\infty^{ur,ab,cs}(p)/F_\infty),$$

where $F_\infty^{ur,ab}(p)$ denotes the maximal unramified abelian pro-p-extension of F_∞ and we write $F_\infty^{ur,ab,cs}(p)$ for the maximal subextension of $F_\infty^{ur,ab}(p)/F_\infty$ such that every prime above Σ is completely decomposed in $F_\infty^{ur,ab,cs}(p)/F_\infty$. Using the isomorphism (2.2.2), we have an exact sequence by ([Ven00], Proposition 3.1.3 (ii)), which based on work of Jannsen ([Jan89], Theorem 5.4),

$$0 \to \varprojlim_n (\mathcal{O}_{F_n}^{\times} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \to \mathbb{H}_{\Sigma}^1 \to \bigoplus_{\nu \in \Sigma_{un}} \mathrm{c\text{-}Ind}_{\mathcal{G}}^{\mathcal{G}_\nu} \mathbb{Z}_p \xrightarrow{\gamma} X_{nr} \to X_{cs}^{\Sigma} \to 0, \tag{2.2.3}$$

where $\Sigma_{un} = \{\nu \in \Sigma_f \mid p^\infty \nmid f_\nu\}$, $f_\nu = [k_{\infty,\bar{\nu}} : k_\nu]$, $k_{\infty,\bar{\nu}}$ denotes the residue field of $F_{\infty,\bar{\nu}}$, k_ν denotes the residue field of F_ν and $\bar{\nu}$ is some prime of F_∞ above ν. For our extension F_∞/F, since the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{cyc}$ is contained in F_∞ we see that $\Sigma_{un} \subseteq \Sigma_p = \{\nu \mid \nu \text{ lies above } p\}$.

The Kummer sequence also gives an exact sequence

$$1 \longrightarrow \varprojlim_n \big(\mathrm{Pic}(\mathcal{O}_{F_n,\Sigma})\{p\}\big) \longrightarrow \mathbb{H}_{\Sigma}^2 \longrightarrow \bigoplus_{\nu \in \Sigma_f} \Lambda(\mathcal{G}) \otimes_{\Lambda(\mathcal{G}_\nu)} \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow 0. \tag{2.2.4}$$

It is also explained in section A.3.4 that we have a natural surjection

$$\varprojlim_n \big(Cl(F_n)\{p\}\big) \twoheadrightarrow \varprojlim_n \big(\mathrm{Pic}(\mathcal{O}_{F_n,\Sigma})\{p\}\big) \tag{2.2.5}$$

the kernel of which is a finitely generated $\mathbb{Z}_p$-module.

2.3 Statement of the Global Conjecture

Writing $\mathcal{H}$ for the closed normal subgroup of $\mathcal{G}$ corresponding to $\mathbb{Q}_{cyc} \subseteq \mathbb{Q}(\mu_{p^\infty})$, i.e. $\mathcal{G}/\mathcal{H} \cong \mathbb{Z}_p$, the Ore sets $\mathcal{S}$ and $\mathcal{S}^*$ are defined as in [CFK+05] by

$$\mathcal{S} = \{f \in \Lambda(\mathcal{G}) \mid \Lambda(\mathcal{G})/\Lambda(\mathcal{G})f \text{ is finitely generated as a } \Lambda(\mathcal{H}) - \text{module}\}$$

and

$$\mathcal{S}^* = \bigcup_{n \geq 0} p^n S.$$

Note that the exact sequence (2.2.3) implies that

$$\mathcal{S}^{-1}\big(\varprojlim_n (\mathcal{O}_{F_n}^{\times} \otimes_{\mathbb{Z}} \mathbb{Z}_p)\big) \cong \mathcal{S}^{-1}\mathbb{H}_{\Sigma}^1, \tag{2.3.1}$$

since $\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_\nu}\mathbb{Z}_p$ is finitely generated over $\mathbb{Z}_p$ for any ν above p and hence $\mathcal{S}$-torsion by ([CFK+05], Proposition 2.3). We define

$$\mathcal{A}_\infty = \varprojlim_n \big(Cl(F_n)\{p\}\big)$$

and note that due to (2.2.5) and (2.2.4) we have an exact sequence

$$0 \longrightarrow \mathcal{S}^{-1}\mathcal{A}_\infty \longrightarrow \mathcal{S}^{-1}\mathbb{H}^2_\Sigma \longrightarrow \bigoplus_{\nu\in\Sigma_f} \mathcal{S}^{-1}\big(\Lambda(\mathcal{G}) \otimes_{\Lambda(\mathcal{G}_\nu)} \mathbb{Z}_p\big) \longrightarrow 0. \tag{2.3.2}$$

From now on we make the following assumption.

Assumption 2.3.1. *There exists an element $u = (u_n)_n \in \varprojlim_n \mathcal{O}^\times_{F_n}$ such that the map $\Lambda(\mathcal{G})_{\mathcal{S}^*} \to (\mathcal{S}^*)^{-1}(\varprojlim_n \mathcal{O}^\times_{F_n} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ induced by $1 \mapsto u$ is an isomorphism of $\Lambda(\mathcal{G})_{\mathcal{S}^*}$-modules.*

In particular, the isomorphism (2.3.1) implies that $\mathbb{H}^1_\Sigma/\Lambda u$ is $\mathcal{S}^*$-torsion. Compare remark 2.4.40 for a discussion of this assumption in the abelian CM case considered in section 2.4.

Assumption 2.3.2. *If the base field F equals $\mathbb{Q}$, we assume that the element u from assumption 2.3.1 is fixed by complex conjugation (induced by the fixed embedding $F_\infty \subset \mathbb{C}$).*

For an Artin representation $\rho : \mathcal{G} \longrightarrow \mathrm{Aut}(V_\rho)$ that factors through $\mathcal{G}_n = \mathrm{Gal}(F_n/F)$, but not through $\mathcal{G}_{n-1} = \mathrm{Gal}(F_{n-1}/F)$, and for a unit u as in assumption 2.3.1 satisfying assumption 2.3.2 if $F = \mathbb{Q}$ we make the following definition.

Definition 2.3.3. *For u and ρ as above we define the regulator*

$$R(u,\rho) = \begin{cases} \det\big(\sum_{g\in\mathcal{G}_n/<\iota>} \log|g(u_n)|\,\rho(g^{-1})\ ; V_\rho^+\big) & \text{if } F = \mathbb{Q}, \\ \det\big(\sum_{g\in\mathcal{G}_n} \log|g(u_n)|\,\rho(g^{-1})\ ; V_\rho\big) & \text{if } K \text{ is quadratic imaginary,} \end{cases}$$

where we write V_ρ^+ for the subspace of V_ρ on which complex conjugation ι acts as the identity.

We make the following torsion assumption.

Assumption 2.3.4. *We assume that $\mathbb{H}^2_\Sigma$ is $\mathcal{S}^*$-torsion.*

Remark 2.3.5. In the CM elliptic curve case E/K, K quadratic imaginary, where we consider the abelian extension $K(E[p^\infty])/K$, $G = G(K(E[p^\infty])/K)$, we will later show that the term $\bigoplus_{\nu\in\Sigma_f\smallsetminus\Sigma_p} S^{-1}\big(\Lambda(G)\otimes_{\Lambda(G_\nu)}\mathbb{Z}_p\big)$ from (2.3.2) vanishes, see corollary 2.4.34. The term $\bigoplus_{\nu\in\Sigma_p} S^{-1}\big(\Lambda(G)\otimes_{\Lambda(G_\nu)}\mathbb{Z}_p\big)$ also vanishes since the decomposition groups of primes of K above p have finite index in G. Therefore, in this situation, the condition that $\mathbb{H}^2_\Sigma$ is S^*-torsion is equivalent to $\mathcal{A}_\infty$ being S^*-torsion, by (2.3.2).

Now we can formulate the first conjecture. We refer to [CFK+05] for a detailed explanation of how one can evaluate elements of $K_1(\Lambda(\mathcal{G})_{\mathcal{S}^*})$ at Artin representations.

Conjecture 2.3.6 (Global Conjecture). *Under the assumption 2.3.1 (and 2.3.2 if $F = \mathbb{Q}$), there exists $L_{p,u} \in K_1(\Lambda(\mathcal{G})_{S^*})$ such that*

(i) *The value of $L_{p,u}$ at an Artin representation ρ of $\mathcal{G}$ is given by*

$$L_{p,u}(\rho) = \lim_{s\to 0} \frac{s^{-r_\Sigma(\rho)} L_{\Sigma_f}(\rho, s)}{R(u,\rho)},$$

where $r_\Sigma(\rho)$ is the order of vanishing of $L_{\Sigma_f}(\rho, s)$ at $s = 0$, and

(ii) *under the connecting homomorphism $\partial : K_1(\Lambda(\mathcal{G})_{S^*}) \longrightarrow K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$ the element $L_{p,u}$ maps to*

$$\partial(L_{p,u}) = [\mathbb{H}^2_\Sigma] - [\mathbb{H}^1_\Sigma/\Lambda(\mathcal{G})u]. \tag{2.3.3}$$

2.4 The CM case

We fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and a prime number $p \in \mathbb{Z}$, $p \neq 2, 3$. By the CM case we mean the case of an elliptic curve E defined over $\mathbb{Q}$ or, more generally, over K, an imaginary quadratic number field, such that E has complex multiplication by the full ring of integers $\mathcal{O}_K$ of K. In this section, under a torsion assumption and an assumption on the reduction type of E above p, we will show that an element as in assumption 2.3.1 exists and prove conjecture 2.3.6 in the cases outlined in the introduction of this chapter.

Henceforth, we make the fundamental assumption that our elliptic curve E has good ordinary reduction at (or, if E is only defined over K, above) the fixed prime p. Let us recall Deuring's reduction criterion, see proposition A.6.2, stating that the assumption on the reduction type is equivalent to the following assumption.

Assumption 2.4.1. *The prime p splits in K, i.e., $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_K$, where $\mathfrak{p}$ is unequal to its complex conjugate $\bar{\mathfrak{p}}$.*

We will write $\mathfrak{f}$ for the conductor of the Größencharacter $\psi = \psi_E$ attached to E by the theory of complex multiplication, the square of which is the conductor of E/K, see theorem A.6.8 or, for example, [Coab]. We also write $K(\mathfrak{f}p^\infty) = \cup_n K(\mathfrak{f}p^n)$ for the union of the ray class fields $K(\mathfrak{f}p^n)$ of K with respect to the moduli $\mathfrak{f}p^n$ for various $n \geq 1$.

Recall from subsection A.6.1 or [dS87], that the field $K_\infty := K(E[p^\infty])$ is abelian over K and the field $K(\mathfrak{f}p^\infty)$ is finite over K_∞. We write $G = \mathrm{Gal}(K_\infty/K)$ for the Galois group of K_∞ over K. The field K_∞ contains both, K^{cyc} and K^{acyc}, the cyclotomic and the anti-cyclotomic $\mathbb{Z}_p$-extension of the quadratic imaginary field K, respectively. K^{cyc} and K^{acyc} are linearly disjoint over K since $p \neq 2$. We have a decomposition

$$G \cong \Delta \times \Gamma_{cyc} \times \Gamma_{acyc}, \tag{2.4.1}$$

where $\Delta \cong \mathbb{Z}/(p-1) \times \mathbb{Z}/(p-1)$ is a finite group of order $(p-1)^2$, $\Gamma_{cyc} \cong G(K^{cyc}/K) \cong \mathbb{Z}_p$ and $\Gamma_{acyc} \cong G(K^{acyc}/K) \cong \mathbb{Z}_p$.

2.4.1 Notation

Throughout the section, unless stated otherwise, we use the following notation.

K	quadr. imag. number field, of class number 1 from assumption 2.4.4 onwards
$K(\mathfrak{a})$	the ray class field of K modulo some integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$
$\bar{K}$	algebraic closure of K
F	finite abelian extension of K in $\bar{K}$ containing the Hilbert class field $K(1)$
$\mu_\infty(F)$	group of all roots of unity in F
$\mu_{p^\infty}(F)$	group of all p-power roots of unity in F for some prime p
$I(F/K)$	augmentation ideal in $\mathbb{Z}[G(F/K)]$
E	elliptic curve def. over K with CM by $\mathcal{O}_K$, later required to be def. over $\mathbb{Q}$
ψ_E	Größencharacter attached to E/K
$\mathfrak{f}$	conductor of ψ_E
p	prime number of $\mathbb{Z}$, $p \geq 5$, that splits in K and such that $(p, \mathfrak{f}) = 1$
$\mathfrak{p}, \bar{\mathfrak{p}}$	the two distinct primes of K above p
$F_{k,n}$	ray class field $K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$
$K_{k,n}$	the field $K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$
C_F	group defined by elements of the form (2.4.6)
$\mathcal{C}(F)$	$= \mu_\infty(F)C_F$ (Rubin's elliptic units for F)
$\Theta_\mathfrak{m}$	group defined over $\mathbb{Z}[G(K(\mathfrak{m})/K)]$ by elements of the form (2.4.7)
$C_\mathfrak{m}$	$= \{x \in \mathcal{O}_{K(\mathfrak{m})}^\times \mid x^{12} \in \mu_\infty(K(\mathfrak{m}))\Theta_\mathfrak{m}\}$ (De Shalit's elliptic units for $K(\mathfrak{m})$)
C'_F	subgroup of C_F, see definition 2.4.9
D_F	subgroup of C_F, see definition 2.4.9
$C''_{K_{k,n}}$	$= I(K_{k,n}/K)N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}$ (subgroup of $C'_{K_{k,n}}$), see definition 2.4.15
κ	the cyclotomic character.

2.4.2 Global and semi-local units

First, we recall that Leopoldt's conjecture holds for any finite abelian extension F of our quadratic imaginary field K, see ([NSW08], Theorem (10.3.16)) for a proof. This implies, or, in fact, is equivalent to the fact that the map

$$\mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \prod_{\nu | p} \hat{\mathcal{O}}_{F_\nu}^\times, \tag{2.4.2}$$

induced by the diagonal embedding $\mathcal{O}_F^\times \hookrightarrow \prod_{\nu|p} \mathcal{O}_{F_\nu}^\times$, is injective. Here, for any abelian group A we define $\hat{A}$ to be the p-adic completion of A

$$\hat{A} = \varprojlim_n A/p^n A. \tag{2.4.3}$$

Assume that p splits in $K/\mathbb{Q}$ and write $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ for the two distinct primes of K above p. As Bley remarks in ([Ble06], Remark 5.2) and kindly explained to the author, adjusting the proof of the Leopoldt conjecture for an abelian extension F of K, one can even show that

$$\mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \prod_{\nu | \mathfrak{p}} \hat{\mathcal{O}}_{F_\nu}^\times \tag{2.4.4}$$

is an embedding, where we take the product only over the primes of F above $\mathfrak{p}$. We will say that the *strong* version of the Leopoldt conjecture holds for F/K. This observation will prove useful for our purposes since it allows us to identify $\mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$ with the topological closure $\bar{\mathcal{E}}(F)$ of $\mathcal{O}_F^\times$ in $\prod_{\nu|\mathfrak{p}} \hat{\mathcal{O}}_{F_\nu}^\times$. The notation $\bar{\mathcal{E}}(F)$ is adopted from Rubin's article [Rub91].

We recall that for any finite prime ν of F the inclusion $\mathcal{O}_{F_\nu}^1 \hookrightarrow \mathcal{O}_{F_\nu}^\times$ of principal local into local units induces an isomorphism

$$\mathcal{O}_{F_\nu}^1 \cong \hat{\mathcal{O}}_{F_\nu}^\times.$$

Let $p = \mathrm{char}(k(\nu))$, the characteristic of the residue field. The local units $\mathcal{O}_{F_\nu}^\times$ admit a decomposition $\mathcal{O}_{F_\nu}^\times = \mathcal{O}_{F_\nu}^1 \times V_{F_\nu}$ into principal units and a finite group of order prime to p. In particular, we can project a local unit $x \in \mathcal{O}_{F_\nu}^\times$ to its principal part $pr_{\nu,1}(x)$. We will later frequently use the commutativity of the following diagram

$$\begin{array}{ccc}
\mathcal{O}_F^\times & \hookrightarrow & \prod_{\nu|\mathfrak{p}} \mathcal{O}_{F_\nu}^\times \\
\downarrow & & \downarrow (pr_{\nu,1})_\nu \\
\mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p & & \prod_{\nu|\mathfrak{p}} \mathcal{O}_{F_\nu}^1 \\
& \searrow & \downarrow \wr \\
& & \prod_{\nu|\mathfrak{p}} \hat{\mathcal{O}}_{F_\nu}^\times
\end{array} \tag{2.4.5}$$

which follows from the fact that for $x \in \mathcal{O}_F^\times$ and any place ν above $\mathfrak{p}$ we can write $x = pr_{\nu,1}(x)y_\nu$ in $\mathcal{O}_{F_\nu}^\times$ for some y_ν in V_{F_ν} of order n_ν prime to p. Writing $n = \prod_\nu n_\nu$, in $\mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$ we then have $x \otimes 1 = x^n \otimes \frac{1}{n}$ and this maps to $\frac{1}{n}(x^n)_\nu = \frac{1}{n}(pr_{\nu,1}(x)^n)_\nu = (pr_{\nu,1}(x))_\nu$ in $\prod_{\nu|\mathfrak{p}} \hat{\mathcal{O}}_{F_\nu}^\times$.

Next, we introduce some notation for the tower $K_{k,n}, k, n \geq 1$, where $K_{k,n} = K(E[\bar{\mathfrak{p}}^k \mathfrak{p}^n])$ and E/K is an elliptic curve with complex multiplication by $\mathcal{O}_K$, K quadratic imaginary such that p splits in K into $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. We assume that K and all of its algebraic extensions are contained in some fixed algebraic closure $\bar{\mathbb{Q}}$. Let us also fix an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$. Assume that $\mathfrak{p}$ is the prime of K determined by this embedding. For the semi-local units we will write

$$\mathcal{U}_\infty = \varprojlim_{k,n} \prod_{\nu|\mathfrak{p}} \mathcal{O}^1_{K_{k,n,\nu}},$$

where the limit is taken with respect to the norm maps and for all k and n, ν ranges over all primes of $K_{k,n}$ above $\mathfrak{p}$. We note that

$$\mathcal{U}_\infty \cong \varprojlim_{k,n} \prod_{\nu|\mathfrak{p}} \hat{\mathcal{O}}^\times_{K_{k,n,\nu}},$$

since $\mathcal{O}^1_{K_{k,n,\nu}} \cong \hat{\mathcal{O}}^\times_{K_{k,n,\nu}}$ for all k, n and every place ν above $\mathfrak{p}$. For the global units we will write

$$\bar{\mathcal{E}}_\infty = \varprojlim_{k,n} \bar{\mathcal{E}}(K_{k,n}),$$

so that (2.4.4) induces an embedding $\bar{\mathcal{E}}_\infty \hookrightarrow \mathcal{U}_\infty$.

Remark 2.4.2. Write $G = G(K_\infty/K)$, where $K_\infty = \cup_{k,n\geq 1} K_{k,n}$ is the trivializing extension for the action of G_K on the p-adic Tate module T_pE of E/K. Recall that since G is a p-adic Lie group, $\Lambda(G)$ is Noetherian, see ([Laz65], V 2.2.4). We remark that $\mathcal{U}_\infty$ embeds into $\Lambda(G)$ and is therefore Noetherian, see ([Rub91], Theorem 5.1. (ii)) which builds on a result of Wintenberger in [Win80] that we will use later. It follows that any submodule of $\mathcal{U}_\infty$, in particular $\bar{\mathcal{E}}_\infty$, is finitely generated over $\Lambda(G)$. Since $\Lambda(G)$ is compact, each submodule of $\mathcal{U}_\infty$ (as the continuous image of finitely many copies of $\Lambda(G)$) is compact.

For all $k, n \in \mathbb{N}$ the p-adic completion $\bar{\mathcal{E}}(K_{k,n})$ of $\mathcal{O}^\times_{K_{k,n}}$ is separated as a topological space. In particular, singletons $\{x\} \subseteq \bar{\mathcal{E}}(K_{k,n})$ are closed for $x \in \bar{\mathcal{E}}(K_{k,n})$. We will now prove a useful lemma that we will need later when we deal with elliptic units.

Lemma 2.4.3. *Let $\mathcal{D}_\infty$ be a $\Lambda(G)$-submodule of $\bar{\mathcal{E}}_\infty$ and let $\mathcal{D}'_{k,n}$, $k, n \geq 1$, be norm-compatible submodules of $\bar{\mathcal{E}}(K_{k,n})$ such that the projection maps $pr_{k,n} : \bar{\mathcal{E}}_\infty \longrightarrow \bar{\mathcal{E}}(K_{k,n})$ induce surjections*

$$\mathcal{D}_\infty \twoheadrightarrow \mathcal{D}'_{k,n}$$

for all $k, n \geq 1$ (in particular, we require that the image of $\mathcal{D}_\infty$ under the projection is contained in $\mathcal{D}'_{k,n}$). Then, passing to the projective limit with respect to k, n induces an isomorphism

$$\mathcal{D}_\infty \cong \varprojlim_{k,n} \mathcal{D}'_{k,n}$$

of $\Lambda(G)$-modules.

Proof. This follows from the fact that taking projective limits of exact sequences of compact groups preserves exactness. □

2.4.3 Elliptic units

We will now turn our attention to the study of elliptic units. In the theory of abelian extensions of an imaginary quadratic field K elliptic units play a role analogous to the role played by cyclotomic units in the theory of abelian extensions of $\mathbb{Q}$. For basic facts about elliptic units our main references are the papers [Rub91] by Rubin and [dS87] by de Shalit. In ([Rub91], Theorem 7.7), for certain extensions K_∞/K, Rubin gives a description of the projective limit of the p-adic completions of certain elliptic units for subfields F of K_∞/K that he defines earlier in the same article (these are the elliptic units that satisfy the analytic class number formula given in ([Rub91], Theorem 1.3)). In case K_∞/K is given by $K_\infty = K(E[p^\infty])$, K quadratic imaginary, however, where E/K is an elliptic curve with complex multiplication by $\mathcal{O}_K$ with good ordinary reduction above a split prime p, the description Rubin gives in (loc. cit., Theorem 7.7 (i)) does not seem to describe the projective limit of elliptic units satisfying the analytic number formula, but rather the limit considered by Yager in ([Yag82], Lemma 28, Theorem 29). Rubin's elliptic units (in the $K(E[p^\infty])/K$ case) contain Yager's units, but also they are strictly bigger. After recalling the definition of the Coleman map in the next subsection, we will determine the precise structure of the projective limit of Rubin's elliptic units in theorem 2.4.31 for elliptic curves whose conductor is a prime power.

The comparison of the two (Rubin's and Yager's units) will be the main theme of this subsection. The task will be to study Rubin's elliptic units and, step by step, determine a relatively small set of generators. The main results of this subsection are corollary 2.4.13, which describes the projective limit of Rubin's elliptic units for our extension K_∞/K, and theorem 2.4.16, which states that the quotient of the limits of Rubin's and (a slight variant of) de Shalit's elliptic units is S-torsion and gives a concrete element of S that annihilates the quotient.

For Robert's treatment of elliptic units see [Rob73], [Rob90] and [Rob90]. There are other useful accounts due to Rubin in the appendix of [Rub87] and due to Coates and Wiles in section 5 of [CW77] and in section 3 of [CW78]. The different notation used in some of the above papers is compared by Bley in [Ble04].

After writing this section the author found the paper [Vig12] by Viguié, who proves a similar statement as lemma 2.4.8 from this subsection, compare ([Vig12], Lemma 2.4, Corollary 2.5). He also determines a set of generators for projective limits of elliptic units for a certain $\mathbb{Z}_p$-extension, see (loc. cit., Lemma 2.7). Our situation will be rather different in that we deal with a $\mathbb{Z}_p^2$-extension, which requires different ideas.

Let us start by recalling Rubin's definition of elliptic units for a number field F which is an abelian Galois extension of a quadratic imaginary field K containing the Hilbert class field H of K. For an integral ideal $\mathfrak{m}$ of K we denote by $K(\mathfrak{m})$ the ray class field of K modulo $\mathfrak{m}$. We fix an embedding $\bar{K} \subset \mathbb{C}$ and a period lattice $L \subset \mathbb{C}$ of some elliptic curve defined over H with complex multiplication by $\mathcal{O}_K$; for the existence of such a curve Rubin refers to ([Shi71], theorem 5.7). For any integral ideal $\mathfrak{a} \subset \mathcal{O}_K$, $(\mathfrak{a}, 6) = 1$, Rubin then considers the meromorphic function

$$\Theta_0(z; \mathfrak{a}) = \Theta_0(z; L, \mathfrak{a}) = \Big(\frac{\Delta(L)^{N\mathfrak{a}}}{\Delta(\mathfrak{a}^{-1}L)}\Big)^{1/12} \prod_{u \in (\mathfrak{a}^{-1}L/L)/\pm 1} \big(\wp(z; L) - \wp(u; L)\big)^{-1},$$

where Δ is the Ramanujan Δ-function, a twelfth root of $\frac{\Delta(L)^{N\mathfrak{a}}}{\Delta(\mathfrak{a}^{-1}L)}$ is fixed and $\wp(z; L)$ is the Weierstraß $\wp$-function for the lattice L.

Now, let $\mathfrak{m}$ be an integral ideal of K such that $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\mathfrak{m}$ is injective and let $\tau \in \mathbb{C}/L$ be an element of order exactly $\mathfrak{m}$. It is shown in ([Ble04], Proposition 2.2) that $\Theta_0(\tau; \mathfrak{a})$ belongs to $K(\mathfrak{m})$. Rubin then defines the group C_F generated by the various

$$\big(N_{FK(\mathfrak{m})/F}\ \Theta_0(\tau; \mathfrak{a})\big)^{\sigma - 1}, \tag{2.4.6}$$

where σ ranges through $\mathrm{Gal}(F/K)$, $\mathfrak{m}$ through the integral ideals of K such that $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\mathfrak{m}$ is injective, $\mathfrak{a}$ through integral ideals such that $(\mathfrak{a}, 6\mathfrak{m}) = 1$ and τ through primitive $\mathfrak{m}$-division points. $N_{FK(\mathfrak{m})/F}$ denotes the norm map from $FK(\mathfrak{m})$ to F and we note that the elements $\sigma - 1$ generate the augmentation ideal $I(F/K)$ of $\mathbb{Z}[G(F/K)]$. Rubin then defines the elliptic units of F to be

$$\mathcal{C}(F) = \mu_\infty(F) C_F,$$

where $\mu_\infty(F)$ is the group of all roots of unity in F.

Next we briefly recall the definition of elliptic units used by De Shalit. He considers the function

$$\Theta(z; L, \mathfrak{a}) = \Theta_0(z; \mathfrak{a})^{12},$$

which is an elliptic function with respect to L and can be expressed in terms of the fundamental theta function, which is noted in ([dS87], II, 2.3). Moreover, $\Theta(z; L, \mathfrak{a})$ satisfies the monogeneity relation

$$\Theta(cz; cL, \mathfrak{a}) = \Theta(z; L, \mathfrak{a}), \quad c \in \mathbb{C}^\times.$$

Assumption 2.4.4. *From now on we assume that K has class number one. Note that this is automatically satisfied whenever we consider an elliptic curve E/K with complex multiplication by $\mathcal{O}_K$, see proposition A.6.1.*

So we can find Ω, m such that $L = \mathcal{O}_K \Omega$ and $\mathfrak{m} = (m)$ for any integral ideal $\mathfrak{m}$ of K. With this notation $\tau = \Omega/m$ is a point of order exactly m in $\mathbb{C}/L$. De Shalit then defines $\Theta_\mathfrak{m}$ to be the subgroup of $K(\mathfrak{m})^\times$ generated by

$$\Theta(1; \mathfrak{m}, \mathfrak{a}) = \Theta(\Omega/m; L, \mathfrak{a}), \tag{2.4.7}$$

where $\mathfrak{a}$ ranges through the integral ideals of K such that $(\mathfrak{a}, 6\mathfrak{m}) = 1$. If $\mathfrak{m}$ is divisible by at least two distinct primes, then $\Theta_\mathfrak{m}$ is a subgroup of the group of units $\mathcal{O}_{K(\mathfrak{m})}^\times$ in $K(\mathfrak{m})^\times$. He then defines $C_{\mathfrak{m}}$ to be the group of units in $K(\mathfrak{m})^\times$ whose 12-th power belongs to $\mu_\infty(K(\mathfrak{m}))\Theta_{\mathfrak{m}}$. The group $C_{\mathfrak{m}}$ is $G(K(\mathfrak{m})/K)$-stable, which follows from ([dS87], II, proposition 2.4 (ii)).

The main theorem of complex multiplication can be used to show that the values of Θ at two different primitive $\mathfrak{m}$-division points are related through the action of the Galois group $G(K(\mathfrak{m})/K)$, which we want to illustrate in the next remark. Let us first introduce some notation for arithmetic Frobenius elements.

Definition 2.4.5. *Let F/K be an abelian (finite or infinite) extension in which the prime ideal $\mathfrak{q}$ is unramified. We then write*

$$(\mathfrak{q}, F/K) \in D_{\mathfrak{q}} \subset G(F/K)$$

for the arithmetic Frobenius at $\mathfrak{q}$ which (topologically) generates the decomposition group $D_{\mathfrak{q}}$. If $\mathfrak{c}$ is an ideal which has a prime decomposition $\prod_{i=1}^r \mathfrak{q}_i^{m_i}$ and each $\mathfrak{q}_i$ is unramified in F/K, then we define

$$(\mathfrak{q}, F/K) := \prod_{i=1}^r (\mathfrak{q}_i, F/K)^{m_i}.$$

Remark 2.4.6. Assume that the conductor $\mathfrak{f}_E$ associated to the Größencharacter ψ_E divides $\mathfrak{m}$. Now, if τ is any primitive $\mathfrak{m}$-division point we can find $c \in \mathcal{O}_K$, c prime to $\mathfrak{m}$, such that $\tau = c\frac{\Omega}{m}$. Let us write $\sigma_c = ((c), K(\mathfrak{m})/K)$ in $G(K(\mathfrak{m})/K)$. Then the Größencharacter ψ_E maps σ_c to a generator of (c), so we can find a unit u_c in $\mathcal{O}_K^\times$ such that $\psi_E((c)) = u_c c$. Then, by ([Rub87], Proposition 12.3 (i)) and by the main theorem of complex multiplication (the part that says that σ_c acts on $E[\mathfrak{m}]$ through ψ_E), we have

$$\Theta(\Omega/m; L, \mathfrak{a})^{\sigma_c} = \Theta(\psi_E((c))(\Omega/m); L, \mathfrak{a}) = \Theta(u_c c(\Omega/m); L, \mathfrak{a}) = \Theta(\tau; L, \mathfrak{a}), \tag{2.4.8}$$

where, for the last equation, we have used the monogeneity property and the fact that $u_c^{-1}L = L$. We conclude that the values of Θ at two different primitive $\mathfrak{m}$ division points belong to the same orbit under the action of $G(K(\mathfrak{m})/K)$.

Note that Rubin's group C_F for arbitrary fields F, in general, is rather large, since in the definition of generators as in (2.4.6) he allows $\mathfrak{m}$ to range through all integral ideals of K such that $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\mathfrak{m}$ is injective. Other authors, e.g. Yager in [Yag82], consider only the conductor $\mathfrak{q}_F$ of the extension F/K they are interested in, i.e. they take $\left(N_{K(\mathfrak{q}_F)/F}\,\Theta_0(\tau;\mathfrak{a})\right)^{\sigma-1}$ as generators, τ a primitive $\mathfrak{q}_F$-division point and $\mathfrak{a}$, σ as above.

We will eventually be interested in the fields $F = K_{k,n} := K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$ for an elliptic curve E/K with complex multiplication by $\mathcal{O}_K$, where K is an imaginary quadratic number field and $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are distinct primes of K above a rational prime p, at which E/K has good reduction. In our comparison of Rubin's and de Shalit's elliptic units for such fields the following lemma is our starting point, which says that in the definition of $C_{K_{k,n}}$ we can restrict ourselves to certain integral ideals $\mathfrak{m}$ dividing the conductor of $K_{k,n}$. We will prove in lemma 2.4.17 that the conductor of $K_{k,n}$, for $k,n \geq 0$, $(k,n) \neq (0,0)$, is given by $\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$, where $\mathfrak{f}$ is the conductor of ψ_E.

Remark 2.4.7. Note that since K is quadratic imaginary, $\mathcal{O}_K^\times$ consists only of a finite number of roots of unity. Therefore, for any prime $\mathfrak{q}$, the map

$$\mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K/\mathfrak{q}^n)^\times$$

will always become injective for n large enough. Likewise, for any non-trivial ideal $\mathfrak{b}$ prime to $\mathfrak{q}$

$$\mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K/\mathfrak{q}^n\mathfrak{b})^\times$$

will always become injective for n large enough, since $(\mathcal{O}_K/\mathfrak{q}^n\mathfrak{b})^\times \hookrightarrow (\mathcal{O}_K/\mathfrak{q}^n)^\times \times (\mathcal{O}_K/\mathfrak{b})^\times$.

Lemma 2.4.8. *Let K be a quadratic imaginary number field and E/K an elliptic curve with complex multiplication by $\mathcal{O}_K$. Moreover, let $p \in \mathbb{Z}$, $p \neq 2,3$, be a prime that splits in K into distinct primes $\mathfrak{p} = (\pi)$ and $\bar{\mathfrak{p}} = (\bar{\pi})$ and assume that E has good reduction at $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. Let $k, n \geq 1$ such that both $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\bar{\mathfrak{p}}^k$ and $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\mathfrak{p}^n$ are injective. Let us write $F = K_{k,n} = K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$. Then, as a $\mathbb{Z}_p[G(F/K)]$-module, $C_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is already generated by elements of the form*

$$\left(N_{FK(\mathfrak{m})/F}\ \Theta(\tau;\mathfrak{a})\right)^{\sigma-1},$$

where σ ranges through $\mathrm{Gal}(F/K)$, $\mathfrak{m}$ through the integral ideals of K such that either

$$\mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n \text{ or } \mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^k \text{ or } \mathfrak{m} = \mathfrak{f}'\mathfrak{p}^n \text{ for some divisor } \mathfrak{f}' \text{ of } \mathfrak{f},$$

$\mathfrak{a}$ runs through integral ideals such that $(\mathfrak{a}, 6\mathfrak{m}) = 1$ and τ through primitive $\mathfrak{m}$-division points.

Proof. First note that after extending scalars, since 12 is a unit in $\mathbb{Z}_p$, we have

$$\left(N_{FK(\mathfrak{m})/F}\ \Theta_0(\tau;\mathfrak{a})\right)^{\sigma-1} \otimes 1 = \left(N_{FK(\mathfrak{m})/F}\ \Theta(\tau;\mathfrak{a})\right)^{\sigma-1} \otimes \frac{1}{12},$$

so clearly all elements of the form $\left(N_{FK(\mathfrak{m})/F}\ \Theta(\tau;\mathfrak{a})\right)^{\sigma-1}$, for general $\mathfrak{m}$, τ, $\mathfrak{a}$ and σ as in (2.4.6), generate $C_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ as a $\mathbb{Z}_p$-module. Hence, from now on it is sufficient to consider the function $\Theta(z,\mathfrak{a}) = \Theta(z, L, \mathfrak{a})$ (we omit the L from the notation).

Let us now fix an integral ideal $\mathfrak{m}$ of K such that $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\mathfrak{m}$ is injective. Write

$$x := N_{FK(\mathfrak{m})/F}\ \Theta(\tau;\mathfrak{a}),$$

where $\mathfrak{a}$ is an integral ideal such that $(\mathfrak{a}, 6\mathfrak{m}) = 1$ and τ is a primitive $\mathfrak{m}$-division point. We will show that $x^{\sigma-1}$, for any $\sigma \in G(F/K)$, is already contained in the module generated by the elements from the statement of the lemma. We will show step by step that we can impose more conditions on $\mathfrak{m}$ and still obtain a set of $\mathbb{Z}_p[G(K_{k,n}/K)]$-generators for $C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Let us first make some general definitions. We define $\mathfrak{f}' = g.c.d.(\mathfrak{f}, \mathfrak{m})$. We can then write

$$\mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}\mathfrak{m}',$$

for some $\mathfrak{m}'$ such that $g.c.d.(\mathfrak{m}', p) = 1$, so that n', resp. k', are precisely the exponents of $\mathfrak{p}$, resp. $\bar{\mathfrak{p}}$, in $\mathfrak{m}$. We need not have $g.c.d.(\mathfrak{m}', \mathfrak{f}) = 1$. Let us define $\mathfrak{q} = g.c.d.(\mathfrak{m}, \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$, so that we have

$$F \cap K(\mathfrak{m}) \subset K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n) \cap K(\mathfrak{m}) = K(\mathfrak{q}),$$

where the last equality is a simple excercise in class field theory. Since $\mathfrak{f}$ and p are prime to each other, we have an equality

$$\mathfrak{q} = \mathfrak{f}'\bar{\mathfrak{p}}^{\min\{k,k'\}}\mathfrak{p}^{\min\{n,n'\}}.$$

For the norm map $N_{FK(\mathfrak{m})/F}$ restricted to $K(\mathfrak{m})$ we can write

$$N_{FK(\mathfrak{m})/F} = N_{K(\mathfrak{m})/(F\cap K(\mathfrak{m}))} = N_{K(\mathfrak{q})/(F\cap K(\mathfrak{m}))} \circ N_{K(\mathfrak{m})/K(\mathfrak{q})}, \tag{2.4.9}$$

where we note that $F \cap K(\mathfrak{m}) = F \cap K(\mathfrak{q})$. Let us now start with the computations. We will show that we may exclude the following classes of $\mathfrak{m}$ and are still left with a set of $\mathbb{Z}_p[G(K_{k,n}/K)]$-generators for $C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

1. Case: $g.c.d.(\mathfrak{m}, p) = 1$.

In this case, since E/K has good reduction at $\mathfrak{p}$ and $\bar{\mathfrak{p}}$, we also have $g.c.d.(\mathfrak{m}\mathfrak{f}, p) = 1$. By ([dS87], II, proposition 1.6, corollary 1.7) we know that $K(\mathfrak{m}\mathfrak{f}) = K(E[\mathfrak{m}\mathfrak{f}])$ and that $K(E[\mathfrak{m}\mathfrak{f}])$ and $F = K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$ are linearly disjoint over K. Therefore, we have an inclusion

$$F \cap K(\mathfrak{m}) \subset F \cap K(\mathfrak{m}\mathfrak{f}) = K,$$

which implies that $G(FK(\mathfrak{m})/F) \cong G(K(\mathfrak{m})/K)$. This shows that if we restrict the norm map $N_{FK(\mathfrak{m})/F}$ to $K(\mathfrak{m})$, then $N_{FK(\mathfrak{m})/F} = N_{K(\mathfrak{m})/K}$. We conclude that

$$x^{\sigma-1} = \left(N_{K(\mathfrak{m})/K}\ \Theta(\tau;\mathfrak{a})\right)^{\sigma-1} = 1.$$

since σ fixes K. From now on, we may and will assume that $g.c.d.(\mathfrak{m}, p) \neq 1$, i.e., that $\mathfrak{p} \mid \mathfrak{m}$ or $\bar{\mathfrak{p}} \mid \mathfrak{m}$.

2. Case: $n' > n$ or $k' > k$.

If $n' > n$, then ([dS87], II, proposition 2.5), see also ([Rub99], corollary 7.7, p. 197) for a more detailed proof, shows that

$$N_{K(\mathfrak{m})/K(\mathfrak{m}/\mathfrak{p})}\ \Theta(\tau;\mathfrak{a}) = \Theta(\pi\tau;\mathfrak{a}),$$

where $\pi\tau$ is now clearly a primitive $\frac{\mathfrak{m}}{\mathfrak{p}}$-division point. We note that here we use the fact that $\mathfrak{p}^n \mid \frac{\mathfrak{m}}{\mathfrak{p}}$ and that $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\mathfrak{p}^n$ is injective, i.e., that there is precisely one root of unity in K that is congruent to 1 modulo $\mathfrak{p}^n$. Since $\mathfrak{q} \mid \frac{\mathfrak{m}}{\mathfrak{p}}$, we also have

$$F \cap K(\mathfrak{m}) \;=\; F \cap K(\mathfrak{m}/\mathfrak{p}).$$

Using (2.4.9), this shows that $x = N_{FK(\mathfrak{m}/\mathfrak{p})/F}\ \Theta(\pi\tau;\mathfrak{a})$. Proceeding inductively, we may and will assume that $n' \leq n$. Analogously, we can show that we may assume that $k' \leq k$.

3. Case: $1 \leq n' < n$ or $1 \leq k' < k$.

Without loss of generality, let us assume that $n' \geq 1$ (if $n' = 0$, then, by the first case, we may assume that $k' \geq 1$ and the following works precisely in the same way for k'). So $\mathfrak{p} \mid \mathfrak{m}$. While we have used ([dS87], II, proposition 2.5) above to see that we may make the exponent n' of $\mathfrak{p}$ in $\mathfrak{m}$ smaller if $n' > n$, we now use it to see that we may make it bigger whenever $n' < n$. In fact, by the above-cited proposition we have

$$\Theta(\tau;\mathfrak{a}) = N_{K(\mathfrak{m}\mathfrak{p})/K(\mathfrak{m})}\Theta\Big(\frac{\tau}{\pi};\mathfrak{a}\Big),$$

where, if we consider τ as an element of $E(\mathbb{C})$, we write $\frac{\tau}{\pi}$ for some primitive $\mathfrak{m}\mathfrak{p}$-division point in $E(\mathbb{C})$ such that $\pi\frac{\tau}{\pi} = \tau$ (while if we consider τ as an element of $\mathbb{C}/L$ then we can actually divide τ by π - this depends on whether we view Θ as a function on $E(\mathbb{C})$ or on $\mathbb{C}/L$). Using (2.4.9) again, it follows that

$$x = N_{K(\mathfrak{m}\mathfrak{p})/(F\cap K(\mathfrak{m}))}\Theta\Big(\frac{\tau}{\pi};\mathfrak{a}\Big) = N_{(F\cap K(\mathfrak{m}\mathfrak{p}))/(F\cap K(\mathfrak{m}))}\circ N_{K(\mathfrak{m}\mathfrak{p})/(F\cap K(\mathfrak{m}\mathfrak{p}))}\Theta\Big(\frac{\tau}{\pi};\mathfrak{a}\Big),$$

showing that x is just a product of $G(F/K)$-conjugates of $N_{K(\mathfrak{m}\mathfrak{p})/(F\cap K(\mathfrak{m}\mathfrak{p}))}\Theta\big(\frac{\tau}{\pi};\mathfrak{a}\big)$. Proceeding inductively, we may assume that $n' = n$.

We conclude that so far we may assume $k' \leq k$ and $n' \leq n$ and either $n = n'$ or $k = k'$. If both, k' and n' are greater than zero, then the last argument shows that we may assume that $k' = k$ and $n' = n$.

In the last step we made $\mathfrak{m}$ larger so that $\mathfrak{p}^n \mid \mathfrak{m}$ (or $\bar{\mathfrak{p}}^k \mid \mathfrak{m}$). By our assumption on n and k, it follows that there is only one root of unity in K that is congruent to 1 modulo $\frac{\mathfrak{m}}{\mathfrak{m}'}$. This enables us to use ([dS87], II, proposition 2.5) in the next step to eliminate $\mathfrak{m}'$.

<u>4. Case:</u> $\mathfrak{m}' \neq 1$.
Let $\mathfrak{l} = (l)$ be a prime ideal of K dividing $\mathfrak{m}'$. In particular, $\mathfrak{l}$ is prime to p. First note that

$$\mathfrak{q} = g.c.d.\Big(\frac{\mathfrak{m}}{\mathfrak{l}}, \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n\Big).$$

In fact, if $g.c.d.\big(\frac{\mathfrak{m}}{\mathfrak{l}}, \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n\big)$ were equal to $\frac{\mathfrak{q}}{\mathfrak{l}}$ (it certainly cannot be anything else), write $\mathfrak{l}^r$ for the exact power of $\mathfrak{l}$ in $\mathfrak{q}$. We then see that $\mathfrak{l}^r \mid \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$, and hence $\mathfrak{l}^r \mid \mathfrak{f}$. Moreover, $\mathfrak{l}^r \mid \mathfrak{m}$, so that $\mathfrak{l}^r \mid \mathfrak{f}'$. By the assumption $g.c.d.\big(\frac{\mathfrak{m}}{\mathfrak{l}}, \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n\big) = \mathfrak{q}/\mathfrak{l}$, we have $\mathfrak{l}^r \nmid \frac{\mathfrak{m}}{\mathfrak{l}}$. On the other hand, $\mathfrak{l}^r \mid \mathfrak{f}'\frac{\mathfrak{m}'}{\mathfrak{l}}$ and $\mathfrak{f}'\frac{\mathfrak{m}'}{\mathfrak{l}} \mid \frac{\mathfrak{m}}{\mathfrak{l}}$. This is a contradiction, showing that $\mathfrak{q} = g.c.d.\big(\frac{\mathfrak{m}}{\mathfrak{l}}, \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n\big)$ holds.

By (loc. cit.) we have

$$N_{K(\mathfrak{m})/K(\mathfrak{m}/\mathfrak{l})}\ \Theta(\tau;\mathfrak{a}) = \begin{cases}\Theta(l\tau;\mathfrak{a}) & \text{if } \mathfrak{l} \mid \frac{\mathfrak{m}}{\mathfrak{l}},\\ \Theta(l\tau;\mathfrak{a})^{1-\sigma_{\mathfrak{l}}^{-1}} & \text{if } \mathfrak{l} \nmid \frac{\mathfrak{m}}{\mathfrak{l}},\end{cases}$$

where, in the case $\mathfrak{l} \nmid \frac{\mathfrak{m}}{\mathfrak{l}}$, $\sigma_{\mathfrak{l}} = \big(\mathfrak{l}, K\big(\frac{\mathfrak{m}}{\mathfrak{l}}\big)/K\big)$. We conclude that

$$x = N_{K(\mathfrak{m})/(F\cap K(\mathfrak{q}))}\ \Theta(\tau;\mathfrak{a}) = \begin{cases} N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}\ \Theta(l\tau;\mathfrak{a}) & \text{if } \mathfrak{l} \mid \frac{\mathfrak{m}}{\mathfrak{l}},\\ N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}\ \Big(\Theta(l\tau;\mathfrak{a})^{1-\sigma_{\mathfrak{l}}^{-1}}\Big) & \text{if } \mathfrak{l} \nmid \frac{\mathfrak{m}}{\mathfrak{l}}.\end{cases}$$

In the latter case, since all of the involved Galois groups are abelian, we see that

$$N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}\left(\Theta(l\tau;\mathfrak{a})^{1-\sigma_{\mathfrak{l}}^{-1}}\right)=\left(N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}\ \Theta(l\tau;\mathfrak{a})\right)^{1-\tilde{\sigma}_{\mathfrak{l}}^{-1}},$$

where we write $\tilde{\sigma}_{\mathfrak{l}}$ for any lift to F of the restriction of $\sigma_{\mathfrak{l}}$ to $F\cap K(\mathfrak{q})$. In any case, we see that x is a product of $G(F/K)$-conjugates of $N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}\ \Theta(l\tau;\mathfrak{a})$. We conclude that we may assume that $\mathfrak{m}'$ is trivial.

We have shown that we may restrict to $\mathfrak{m}$ of the form $\mathfrak{m}=\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n$ or $\mathfrak{m}=\mathfrak{f}'\bar{\mathfrak{p}}^k$ or $\mathfrak{m}=\mathfrak{f}'\mathfrak{p}^n$ for some divisor $\mathfrak{f}'$ of $\mathfrak{f}$ and still get a generating set; in any case $\mathfrak{m}\mid\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$. □

We now *split* the set of $\mathbb{Z}_p[G(F/K)]$-generators of $C_F\otimes_{\mathbb{Z}}\mathbb{Z}_p$ determined in lemma 2.4.8 ($F=K_{k,n}$ as in the lemma) and define two new modules.

Definition 2.4.9. *Let the setting be as in lemma 2.4.8, in particular, $n,k\geq 1$ and we write $F=K_{k,n}$. We define C'_F to be the subgroup of C_F generated by elements of the form*

$$\left(N_{FK(\mathfrak{m})/F}\ \Theta(\tau;\mathfrak{a})\right)^{\sigma-1},$$

where σ ranges through $\mathrm{Gal}(F/K)$, $\mathfrak{m}$ *through the integral ideals of K such that*

$$\mathfrak{m}=\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n \text{ for some divisor } \mathfrak{f}' \text{ of } \mathfrak{f},$$

$\mathfrak{a}$ *runs through integral ideals such that* $(\mathfrak{a},6\mathfrak{m})=1$ *and τ through primitive* $\mathfrak{m}$*-division points.*

Moreover, we define D_F to be the subgroup of C_F generated by elements of the form

$$\left(N_{FK(\mathfrak{m})/F}\ \Theta(\tau;\mathfrak{a})\right)^{\sigma-1},$$

where σ ranges through $\mathrm{Gal}(F/K)$, $\mathfrak{m}$ *through the integral ideals of K such that*

$$\mathfrak{m}=\mathfrak{f}'\bar{\mathfrak{p}}^k \text{ or } \mathfrak{m}=\mathfrak{f}'\mathfrak{p}^n \text{ for some divisor } \mathfrak{f}' \text{ of } \mathfrak{f},$$

$\mathfrak{a}$ *runs through integral ideals such that* $(\mathfrak{a},6\mathfrak{m})=1$ *and τ through primitive* $\mathfrak{m}$*-division points.*

Remark 2.4.10. First note that, by definition and lemma 2.4.8, we have $\left(C'_F D_F\right)\otimes_{\mathbb{Z}}\mathbb{Z}_p=C_F\otimes_{\mathbb{Z}}\mathbb{Z}_p$. Also, C'_F and D_F are $G(F/K)$-stable, see ([dS87], II, proposition 2.4). Moreover, it is not a difficult exercise to show that the norm maps $N_{K_{k,n}/K_{k',n'}}$, $k\geq k'\geq 1$, $n\geq n'\geq 1$, restrict to maps $C'_{K_{k,n}}\longrightarrow C'_{K_{k',n'}}$ and $D_{K_{k,n}}\longrightarrow D_{K_{k',n'}}$, respectively.

Note that, in general, elements of the form

$$\Theta(\tau;\mathfrak{a})\ \in\ K(\mathfrak{m})$$

for a primitive $\mathfrak{m}$-division point τ, where $\mathfrak{m}=\mathfrak{p}^n$ or $\mathfrak{m}=\bar{\mathfrak{p}}^k$, i.e., where $\mathfrak{f}'$ is trivial and $\mathfrak{m}$ is divisible by only one prime, are not units in $\mathcal{O}_{K_{k,n}}$. However, in case $\mathfrak{m}=\mathfrak{p}^n$, they are units outside the primes above $\mathfrak{p}$ and in case $\mathfrak{m} = \bar{\mathfrak{p}}^k$, they are units outside the primes above $\bar{\mathfrak{p}}$, see (loc. cit.). Moreover, in our definition of C_F, C'_F and D_F, we twist by $\sigma - 1$, $\sigma \in G(F/K)$ (which we can lift to $G(FK(\mathfrak{m})/K)$ and then restrict to $G(K(\mathfrak{m})/K)$). We claim that, in case $\mathfrak{m} = \mathfrak{p}^n$, $\big(\Theta(\tau;\mathfrak{a})\big)^{\sigma-1}$ is also a unit above $\mathfrak{p}$ and therefore belongs to $\mathcal{O}^\times_{K(\mathfrak{m})}$. And similarly, in case $\mathfrak{m} = \bar{\mathfrak{p}}^k$, $\big(\Theta(\tau;\mathfrak{a})\big)^{\sigma-1}$ is also a unit above $\bar{\mathfrak{p}}$

To see this, let us consider the case $\mathfrak{m} = \mathfrak{p}^n$, the other one works analogously. Let $\mathfrak{P}$ be a prime of $K(\mathfrak{p}^n)$ above $\mathfrak{p}$. And consider the decomposition group $D_\mathfrak{p}$ of $\mathfrak{p}$ in $G(K(\mathfrak{p}^n)/K)$. It is a fact that for the fixed field

$$Z_\mathfrak{p} = K(\mathfrak{p}^n)^{D_\mathfrak{p}}$$

and the prime $\mathfrak{P}_Z$ of $Z_\mathfrak{p}$ below $\mathfrak{P}$, $\mathfrak{P}_Z$ has ramification index 1 over K, see ([Neu07], I, Satz 9.3). This means that $\mathfrak{p}$ is unramified in $Z_\mathfrak{p}$. But $Z_\mathfrak{p}$ is also contained in $K(\mathfrak{p}^n)$, showing that it is unramified everywhere and therefore contained in the Hilbert class field of K, which is K itself. We conclude that $D_\mathfrak{p} = G(K(\mathfrak{p}^n)/K)$, which means that there is only one prime of $K(\mathfrak{p}^n)$ above $\mathfrak{p}$. In particular, any element σ in $G(K(\mathfrak{p}^n)/K)$ fixes the unique prime $\mathfrak{P}$ above $\mathfrak{p}$, which implies for any $a \in K(\mathfrak{p}^n), a \neq 0$, that $\sigma(a)/a$ is integral and a unit at $\mathfrak{P}$.

With the above definitions lemma 2.4.8 implies that for all $k, n \geq 1$ as in the lemma, we have surjections of $\mathbb{Z}_p[G(K_{k,n}/K)]$-modules

$$D_{K_{k,n}} \otimes_\mathbb{Z} \mathbb{Z}_p \twoheadrightarrow \left(C_{K_{k,n}}/C'_{K_{k,n}}\right) \otimes_\mathbb{Z} \mathbb{Z}_p.$$

The next lemma shows that the natural inclusions $C'_{K_{k,n}} \hookrightarrow C_{K_{k,n}}$ induce isomorphisms of $\Lambda(G)$-modules

$$\varprojlim_{k,n}(C'_{K_{k,n}} \otimes_\mathbb{Z} \mathbb{Z}_p) \cong \varprojlim_{k,n}(C_{K_{k,n}} \otimes_\mathbb{Z} \mathbb{Z}_p). \tag{2.4.10}$$

Lemma 2.4.11. *We have the following identity*

$$\varprojlim_{k,n}(D_{K_{k,n}} \otimes_\mathbb{Z} \mathbb{Z}_p) = 0,$$

where the limit is taken with respect to the norm maps.

Proof. In remark 2.4.10 we have explained that $D_{K_{k,n}} \subset \mathcal{O}^\times_{K_{k,n}}$. This inclusion induces

$$D_{K_{k,n}} \otimes_\mathbb{Z} \mathbb{Z}_p \hookrightarrow \mathcal{O}^\times_{K_{k,n}} \otimes_\mathbb{Z} \mathbb{Z}_p,$$

and we note that by Dirichlet's unit theorem the group on the right is given by the direct sum of a finite number of copies of $\mathbb{Z}_p$ and the finite group of p-power roots of unity in $K_{k,n}$.

Let us make a few more observations. For any integral ideal $\mathfrak{a}$ of K we always have $K(\mathfrak{a}) \subset K(E[\mathfrak{a}])$, see ([Sil99], II, Theorem 5.6). It follows from proposition A.6.3 that for all $k, n \geq 1$

$$\left(K_{k,n} \cap K(\mathfrak{f}'\bar{\mathfrak{p}}^k)\right) \subset \left(K_{k,n} \cap K(E[\mathfrak{f}'\bar{\mathfrak{p}}^k])\right) = K_{k,0}. \tag{2.4.11}$$

Likewise, we have for all $k,n\geq 1$

$$\Big(K_{k,n}\cap K(\mathfrak{f}'\mathfrak{p}^n)\Big)\subset\Big(K_{k,n}\cap K(E[\mathfrak{f}'\mathfrak{p}^n])\Big)=K_{0,n}. \tag{2.4.12}$$

For any $r\geq 1$, let us consider an arbitrary generator $d_{k+r,n+r}=\big(N_{K_{k+r,n+r}K(\mathfrak{m})/K_{k+r,n+r}}\ \Theta(\tau;\mathfrak{a})\big)^{\sigma-1}$ of $D_{K_{k+r,n+r}}$, where

$$\mathfrak{m}=\mathfrak{f}'\bar{\mathfrak{p}}^{k+r}\text{ or }\mathfrak{m}=\mathfrak{f}'\mathfrak{p}^{n+r}\text{ for some divisor }\mathfrak{f}'\text{ of }\mathfrak{f}.$$

First assume that $\mathfrak{m}=\mathfrak{f}'\bar{\mathfrak{p}}^{k+r}$. Note that for $k,n\geq 1$ the Galois group $G(K_{k+r,n+r}/K_{k+r,n})$ is of order p^r, which follows from ([dS87], II, corollary 1.7), and any $g\in G(K_{k+r,n+r}/K_{k+r,n})$ fixes $K_{k+r,0}$. Then, (2.4.11) shows that for $k,n\geq 1$ we have

$$\begin{aligned}N_{K_{k+r,n+r}/K_{k,n}}(d_{k+r,n+r})&=\Big(N_{K_{k+r,n+r}/K_{k,n}}\circ N_{K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r})/(K_{k+r,0}\cap K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r}))}\ \Theta(\tau;\mathfrak{a})\Big)^{\sigma-1}\\&=\Big(N_{K_{k+r,n}/K_{k,n}}\circ N_{K_{k+r,n+r}/K_{k+r,n}}\circ N_{K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r})/(K_{k+r,0}\cap K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r}))}\ \Theta(\tau;\mathfrak{a})\Big)^{\sigma-1}\\&=\Big(N_{K_{k+r,n}/K_{k,n}}\circ N_{K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r})/(K_{k+r,0}\cap K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r}))}\ \Theta(\tau;\mathfrak{a})\Big)^{p^r(\sigma-1)}.\end{aligned}$$

By a similar argument for $\mathfrak{m}=\mathfrak{f}'\mathfrak{p}^{n+r}$, for $k,n\geq 1$, we have

$$N_{K_{k+r,n+r}/K_{k,n}}(d_{k+r,n+r})=\Big(N_{K_{k,n+r}/K_{k,n}}\circ N_{K(\mathfrak{f}'\mathfrak{p}^{n+r})/(K_{0,n+r}\cap K(\mathfrak{f}'\mathfrak{p}^{n+r})}\ \Theta(\tau;\mathfrak{a})\Big)^{p^r(\sigma-1)}.$$

which follows from (2.4.12). These two cases imply that for any element d of $D_{K_{k+r,n+r}}$ we have

$$N_{K_{k+r,n+r}/K_{k,n}}(d)=c^{p^r} \tag{2.4.13}$$

for some unit c in $\mathcal{O}^\times_{K_{k,n}}$.

Now, let $(a_{k,n})_{k,n}$ be an element of $\varprojlim_{k,n} D_{K_{k,n}}\otimes_{\mathbb{Z}}\mathbb{Z}_p$. Let $k,n\geq 1$ be big enough so that they satisfy the conditions of lemma 2.4.8, i.e., such that both $\mathcal{O}_K^\times\longrightarrow\mathcal{O}_K/\bar{\mathfrak{p}}^k$ and $\mathcal{O}_K^\times\longrightarrow\mathcal{O}_K/\mathfrak{p}^n$ are injective.

For any $r\geq 1$ the element $a_{k+r,n+r}\in D_{K_{k+r,n+r}}\otimes_{\mathbb{Z}}\mathbb{Z}_p$ is of the form

$$a_{k+r,n+r}=\sum_{i=1}^m d_i\otimes b_i$$

for some $d_i\in D_{K_{k+r,n+r}}$ and $b_i\in\mathbb{Z}_p$, $i=1,\dots,m$. Using (2.4.13) we see that we can find $c_1,\dots,c_m$ in $\mathcal{O}^\times_{K_{k,n}}$ such that

$$\begin{aligned}a_{k,n}&=\big(N_{K_{k+r,n+r}/K_{k,n}}\otimes\mathrm{id}_{\mathbb{Z}_p}\big)(a_{k+r,n+r})\\&=\sum_{i=1}^m c_i^{p^r}\otimes b_i\\&=\Big(\sum_{i=1}^m c_i\otimes b_i\Big)p^r,\end{aligned}$$

and we see that as an element of $\mathcal{O}_{K_{k,n}}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$, $a_{k,n}$ is divisible by an arbitrarily large (we can choose any $r \geq 1$) power of p. By the remark made at the beginning of the proof, we see that only the trivial element satisfies this divisibility property. □

According to the definition we gave, elliptic units of an abelian extension F of K contain the roots of unity of F. Eventually, we will be interested in projective limits of elliptic units and need the following vanishing result for p-power roots of unity for $\mathbb{Z}_p^2$-extensions of K.

Lemma 2.4.12. *Let L be a number field and M/L an extension containing a $\mathbb{Z}_p$-extension L_∞/L that is independent of the cyclotomic $\mathbb{Z}_p$-extension L_{cyc}/L of L. Then, we have*

$$\varprojlim_{L \subseteq_f L' \subset M} \mu_{p^\infty}(L') = 1,$$

where $\mu_{p^\infty}(L')$ denotes the group of p-power roots of unity in L' and the limit ranges through the finite extensions L' of L contained in M and is taken with respect to norm maps.

Proof. Let $(\zeta_{L'})_{L'}$ be an element of $\varprojlim_{L \subseteq_f L' \subset M} \mu_{p^\infty}(L')$. Let us show that $\zeta_{L'} = 1$ for any finite extension L'. For any finite extension L' of L the composite $L'L_\infty$ contains only finitely many p-power roots of unity since L_∞/L is independent of the cyclotomic $\mathbb{Z}_p$-extension L_{cyc}/L. In fact, assume the contrary. Then, $L'L_\infty/L$ contains $L(\mu_{p^\infty})$ and therefore the $\mathbb{Z}_p^2$-extension $L_{cyc}L_\infty/L$, which is impossible since $L'L_\infty/L$ is a finite extension $L'L_\infty/L_\infty$ of the $\mathbb{Z}_p$-extension L_∞/L.

Let ζ_{p^n} be a primitive p^n-th root of unity belonging to $L'L_\infty$ such that n is maximal with respect to this property. Write L'_m for the m-th layer of the $\mathbb{Z}_p$-extension $L'L_\infty/L'$ (note that $G(L'L_\infty/L')$ embedds into $G(L_\infty/L) \cong \mathbb{Z}_p$ and the image is the continuous image of a compact set in a Hausdorff space and therefore closed in $G(L_\infty/L)$, hence the image is of the form $p^n\mathbb{Z}_p \subset \mathbb{Z}_p$ and it follows that $G(L'L_\infty/L')$ is a $\mathbb{Z}_p$-extension). Then $G(L'_m/L')$ has order p^m. Let k be large enough so that ζ_{p^n} belongs to L'_k (such k exists since $L'L_\infty = \bigcup_m L'_m$). Then, we have

$$\zeta_{L'} = N_{L'_{k+n}/L'}(\zeta_{L'_{k+n}}) = N_{L'_k/L'}\big(N_{L'_{k+n}/L'_k}(\zeta_{L'_{k+n}})\big) = N_{L'_k/L'}(\zeta_{L'_{k+n}}^{p^n}) = N_{L'_k/L'}(1) = 1,$$

since $\zeta_{L'_{k+n}} \in \mu_{p^\infty}(L'L_\infty) = \mu_{p^n} \subset L'_k$. □

Let us now recall that Rubin's elliptic units for an abelian finite extension F of K were defined by $\mathcal{C}(F) = \mu_\infty(F)C_F$, where $\mu_\infty(F)$ is the group of all roots of unity in F. Tensoring with $\mathbb{Z}_p$ kills the roots of unity of order prime to p, so that as subgroups of $\mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$ (note that $\mathbb{Z}_p$ is flat as a $\mathbb{Z}$-module) we have an equality

$$\mathcal{C}(F) \otimes_{\mathbb{Z}} \mathbb{Z}_p = \big(\mu_{p^\infty}(F)C_F\big) \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$

where $\mu_{p^\infty}(F)$ is the group of p-power roots of unity in F. For the fields $K_{k,n} = K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$ from lemma 2.4.8 let us consider the inclusions

$$\iota_{k,n} : C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \big(\mu_{p^\infty}(K_{k,n})C_{K_{k,n}}\big) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Certainly, we have surjections

$$\mu_{p^\infty}(K_{k,n}) \cong \mu_{p^\infty}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \twoheadrightarrow \operatorname{coker}(\iota_{k,n}).$$

Passing to the projective limit, lemma 2.4.12 shows that $\varprojlim_{k,n} \operatorname{coker}(\iota_{k,n}) = 0$ (to be able to apply the lemma note that K_∞/K contains the cyclotomic and the anti-cyclotomic $\mathbb{Z}_p$-extension), so that

$$\varprojlim_{k,n}(C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p).$$

Together with (2.4.10) this proves the following corollary.

Corollary 2.4.13. *The natural inclusions induce an equality*

$$\varprojlim_{k,n}(C'_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \varprojlim_{k,n}(C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p).$$

Let us prove one more technical lemma that shows that multiplication with the augmentation ideal commutes with passing to the limit. We will write

$$F_{k,n} = K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$$

for the ray class field of K modulo $\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$. Recall the definition of $\Theta_{\mathfrak{m}}$ from (2.4.7) and remark 2.4.6.

Lemma 2.4.14. *Let p be a prime number, $(p,6) = 1$, that splits in K into distinct primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. Then, as subgroups of $\varprojlim_{n,k}(\mathcal{O}^\times_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ we have the identity*

$$I \varprojlim_{k,n}\big((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\big) \;=\; \varprojlim_{n,k}\Big(\big(I(K_{k,n}/K)N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}\big) \otimes_{\mathbb{Z}} \mathbb{Z}_p\Big), \tag{2.4.14}$$

where we write I for the augmentation ideal $I(K_\infty/K)$, $K_\infty = \cup_{n,k}K(E[\mathfrak{p}^n\bar{\mathfrak{p}}^k])$.

Proof. Let us write I_∞ for the augmentation ideal $I(F_\infty/K)$, $F_\infty = \cup_{n,k}K(\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k)$. For $n', k' \geq 1$ let us consider the projection maps

$$I_\infty \varprojlim_{n,k}(\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \twoheadrightarrow \big(I(F_{k',n'}/K)\Theta_{\mathfrak{f}\mathfrak{p}^{n'}\bar{\mathfrak{p}}^{k'}}\big) \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$

which are surjective since the norm maps on the groups $\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}$ are surjective, see ([dS87], II, 2.3 and proof of Proposition 2.4 (iii)). Considering $\big(I_\infty \varprojlim_{n,k}(\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k} \otimes_{\mathbb{Z}} \mathbb{Z}_p)\big)_{n',k'}$ as a projective system with respect to n', k' and identity maps, we can pass to the projective limit with respect to n', k' and get the identity

$$I_\infty \varprojlim_{n,k}(\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \varprojlim_{n',k'}\big((I(F_{k',n'}/K)\Theta_{\mathfrak{f}\mathfrak{p}^{n'}\bar{\mathfrak{p}}^{k'}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\big)$$

as subgroups of $\varprojlim_{n,k}(\mathcal{O}^\times_{K(\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k)} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$, compare lemma 2.4.3. This equality fits into the commutative diagram

$$\begin{array}{ccc} I_\infty \varprojlim_{n,k}(\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k} \otimes_{\mathbb{Z}} \mathbb{Z}_p) & = & \varprojlim_{n',k'}\big((I(F_{k',n'}/K)\Theta_{\mathfrak{f}\mathfrak{p}^{n'}\bar{\mathfrak{p}}^{k'}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\big) \\ \downarrow & & \downarrow \\ I \varprojlim_{n,k}\big((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\big) & \hookrightarrow & \varprojlim_{n',k'}\Big(\big(I(K_{n',k'}/K)N_{F_{k',n'}/K_{k',n'}}\Theta_{\mathfrak{f}\mathfrak{p}^{n'}\bar{\mathfrak{p}}^{k'}}\big) \otimes_{\mathbb{Z}} \mathbb{Z}_p\Big), \end{array}$$

where the vertical maps are given by the norm maps and from which we conclude that the lower horizontal map defines an equality. □

We remark that for $k, n \geq 1$ the group $I(K_{k,n}/K)N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}$ is precisely the subgroup of $C'_{K_{k,n}}$ generated by elements of the form

$$\big(N_{K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\ \Theta(\tau;\mathfrak{a})\big)^{\sigma-1},$$

where σ ranges through $\mathrm{Gal}(K_{k,n}/K)$, $\mathfrak{a}$ runs through integral ideals such that $(\mathfrak{a}, 6\mathfrak{f}p) = 1$ and τ through primitive $\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$-division points.

Definition 2.4.15. *For $k, n \geq 1$, we define $C''_{K_{k,n}}$ to be the subgroup $I(K_{k,n}/K)N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}$ of $C'_{K_{k,n}}$, which was defined in definition 2.4.9.*

With this notation the previous lemma says

$$I \varprojlim_{k,n}\big((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\big) = \varprojlim_{n,k}(C''_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$$

and by corollary 2.4.13 these modules are submodules of $\varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$. We now come to the main result of this section, which uses most of the results proven so far in this section and ([Rub99], corollary 7.7). In order to state it we need one more definition. For any prime ideal $\mathfrak{l}$ dividing $\mathfrak{f}$ we define a Galois automorphism $\sigma_{\mathfrak{l}}$ in $G(K_\infty/K)$ as follows. Write $n_{\mathfrak{l}}$ for the exact exponent of $\mathfrak{l}$ in $\mathfrak{f}$. Then, we can consider the arithmetic Frobenius

$$\Big(\mathfrak{l}, K\big(p^\infty \frac{\mathfrak{f}}{\mathfrak{l}^{n_{\mathfrak{l}}}}\big)/K\Big)$$

at $\mathfrak{l}$ in $G(K\big(p^\infty \frac{\mathfrak{f}}{\mathfrak{l}^{n_{\mathfrak{l}}}}\big)/K)$, take a lift of it to $G(K(p^\infty\mathfrak{f})/K)$ and write $\sigma_{\mathfrak{l}}$ for the restriction to $G(K_\infty/K)$.

Theorem 2.4.16. *Fix any prime ideal $\mathfrak{c}$ of $\mathcal{O}_K$, such that $(\mathfrak{c}, 6p\mathfrak{f}) = 1$. The quotient of the two modules*

$$I \varprojlim_{k,n}\big((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\big) \subset \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$$

is annihilated by the element

$$(\sigma_{\mathfrak{c}} - N\mathfrak{c}) \cdot \prod_{\mathfrak{l}\mid\mathfrak{f}} (1 - \sigma_{\mathfrak{l}}^{-1}),$$

where $\sigma_{\mathfrak{c}} = (\mathfrak{c}, K_\infty/K)$ *and the product is taken over the primes dividing the conductor* $\mathfrak{f}$*. In particular, the quotient is* S*-torsion.*

Proof. For the last statement about the quotient being S-torsion, just recall from lemmata A.9.2 and A.9.5 that choosing $\mathfrak{c}$ to be equal to a prime $\mathfrak{q}$ such that $N(\mathfrak{q})$ is congruent to 1 modulo p, the element $(\sigma_{\mathfrak{c}} - N\mathfrak{c}) \cdot \prod_{\mathfrak{l}\mid\mathfrak{f}}(1 - \sigma_{\mathfrak{l}}^{-1})$ belongs to S. Let us now prove the theorem.

By corollary 2.4.13 and lemma 2.4.14 the statement of this theorem is equivalent to proving that the quotient of

$$\varprojlim_{n,k} (C''_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \ \subset\ \varprojlim_{k,n} (C'_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$$

is annihilated by $(\sigma_{\mathfrak{c}} - N\mathfrak{c}) \cdot \prod_{\mathfrak{l}\mid\mathfrak{f}}(1 - \sigma_{\mathfrak{l}}^{-1})$. This quotient is isomorphic to

$$\varprojlim_{n,k} \big((C'_{K_{k,n}}/C''_{K_{k,n}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \big)$$

and it is clearly sufficient to show that for all $k, n \geq 1$ as in lemma 2.4.8 (i.e. such that both $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\bar{\mathfrak{p}}^k$ and $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\mathfrak{p}^n$ are injective)

$$\big(C'_{K_{k,n}}/C''_{K_{k,n}}\big) \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

is annihilated by $(\sigma_{\mathfrak{c}} - N\mathfrak{c}) \cdot \prod_{\mathfrak{l}\mid\mathfrak{f}}(1 - \sigma_{\mathfrak{l}}^{-1})$. Take an arbitrary generator of $C'_{K_{k,n}}$, which is of the form

$$\big(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\ \Theta(\tau; \mathfrak{a})\big)^{\sigma-1},$$

where σ belongs to $\mathrm{Gal}(K_{k,n}/K)$, $\mathfrak{f}'$ is some divisor of $\mathfrak{f}$, $\mathfrak{a}$ is an integral ideal such that $(\mathfrak{a}, 6\mathfrak{f}'p) = 1$ and τ is a primitive $\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n$-division point. We will show that this generator multiplied by $(\sigma_{\mathfrak{c}} - N\mathfrak{c}) \cdot \prod_{\mathfrak{l}\mid\mathfrak{f}}(1 - \sigma_{\mathfrak{l}}^{-1})$ belongs to $C''_{K_{k,n}}$.

Recall that we write

$$\mathfrak{f} = \prod_{\mathfrak{l}\mid\mathfrak{f}} \mathfrak{l}^{n_{\mathfrak{l}}},$$

where $n_{\mathfrak{l}} \geq 0$ is the exponent of the prime $\mathfrak{l}$ in the decomposition of $\mathfrak{f}$.

If $\mathfrak{l} \mid \mathfrak{f}'$, then we may assume that $\mathfrak{l}^{n_{\mathfrak{l}}} \mid \mathfrak{f}'$. This can be shown just as the third case in the proof of lemma 2.4.8. In fact, if l is an $\mathcal{O}_K$-generator of $\mathfrak{l}$ and $m_{\mathfrak{l}}$, $m_{\mathfrak{l}} < n_{\mathfrak{l}}$, the exact exponent of $\mathfrak{l}$ in $\mathfrak{f}'$, then, by ([Rub99], corollary 7.7), we have

$$N_{K(\mathfrak{l}^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)} \Theta\Big(\frac{\tau}{l^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}}; \mathfrak{a}\Big) = \Theta(\tau; \mathfrak{a})$$

which yields

$$\big(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\ \Theta(\tau; \mathfrak{a})\big)^{\sigma-1} = \big(N_{K(\mathfrak{l}^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/(K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)\cap K_{k,n})} \Theta\Big(\frac{\tau}{l^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}}; \mathfrak{a}\Big)\big)^{\sigma-1},$$

showing that our arbitrary generator is a product of Galois conjugates of

$$\left(N_{K(\mathfrak{l}^{n_\mathfrak{l}-m_\mathfrak{l}}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/(K(\mathfrak{l}^{n_\mathfrak{l}-m_\mathfrak{l}}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)\cap K_{k,n})}\Theta\left(\frac{\tau}{l^{n_\mathfrak{l}-m_\mathfrak{l}}};\mathfrak{a}\right)\right)^{\sigma-1}.$$

This shows that we may assume that the exponent of $\mathfrak{l}$ in $\mathfrak{f}$ is equal to $n_\mathfrak{l}$ whenever $\mathfrak{l}$ already divides $\mathfrak{f}$.

We now turn our attention to primes $\mathfrak{l}$ dividing $\mathfrak{f}$ but not dividing $\mathfrak{f}'$. It is now, that the element $(\sigma_\mathfrak{c} - N\mathfrak{c})\cdot\prod_{\mathfrak{l}|\mathfrak{f}}(1-\sigma_\mathfrak{l}^{-1})$ comes into play. The next observation will explain why we need the term $(\sigma_\mathfrak{c} - N\mathfrak{c})$. For our arbitrary generator

$$\left(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\ \Theta(\tau;\mathfrak{a})\right)^{\sigma-1}$$

of $C'_{K_{k,n}}$ we allow any $\mathfrak{a}$ prime to $6p\mathfrak{f}'$. In particular, $\mathfrak{l}$ might divide $\mathfrak{a}$. But we want to use ([Rub99], corollary 7.7) again, which we can only do for $\mathfrak{a}$ prime to $\mathfrak{l}$. Writing $\sigma_\mathfrak{c}$ also for the lift $(\mathfrak{c}, F_\infty/K)$ to $G(F_\infty/K)$, ([dS87], II, proposition 2.4) shows that

$$\begin{aligned}\Theta(\tau;\mathfrak{a})^{(\sigma_\mathfrak{c}-N\mathfrak{c})} &= \frac{\Theta(\tau;\mathfrak{ac})}{\Theta(\tau;\mathfrak{c})^{N\mathfrak{a}}\cdot\Theta(\tau;\mathfrak{a})^{N\mathfrak{c}}}\\ &= \Theta(\tau;\mathfrak{c})^{(\sigma_\mathfrak{a}-N\mathfrak{a})},\end{aligned}$$

so that

$$\left(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\ \Theta(\tau;\mathfrak{a})\right)^{(\sigma_\mathfrak{c}-N\mathfrak{c})(\sigma-1)} = \left(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\ \Theta(\tau;\mathfrak{c})\right)^{(\sigma_\mathfrak{a}-N\mathfrak{a})(\sigma-1)}.$$

We see that it is sufficient to show that

$$\left(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\ \Theta(\tau;\mathfrak{c})\right)^{(\sigma_\mathfrak{a}-N\mathfrak{a})(\sigma-1)\prod_{\mathfrak{l}|\mathfrak{f}}(1-\sigma_\mathfrak{l}^{-1})} \tag{2.4.15}$$

belongs to $C''_{K_{k,n}}$. Now, for a prime $\mathfrak{l}$ dividing $\mathfrak{f}$ but not dividing $\mathfrak{f}'$, ([Rub99], corollary 7.7) yields

$$N_{K(\mathfrak{l}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)}\ \Theta\left(\frac{\tau}{l};\mathfrak{c}\right) = \Theta(\tau;\mathfrak{c})^{(1-\sigma_\mathfrak{l}^{-1})},$$

where we write $\sigma_\mathfrak{l}$ also for the lift of $\left(\mathfrak{l}, K\left(p^\infty\frac{\mathfrak{f}}{\mathfrak{l}^{n_\mathfrak{l}}}\right)/K\right)$ to $G(K(p^\infty\mathfrak{f})/K)$ as in the definition of $\sigma_\mathfrak{l}$. Applying this to all the primes $\mathfrak{l}_1,\ldots,\mathfrak{l}_r$ dividing $\mathfrak{f}$ but not dividing $\mathfrak{f}'$ we see that the element from (2.4.15) is equal to

$$\left(N_{K(\mathfrak{l}_1\ldots\mathfrak{l}_r\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/(K_{k,n}\cap K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n))}\ \Theta\left(\frac{\tau}{l_1\ldots l_r};\mathfrak{c}\right)\right)^{(\sigma_\mathfrak{a}-N\mathfrak{a})(\sigma-1)\prod_{\mathfrak{l}|\mathfrak{f}'}(1-\sigma_\mathfrak{l}^{-1})}, \tag{2.4.16}$$

where we write l_i for generators of $\mathfrak{l}_i$. Now we can proceed as in the first step, when we showed that if $\mathfrak{l} \mid \mathfrak{f}'$, then we may assume that $\mathfrak{l}^{n_\mathfrak{l}} \mid \mathfrak{f}'$, showing that the element from (2.4.16) belongs to $C''_{K_{k,n}}$. □

2.4.4 The formal group $\hat{E}$ and Coleman's theorem in a semi-local framework

Let K be a quadratic imaginary number field of class number one and let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}_K$. Assume that E/K has good ordinary reduction above $p \in \mathbb{Z}$. We have noted before that this implies that p splits in K into distinct primes $\mathfrak{p} = (\pi)$ and $\bar{\mathfrak{p}} = (\bar{\pi})$. We write $\mathfrak{f} = \mathfrak{f}_\psi$ for the conductor of the Größencharacter ψ attached to E/K and L for the period lattice associated to a fixed global minimal Weierstraß equation for E (recall that K has class number 1). Moreover, we fix $\Omega \in L$ such that

$$\mathcal{O}_K \Omega = L.$$

Let us fix an embedding $\bar{\mathbb{Q}} \subset \mathbb{C}_p$, where $\mathbb{C}_p$ denotes the completion $\hat{\bar{\mathbb{Q}}}_p$ of an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$.

In this subsection we recall some work by de Shalit on the formal group $\hat{E}$ (corresponding to the fixed Weierstraß equation) and Coleman's theorem in a semi-local framework. We also prove some probably well-known results for which a reference could not be found. We will write

$$F_{k,n} := K(\mathfrak{m}_0 \bar{\mathfrak{p}}^k \mathfrak{p}^n), \quad (\mathfrak{m}_0, p) = 1,$$

for the ray class fields of K of modulus $\mathfrak{m}_0 \bar{\mathfrak{p}}^k \mathfrak{p}^n$. We are mostly interested in the case $\mathfrak{m}_0 = \mathfrak{f}$. This is because we want to study fields of the form

$$K_{k,n} := K(E[\bar{\pi}^k \pi^n]),$$

the conductors of which over K are precisely $\mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n$, which we now prove.

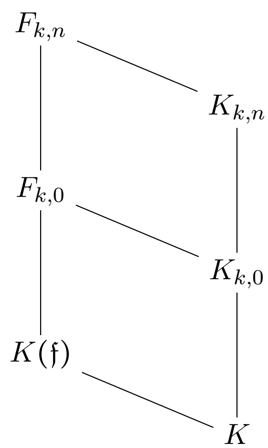
Lemma 2.4.17. *Whenever $k, n \geq 0$, $(k,n) \neq (0,0)$, the conductor of $K_{k,n} = K(E[\bar{\pi}^k \pi^n])$ is $\mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n$.*

Proof. This lemma has already been proved by Coates and Wiles for fields of the form $K_{k,0}$, $k \geq 1$, and $K_{0,n}$, $n \geq 1$, see ([CW77], lemma 4). For general $K_{k,n}$ we may therefore assume that both $k \geq 1$ and $n \geq 1$. Write $\mathfrak{g}$ for the conductor of $K_{k,n}$. The inclusion

$$K_{k,0} \subset K_{k,n} \subset K(\mathfrak{g})$$

and the result of Coates and Wiles (loc. sit.) shows that $\mathfrak{f}\bar{\mathfrak{p}}^k \mid \mathfrak{g}$. Similarly, one gets $\mathfrak{f}\mathfrak{p}^n \mid \mathfrak{g}$. It follows that $\mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n \mid \mathfrak{g}$. On the other hand, according to ([dS87], II, proposition 1.6) we have $K(E[\mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n]) = K(\mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n)$. Since $K_{k,n} \subset K(E[\mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n])$ we also see that $\mathfrak{g} \mid \mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n$. □

For $\mathfrak{m}_0 = \mathfrak{f}$ and $k \geq 1$, we have the following diagram



We have $F_{k,n} = K(E[\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n]) = K_{k,n}K(E[\mathfrak{f}])$, see, as before, ([dS87], II, proposition 1.6) for the first equality and note that for two integral ideals $\mathfrak{m}, \mathfrak{n}$ of $\mathcal{O}_K$ we have $K(E[\mathfrak{m}])K(E[\mathfrak{n}]) = K(E[l.c.m.(\mathfrak{m}, \mathfrak{n})])$, see proposition A.6.3. Moreover, for the conductor $\mathfrak{f}$ of E it holds that $K(E[\mathfrak{f}]) = K(\mathfrak{f})$, see (loc. cit.). It follows that

$$F_{k,n} = F_{k,0}K_{k,n}. \tag{2.4.17}$$

Moreover, we have

$$K_{k,n} \cap F_{k,0} = K_{k,0} \tag{2.4.18}$$

since every prime above $\mathfrak{p}$ is unramified in $F_{k,0}/K_{k,0}$ by definition and totally ramified in $K_{k,n}/K_{k,0}$, see ([dS87], II, proposition 1.9). We conclude from (2.4.17) and (2.4.18) that

$$G(F_{k,n}/K_{k,n}) \cong G(F_{k,0}/K_{k,0}) \tag{2.4.19}$$

for every $n \geq 1$. We define

$$F_{k,\infty} := \bigcup_{n\geq 1} F_{k,n} \quad \text{and} \quad F_\infty := \bigcup_{k\geq 1, n\geq 1} F_{k,n}$$

and likewise

$$K_{k,\infty} := \bigcup_{n\geq 1} K_{k,n} \quad \text{and} \quad K_\infty := \bigcup_{k\geq 1, n\geq 1} K_{k,n}.$$

Again, if $\mathfrak{m}_0$ is divisible by the conductor of E, F_∞/K_∞ is a finite extension. We define $\mathfrak{m}_k = \mathfrak{m}_0\bar{\mathfrak{p}}^k$ and from now on we fix some $k \geq 1$ such that $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\bar{\mathfrak{p}}^k$ is injective. Note that $\mathfrak{p}$ is unramified in $K_{k,0}/K$, see ([dS87], II, Proposition 1.9). We define the following semi-local objects

$$K_{k,n,\mathfrak{p}} := K_{k,n} \otimes_K K_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} K_{k,n,\mathfrak{P}} \quad \text{and} \quad \mathcal{O}_{k,n,\mathfrak{p}} := \mathcal{O}_{K_{k,n}} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{p}} \cong \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{K_{k,n,\mathfrak{P}}},$$

where, in the products, the primes $\mathfrak{P}$ range through the primes of $K_{k,n}$ above $\mathfrak{p}$. We will write

$$G_k = G(K_{k,\infty}/K)$$

Moreover, we will write

$$U_{k,n} = \mathcal{O}^1_{k,n,\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}^1_{K_{k,n,\mathfrak{P}}} \cong \prod_{\mathfrak{P}|\mathfrak{p}} \hat{\mathcal{O}}^\times_{K_{k,n,\mathfrak{P}}}$$

for the subgroup of principal units in the group of semi-local units $\mathcal{O}^\times_{k,n,\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}^\times_{K_{k,n,\mathfrak{P}}}$.

Remark 2.4.18. (i) As de Shalit, for every prime ideal $\mathfrak{P}$ of $K_{k,0}$ above $\mathfrak{p}$ we consider $\hat{E}$ as a Lubin-Tate formal group of height one (recall our splitting assumption) relative to the unramified extension $K_{k,0,\mathfrak{P}}/K_\mathfrak{p}$. At times, we will also consider $\hat{E}$ as a formal group with coefficients in $\mathcal{O}_{K_{k,0}} \otimes \mathcal{O}_{K_\mathfrak{p}} \cong \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{K_{k,0,\mathfrak{P}}}$. For an excellent survey on commutative one dimensional formal groups see ([dS87], section I.1).

(ii) Note that de Shalit, see (loc. cit., p. 64), starts with an integral ideal $\mathfrak{f}$ and then fixes a Größencharacter dividing this ideal. He then considers the ray class fields $K(\mathfrak{f}\mathfrak{p}^n)$ which coincide with the extensions generated by $\mathfrak{f}\mathfrak{p}^n$-division points of an elliptic curve associated to the chosen Größencharacter. In contrast, we start with a fixed elliptic curve E and are interested in extensions induced by division points the orders of which are prime to the conductor of E. These fields are, in general, smaller than the ray class fields for moduli divisible by the conductor. Coleman's machinery applies to a norm-coherent system of units in a tower of fields obtained by division points of $\hat{E}$. As mentioned above, in de Shalit's setting these coincide with the ray class fields, so the reader should not be confused that de Shalit does but we do not work over the ray class fields.

(iii) Moreover, note that de Shalit fixes, see (loc. cit., p. 64), for every ideal of the form $\mathfrak{f}\bar{\mathfrak{p}}^k$ a Größencharacter $\psi_{\mathfrak{f}\bar{\mathfrak{p}}^k}$ of type $(1,0)$ over K and with conductor dividing $\mathfrak{f}\bar{\mathfrak{p}}^k$ and an elltipic curve $E_{\mathfrak{f}\bar{\mathfrak{p}}^k}$ over $K(\mathfrak{f}\bar{\mathfrak{p}}^k)$ for which $\psi_{E_{\mathfrak{f}\bar{\mathfrak{p}}^k}}/K(\mathfrak{f}\bar{\mathfrak{p}}^k)$ is equal to $\psi_{E_{\mathfrak{f}\bar{\mathfrak{p}}^k}} = \psi_{\mathfrak{f}\bar{\mathfrak{p}}^k} \circ N_{K(\mathfrak{f}\bar{\mathfrak{p}}^k)/K}$. If, as we do, one starts with an elliptic curve E/K with CM, denote by ψ the Größencharacter of type $(1,0)$ over K attached to E/K and write $\mathfrak{f}$ for its conductor. Then, for every ideal $\mathfrak{f}\bar{\mathfrak{p}}^k$ one can simply consider E as an elliptic curve defined over $K(\mathfrak{f}\bar{\mathfrak{p}}^k)$ and take E as $E_{\mathfrak{f}\bar{\mathfrak{p}}^k}$ and ψ as $\psi_{\mathfrak{f}\bar{\mathfrak{p}}^k}$. This is possible, since the Größencharacter attached to $E/K(\mathfrak{f}\bar{\mathfrak{p}}^k)$ is given by

$$\psi \circ N_{K(\mathfrak{f}\bar{\mathfrak{p}}^k)/K},$$

see Perrin Riou's article ([PR84], II, §1.2, p.26).

Next, we want to introduce p-adic periods. Let us define the fields in which they live. We note that $K_{\infty,0} = K(E[\bar{\mathfrak{p}}^\infty])$ is an extension of K in which $\mathfrak{p}$ is unramified and finitely decomposed, see ([dS87], II Proposition 1.9). Hence, $K_{\infty,0,\mathfrak{p}} := K_{\infty,0} \otimes_K K_\mathfrak{p}$ is a finite product of fields each unramified over $K_\mathfrak{p}$. Likewise, we write $\mathcal{O}_{K_{\infty,0,\mathfrak{p}}} := \mathcal{O}_{K_{\infty,0}} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{p}}$, only to define

$$\hat{D} = \hat{\mathcal{O}}_{K_{\infty,0,\mathfrak{p}}}$$

to be the completion of $\mathcal{O}_{K_{\infty,0,\mathfrak{p}}}$. We now quote proposition 4.3 from chapter II of [dS87].

Proposition 2.4.19. *There is an isomorphism of formal groups defined over the ring $\hat{D}$,*

$$\theta : \hat{\mathbb{G}}_m \cong \hat{E},$$

given by

$$\theta(X) = \Omega_p X + \text{ terms of degree } \geq 2 \quad \in \hat{D}[[X]],$$

with $\Omega_p \in \hat{D}^\times$.

We write $\phi = \sigma_{\mathfrak{p}}$ for the arithmetic Frobenius at $\mathfrak{p}$ in $G(K_{\infty,0}/K)$ and note that $G(K_{\infty,0}/K)$ acts on $K_{\infty,0} \otimes_K K_{\mathfrak{p}}$ via the action on the first factor and that, by continuity, this action extends to the completion.

Definition 2.4.20. *Let us fix a generator $(\zeta_n)_n$ of $\varprojlim_n \mu_{p^n}(\bar{K})$, i.e., a compatible system of primitive p-power roots of unity.*

Moreover, we have remarked above that $\mathfrak{p}$ is finitely decomposed in $K_{\infty,0}/K$. It follows that there exists a smallest $k_0 \geq 1$ such that the number of primes in $K_{k_0,0}$ above $\mathfrak{p}$ is the same as the number of primes in $K_{\infty,0}$ above $\mathfrak{p}$.

We will write

$$\omega_n = \theta^{\phi^{-n}}(\zeta_n - 1).$$

Also, from now on we fix some $k \geq k_0$. The semi-local version of Coleman's theorem, see ([dS87], II, Proposition 4.5), says that for every

$$u = (u_n)_n \in U_{k,\infty} := \varprojlim_n U_{k,n}$$

there exists a unique power series $g_u(T) \in \mathcal{O}_{k,0,\mathfrak{p}}[[T]]^\times$ such that

$$u_n = (\phi^{-n} g_u)(\omega_n).$$

Moreover, see ([dS87], I, section 3.4 and II, Proposition 4.6), there is a unique G_k-homomorphism

$$i_k : U_{k,\infty} \longrightarrow \Lambda(G_k, \hat{D}), \quad i_k(u) = \lambda_u \tag{2.4.20}$$

such that

$$\widetilde{\log(g_u)} \circ \theta(X) = \int_{G_{k,0}} (1 + X)^{\kappa(\sigma)} d\lambda_u(\sigma), \tag{2.4.21}$$

where $G_{k,0} = \mathrm{Gal}(K_{k,\infty}/K_{k,0})$, κ denotes the $\mathbb{Z}_p^\times$-valued character defined by the action of $G_{k,0}$ on $E[\mathfrak{p}^\infty]$ and

$$\widetilde{\log g}(T) = \log g(T) - \frac{1}{p} \sum_{\omega \in \hat{E}[\mathfrak{p}]} \log g(T[+]\omega),$$

where, in turn, $\hat{E}[\mathfrak{p}]$ denotes the set of division points of level 1 in $\hat{E}$ and $[+]$ is addition induced by the formal group. The division points in $\hat{E}$ are, by definition, a subset of the valuation ideal of $\mathbb{C}_p$, see ([dS87], I.1.7).

Remark 2.4.21. We want to explain how the measure λ_u from equation (2.4.21) is obtained in the semi-local framework. First note that every prime $\mathfrak{P}'$ of $K_{k,0}$ above $\mathfrak{p}$ is totally ramified in $K_{k,\infty}/K_{k,0}$ so that for every $n \geq 1$ there is a unique prime in $K_{k,n}$ above $\mathfrak{P}'$, which we will also denote by $\mathfrak{P}'$. With this notation we then have $G_{k,0} \cong G(K_{k,\infty,\mathfrak{P}'}/K_{k,0,\mathfrak{P}'})$. Also note that $U_{k,\infty}$ admits a decomposition $\prod_{\mathfrak{P}} U_{k,\infty,\mathfrak{P}} \cong U_{k,\infty}$ into $\mathfrak{P}$-parts $U_{k,\infty,\mathfrak{P}} := \varprojlim_n \mathcal{O}^1_{K_{k,n,\mathfrak{P}}}$ for primes $\mathfrak{P}$ in $K_{k,0}$ above $\mathfrak{p}$. Now let $(u_{\mathfrak{P}})_{\mathfrak{P}}$ be an arbitrary element in $\prod_{\mathfrak{P}} U_{k,\infty,\mathfrak{P}}$. For every prime $\mathfrak{P}'$ of $K_{k,0}$ above $\mathfrak{p}$ the local theory, see ([dS87], I, Definition 3.4), gives us a map

$$i_{k,\mathfrak{P}'} : U_{k,\infty,\mathfrak{P}'} \longrightarrow \Lambda(G(K_{k,\infty,\mathfrak{P}'}/K_{k,0,\mathfrak{P}'}), \hat{\mathbb{Z}}_p^{ur}) \tag{2.4.22}$$

so that for $u_{\mathfrak{P}'}$ we get a $\hat{\mathbb{Z}}_p^{ur}$-valued measure

$$i_{k,\mathfrak{P}'}(u_{\mathfrak{P}'}) = \lambda_{u_{\mathfrak{P}'}}$$

on $G(K_{k,\infty,\mathfrak{P}'}/K_{k,0,\mathfrak{P}'})$. By the method explained on page 20 in [dS87], every such $\lambda_{u_{\mathfrak{P}'}}$ can be extended to $G_{k,\mathfrak{p}} = G(K_{k,\infty,\mathfrak{P}'}/K_{\mathfrak{p}})$, the decomposition group of $\mathfrak{p}$ in G_k which is independent of $\mathfrak{P}'$, so that, putting together the local maps for all $\mathfrak{P}$, we get a $G_{k,\mathfrak{p}}$-linear map

$$U_{k,\infty} \cong \prod_{\mathfrak{P}} U_{k,\infty,\mathfrak{P}} \longrightarrow \Lambda(G_{k,\mathfrak{p}}, \prod_{\mathfrak{P}|\mathfrak{p}} \hat{\mathbb{Z}}_p^{ur}), \quad (u_{\mathfrak{P}})_{\mathfrak{P}} \longmapsto \Big(H \mapsto (\lambda_{u_{\mathfrak{P}'}}(H))_{\mathfrak{P}'} \Big),$$

where H denotes any compact open subset of $G_{k,\mathfrak{p}}$. Now, the map (2.4.20) is obtained by the universal property of $\mathrm{Coind}_{G_k}^{G_{k,\mathfrak{p}}}$.

The map (2.4.20) takes values in $\hat{D}$-valued measures on G_k. However, eventually, as de Shalit remarks, we want to integrate $\mathbb{C}_p$-valued characters of G_k, which are in general not $\hat{K}_{\infty,0,\mathfrak{p}}$-valued. Our fixed embedding $\bar{\mathbb{Q}} \subset \mathbb{C}_p$, which determines a prime $\bar{\mathfrak{P}}$ of $\bar{\mathbb{Q}}$ above $\mathfrak{p}$, induces a map

$$\hat{K}_{\infty,0,\mathfrak{p}} = (K_{\infty,0} \otimes_K K_{\mathfrak{p}})\widehat{\ } \longrightarrow \mathbb{C}_p \tag{2.4.23}$$

that sends the component of $(K_{\infty,0} \otimes_K K_{\mathfrak{p}})\widehat{\ }$ corresponding to the prime of $K_{\infty,0}$ below $\bar{\mathfrak{P}}$ isomorphically to a subfield of $\mathbb{C}_p$ and the other components to 0. As de Shalit, we will write λ^0 for the image of λ under the map $\Lambda(G_k, \hat{K}_{\infty,0,\mathfrak{p}}) \to \Lambda(G_k, \mathbb{C}_p)$ induced by (2.4.23). We also note that the restriction of (2.4.23) to $\hat{D}$ takes values in $\hat{\mathbb{Z}}_p^{ur}$ since $\mathfrak{p}$ is unramified in $K_{\infty,0}/K$. Therefore, since for $u \in U_{k,\infty}$, $i_k(u) = \lambda_u$ belongs to $\Lambda(G_k, \hat{D})$, we can interpret λ_u^0 as an element of $\Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})$.

Definition 2.4.22. *We define*

$$\mathbb{L}_k : U_{k,\infty} \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur} \longrightarrow \Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})$$

as the map induced by the composition of i_k with the map $\Lambda(G_k, \hat{D}) \to \Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})$ induced by (2.4.23), so that $\mathbb{L}_k(u) = \lambda_u^0$.

Remark 2.4.23. We have explained in remark 2.4.21 how the map (2.4.20) is constructed. We obtained a $\prod_{\mathfrak{P}'|\mathfrak{p}} \hat{\mathbb{Z}}_p^{ur}$-valued measure on G_k and then, in order to define $\mathbb{L}_k$ we projected to the $\hat{\mathbb{Z}}_p^{ur}$-factor corresponding to the prime of $K_{\infty,0}$ below $\bar{\mathfrak{P}}$, the prime of $\bar{\mathbb{Q}}$ corresponding to our fixed embedding $\bar{\mathbb{Q}} \subset \mathbb{C}_p$. Let us write $\mathfrak{P}$ for the prime of $K_{k,0}$ below $\bar{\mathfrak{P}}$. We now want to remark that using the isomorphisms

$$\mathrm{Coind}_{G_k}^{G_{k,\mathfrak{p}}} \Lambda(G_{k,\mathfrak{p}}, \prod_{\mathfrak{P}'|\mathfrak{p}} \hat{\mathbb{Z}}_p^{ur}) \cong \mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}} \Lambda(G_{k,\mathfrak{p}}, \prod_{\mathfrak{P}'|\mathfrak{p}} \hat{\mathbb{Z}}_p^{ur}) \cong \Lambda(G_k, \prod_{\mathfrak{P}'|\mathfrak{p}} \hat{\mathbb{Z}}_p^{ur})$$

($G_{k,\mathfrak{p}}$ is of finite index in G_k) and

$$\mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}} U_{k,\infty,\mathfrak{P}} \cong \prod_{\mathfrak{P}'} U_{k,\infty,\mathfrak{P}'} \cong U_{k,\infty}$$

it is a tedious, yet straighforward exercise to show that $\mathbb{L}_k$ is the same map as the one obtained from applying $\mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}}$ to the map

$$i_{k,\mathfrak{P}} : U_{k,\infty,\mathfrak{P}} \longrightarrow \Lambda(G_{k,\mathfrak{p}}, \hat{\mathbb{Z}}_p^{ur}), \quad u \longmapsto \Big(H \mapsto \lambda_u(H)\Big)$$

from (2.4.22) (recall that the measures there can be extended to $G_{k,\mathfrak{p}}$) for the prime $\mathfrak{P}$.

Next we want to study the images of $\varprojlim_k U_{k,\infty}$ and of elliptic units under the map $\varprojlim_k \mathbb{L}_k$ (such a limit map exists as we show later). We defined the semi-local principal units $U_{k,n}$ for $K_{k,n}$. Let us define the elliptic units we are particularly interested in.

Definition 2.4.24. *Assume that p is prime to 6 and set $\mathfrak{m}_0 = \mathfrak{f}$, where $\mathfrak{f} = \mathfrak{f}_E = (f)$ is the conductor of E. For $k, n \geq 1$ and an integral ideal $\mathfrak{a}$, $(\mathfrak{a}, \mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p}) = 1$, define*

$$e'_{k,n}(\mathfrak{a}) := \Theta\Big(\frac{\Omega}{f\bar{\pi}^k\pi^n}, L, \mathfrak{a}\Big) \in \mathcal{O}^{\times}_{F_{k,n}},$$

which defines a norm-compatible system $e'(\mathfrak{a}) = (e'_{k,n}(\mathfrak{a}))_{k,n} \in \varprojlim_{k,n} \mathcal{O}^{\times}_{F_{k,n}}$ of global units. The fact that the $e'_{k,n}(\mathfrak{a})$ are norm-compatible follows from the distribution relation satisfied by Θ, compare ([dS87], II, 2.3 and proof of Proposition 2.4 (iii)). Ultimately, we are interested in elliptic units of the fields $K_{k,n}$ and therefore define

$$e_{k,n}(\mathfrak{a}) := N_{F_{k,n}/K_{k,n}}(e'_{k,n}(\mathfrak{a})) \in \mathcal{O}^{\times}_{K_{k,n}},$$

which, again, gives a norm-compatible system $e(\mathfrak{a}) = (e_{k,n}(\mathfrak{a}))_{k,n} \in \varprojlim_{k,n} \mathcal{O}^{\times}_{K_{k,n}}$ of global units. For fixed $k \geq 1$, the norm-compatible system $e(\mathfrak{a})$ maps to a norm-compatible system $e_k(\mathfrak{a}) = (e_{k,n}(\mathfrak{a}))_n$,

$$\varprojlim_{k',n'} \mathcal{O}^{\times}_{k',n'} \longrightarrow \varprojlim_{n} \mathcal{O}^{\times}_{k,n}, \quad e(\mathfrak{a}) \longmapsto e_k(\mathfrak{a}).$$

Let us now think of $\varprojlim_n \mathcal{O}_{k,n}^\times$ *as embedded into the semi-local units* $\varprojlim_n \mathcal{O}_{k,n,\mathfrak{p}}^\times$ *(recall* $\mathcal{O}_{k,n,\mathfrak{p}} \cong \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{K_{k,n,\mathfrak{P}}}$*) and write* $u_k(\mathfrak{a})$ *for the projection of* $e_k(\mathfrak{a})$ *to the pro-p part* $U_{k,\infty}$ *of* $\varprojlim_n \mathcal{O}_{k,n,\mathfrak{p}}^\times$*, in symbols,*

$$\varprojlim_n \mathcal{O}_{k,n,\mathfrak{p}}^\times \longrightarrow U_{k,\infty}, \quad e_k(\mathfrak{a}) \longmapsto u_k(\mathfrak{a}).$$

Likewise we write $u(\mathfrak{a})$ *for the projection of* $e(\mathfrak{a})$ *to the pro-p part* $\mathcal{U}_\infty = \varprojlim_{k,n} U_{k,n}$ *of* $\varprojlim_{k,n} \mathcal{O}_{k,n,\mathfrak{p}}^\times$*. We define*

$$\lambda_{k,\mathfrak{a}} := \lambda^0_{u_k(\mathfrak{a})} = \mathbb{L}_k(u_k(\mathfrak{a})),$$

as the p-adic integral measure on G_k *corresponding to* $u_k(\mathfrak{a})$*. We also define*

$$\lambda_k := \frac{1}{12} \cdot \frac{\lambda_{k,\mathfrak{a}}}{x_{k,\mathfrak{a}}} \quad \in \; Q(\Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})),$$

where $x_{k,\mathfrak{a}} := \sigma_{k,\mathfrak{a}} - N\mathfrak{a}$*,* $\sigma_{k,\mathfrak{a}} = (\mathfrak{a}, K_{k,\infty}/K) \in G_k$*. It can be shown that* λ_k *is independent of* $\mathfrak{a}$ *and actually an integral measure, see ([dS87], II proof of Theorem 4.12), so that* $\lambda_k \in \Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})$*. Lastly, using the fact that for* $k' \geq k \geq 1$*,* $\lambda_{k'}$ *maps to* λ_k *under the canonical projection* $\Lambda(G_{k'}, \hat{\mathbb{Z}}_p^{ur}) \twoheadrightarrow \Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})$*, see ([dS87], II, Theorem 4.12), we define*

$$\lambda = (\lambda_k)_k \in \Lambda(G, \hat{\mathbb{Z}}_p^{ur}), \tag{2.4.24}$$

where $G = G(K_\infty/K)$*,* $K_\infty = \cup_{n,k} K_{k,n}$*.*

As before, we write

$$G_{k,\mathfrak{p}} \subset G_k$$

for the decomposition group of $\mathfrak{p}$ in G_k. For a fixed prime $\mathfrak{P}$ of $K_{k,0}$ above $\mathfrak{p}$ we write $K_{k,\infty,\mathfrak{P}}$ for the completion of $K_{k,\infty}$ at the unique prime above $\mathfrak{P}$. With this notation $G_{k,\mathfrak{p}} \cong G(K_{k,\infty,\mathfrak{P}}/K_\mathfrak{p})$. Likewise we denote by

$$G_\mathfrak{p} \subset G$$

the decomposition group of $\mathfrak{p}$ in $G = G(K_\infty/K)$. Fixing a prime $\mathfrak{P}$ of K_∞ above $\mathfrak{p}$ and, by abuse of notation, writing $\mathfrak{P}$ also for the primes of $K_{k,n}$ below $\mathfrak{P}$, we have maps $G_\mathfrak{p} \cong G(K_{\infty,\mathfrak{P}}/K_\mathfrak{p}) \twoheadrightarrow G(K_{k,\infty,\mathfrak{P}}/K_\mathfrak{p}) \cong G_{k,\mathfrak{p}}$. Let us write

$$J \subset \mathbb{Z}_p[[G]] \tag{2.4.25}$$

for the annihilator of $\mu_{p^\infty}(K_\infty)$.

The images of $U_{k,\infty}\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur}$ and $\left(\varprojlim_n (\Theta_{\mathfrak{m}_k\mathfrak{p}^n} \otimes \mathbb{Z}_p)\right)\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur}$ under $\mathbb{L}_k$ are determined in ([dS87], III, Proposition 1.3 and Proposition 1.4). Closely following de Shalit's proofs, in the next theorem we explain that there is an injective map $\mathbb{L} = \varprojlim_k \mathbb{L}_k$ of $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$-modules and we will determine the images of both

$$\mathcal{U}_\infty\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur} \quad \text{and} \quad \mathcal{D}_\infty\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur},$$

under $\mathbb{L}$, where $\mathcal{U}_\infty = \varprojlim_{k,n} U_{k,n}$ and we define

$$\mathcal{D}_\infty = I \varprojlim_{n,k} \big((N_{F_{n,k}/K_{n,k}} \Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \big). \tag{2.4.26}$$

At some points in the proof we provide some more explanation than can be found in (loc. cit.).

Theorem 2.4.25. *Assume that $(p,6) = 1$. Then, there is a map $\mathbb{L} = \varprojlim_k \mathbb{L}_k$ that fits into an exact sequence of $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$-modules*

$$0 \longrightarrow \mathcal{U}_\infty \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur} \xrightarrow{\mathbb{L}} \Lambda(G, \hat{\mathbb{Z}}_p^{ur}) \longrightarrow \operatorname{Ind}_G^{G_\mathfrak{p}} \hat{\mathbb{Z}}_p^{ur}(1) \longrightarrow 0. \tag{2.4.27}$$

In particular, $\mathcal{U}_\infty \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur} \cong \big(\operatorname{Ann}_{\Lambda(G,\hat{\mathbb{Z}}_p^{ur})} \mu_{p^\infty}(K_\infty \otimes_K K_\mathfrak{p})\big) \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur}$. Moreover, $\mathbb{L}$ induces an isomorphism

$$\mathcal{D}_\infty \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur} \cong \Lambda(G, \hat{\mathbb{Z}}_p^{ur}) I J \lambda$$

where we write I for the augmentation ideal $I(K_\infty/K)$, J is the annihilator of $\mu_{p^\infty}(K_\infty)$, λ was defined in (2.4.47) and $\mathcal{D}_\infty$ was defined in (2.4.26).

Proof. The exact sequence (2.4.27) is the semi-local version of an exact sequence arising in a local framework. In fact, for $k \geq 1$, write $\mathfrak{P}$ for the prime of $K_{k,0}$ below the prime $\bar{\mathfrak{P}}$ of $\bar{\mathbb{Q}}$ corresponding to our fixed embedding $\bar{\mathbb{Q}} \subset \mathbb{C}_p$. Then, we have $G_{k,\mathfrak{p}} \cong G(K_{k,\infty,\mathfrak{P}}/K_\mathfrak{p})$. We write $U_{k,\infty,\mathfrak{P}}$ for the $\mathfrak{P}$-part of $U_{k,\infty}$, i.e., for $\varprojlim_n \mathcal{O}^1_{K_{k,n,\mathfrak{P}}}$, where, by abuse of notation, we also write $\mathfrak{P}$ for the unique prime of $K_{k,n}$ above $\mathfrak{P}$. We define $N_k \in \mathbb{N} \cup \{\infty\}$ to be the largest integer such that $\zeta_{p^{N_k}}$, a primitive p^{N_k}-th root of unity, belongs to $K_{k,\infty,\mathfrak{P}}$. Then, de Shalit proves, see ([dS87], I, Theorem 3.7), that there is an exact sequence

$$0 \longrightarrow U_{k,\infty,\mathfrak{P}} \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur} \longrightarrow \Lambda(G_{k,\mathfrak{p}}, \hat{\mathbb{Z}}_p^{ur}) \longrightarrow \big(\hat{\mathbb{Z}}_p^{ur}/p^{N_k}\big)(1) \longrightarrow 0, \tag{2.4.28}$$

where $\hat{\mathbb{Z}}_p^{ur}/p^{N_k}$ should be replaced by $\hat{\mathbb{Z}}_p^{ur}$ in case $N_k = \infty$. We have a similar exact sequence for any other $k' \geq 1$. If $k' \geq k$, and if we write $\mathfrak{P}'$ for the prime of $K_{k',0}$ below $\bar{\mathfrak{P}}$, so that there is a canonical map $G(K_{k',\infty,\mathfrak{P}'}/K_\mathfrak{p}) \twoheadrightarrow G(K_{k,\infty,\mathfrak{P}}/K_\mathfrak{p})$, then the two sequences for k' and k fit into a commutative diagram, see ([dS87], diagram (16) in I, 3.8),

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_{k',\infty,\mathfrak{P}'} \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur} & \longrightarrow & \Lambda(G_{k',\mathfrak{p}}, \hat{\mathbb{Z}}_p^{ur}) & \longrightarrow & \big(\hat{\mathbb{Z}}_p^{ur}/p^{N_{k'}}\big)(1) & \longrightarrow & 0 \\ & & \big\downarrow {\scriptstyle N_{k',k,\mathfrak{p}}} & & \big\downarrow & & \big\downarrow & & \\ 0 & \longrightarrow & U_{k,\infty,\mathfrak{P}} \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur} & \longrightarrow & \Lambda(G_{k,\mathfrak{p}}, \hat{\mathbb{Z}}_p^{ur}) & \longrightarrow & \big(\hat{\mathbb{Z}}_p^{ur}/p^{N_k}\big)(1) & \longrightarrow & 0 \end{array} \tag{2.4.29}$$

where the vertical map $N_{k',k,\mathfrak{p}}$ on the left is induced by the norm maps $N_{K_{k',n,\mathfrak{P}'}/K_{k,n,\mathfrak{P}}}$ and the other two vertical maps are the natural projections. For a proof of the commutativity of diagram (2.4.29) see also the detailed account found in ([Ven13], section 2) that deals with the mutliplicative formal group. Note that all vertical maps are surjective, which is clear for the projections in the middle and on the right. For the vertical map on the left this follows from the fact that for unramified extensions ($K_{k',n}/K_{k,n}$, $k' \geq k$, is unramified at the primes above $\mathfrak{p}$ since E has good reduction at $\mathfrak{p}$, see ([dS87], II, prop. 1.9)) the norm map is surjective on principal units, see ([Ser95], V, §2, proposition 3) or ([FV02], III, corollary to proposition 1.2, p.69).

Let us first make some general remarks about a $G_{k',\mathfrak{p}}$-module M, a $G_{k,\mathfrak{p}}$-module N and a map $\phi : M \longrightarrow N$ that is a $G_{k',\mathfrak{p}}$-module homomorphism if we consider N as a $G_{k',\mathfrak{p}}$-module via the canonical map $G_{k',\mathfrak{p}} \twoheadrightarrow G_{k,\mathfrak{p}}$, $k' \geq k$. First we can consider the map from the universal property of $\mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}} N$ which is a $G_{k,\mathfrak{p}}$-linear map $N \longrightarrow \mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}} N$. We can consider $\mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}} N$ as a $G_{k'}$-module via the map $G_{k'} \twoheadrightarrow G_k$ and then, by restriction, as a $G_{k',\mathfrak{p}}$-module. The composite map $M \xrightarrow{\phi} N \longrightarrow \mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}} N$ is then a $G_{k',\mathfrak{p}}$-linear map. By the universal property of $\mathrm{Ind}_{G_{k'}}^{G_{k',\mathfrak{p}}} M$ we get a unique $G_{k'}$-linear map $\mathrm{Ind}(\phi) : \mathrm{Ind}_{G_{k'}}^{G_{k',\mathfrak{p}}} M \longrightarrow \mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}} N$ induced by ϕ. This construction is functorial with respect to both N and M and the map $\mathrm{Ind}(\phi)$ is surjective if ϕ is surjective (note that for every $k'' \geq 1$ the group $G_{k'',\mathfrak{p}}$ is of finite index in $G_{k''}$).

Now, we see that we can apply $\mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}}$ to the lower horizontal sequence of (2.4.29) and then apply $\mathrm{Ind}_{G_{k'}}^{G_{k',\mathfrak{p}}}$ to the upper sequence and get a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_{k',\infty}\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur} & \xrightarrow{\mathbb{L}_{k'}} & \Lambda(G_{k'},\hat{\mathbb{Z}}_p^{ur}) & \longrightarrow & \mathrm{Ind}_{G_{k'}}^{G_{k',\mathfrak{p}}}\left(\hat{\mathbb{Z}}_p^{ur}/p^{N_{k'}}\right)(1) & \longrightarrow & 0 \\ & & \big\downarrow N_{k',k} & & \big\downarrow & & \big\downarrow & & \\ 0 & \longrightarrow & U_{k,\infty}\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur} & \xrightarrow{\mathbb{L}_{k}} & \Lambda(G_{k},\hat{\mathbb{Z}}_p^{ur}) & \longrightarrow & \mathrm{Ind}_{G_{k}}^{G_{k,\mathfrak{p}}}\left(\hat{\mathbb{Z}}_p^{ur}/p^{N_{k}}\right)(1) & \longrightarrow & 0 \end{array} \tag{2.4.30}$$

where the vertical map $N_{k',k}$ on the left is induced by the norm maps $N_{K_{k',n}/K_{k,n}}$ and the other two vertical maps are the canonical projections. As we have noted above $N_{k',k}$ is surjective. Compare remark 2.4.23 for the fact that appying $\mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}}$ and $\mathrm{Ind}_{G_{k'}}^{G_{k',\mathfrak{p}}}$ to diagram (2.4.29), in fact, gives the maps $\mathbb{L}_k$ and $\mathbb{L}_{k'}$ in (2.4.30). Next, we recall that $G_{\mathfrak{p}}$ is of finite index in G and it is straightforward to write down an isomorphism

$$\mathrm{Ind}_G^{G_{\mathfrak{p}}}\hat{\mathbb{Z}}_p^{ur}(1) \cong \mathrm{Ind}_G^{G_{\mathfrak{p}}}\Big(\varprojlim_k \left(\hat{\mathbb{Z}}_p^{ur}/p^{N_k}\right)(1)\Big) \cong \varprojlim_k \Big(\mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}}\left(\hat{\mathbb{Z}}_p^{ur}/p^{N_k}\right)(1)\Big).$$

We are no longer dealing with compact modules, which is why we need the following fact. The first right derived functor of the left-exact $\varprojlim_k$ applied to a projective system with surjective transition maps vanishes, see ([Wei94], chapter 3, lemma 3.5.3). Therefore, passing to the projective limit with respect to k, $k \geq 1$, and the vertical maps from (2.4.30), we obtain the desired exact sequence

$$0 \longrightarrow \mathcal{U}_\infty \hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur} \xrightarrow{\mathbb{L}} \Lambda(G,\hat{\mathbb{Z}}_p^{ur}) \longrightarrow \mathrm{Ind}_G^{G_{\mathfrak{p}}}\hat{\mathbb{Z}}_p^{ur}(1) \longrightarrow 0. \tag{2.4.31}$$

We will now prove the second statement about the image under $\mathbb{L}$ of the elliptic units.

The elements $e(\mathfrak{a})$, $(\mathfrak{a}, \mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p}) = 1$, from definition 2.4.24, generate

$$\varprojlim_{n,k} \left(N_{F_{n,k}/K_{n,k}} (\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \right) \tag{2.4.32}$$

as a $\Lambda(G)$-module, which follows from lemma 2.4.3 applied to the module generated by the $e(\mathfrak{a})$, $(\mathfrak{a}, \mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p}) = 1$, which surjects onto the various $N_{F_{n,k}/K_{n,k}} \Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}$, $k, n \geq 1$.

We know that $\varprojlim_{n,k} \left(N_{F_{n,k}/K_{n,k}} (\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \right)$, as a submodule of the global units $\bar{\mathcal{E}}_\infty$, can be embedded into

$$\varprojlim_{n,k} \prod_{\mathfrak{P}|\mathfrak{p}} \hat{\mathcal{O}}^\times_{K_{n,k},\mathfrak{P}} \cong \varprojlim_{n,k} \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}^1_{K_{n,k},\mathfrak{P}} = \mathcal{U}_\infty$$

and the elements $e(\mathfrak{a})$, $(\mathfrak{a}, \mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p}) = 1$, under this identification, coincide with $u(\mathfrak{a})$, by which we denote the projections of the elements $e(\mathfrak{a}) \in \varprojlim_{n,k} \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}^\times_{K_{n,k},\mathfrak{P}}$ to their pro-p-parts in $\mathcal{U}_\infty$, compare diagram (2.4.5). With this notation the elements $u(\mathfrak{a})$, $(\mathfrak{a}, \mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p}) = 1$, generate (2.4.32) considered as a $\Lambda(G)$-submodule of $\mathcal{U}_\infty$.

The image of $u(\mathfrak{a})$ under $\mathbb{L}$ is given by

$$\mathbb{L}(u(\mathfrak{a})) = \left(\mathbb{L}_k(u_k(\mathfrak{a}))\right)_k = (\lambda_{k,\mathfrak{a}})_k = (12 x_{k,\mathfrak{a}} \lambda_k)_k = 12 x_\mathfrak{a} \lambda,$$

where $x_\mathfrak{a} = \sigma_\mathfrak{a} - N\mathfrak{a}$, $\sigma_\mathfrak{a} = (\mathfrak{a}, K_\infty/K) \in G$ and $x_{k,\mathfrak{a}}$ is the image of $x_\mathfrak{a}$ in $\Lambda(G_k)$. Note that 12 is a unit in $\mathbb{Z}_p$ by the assumption on p. The statement now follows from the fact that the elements $x_\mathfrak{a} = \sigma_\mathfrak{a} - N\mathfrak{a}$ for varying $\mathfrak{a}$, $(\mathfrak{a}, \mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}) = 1$, generate J, which is proved in lemma 2.4.27 below. □

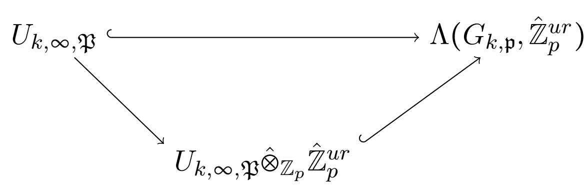
Corollary 2.4.26. *The map $\mathbb{L}$ restricts to an injective $\Lambda(G)$-homomorphism*

$$\mathcal{U}_\infty \hookrightarrow \Lambda(G, \hat{\mathbb{Z}}_p^{ur})$$

and this restriction defines an isomorphism of $\Lambda(G)$-modules

$$\mathcal{D}_\infty \cong IJ\lambda.$$

Proof. First note that as de Shalit remarks ([dS87], I, 3.4 Corollary), the first non-trivial map in (2.4.28) is the linear extension of an injective $\Lambda(G_{k,\mathfrak{p}})$-homomorphism $U_{k,\infty,\mathfrak{P}} \hookrightarrow \Lambda(G_{k,\mathfrak{p}}, \hat{\mathbb{Z}}_p^{ur})$. This means we have the following commutative diagram



so that applying the exact functor $\mathrm{Ind}_{G_k}^{G_{k,\mathfrak{p}}}$ and then passing to the projective limit we get

$$\begin{array}{ccc} \mathcal{U}_\infty & \xrightarrow{\ \mathbb{L}_{|\mathcal{U}_\infty}\ } & \Lambda(G, \hat{\mathbb{Z}}_p^{ur}) \\ & \searrow \qquad \nearrow_{\mathbb{L}} & \\ & \mathcal{U}_\infty \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur} & \end{array}$$

showing the first part of the corollary and that the canonical map $\mathcal{U}_\infty \to \mathcal{U}_\infty \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur}$ is actually injective. The statement about the elliptic units follows exactly as in the proof of the previous theorem. □

Lemma 2.4.27. *The annihilator $J = \mathrm{Ann}_{\Lambda(G)}(\mu_{p^\infty}(K_\infty))$ of $\mu_{p^\infty}(K_\infty)$ in $\Lambda(G)$ is generated by $\sigma_\mathfrak{a} - N\mathfrak{a}$, $\mathfrak{a}$, $(\mathfrak{a}, 6\mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}) = 1$, where $\sigma_\mathfrak{a} = (\mathfrak{a}, K_\infty/K)$.*

Proof. For each n we denote by l_n the greatest number such that $K_{n,n} = K(E[p^n])$ contains a primitive p^{l_n}-th root of unity. Then, for each $n \geq 1$ we consider the $\mathbb{Z}_p/(p^{l_n})[G(K_{n,n}/K)]$-module $\mu_{p^\infty}(K_{n,n})$. Let $\sum_g a_g g$ be an element of $\mathbb{Z}_p/(p^{l_n})[G(K_{n,n}/K)]$ that annihilates $\mu_{p^\infty}(K_{n,n})$. By Čebotarev's density theorem, for all $g \in G(K_{n,n}/K)$ we can find a prime ideal $\mathfrak{q}_g$ prime to $6\mathfrak{f}p$ such that $g = (\mathfrak{q}_g, K_{n,n}/K)$. We can then write

$$\sum_g a_g g = \sum_g a_g (g - \overline{N\mathfrak{q}_g}) + \sum_g a_g \overline{N\mathfrak{q}_g}.$$

Clearly, $\sum_g a_g(g - \overline{N\mathfrak{q}_g})$ belongs to the annihilator of $\mu_{p^\infty}(K_{n,n})$ (since $g = (\mathfrak{q}_g, K_{n,n}/K)$ acts as multiplication by $N\mathfrak{q}_g$ on $\mu_{p^\infty}(K_{n,n})$) and we see that $\sum_g a_g \overline{N\mathfrak{q}_g}$, which is just the residue class of an integer, must be congruent to 0 modulo (p^{k_n}), which implies that $\sum_g a_g g = \sum_g a_g(g - \overline{N\mathfrak{q}_g})$ in $\mathbb{Z}_p/(p^{l_n})[G(K_{n,n}/K)]$. We see that $\mathrm{Ann}_{\mathbb{Z}_p/(p^{l_n})[G(K_{n,n}/K)]}(\mu_{p^\infty}(K_{n,n}))$ is generated by elements of the form $(\mathfrak{a}, K_{n,n}/K) - \overline{N\mathfrak{a}}$, $(\mathfrak{a}, 6\mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}) = 1$.

For each $n \geq 1$ we can now consider the exact sequence

$$0 \to \mathrm{Ann}_{\mathbb{Z}_p/(p^{l_n})[G(K_{n,n}/K)]}(\mu_{p^\infty}(K_{n,n})) \to \mathbb{Z}_p/(p^{l_n})[G(K_{n,n}/K)] \to \mathbb{Z}_p/(p^{l_n})(1) \to 0.$$

Passing to the projective limit, we get

$$J = \varprojlim_n \mathrm{Ann}_{\mathbb{Z}_p/(p^{l_n})[G(K_{n,n}/K)]}(\mu_{p^\infty}(K_{n,n})).$$

Writing J_0 for the ideal of $\Lambda(G)$ generated by elements of the form $\sigma_\mathfrak{a} - N\mathfrak{a}$, $\mathfrak{a}$, $(\mathfrak{a}, 6\mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}) = 1$, we have shown above that for each $n \geq 1$ the natural projection $\Lambda(G) \twoheadrightarrow \mathbb{Z}_p/(p^{l_n})[G(K_{n,n}/K)]$ induces a surjection $J_0 \twoheadrightarrow \mathrm{Ann}_{\mathbb{Z}_p/(p^{l_n})[G(K_{n,n}/K)]}(\mu_{p^\infty}(K_{n,n}))$. Since $\Lambda(G)$ is compact and Noetherian, see remark 2.4.2, J_0 is also compact. Therefore, passing to the limit we get the desired surjection $J_0 \twoheadrightarrow J$, which concludes the proof. □

2.4.5 Triviality of the annihilator $\mathrm{Ann}_{\Lambda(G,\hat{\mathbb{Z}}_p^{ur})}(\lambda)$

Let the setting be as in the previous subsection 2.4.4. In particular, we write $G = G(K_\infty/K)$. We also set $\mathfrak{m}_0 = \mathfrak{f}_\psi$ such that F_∞/K_∞ is a finite extension. We want to show that λ is not a zero-divisor in $\Lambda(G,\hat{\mathbb{Z}}_p^{ur})$ which is the main result of this subsection. We will relate λ to elliptic units studied by Yager in [Yag82] and use the fact that $\Lambda(G,\hat{\mathbb{Z}}_p^{ur})$ is a finite product of integral domains and that Yager's elliptic units each correspond to a finite number of power series in $\hat{\mathbb{Z}}_p^{ur}[[T_1,T_2]]$ each of which interpolates non-zero L-values. Let us fix a non-trivial prime ideal $\mathfrak{c}$ of K prime to $6p\mathfrak{f}$ and write

$$y_\mathfrak{c} := 1-\sigma_\mathfrak{c} = 1-(\mathfrak{c},K_\infty/K)\in\Lambda(G,\hat{\mathbb{Z}}_p^{ur}),$$

which is not a zero-divisor in $\Lambda(G,\hat{\mathbb{Z}}_p^{ur})$. In fact, K_∞/K contains the cyclotomic $\mathbb{Z}_p$-extension in which $\mathfrak{c}$ is unramified. Hence, powers of Frobenius elements for $\mathfrak{c}$ do not have finite order in G. This is sufficient for $y_\mathfrak{c}$ not to be a zero-divisor, which can be seen from the aforementioned decomposition of $\Lambda(G,\hat{\mathbb{Z}}_p^{ur})$ into $(p-1)^2$ integral domains from section A.9

$$\Lambda(G,\hat{\mathbb{Z}}_p^{ur})\cong\hat{\mathbb{Z}}_p^{ur}[[\Delta\times\Gamma]]\cong\prod_{\chi\in\hat{\Delta}}\hat{\mathbb{Z}}_p^{ur}[[T_1,T_2]], \tag{2.4.33}$$

where Δ is a finite group of order $(p-1)^2$, $\Gamma\cong\mathbb{Z}_p^2$ and $\hat{\Delta}$ denotes the character group of Δ. An element in $\Lambda(G,\hat{\mathbb{Z}}_p^{ur})$ is not a zero-divisor if and only if it is non-zero in every χ-component $\hat{\mathbb{Z}}_p^{ur}[[T_1,T_2]]$ for χ running through $\hat{\Delta}$. Recall the definition of the characters χ_i, $i=1,2$, from section A.9 which, together, generate $\hat{\Delta}$.

Proposition 2.4.28. *The element λ from definition 2.4.24 is not a zero-divisor in $\Lambda(G,\hat{\mathbb{Z}}_p^{ur})$.*

Proof. Clearly, it is sufficient to show that for some integral ideal $\mathfrak{a}$ of K, $(\mathfrak{a},6p\mathfrak{f})=1$, the element $y_\mathfrak{c}12x_\mathfrak{a}\lambda=\mathbb{L}(y_\mathfrak{c}u(\mathfrak{a}))$ is not a zero-divisor, which is to say that $0=\mathrm{ann}_{\Lambda(G,\hat{\mathbb{Z}}_p^{ur})}(y_\mathfrak{c}12x_\mathfrak{a}\lambda)=\mathrm{ann}_{\Lambda(G,\hat{\mathbb{Z}}_p^{ur})}(y_\mathfrak{c}u(\mathfrak{a}))$. Here, for a ring R, an R-module M and an element $m\in M$, we write $\mathrm{ann}_R m$ for the annihilator of m in R.

Now, we want to relate $y_\mathfrak{c}u(\mathfrak{a})$ to the units studied by Yager in [Yag82]. For $k,n\geq 0$, write $\rho=\frac{\Omega}{f\bar{\pi}^{k+1}\pi^{n+1}}$, which is a primitive $\mathfrak{f}\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^{n+1}$-division point for L. First note that, by ([dS87], II, Proposition 2.4 (ii)), for all $k,n\geq 1$ and an integral ideal $\mathfrak{a}$, $(\mathfrak{a},\mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p})=1$, we have

$$y'_\mathfrak{c}e'_{k+1,n+1}(\mathfrak{a})=\frac{\Theta\big(\rho,L,\mathfrak{a}\big)\Theta\big(\rho,L,\mathfrak{c}\big)^{N\mathfrak{a}}}{\Theta\big(\rho,L,\mathfrak{a}\mathfrak{c}\big)}\in\mathcal{O}_{F_{k,n}}^\times, \tag{2.4.34}$$

where we write $y'_\mathfrak{c}=1-(\mathfrak{c},F_\infty/K)$. Now, we choose and fix a non-trivial $\mathfrak{a}$ coprime to $\mathfrak{c}$ and define a map

$$\mu:\ \{\text{integral ideals of } K \text{ prime to } 6p\mathfrak{f}\}\longrightarrow\mathbb{Z}$$

by

$$\mu(\mathfrak{a}) = 1, \quad \mu(\mathfrak{c}) = N\mathfrak{a}, \quad \mu(\mathfrak{a}\mathfrak{c}) = -1, \quad \mu(\mathfrak{d}) = 0, \tag{2.4.35}$$

for all other ideals $\mathfrak{d}$ of K. Using the Chinese remainder theorem ($\mathcal{O}_K$ is a principal ideal domain), we then get

$$\sum_{\mathfrak{b}} (N\mathfrak{b} - 1)\mu(\mathfrak{b}) = (N\mathfrak{a} - 1) + (N\mathfrak{c} - 1)N\mathfrak{a} - (N\mathfrak{a}\mathfrak{c} - 1) = 0$$

where the sum is taken over all integral ideals of K prime to $6p\mathfrak{f}$. Yager, see ([Yag82], section 4), then defines

$$\Theta(z, L, \mu) = \prod_{\mathfrak{b}} \Theta(z, L, \mathfrak{b})^{\mu(\mathfrak{b})},$$

where the product is taken over all integral ideals of K prime to $6p\mathfrak{f}$. With this notation the identity (2.4.34) says

$$y'_{\mathfrak{c}} e'_{k+1,n+1}(\mathfrak{a}) = \Theta(\rho, L, \mu). \tag{2.4.36}$$

Next, let $(\tau_n)_n$, $\tau_n \in \mathbb{C}$, be a compatible system of primitive $\mathfrak{p}^{n+1}$-division points for L - for example, $\tau_n = \frac{\Omega}{\pi^{n+1}}$. Moreover, since $\bar{\pi}$ is a unit in $\mathcal{O}_{K_\mathfrak{p}}$, we can choose elements $\epsilon_n \in \mathcal{O}_K$ such that

$$\epsilon_n \bar{\pi} \equiv 1 \mod \mathfrak{p}^{n+1}.$$

Moreover, Čebotarev's density theorem, see ([Neu07], VII, Theorem 13.4), allows us to choose a prime $\mathfrak{q}_{k,n}$ of K, $(\mathfrak{q}_{k,n}, 6p\mathfrak{f}) = 1$, such that

$$(\mathfrak{q}_{k,n}, F_{k+1,0}/K) = (\mathfrak{p}, F_{k+1,0}/K)^{-n} \quad \in G(F_{k+1,0}/K),$$

where we recall that $F_{k,n} = K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$. Now, we note that Yager, in ([Yag82], Corollary 9), defines norm-compatible elements

$$e_{n,k}(\mu) \in \mathcal{O}^\times_{K_{k+1,n+1}},$$

where we recall that $K_{k,n} = K(E[\bar{\pi}^k\pi^n])$. Unwinding Yager's definition of these elements, one can show that they are given by

$$e_{n,k}(\mu) = N_{F_{k+1,n+1}/K_{k+1,n+1}}\Big(\Theta\big(\epsilon_n^{k+1}\tau_n + \psi(\mathfrak{q}_{k,n})\frac{\Omega}{f\bar{\pi}^{k+1}}, L, \mu\big)\Big). \tag{2.4.37}$$

For those trying to derive this equality from Yager's definitions, we note that one uses the addition theorem for the Weierstraß $\wp$-function, see ([Lan87] chapter 1, section 3), in order to see, as Yager remarks, that $\Theta\big(z + \frac{\Omega}{f\bar{\pi}^{k+1}}, L, \mathfrak{b}\big)$ is a rational function of $\wp(z)$ and $\wp'(z)$ with coefficients in $F_{k+1,0}$ for any integral ideal $\mathfrak{b}$ of K prime to $6p\mathfrak{f}$. From this expression as a rational function of $\wp(z)$ and $\wp'(z)$ and the main theorem of complex multiplication, saying that $(\mathfrak{q}_{k,n}, F_{k+1,0}/K)(\wp(\frac{\Omega}{f\bar{\pi}^{k+1}})) = \wp(\psi(\mathfrak{q}_{k,n})\frac{\Omega}{f\bar{\pi}^{k+1}})$ holds (and a similar equation for $\wp'$), one can then show that

$$\Theta^{(\mathfrak{q}_{k,n}, F_{k+1,0}/K)}\big(z + \frac{\Omega}{f\bar{\pi}^{k+1}}, L, \mathfrak{b}\big) = \Theta\big(z + \psi(\mathfrak{q}_{k,n})\frac{\Omega}{f\bar{\pi}^{k+1}}, L, \mathfrak{b}\big),$$

where the left-hand side denotes the function obtained by letting $(\mathfrak{q}_{k,n}, F_{k+1,0}/K)$ act on the coefficients of $\Theta\big(z+\frac{\Omega}{f\bar{\pi}^{k+1}}, L, \mathfrak{b}\big)$. The last ingredient for (2.4.37) is the isomorphism from (2.4.19) and the fact that $\wp(\epsilon_n^{k+1}\tau_n), \wp'(\epsilon_n^{k+1}\tau_n) \in K_{k+1,n+1}$ are fixed by any element in $G(F_{k+1,n+1}/K_{k+1,n+1})$.

Now, we proceed with the proof. Note that $\epsilon_n^{k+1}\tau_n + \psi(\mathfrak{q}_{k,n})\frac{\Omega}{f\bar{\pi}^{k+1}}$ is a primitive $\mathfrak{f}\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^{n+1}$-divison point for L. To see this, write $\pi^{n+1}\tau_n = a_n\Omega$ for some $a_n \in \mathcal{O}_K$ prime to $\mathfrak{p}$, consider the identity

$$\epsilon_n^{k+1}\tau_n + \psi(\mathfrak{q}_{k,n})\frac{\Omega}{f\bar{\pi}^{k+1}} = \big(f\bar{\pi}^{k+1}\epsilon_n^{k+1}a_n + \pi^{n+1}\psi(\mathfrak{q}_{k,n})\big)\frac{\Omega}{f\bar{\pi}^{k+1}\pi^{n+1}}$$

and note that the residue class of $f\bar{\pi}^{k+1}\epsilon_n^{k+1}a_n + \pi^{n+1}\psi(\mathfrak{q}_{k,n})$ is non-zero in $\mathcal{O}_K/\mathfrak{f}$, $\mathcal{O}_K/\mathfrak{p}$ and in $\mathcal{O}_K/\bar{\mathfrak{P}}$ by the choice of $\mathfrak{q}_{k,n}$ (recall that $\psi(\mathfrak{q}_{k,n})$ is a generator of $\mathfrak{q}_{k,n}$).

Knowing that $\epsilon_n^{k+1}\tau_n+\psi(\mathfrak{q}_{k,n})\frac{\Omega}{f\bar{\pi}^{k+1}}$ is a primitive $\mathfrak{f}\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^{n+1}$-divison point, we see from remark 2.4.6 that we can find an integral ideal $\mathfrak{d}_{k,n}$ of K prime to $\mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}$ such that

$$\Theta\Big(\frac{\Omega}{f\bar{\pi}^{k+1}\pi^{n+1}}, L, \mu\Big)^{\sigma'_{\mathfrak{d}_{k,n}}} = \Theta\Big(\epsilon_n^{k+1}\tau_n + \psi(\mathfrak{q}_{k,n})\frac{\Omega}{f\bar{\pi}^{k+1}}, L, \mu\Big), \tag{2.4.38}$$

where $\sigma'_{\mathfrak{d}_{k,n}} = (\mathfrak{d}_{k,n}, F_{k+1,n+1}/K)$. We conclude from (2.4.37), (2.4.38) and (2.4.36) that Yager's elliptic unit $e_{n,k}(\mu)$ is equal to

$$\begin{aligned} e_{n,k}(\mu) &= N_{F_{k+1,n+1}/K_{k+1,n+1}}\Big(\Theta\Big(\frac{\Omega}{f\bar{\pi}^{k+1}\pi^{n+1}}, L, \mu\Big)^{\sigma'_{\mathfrak{d}_{k,n}}}\Big) \\ &= \Big(N_{F_{k+1,n+1}/K_{k+1,n+1}}\big(y'_{\mathfrak{c}}e'_{k+1,n+1}(\mathfrak{a})\big)\Big)^{\sigma_{\mathfrak{d}_{k,n}}} \\ &= y_{\mathfrak{c}}e_{k+1,n+1}(\mathfrak{a})^{\sigma_{\mathfrak{d}_{k,n}}}, \end{aligned} \tag{2.4.39}$$

where $\sigma_{\mathfrak{d}_{k,n}} = (\mathfrak{d}_{k,n}, K_{k+1,n+1}/K)$, $y_{\mathfrak{c}} = 1-(\mathfrak{c}, K_\infty/K) \in \Lambda(G)$ and $e_{k+1,n+1}(\mathfrak{a})$ is our elliptic unit from definition 2.4.24. If we write $u(\mu)$ for the projection of $(e_{n,k}(\mu))_{n,k}$ to $\mathcal{U}_\infty$, a simple compactness argument shows that we can find $\delta \in \Lambda(G)$ such that

$$\delta y_{\mathfrak{c}}u(\mathfrak{a}) = u(\mu). \tag{2.4.40}$$

In fact, if we write $u_{n,k}(\mu)$ for the projection of $e_{n,k}(\mu)$ to $\mathcal{O}^1_{k+1,n+1,\mathfrak{p}}$, then, for all $k,n \geq 1$ the preimage of the closed set $\{u_{n,k}(\mu)\}$ under the continuous projection maps $\Lambda(G)y_{\mathfrak{c}}u(\mathfrak{a}) \longrightarrow \mathcal{O}^1_{k+1,n+1,\mathfrak{p}}$ is non-empty by (2.4.39). By compactness of $\Lambda(G)y_{\mathfrak{c}}u(\mathfrak{a})$ and the norm-compatibility of the various $u_{n,k}(\mu)$, the intersection of all those preimages cannot be empty, which is precisely what we claimed.

Now, we recall that our original goal was to show that $\mathrm{ann}_{\Lambda(G,\hat{\mathbb{Z}}_p^{ur})}(y_{\mathfrak{c}}u(\mathfrak{a})) = 0$. For this it is clearly sufficient, by (2.4.40), to show that

$$\mathrm{ann}_{\Lambda(G,\hat{\mathbb{Z}}_p^{ur})}(u(\mu)) = 0. \tag{2.4.41}$$

Let (i_1, i_2) be a pair of integers modulo $p-1$. We recall from section A.9 that we write e_{i_1,i_2} (this has nothing to do with our elliptic units) for the idempotent in $\mathbb{Z}_p[\Delta]$ corresponding to $\chi_1^{i_1}\chi_2^{i_2}$. To show that (2.4.41) holds it is sufficient to show

$$\mathrm{ann}_{\Lambda(G,\hat{\mathbb{Z}}_p^{ur})^{(i_1,i_2)}}(e_{i_1,i_2}u(\mu)) = 0 \tag{2.4.42}$$

for all pairs (i_1, i_2) in $\mathbb{Z}/(p-1)\times\mathbb{Z}/(p-1)$. From now on, let (i_1, i_2) be any pair of integers modulo $p-1$. Recall that upon choosing topological generators γ_1, γ_2 of $\Gamma \cong \mathbb{Z}_p\times\mathbb{Z}_p$ one can define an isomorphism $\Lambda(\Gamma, \hat{\mathbb{Z}}_p^{ur}) \cong \hat{\mathbb{Z}}_p^{ur}[[T_1, T_2]]$, $\gamma_i \mapsto T_i$, $i = 1, 2$, which we use to consider $M^{(i_1,i_2)}$ as a $\hat{\mathbb{Z}}_p^{ur}[[T_1, T_2]]$-module, where M is any $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$-module.

Now, we consider the injective $\mathbb{Z}_p[[T_1, T_2]]$-homomorphisms defined in ([Yag82], Lemma 24)

$$W^{(i_1,i_2)} : \mathcal{U}_\infty^{(i_1,i_2)} \longrightarrow \mathbb{Z}_p[[T_1, T_2]]$$

for each pair (i_1, i_2) as above. Since $\hat{\mathbb{Z}}_p^{ur}$ is topologically flat over $\mathbb{Z}_p$, i.e., the functor $-\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur}$ is exact, we can extend the map $W^{(i_1,i_2)}$ to an injective map

$$W^{(i_1,i_2)} : \mathcal{U}_\infty^{(i_1,i_2)}\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur} \longrightarrow \hat{\mathbb{Z}}_p^{ur}[[T_1, T_2]].$$

We will not give a precise definition of the map $W^{(i_1,i_2)}$, but only use the interpolation property of the power series $W^{(i_1,i_2)}(e_{i_1,i_2}u(\mu))$ given in [Yag82] (note that Yager writes $< e(\mu) >$ for $u(\mu)$) to prove that

$$W^{(i_1,i_2)}(e_{i_1,i_2}u(\mu)) \neq 0. \tag{2.4.43}$$

Assume we have already shown that (2.4.43) holds. Then, if $e_{(i_1,i_2)}\delta e_{(i_1,i_2)}u(\mu) = 0$ for some $\delta \in \Lambda(G, \hat{\mathbb{Z}}_p^{ur})$, let us first note that we can find $\tilde{\delta} \in \Lambda(\Gamma, \hat{\mathbb{Z}}_p^{ur}) \cong \hat{\mathbb{Z}}_p^{ur}[[T_1, T_2]]$ (it is via this isomorphism that the action of $\hat{\mathbb{Z}}_p^{ur}[[T_1, T_2]]$ on $\mathcal{U}_\infty^{(i_1,i_2)}\hat{\otimes}_{\mathbb{Z}_p}\hat{\mathbb{Z}}_p^{ur}$ is defined) such that

$$e_{(i_1,i_2)}\tilde{\delta} = e_{(i_1,i_2)}\delta$$

as elements in $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$. Since $e_{(i_1,i_2)}$ is an idempotent and $e_{(i_1,i_2)}$ and $\tilde{\delta}$ commute, it follows that

$$0 = W^{(i_1,i_2)}(e_{(i_1,i_2)}\delta e_{(i_1,i_2)}u(\mu)) = \tilde{\delta}W^{(i_1,i_2)}(e_{(i_1,i_2)}u(\mu)),$$

from which we conclude that $\tilde{\delta} = 0$ since $\hat{\mathbb{Z}}_p^{ur}[[T_1, T_2]]$ is an integral domain and we have assumed that (2.4.43) holds. It follows that $e_{(i_1,i_2)}\delta = 0$ and, in particular, that (2.4.42) holds, which is what we wanted to show.

Lastly, it remains to prove (2.4.43), which we will do by showing that $W^{(i_1,i_2)}(e_{i_1,i_2}u(\mu))$ interpolates non-zero values. We fix a generator u of $1 + p\mathbb{Z}_p$ and write $\delta_{k,j}$, $k \geq 1, j \leq 0$, for the logarithmic derivative $\mathbb{Z}_p$-module homomorphisms

$$\delta_{k,j} : \mathcal{U}_\infty \longrightarrow (\mathcal{O}_{K_{\infty,0}} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{p}})\widehat{\ }$$

defined in ([Yag82], section 3). Then for all integers $k_1 > -k_2 \geq 0$, $(k_1, k_2) \equiv (i_1, i_2) \mod p-1$, we have the following identities in $(\mathcal{O}_{K_{\infty,0}} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{p}})\widehat{}$

$$\begin{aligned} W^{(i_1,i_2)}(e_{i_1,i_2}u(\mu))(u^{k_1}-1, u^{k_2}-1) &= D' \cdot \Big(1 - \frac{\psi(\mathfrak{p})^{k_1-k_2}}{(N\mathfrak{p})^{1-k_2}}\Big) \cdot \delta_{k_1,k_2}(e_{i_1,i_2}u(\mu)) \\ &= D' \cdot \Big(1 - \frac{\psi(\mathfrak{p})^{k_1-k_2}}{(N\mathfrak{p})^{1-k_2}}\Big) \cdot \delta_{k_1,k_2}(u(\mu)) \\ &= D'' \cdot \Big(1 - \frac{\psi(\mathfrak{p})^{k_1-k_2}}{(N\mathfrak{p})^{1-k_2}}\Big) \cdot (k_1-1)! \cdot \Big(1 - \frac{\bar{\psi}^{k_1-k_2}(\bar{\mathfrak{p}})}{(N\bar{\mathfrak{p}})^{k_1}}\Big) \\ &\cdot \Big(\sum_{\mathfrak{b}} \mu(\mathfrak{b})\big(N\mathfrak{b} - \psi^{k_1}(\mathfrak{b})\bar{\psi}^{k_2}(\mathfrak{b})\big)\Big) \cdot \Big(\frac{2\pi}{\sqrt{d_K}}\Big)^{-k_2} \cdot \frac{L(\bar{\psi}^{k_1-k_2}, k_1)}{\Omega^{k_1-k_2}}, \end{aligned} \tag{2.4.44}$$

where D', D'' are units in $(\mathcal{O}_{K_{\infty,0}} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{p}})\widehat{}$, $-d_K$ denotes the discriminant of K, π for now denotes the smallest positive real number such that $\cos(\pi/2) = 0$ and for the first equation we used theorems 27 and 22 from [Yag82], for the second lemma 6 from (loc. cit.) and for the last equation theorem 15 from (loc. cit.).

The term $\Big(1 - \frac{\psi(\mathfrak{p})^{k_1-k_2}}{(N\mathfrak{p})^{1-k_2}}\Big) \cdot (k_1-1)! \cdot \Big(1 - \frac{\bar{\psi}^{k_1-k_2}(\bar{\mathfrak{p}})}{(N\bar{\mathfrak{p}})^{k_1}}\Big)$ from (2.4.44) is non-zero (just think of it as an element in K and consider the valutations of the individual terms at $\nu_\mathfrak{p}$ and $\nu_{\bar{\mathfrak{p}}}$).

Next we look at the term $\sum_\mathfrak{b} \mu(\mathfrak{b})\big(N\mathfrak{b} - \psi^{k_1}(\mathfrak{b})\bar{\psi}^{k_2}(\mathfrak{b})\big)$ where the sum is taken over all integral ideals of K prime to $6p\mathfrak{f}$. Recalling the definition of μ from (2.4.35) and rearranging some terms (here we use the multiplicativity of the norm N on coprime ideals), we see that it is given by

$$\begin{aligned} \sum_{\mathfrak{b}} \mu(\mathfrak{b})\big(N\mathfrak{b} - \psi^{k_1}(\mathfrak{b})\bar{\psi}^{k_2}(\mathfrak{b})\big) &= \big(N\mathfrak{a} - \psi^{k_1}(\mathfrak{a})\bar{\psi}^{k_2}(\mathfrak{a})\big) + N\mathfrak{a}\big(N\mathfrak{c} - \psi^{k_1}(\mathfrak{c})\bar{\psi}^{k_2}(\mathfrak{c})\big) \\ &\quad - \big(N(\mathfrak{a}\mathfrak{c}) - \psi^{k_1}(\mathfrak{a}\mathfrak{c})\bar{\psi}^{k_2}(\mathfrak{a}\mathfrak{c})\big) \\ &= \Big(N\mathfrak{a} - \psi^{k_1}(\mathfrak{a})\bar{\psi}^{k_2}(\mathfrak{a})\Big) \cdot \Big(1 - \psi^{k_1}(\mathfrak{c})\bar{\psi}^{k_2}(\mathfrak{c})\Big). \end{aligned} \tag{2.4.45}$$

For any fixed $k_2 \leq 0$, $k_2 \equiv i_2 \mod p-1$, the last term can at most be equal to 0 for two different k_1 satisfying $k_1 \geq 1$, $k_1 \equiv i_1 \mod p-1$. In fact, if

$$N\mathfrak{a} = \psi^{k_1}(\mathfrak{a})\bar{\psi}^{k_2}(\mathfrak{a}),$$

then

$$N\mathfrak{a} \neq \psi^{k_1+k(p-1)}(\mathfrak{a})\bar{\psi}^{k_2}(\mathfrak{a})$$

for all $k \in \mathbb{Z} - \{0\}$ since $\psi(\mathfrak{a})$ generates a non-trivial ideal of $\mathcal{O}_K$. The same argument applies to the term $\Big(1 - \psi^{k_1}(\mathfrak{c})\bar{\psi}^{k_2}(\mathfrak{c})\Big)$, so for fixed k_2 there can be at most two elements k_1 as above such that (2.4.45) is equal to 0.

Lastly, we will turn our attention to the term

$$\Big(\frac{2\pi}{\sqrt{d_K}}\Big)^{-k_2} \cdot \frac{L(\bar{\psi}^{k_1-k_2}, k_1)}{\Omega^{k_1-k_2}}, \tag{2.4.46}$$

which is algebraic by Damerell's theorem found in [Dam70] and [Dam71] and, as Yager notes, in fact belongs to K for all integers $k_1 > -k_2 \geq 0$. Greenberg remarks in [Gre85] quite generally for primitive Größencharacters Ψ of type A_0 for an imaginary quadratic field and infinity type $(n, 0)$, $n \geq 1$, that due to the convergence of the Euler product for $L(\Psi, s)$ in the half-plane $\Re(s) > \frac{n}{2} + 1$, the L-function cannot have a zero there. Moreover, Greenberg quotes Lang ([Lan70], chapter 15) for the fact that also $L(\Psi, s) \neq 0$ for $\Re(s) = \frac{n}{2} + 1$. Using the functional equation one can then deduce that there cannot occur any zeros for $0 < \Re(s) \leq \frac{n}{2}$ either (a fact which we will not need).

For our purposes first note that, as Greenberg (loc. cit.) remarks, for the complex conjugation automorphism $c \in G(K/\mathbb{Q})$ we have $L(\bar{\psi}^{k_1-k_2} \circ c, s) = L(\bar{\psi}^{k_1-k_2}, s)$ since c simply permutes the prime ideals of K. Moreover, the Größencharacter $\bar{\psi}^{k_1-k_2} \circ c$ has infinity type $(k_1 - k_2, 0)$. It follows for k_1, k_2 such that $k_1 \geq \frac{k_1-k_2}{2} + 1$, which happens precisely if $k_1 \geq 2 - k_2$, that we have

$$L(\bar{\psi}^{k_1-k_2}, k_1) = L(\bar{\psi}^{k_1-k_2} \circ c, k_1) \neq 0.$$

But for fixed $k_2 \leq 0$, $k_2 \equiv i_2 \mod p-1$, we have $k_1 \geq 2-k_2$ for almost all $k_1 \geq 1$, $k_1 \equiv i_1 \mod p-1$. We have shown that for fixed $k_2 \leq 0$, $k_2 \equiv i_2 \mod p-1$, both (2.4.45) and (2.4.46) are non-zero for almost all $k_1 \geq 1$, $k_1 \equiv i_1 \mod p-1$.

In conclusion, we have shown that $W^{(i_1,i_2)}(e_{i_1,i_2}u(\mu))$ interpolates a non-zero value, so

$$W^{(i_1,i_2)}(e_{i_1,i_2}u(\mu)) \neq 0,$$

which finishes the proof. □

2.4.6 Elliptic units continued

Let the setting be as in section 2.4.4. In particular, we consider an elliptic curve E/K with complex multiplication by $\mathcal{O}_K$ and, as before, write $\mathfrak{f}$ for the conductor of the Größencharacter ψ attached to E/K. Moreover, we write p for a fixed split prime and assume that E/K has good ordinary reduction above p. If E is already defined over $\mathbb{Q}$ and E is a representative with minimal discriminant and conductor in its $\bar{\mathbb{Q}}$-isomorphism class as in ([Sil99], Appendix A, §3), then, by theorem A.6.8 and proposition A.6.9 we know that

$$\mathfrak{f} = \mathfrak{l}^r, \quad r \geq 1,$$

is a prime power for some prime ideal $\mathfrak{l}$. It is precisely this condition that we want to impose on a general elliptic curve E/K with CM by $\mathcal{O}_K$ in this subsection.

Assumption 2.4.29. *We assume that the conductor $\mathfrak{f}$ of the Größencharacter ψ over K is a prime power*

$$\mathfrak{f} = \mathfrak{l}^r$$

for some prime ideal $\mathfrak{l}$ and some $r \geq 1$.

In theorem 2.4.25 and corollary 2.4.26 we have shown that the image of the $\Lambda(G)$-module $I \varprojlim_{k,n} \big((N_{F_{k,n}/K_{k,n}} \Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\big)$ under the map $\mathbb{L}$ in $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$ is equal to $\Lambda(G) I J \lambda$.

Under the above assumption, the image of Rubin's elliptic units $\varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ under $\mathbb{L}$ admits a similar description, the determination of which is the aim of this subsection. Recall from corollary 2.4.13 that

$$\varprojlim_{k,n}(C'_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \mathcal{C}_\infty,$$

where we define $\mathcal{C}_\infty := \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ and $C'_{K_{k,n}}$ was defined in definition 2.4.9. In definition 2.4.24 we defined certain elliptic units that were values under $\Theta(-,-)$ of division points the order of which was divisible by the conductor $\mathfrak{f}$. For our description of $\varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ we also need elliptic units that are values of division points the orders of which are prime to $\mathfrak{f}$. Recall that we write $L_{k,n} = K(\bar{\mathfrak{p}}^k \mathfrak{p}^n)$ for the ray class field of K modulo $\bar{\mathfrak{p}}^k \mathfrak{p}^n$, so that we have $L_{k,n} \subset K_{k,n} \subset F_{k,n} = K(\mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n)$.

Definition 2.4.30. *Assume that p is prime to 6 and prime to $\#(\mathcal{O}_K/\mathfrak{f})^\times$. For $k, n \geq 1$ and an integral ideal $\mathfrak{a}$, $(\mathfrak{a}, \bar{\mathfrak{p}}\mathfrak{p}) = 1$, define*

$$\tilde{e}_{k,n}(\mathfrak{a}) := \Theta\Big(\frac{\Omega}{\bar{\pi}^k \pi^n}, L, \mathfrak{a}\Big) \in \mathcal{O}^\times_{L_{k,n}},$$

which defines a norm-compatible system $\tilde{e}(\mathfrak{a}) = (\tilde{e}_{k,n}(\mathfrak{a}))_{k,n} \in \varprojlim_{k,n} \mathcal{O}^\times_{L_{k,n}}$ of global units. Now let $k, n \geq 1$ such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\bar{\mathfrak{p}}^{k-1}\mathfrak{p}^{n-1})^\times$ is injective. Since, $L_{k,n} \subset K_{k,n}$ and $G(K_{k,n}/K_{k-1,n-1}) \to G(L_{k,n}/L_{k-1,n-1})$ are bijections, see corollary A.6.6, $\tilde{e}(\mathfrak{a})$ is also a norm-compatible system in $\varprojlim_{k,n} \mathcal{O}^\times_{K_{k,n}}$. For fixed $k \geq 1$, the norm-compatible system $\tilde{e}(\mathfrak{a})$ maps to a norm-compatible system $\tilde{e}_k(\mathfrak{a}) = (\tilde{e}_{k,n}(\mathfrak{a}))_n$,

$$\varprojlim_{k',n'} \mathcal{O}^\times_{k',n'} \longrightarrow \varprojlim_{n} \mathcal{O}^\times_{k,n}, \quad \tilde{e}(\mathfrak{a}) \longmapsto \tilde{e}_k(\mathfrak{a}).$$

Let us now think of $\varprojlim_n \mathcal{O}^\times_{k,n}$ as embedded into the semi-local units $\varprojlim_n \mathcal{O}^\times_{k,n,\mathfrak{p}}$ and write $\tilde{u}_k(\mathfrak{a})$ for the projection of $\tilde{e}_k(\mathfrak{a})$ to the pro-p part $U_{k,\infty}$ of $\varprojlim_n \mathcal{O}^\times_{k,n,\mathfrak{p}}$, in symbols,

$$\varprojlim_{n} \mathcal{O}^\times_{k,n,\mathfrak{p}} \longrightarrow U_{k,\infty}, \quad \tilde{e}_k(\mathfrak{a}) \longmapsto \tilde{u}_k(\mathfrak{a}).$$

We define

$$\tilde{\lambda}_{k,\mathfrak{a}} := \lambda^0_{\tilde{u}_k(\mathfrak{a})} = \mathbb{L}_k(\tilde{u}_k(\mathfrak{a})),$$

as the p-adic integral measure on G_k corresponding to $\tilde{u}_k(\mathfrak{a})$. For $\mathfrak{a}$ such that $(\mathfrak{a}, \mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p}) = 1$ we also define

$$\tilde{\lambda}_k := \frac{1}{12} \cdot \frac{\tilde{\lambda}_{k,\mathfrak{a}}}{x_{k,\mathfrak{a}}} \quad \in \; Q(\Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})),$$

where $x_{k,\mathfrak{a}} := \sigma_{k,\mathfrak{a}} - N\mathfrak{a}$, $\sigma_{k,\mathfrak{a}} = (\mathfrak{a}, K_{k,\infty}/K) \in G_k$. For another $\mathfrak{b}$ such that $(\mathfrak{b}, \mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p}) = 1$ we have an equality

$$x_{k,\mathfrak{b}}\tilde{\lambda}_{k,\mathfrak{a}} = x_{k,\mathfrak{a}}\tilde{\lambda}_{k,\mathfrak{b}}$$

since the corresponding equation holds for $\tilde{u}_k(\mathfrak{a})$ and $\tilde{u}_k(\mathfrak{b})$, see ([dS87] II, proposition 2.4 (ii)). It follows as in the proof of ([dS87], II, theorem 4.12) that $\tilde{\lambda}_k$ is independent of $\mathfrak{a}$ and actually an integral measure, so that $\tilde{\lambda}_k \in \Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})$.

Using the fact that for $k' \geq k \geq 1$, $\tilde{u}_{k'}(\mathfrak{a})$ maps to $\tilde{u}_k(\mathfrak{a})$ under the norm map, the commutativity of diagram 2.4.30 shows that $\tilde{\lambda}_{k'}$ maps to $\tilde{\lambda}_k$ under the canonical projection $\Lambda(G_{k'}, \hat{\mathbb{Z}}_p^{ur}) \twoheadrightarrow \Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})$. We can therefore define

$$\tilde{\lambda} = (\tilde{\lambda}_k)_k \in \Lambda(G, \hat{\mathbb{Z}}_p^{ur}), \tag{2.4.47}$$

where $G = G(K_\infty/K)$, $K_\infty = \cup_{n,k} K_{k,n}$.

Having defined $\tilde{\lambda}$ we can now state the main result of this subsection.

Theorem 2.4.31. *The map $\mathbb{L}_{|\mathcal{U}_\infty}$ from corollary 2.4.26 defines an isomorphism of $\Lambda(G)$-modules*

$$\mathcal{C}_\infty \cong IJ\lambda + IJ\tilde{\lambda}$$

where, we recall, $\mathcal{C}_\infty = \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$, I denotes the augmentation ideal $I(K_\infty/K)$ in $\Lambda(G)$, J is the annihilator of $\mu_{p^\infty}(K_\infty)$ in $\Lambda(G)$ and $\tilde{\lambda}$ was defined in (2.4.47).

Proof. We first look at $C'_{K_{k,n}}$ for $k, n \geq 1$ and note that, due to assumption 2.4.29, it is generated by elements

$$\left(N_{K_{k,n}K(\mathfrak{l}^{r'}\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\ \Theta(\tau; \mathfrak{a})\right)^{\sigma-1}, \tag{2.4.48}$$

where σ ranges through $\mathrm{Gal}(K_{k,n}/K)$, $0 \leq r' \leq r$, $\mathfrak{a}$ runs through integral ideals such that $(\mathfrak{a}, 6\mathfrak{l}^{r'}\bar{\mathfrak{p}}\mathfrak{p}) = 1$ and τ through primitive $\mathfrak{l}^{r'}\bar{\mathfrak{p}}^k\mathfrak{p}^n$-division points. If r' is greater or equal to 1 ($\mathfrak{a}$ is then prime to $\mathfrak{l}$), then, by ([dS87], II, proposition 2.5), we have

$$N_{K_{k,n}K(\mathfrak{l}^{r'}\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\ \Theta(\tau; \mathfrak{a}) = N_{K(\mathfrak{l}^r\bar{\mathfrak{p}}^k\mathfrak{p}^n)/(K(\mathfrak{l}^{r'}\bar{\mathfrak{p}}^k\mathfrak{p}^n)\cap K_{k,n})}\ \Theta\Big(\frac{\tau}{l^{r-r'}}; \mathfrak{a}\Big).$$

This shows that in (2.4.48) we may restrict to $r' = 0$ and $r' = r$ and still obtain a set of $\mathbb{Z}[\mathrm{Gal}(K_{k,n}/K)]$ generators of $C'_{K_{k,n}}$. We also may restrict to primitive division points of the form $\frac{\Omega}{\bar{\pi}^k\pi^n}$ and $\frac{\Omega}{l^r\bar{\pi}^k\pi^n}$ since the values of $\Theta(-, \mathfrak{a})$ at other primitive division points are Galois conjugates, see remark 2.4.6 for the case $r' = r$. The case $r' = 0$ follows from ([dS87], II, proposition 2.4 (ii)), the proof of which uses, without mentioning it, (loc. cit., II, lemma 1.4, p.41); see also ([Rub99], theorem 7.4).

So we have shown that

$$C'_{K_{k,n}} = I(K_{k,n}/K)\big(N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}\big) + I(K_{k,n}/K)\Theta_{\bar{\mathfrak{p}}^k\mathfrak{p}^n}, \tag{2.4.49}$$

where +, of course, means the group generated by the two subgroups $I(K_{k,n}/K)\big(N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}\big)$ and $I(K_{k,n}/K)\Theta_{\bar{\mathfrak{p}}^k\mathfrak{p}^n}$ of $\mathcal{O}^\times_{K_{k,n}}$ and the augmentation ideals have coefficients in $\mathbb{Z}$. Even though we are dealing with units we use an additive notation because later we will tensor with $\mathbb{Z}_p$ and then naturally use the additive notation.

We have noted before that for $n' \geq n \geq 1$, $k' \geq k \geq 1$ the norm maps

$$N_{F_{k',n'}/F_{k,n}} : \Theta_{\mathfrak{f}\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}} \longrightarrow \Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}$$

are surjective. It follows that the norm maps

$$N_{K_{k',n'}/K_{k,n}} : N_{F_{k',n'}/K_{k',n'}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}} \longrightarrow N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}$$

are surjective and using corollary A.6.6 we also see that the norm maps

$$N_{K_{k',n'}/K_{k,n}} : \Theta_{\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}} \longrightarrow \Theta_{\bar{\mathfrak{p}}^k\mathfrak{p}^n}$$

are surjective. It follows that the norm maps

$$N_{K_{k',n'}/K_{k,n}} : \Big(\big(N_{F_{k',n'}/K_{k',n'}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}\big) + \Theta_{\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}\Big) \longrightarrow \Big(\big(N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}\big) + \Theta_{\bar{\mathfrak{p}}^k\mathfrak{p}^n}\Big) \tag{2.4.50}$$

are surjective and the same holds after tensoring with $\mathbb{Z}_p$. From this we conclude that the projection maps

$$I \varprojlim_{k',n'} \Big(\Big[\big(N_{F_{k',n'}/K_{k',n'}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}\big) + \Theta_{\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}\Big]\otimes_{\mathbb{Z}}\mathbb{Z}_p\Big) \longrightarrow \Big[I(K_{k,n}/K)\Big(\big(N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}\big) + \Theta_{\bar{\mathfrak{p}}^k\mathfrak{p}^n}\Big)\Big]\otimes_{\mathbb{Z}}\mathbb{Z}_p$$

are surjective and the term on the right, by (2.4.49), is equal to $C'_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Passing to the projective limit with respect to k, n yields an isomorphism

$$I \varprojlim_{k',n'} \Big(\Big[\big(N_{F_{k',n'}/K_{k',n'}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}\big) + \Theta_{\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}\Big] \otimes_{\mathbb{Z}} \mathbb{Z}_p\Big) \cong \varprojlim_{k,n}(C'_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$$

by lemma 2.4.3.

Another compactness argument shows that $\varprojlim_{k',n'} \Big(\Big[\big(N_{F_{k',n'}/K_{k',n'}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}\big) + \Theta_{\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}\Big] \otimes_{\mathbb{Z}} \mathbb{Z}_p\Big)$ is generated over $\Lambda(G)$ by $e(\mathfrak{a})$ and $\tilde{e}(\mathfrak{b})$, where $\mathfrak{a}, \mathfrak{b}$ range through the integral ideals of K such that $(\mathfrak{a}, \mathfrak{l}p) = 1$ and $(\mathfrak{b}, p) = 1$. In fact, this follows from lemma 2.4.3 applied to the module generated by the $e(\mathfrak{a})$ and $\tilde{e}(\mathfrak{b})$, $(\mathfrak{a},\mathfrak{l}p)=1$, $(\mathfrak{b},p)=1$, which surjects onto the various $\Big(\big(N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}\big)+\Theta_{\bar{\mathfrak{p}}^k\mathfrak{p}^n}\Big)\otimes_{\mathbb{Z}}\mathbb{Z}_p$, $k,n\geq 1$.

We embed the global units into the semi-local units $\mathcal{U}_\infty$ as before and write $u(\mathfrak{a})$ and $\tilde{u}(\mathfrak{b})$ for the images of $e(\mathfrak{a})$ and $\tilde{e}(\mathfrak{b})$, respectively. Then, we have

$$\mathbb{L}(u(\mathfrak{a}))=\big(\mathbb{L}_k(u_k(\mathfrak{a}))\big)_k=(\lambda_{k,\mathfrak{a}})_k=(12x_{k,\mathfrak{a}}\lambda_k)_k=12x_{\mathfrak{a}}\lambda,$$

and likewise

$$\mathbb{L}(\tilde{u}(\mathfrak{b}))=\big(\mathbb{L}_k(\tilde{u}_k(\mathfrak{b}))\big)_k=(\tilde{\lambda}_{k,\mathfrak{b}})_k=(12x_{k,\mathfrak{b}}\tilde{\lambda}_k)_k=12x_{\mathfrak{b}}\tilde{\lambda},$$

where, in the last line, $x_{\mathfrak{b}}=\sigma_{\mathfrak{b}}-N\mathfrak{b}$ with $\sigma_{\mathfrak{b}}=(\mathfrak{b},K_\infty/K)$ as usual if $(\mathfrak{b},6p\mathfrak{l})=1$. In case $\mathfrak{l}\mid\mathfrak{b}$ we can consider $(\mathfrak{b},L_\infty/K)$ and then define $\sigma_{\mathfrak{b}}$ to be a lift to $G(K_\infty/K)$. Note that $\mu_{p^\infty}(\bar{K})\subset L_\infty$ (because for any primitive p^n-th root of unity ζ_{p^n} the extension $K(\zeta_{p^n})/K$ is unramified outside the primes above p so the conductor of $K(\zeta_{p^n})/K$ divides a power of p, i.e., $K(\zeta_{p^n})$ is contained in a field $L_{m,m}$ for some $m\geq 1$). It follows that even if $\mathfrak{l}\mid\mathfrak{b}$ the element $x_{\mathfrak{b}}=\sigma_{\mathfrak{b}}-N\mathfrak{b}$ belongs to J. In combination with lemma 2.4.27, this concludes the proof. □

2.4.7 Relations in $K_0(S\text{-tor})$

Let the setting be as in the previous subsection 2.4.6. Moreover, we keep the assumption 2.4.29 that the conductor of ψ is a prime power $\mathfrak{f}=\mathfrak{l}^r$ for some prime $\mathfrak{l}$ and $r\geq 1$. We know from theorem 2.4.16 that the quotient

$$\mathcal{C}_\infty/\mathcal{D}_\infty \tag{2.4.51}$$

is S-torsion and by remark 2.4.2 that it is finitely generated over $\Lambda(G)$. Using corollary 2.4.26 and theorem 2.4.31, we see that its image in $K_0(S\text{-tor})$ is

$$\big[\big(IJ\lambda+IJ\tilde{\lambda}\big)/IJ\lambda\big]=\big[IJ\tilde{\lambda}/\big(IJ\tilde{\lambda}\cap IJ\lambda\big)\big], \tag{2.4.52}$$

where we consider $IJ\lambda$ and $IJ\tilde{\lambda}$ as $\Lambda(G)$-submodules of $\Lambda(G,\hat{\mathbb{Z}}_p^{ur})$. From lemma A.6.4 we know that K_∞/L_∞ is a Galois extension of degree $\omega_K=\#\mu(K)$ and we define the norm element

$$\mathcal{N}:=\mathcal{N}_{K_\infty/L_\infty}:=\sum_{g\in G(K_\infty/L_\infty)} g \quad\in\ \Lambda(G).$$

From the same lemma we know that for all $k,n\geq 1$ such that $\mathcal{O}_K^\times\to(\mathcal{O}_K/\bar{\mathfrak{p}}^k\mathfrak{p}^n)^\times$ is injective, we have bijections

$$G(K_\infty/L_\infty)\cong G(K_{k,n}/L_{k,n}).$$

induced by the restriction maps. It follows from ([dS87], II, proposition 2.5) that for such k,n and for $\mathfrak{a}$ prime to $6p\mathfrak{f}$ we have

$$N_{K_{k,n}/L_{k,n}}e_{k,n}(\mathfrak{a})=N_{F_{k,n}/L_{k,n}}\Theta\Big(\frac{\Omega}{f\bar{\pi}^k\pi^n},L,\mathfrak{a}\Big)=\Theta\Big(\frac{\Omega}{\bar{\pi}^k\pi^n},L,\mathfrak{a}\Big)^{(1-\sigma_{\mathfrak{l}}^{-1})}=\tilde{e}_{k,n}(\mathfrak{a})^{(1-\sigma_{\mathfrak{l}}^{-1})}$$

and also

$$N_{K_{k,n}/L_{k,n}}\tilde{e}_{k,n}(\mathfrak{a}) = \tilde{e}_{k,n}(\mathfrak{a})^{\omega_K}$$

since $\tilde{e}_{k,n}(\mathfrak{a}) = \Theta\big(\frac{\Omega}{\bar{\pi}^k\pi^n}, L, \mathfrak{a}\big)$ belongs to $\mathcal{O}^{\times}_{L_{k,n}}$ and the extension $K_{k,n}/L_{k,n}$ has degree $\omega_K = \#\mu(K)$. It follows from this that for $x_{\mathfrak{a}} = (\mathfrak{a}, K_\infty/K) - N\mathfrak{a}$, $(\mathfrak{a}, 6p\mathfrak{f}) = 1$, we have equations in $\tilde{\Lambda} = \Lambda(G, \hat{\mathbb{Z}}_p^{ur})$

$$\mathcal{N}x_{\mathfrak{a}}\lambda = (1-\sigma_{\mathfrak{l}}^{-1})x_{\mathfrak{a}}\tilde{\lambda} \quad \text{and} \quad \mathcal{N}x_{\mathfrak{a}}\tilde{\lambda} = \omega_K x_{\mathfrak{a}}\tilde{\lambda}$$

and hence, since $x_{\mathfrak{a}}$ is not a zero-divisor, we also have

$$\mathcal{N}\lambda = (1-\sigma_{\mathfrak{l}}^{-1})\tilde{\lambda} \quad \text{and} \quad \mathcal{N}\tilde{\lambda} = \omega_K\tilde{\lambda} \tag{2.4.53}$$

and note that ω_K is a unit in $\mathbb{Z}_p$. This shows that we can apply the following lemma to $R = \Lambda, Q = \tilde{\Lambda}, M = IJ\tilde{\lambda}, N = IJ\lambda, x = \mathcal{N}, y = 1-\sigma_{\mathfrak{l}}^{-1}$ and get

$$\mathcal{N}\cdot\big(IJ\tilde{\lambda}\cap IJ\lambda\big) = (1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}. \tag{2.4.54}$$

Lemma 2.4.32. *Let R be a commutative ring, M, N submodules of a R-module Q and x, y elements of R such that $xM = M$ and $xN = yM$. Then, we have an equality of submodules*

$$x(M\cap N) = yM$$

of Q.

Proof. Clearly, we have $x(M\cap N) \subset \big((xM)\cap(xN)\big) = yM$. On the other hand, for an element $ya \in yM$, with $a \in M$ we can find $a' \in M$ such that $a = xa'$. It follows that $ya = xya'$ and ya' belongs to $M\cap N$ since $xN = yM$. □

Since multiplication with $\mathcal{N}$ induces an isomorphism of $IJ\tilde{\lambda}$ and therefore also of $IJ\tilde{\lambda}\cap IJ\lambda$, equation (2.4.54) shows that the class on the right of (2.4.52) is equal to

$$\big[IJ\tilde{\lambda}/\big(IJ\tilde{\lambda}\cap IJ\lambda\big)\big] = \big[IJ\tilde{\lambda}/\big((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}\big)\big]. \tag{2.4.55}$$

It follows from the lemmata A.9.2 and A.9.5 that all of the modules in the following two exact sequences are S-torsion

$$0\to IJ\tilde{\lambda}/\big((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}\big)\to\Lambda\tilde{\lambda}/\big((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}\big)\to\Lambda\tilde{\lambda}/IJ\tilde{\lambda}\to 0 \tag{2.4.56}$$

and

$$0\to\big((1-\sigma_{\mathfrak{l}}^{-1})\Lambda\tilde{\lambda}\big)/\big((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}\big)\to\Lambda\tilde{\lambda}/\big((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}\big)\to\Lambda\tilde{\lambda}/\big(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\tilde{\lambda}\big)\to 0. \tag{2.4.57}$$

For all modules in the above two exact sequences it is clear that they are finitely generated over Λ, recall that $IJ\tilde{\lambda}/\big((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}\big)$ is isomorphic to (2.4.51). Since $1-\sigma_{\mathfrak{l}}^{-1}$ is not a zero-divisor in $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$, i.e., for any $\Lambda(G)$-submodule M of $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$ multiplication with $1 - \sigma_{\mathfrak{l}}^{-1}$ defines an isomorphism $M \cong (1 - \sigma_{\mathfrak{l}}^{-1})M$, the two exact sequences show that

$$\left[IJ\tilde{\lambda}/\left((1 - \sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}\right)\right] = \left[\Lambda\tilde{\lambda}/\left(\Lambda(1 - \sigma_{\mathfrak{l}}^{-1})\tilde{\lambda}\right)\right]. \tag{2.4.58}$$

Recall the identity on the left of (2.4.53)

$$\mathcal{N}\lambda = (1 - \sigma_{\mathfrak{l}}^{-1})\tilde{\lambda}.$$

Since $1 - \sigma_{\mathfrak{l}}^{-1}$ is not a zero-divisor in $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$ we see that the class on the right of (2.4.58) is equal to

$$\left[\Lambda(1 - \sigma_{\mathfrak{l}}^{-1})\tilde{\lambda}/\left(\Lambda(1 - \sigma_{\mathfrak{l}}^{-1})^2\tilde{\lambda}\right)\right] = \left[\Lambda\mathcal{N}\lambda/\left(\Lambda(1 - \sigma_{\mathfrak{l}}^{-1})\mathcal{N}\lambda\right)\right]. \tag{2.4.59}$$

Theorem 2.4.33. *In $K_0(S\text{-tor})$ we have an equality*

$$[\mathcal{C}_\infty/\mathcal{D}_\infty] = [\Lambda(G/D_{\mathfrak{l}})],$$

where we write $D_{\mathfrak{l}}$ for the decomposition group of $\mathfrak{l}$ in $G = G(K_\infty/K)$.

Proof. Equations (2.4.52), (2.4.55), (2.4.58) and (2.4.59) show that

$$[\mathcal{C}_\infty/\mathcal{D}_\infty] = \left[\Lambda\mathcal{N}\lambda/\left(\Lambda(1 - \sigma_{\mathfrak{l}}^{-1})\mathcal{N}\lambda\right)\right]$$

and since λ is not a zero-divisor in $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$ by proposition 2.4.28 we see that the class on the right is equal to

$$\left[\Lambda\mathcal{N}/\left(\Lambda(1 - \sigma_{\mathfrak{l}}^{-1})\mathcal{N}\right)\right].$$

We remark that $\Lambda\mathcal{N}$ and $\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N}$ are now already submodules of Λ and not only of $\tilde{\Lambda}$. Let us write H' for the closed subgroup $G(K_\infty/L_\infty)$ of G and $pr : \Lambda(G) \twoheadrightarrow \Lambda(G/H')$ for the canonical projection. Then, we have an exact sequence

$$0 \longrightarrow \ker(pr_{|\Lambda(G)\mathcal{N}}) \longrightarrow \Lambda(G)\mathcal{N} \longrightarrow \Lambda(G/H') \longrightarrow 0, \tag{2.4.60}$$

which is exact because under pr the element $\mathcal{N}$ maps to $\omega_K \in \mathbb{Z}_p^\times$. Now, we claim that $\ker(pr_{|\Lambda(G)\mathcal{N}}) = 0$. In fact, let $x\mathcal{N}$, $x \in \Lambda(G)$, belong to $\ker(pr)$. Then, we have

$$0 = pr(x\mathcal{N}) = pr(x)\omega_K,$$

from which we conclude that $x \in \ker(pr)$, because $\omega_K \in \mathbb{Z}_p^\times$. But $\ker(pr)$ is generated over $\Lambda(G)$ by elements of the form $1 - g$, $g \in H'$, and for such elements $(1 - g)\mathcal{N} = 0$ and therefore $x\mathcal{N} = 0$. It follows from (2.4.60) that

$$\Lambda(G)\mathcal{N} \cong \Lambda(G/H'),$$

which is not surprising since ideals generated by norm elements in group rings and augmentation ideals are annihilators of each other, compare ([Neu69], I, §1, (1.3) Satz). We get

$$\Lambda(G)\mathcal{N}\big/\big(\Lambda(G)(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N}\big) \cong \Lambda(G/H')\big/\big(\Lambda(G/H')(1-\bar{\sigma}_{\mathfrak{l}}^{-1})\big), \tag{2.4.61}$$

where we write $\bar{\sigma}_{\mathfrak{l}}$ for the restriction of $\sigma_{\mathfrak{l}}$ to L_∞. Note that, by definition, $\bar{\sigma}_{\mathfrak{l}} = (\mathfrak{l}, L_\infty/K)$ is the arithmetic Frobenius at $\mathfrak{l}$ for the extension L_∞/K, in which $\mathfrak{l}$ is unramified. In particular, $\bar{\sigma}_{\mathfrak{l}}$ topologically generates the decomposition group $D'_{\mathfrak{l}}$ of $\mathfrak{l}$ in $G/H' \cong G(L_\infty/K)$. It follows that

$$\Lambda(G/H')\big/\big(\Lambda(G/H')(1-\bar{\sigma}_{\mathfrak{l}}^{-1})\big) \cong \Lambda\big(G(L_\infty/K)/D'_{\mathfrak{l}}\big). \tag{2.4.62}$$

Next, we claim that any place $\mathfrak{L}$ of L_∞ above $\mathfrak{l}$ does not split in K_∞/L_∞, i.e., for $\mathfrak{L}$ there is a unique extension $\mathfrak{L}'$ to K_∞. We also write $v_{\mathfrak{q}}$ for a non-archimedean place $\mathfrak{q}$ in order to stress that we think of it as a valuation. This means that we have to show that if $\mathfrak{L}'$ is a place of K_∞ above $\mathfrak{L}$, then

$$v_{\mathfrak{L}'} \circ g = v_{\mathfrak{L}'} \tag{2.4.63}$$

for all $g \in G(K_\infty/L_\infty)$. But for any $g \in G(K_\infty/L_\infty)$ and any $k, n \geq 1$, the following lemma 2.4.35 applied to $\mathfrak{m} = \bar{\mathfrak{p}}^k \mathfrak{p}^n$ shows that $(v_{\mathfrak{L}'})_{|K_{k,n}}$, the restriction of $v_{\mathfrak{L}'}$ to $K_{k,n}$, is the unique place of $K_{k,n}$ above $(v_{\mathfrak{L}'})_{|L_{k,n}}$, which implies that

$$(v_{\mathfrak{L}'})_{|K_{k,n}} \circ g_{|K_{k,n}} = (v_{\mathfrak{L}'})_{|K_{k,n}}.$$

This equation holds for all $k, n \geq 1$ and therefore implies the equation from (2.4.63).

Having shown that for any place $\mathfrak{L}$ of L_∞ above $\mathfrak{l}$ there is a unique extension $\mathfrak{L}'$ to K_∞, we can conclude that the canonical restriction map induces an isomorphism

$$G/D_{\mathfrak{l}} \xrightarrow{\sim} G(L_\infty/K)\big/D'_{\mathfrak{l}}, \tag{2.4.64}$$

where we write $D_{\mathfrak{l}}$ for the decomposition group of $\mathfrak{l}$ in $G = G(K_\infty/K)$.

All in all, equations (2.4.61), (2.4.62) and (2.4.64) show that we have an isomorphism of Λ-modules

$$\Lambda\mathcal{N}\big/\big(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N}\big) \cong \Lambda(G/D_{\mathfrak{l}}), \tag{2.4.65}$$

which finishes the proof. □

Before proving the lemma we have referred to above, let us record one immediate consequence of (2.4.65) and lemma A.9.5.

Corollary 2.4.34. *The $\Lambda(G)$-module $\Lambda(G/D_{\mathfrak{l}})$ is S-torsion.*

Lemma 2.4.35. *Let $\mathfrak{m}$ be an integral ideal of K and let $\mathfrak{l}$ be a prime of K such that $(\mathfrak{l}, \mathfrak{m}) = 1$. For any integer $r \geq 1$ and any prime $\mathfrak{L}$ of $K(\mathfrak{m})$ above $\mathfrak{l}$, $\mathfrak{L}$ cannot split in the extension $K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m})$. In particular, $\mathfrak{L}$ cannot split in any subextension $L/K(\mathfrak{m})$ of $K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m})$.*

Proof. Let $\mathfrak{L}$ be a prime of $K(\mathfrak{m})$ above $\mathfrak{l}$. Assume that $\mathfrak{L}$ splits in the extension $K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m})$. Then, the fixed field Z of the decomposition group of $\mathfrak{L}$ in $G(K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m}))$ is strictly bigger than $K(\mathfrak{m})$ and $\mathfrak{L}$ is unramified in the extension $Z/K(\mathfrak{m})$, see ([Neu07], I, §9, (9.3) Satz (iii)) for the last fact. Since $\mathfrak{l}$ is unramified in $K(\mathfrak{m})/K$ this implies that there is one prime of Z above $\mathfrak{l}$ which has ramification index 1 in Z/K. But then, since Z/K is Galois, all primes of Z above $\mathfrak{l}$ have ramification index 1 which means that $\mathfrak{l}$ is unramified in the extension Z/K. In particular, $\mathfrak{l}$ does not divide the conductor of the extension Z/K. But the conductor of Z/K divides $\mathfrak{l}^r\mathfrak{m}$ and therefore must divide $\mathfrak{m}$, which contradicts the fact that Z is strictly bigger than $K(\mathfrak{m})$. Therefore, $\mathfrak{L}$ cannot split in the extension $K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m})$. ◻

2.4.8 Commutative main theorem

Let the setting be as in subsections 2.4.4 and 2.4.6, including assumption 2.4.29. In this subsection we want to derive a commutative main theorem in our CM setting from the results of the previous subsections and from Rubin's proof of the two variable main conjecture.

Remark 2.4.36. We note that the compact p-adic Lie group $G = G(K_\infty/K)$ and its closed normal subgroup $H = G(K_\infty/K^{cyc})$ satisfy the conditions (i), (ii) and (iii) from subsection 1.2.1, for which we recall the isomorphism (A.9.1) from the appendix and that H is abelian and contains a subgroup corresponding to the anticyclotomic $\mathbb{Z}_p$-extension of K, so that H is of dimension 1 as a p-adic Lie group. In particular, the classes of modules that are finitely generated over $\mathbb{Z}_p$ vanish in $K_0(\mathfrak{M}_H(G))$ by corollary 1.2.3.

We write $\Sigma = \{\mathfrak{p}, \bar{\mathfrak{p}}, \mathfrak{l}, \nu_\infty\}$. Assume that $p \neq 2, 3$, as before, and write $\Lambda = \Lambda(G)$. Moreover, for any integral ideal $\mathfrak{b}$ of K prime to $6p\mathfrak{f}$ we define

$$x_\mathfrak{b} = N(\mathfrak{b}) - \sigma_\mathfrak{b} \in \Lambda(G),$$

where $\sigma_\mathfrak{b} = (\mathfrak{b}, K_\infty/K)$. Next we fix an integral auxiliary ideal $\mathfrak{q}$ of K, $(\mathfrak{q}, 6p\mathfrak{f}) = 1$, $\mathfrak{q} \neq \mathcal{O}_K$.

Definition 2.4.37 (Choice of auxiliary $\mathfrak{q}$). *We choose and fix a prime $\mathfrak{q}$ of K, subject to the following conditions:*

(i) $(\mathfrak{q}, 6p\mathfrak{f}) = 1$,

(ii) $N(\mathfrak{q})$ *is congruent to* 1 *modulo* p, *in symbols*

$$N(\mathfrak{q}) \equiv 1 \bmod p.$$

Note that by Dirichlet's theorem on arithmetic progressions infinitely many such prime ideals exist, compare ([Neu07], VII, (5.14) p. 490). Henceforth, we will write q for the prime of $\mathbb{Q}$ below $\mathfrak{q}$.

Remark 2.4.38. By lemma A.9.2 the element $x_\mathfrak{q}$ belongs to the Ore set S of Λ.

Let us write $I = I(K_\infty/K)$ for the kernel of the augmentation map $\mathrm{aug} : \Lambda(G) \to \mathbb{Z}_p$ and J for the annihilator in $\Lambda(G)$ of $\mu_{p^\infty} = \mu_{p^\infty}(K_\infty) = \{\zeta \in K_\infty \mid \zeta^{p^n} = 1 \text{ for some } n \geq 1\}$.

Lemma 2.4.39. *Assume that $p \neq 2$. Then, the ideals I and J are coprime, i.e., $I + J = \Lambda(G)$. In particular, we have an equality of ideals $IJ = I \cap J$.*

Proof. Fix an element $q \in \mathbb{Z}$ such that q and $q-1$ belong to $\mathbb{Z}_p^\times$. This is possible by our assumption on p. Then, $1-q$ certainly belongs to $\mathbb{Z}_p^\times$. Now, fix an element $\sigma \in G$ that acts on $\varprojlim_n \mu_{p^n}$ as multiplication by $1-q$, which is possible since the cyclotomic character $\chi_{cyc} : G \twoheadrightarrow \mathbb{Z}_p^\times$ is surjective. Then, $q = 1 - \sigma + \sigma - (1-q)$ belongs to $I + J$. But q is also a unit, which concludes the proof of the first claim. The second claim is easily derived from the first, see ([BIV98], p.12). □

We now come to our main theorem in the commutative setting. Recall that we write

$$\mathcal{C}_\infty = \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p), \quad \mathcal{D}_\infty = I \varprojlim_{k,n}\big((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\big)$$

for the elliptic units, $\mathcal{D}_\infty \subset \mathcal{C}_\infty$, and

$$\bar{\mathcal{E}}_\infty = \varprojlim_{k,n}(\mathcal{O}^\times_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$$

for the global units, $\mathcal{D}_\infty \subset \mathcal{C}_\infty \subset \bar{\mathcal{E}}_\infty$. It follows from (2.2.3) (note that $\Sigma_{ur} = \varnothing$ since $\bar{\mathfrak{p}}$ (resp. $\mathfrak{p}$) is unramified in $\cup_{n\geq 1}K(E[\pi^n])$ (resp. $\cup_{k\geq 1}K(E[\bar{\pi}^k])$) that $\bar{\mathcal{E}}_\infty \cong \mathbb{H}^1_\Sigma$.

Let us recall the following exact sequence from K-theory

$$\ldots \longrightarrow K_1(\Lambda) \longrightarrow K_1(\Lambda_{S^*}) \xrightarrow{\partial} K_0(\mathfrak{M}_H(G)) \longrightarrow K_0(\Lambda) \longrightarrow K_0(\Lambda_{S^*}) \to 0,$$

where, we recall, $\mathfrak{M}_H(G)$ is the category of finitely generated Λ-modules that are S^*-torsion. Note that we have a canonical map $K_0(S\text{-tor}) \longrightarrow K_0(\mathfrak{M}_H(G))$, where S-tor denotes the category of finitely generated Λ-modules that are S-torsion.

Remark 2.4.40 (S^*-torsion modules). (i) Recall the definition of the compatible system $u(\mathfrak{q})$ of elliptic units

$$u(\mathfrak{q}) \in \varprojlim_{k,n}\big((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\big) \subset \bar{\mathcal{E}}_\infty \subset \mathcal{U}_\infty$$

from definition 2.4.24. The module $\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty$ is always $\Lambda(G)$-torsion, see ([Rub91], Corollary 7.8). We want to remark that under the assumption that $\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty$ is not only $\Lambda(G)$-torsion but even S^*-torsion, $\mathbb{H}^1_\Sigma/\Lambda u(\mathfrak{q})$ is also S^*-torsion. In fact, let us fix an auxilliary prime ideal $\mathfrak{c}$ of K prime to $6p\mathfrak{f}$. Then $y_\mathfrak{c} := 1 - (\mathfrak{c}, K_\infty/K) \in I$ belongs to S, see lemma A.9.3. Corollary 2.4.26 shows that $\mathbb{L}$ induces an isomorphism

$$\mathcal{D}_\infty\big/\Lambda y_\mathfrak{c} u(\mathfrak{q}) \cong IJ\lambda\big/\Lambda y_\mathfrak{c} x_\mathfrak{q}\lambda,$$

and these modules are S-torsion since $y_{\mathfrak{c}}x_{\mathfrak{q}}$ belongs to S, see lemmata A.9.2 and A.9.3. In theorem 2.4.16 we have seen that $\mathcal{C}_\infty/\mathcal{D}_\infty$ is S-torsion. Hence, $\mathcal{C}_\infty/\Lambda y_{\mathfrak{c}}u(\mathfrak{q})$ is S-torsion. Under the assumption that $\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty$ is S^*-torsion, we see that $\bar{\mathcal{E}}_\infty/\Lambda y_{\mathfrak{c}}u(\mathfrak{q})$ is S^*-torsion. Since $\Lambda u(\mathfrak{q})\big/\Lambda y_{\mathfrak{c}}u(\mathfrak{q})$ is S-torsion, we conclude that $\bar{\mathcal{E}}_\infty/\Lambda u(\mathfrak{q}) \cong \mathbb{H}^1_\Sigma/\Lambda u(\mathfrak{q})$ is S^*-torsion.

(ii) It is also a fact that $\mathcal{A}_\infty = \varprojlim_{k,n}\big(Cl(K_{k,n})\{p\}\big)$ is always $\Lambda(G)$-torsion, see ([Rub91], Theorem 5.4). Recall remark 2.3.5, where we explained that the assumption of $\mathcal{A}_\infty$ being S^*-torsion is equivalent to $\mathbb{H}^2_\Sigma$ being S^*-torsion, which follows from (2.3.2) and corollary 2.4.34.

(iii) Lastly, we want to remark that we may conclude from Rubin's main theorem 4.1 (i) in [Rub91] (proof of the 2-variable main conjecture), that $\mathcal{A}_\infty$ being S^*-torsion is equivalent to $\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty$ being S^*-torsion. Indeed, this follows from the fact, as Rubin shows, that $\mathcal{A}_\infty$ and $\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty$ have the same characteristic ideal. In conclusion, if we assume that either $\mathcal{A}_\infty$ or $\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty$ is S^*-torsion, then the other is S^*-torsion and by (i) and (ii) $\mathbb{H}^1_\Sigma/\Lambda u(\mathfrak{q})$ and $\mathbb{H}^2_\Sigma$ are S^*-torsion.

(iv) For the previous point (iii) we should note that for our G $((\cong \mathbb{Z}_p^\times)^2)$ one can show that a finitely generated pseudo-null (in the sense of Rubin [Rub91]) $\Lambda(G)$-module M is S^*-torsion.

For an Artin character $\chi : G_K \longrightarrow \mathbb{C}^\times$ factoring through $G(K_{k,n}/K)$ we write

$$L_{\Sigma_f}(\chi, s) = \sum_{\substack{\mathfrak{b}\subset\mathcal{O}_K\\(\mathfrak{b},\Sigma_f)=1}} \frac{\chi(\mathfrak{b})}{N(\mathfrak{b})^s} \qquad s\in\mathbb{C},\ \Re(s)>1$$

for the L-function attached to χ, where $\chi(\mathfrak{b}) = \chi((\mathfrak{b}, K_{k,n}/K))$. This L-function can also be expressed in terms of partial ζ-functions

$$L_{\Sigma_f}(\chi, s) = \sum_{\sigma\in G(K_{k,n}/K)} \chi(\sigma)\zeta_{K_{k,n}/K,\Sigma}(\sigma, s) \qquad s\in\mathbb{C},\ \Re(s)>1,$$

where

$$\zeta_{K_{k,n}/K,\Sigma}(\sigma, s) = \sum_{\substack{\mathfrak{b}\subset\mathcal{O}_K,(\mathfrak{b},\Sigma_f)=1\\(\mathfrak{b},K_{k,n}/K)=\sigma}} \frac{1}{N(\mathfrak{b})^s} \qquad s\in\mathbb{C},\ \Re(s)>1.$$

Theorem 2.4.41 (Commutative main theorem). *Assume that $\mathfrak{f} = \mathfrak{l}^r$ for some prime $\mathfrak{l}$ of K. Moreover, assume that $\mathcal{A}_\infty = \varprojlim_{k,n}(Cl(K_{k,n})\{p\})$ is S^*-torsion. Then, under the connecting homomorphism ∂, the class $[1/x_{\mathfrak{q}}] \in K_1(\Lambda_{S^*})$ of the element $\frac{1}{x_{\mathfrak{q}}} \in \Lambda_S^\times$ maps to*

$$\partial\big([1/x_{\mathfrak{q}}]\big) = -[\Lambda/\Lambda x_{\mathfrak{q}}] = [\mathbb{H}^2_\Sigma] - [\mathbb{H}^1_\Sigma/\Lambda u(\mathfrak{q})] \quad \text{in} \quad K_0(\mathfrak{M}_H(G)). \tag{2.4.66}$$

Moreover, $\frac{1}{x_{\mathfrak{q}}} = \frac{1}{(N\mathfrak{q}-\sigma_{\mathfrak{q}})}$ *satisfies the following interpolation property. Let* χ *be a complex Artin character* $\chi : G_K \longrightarrow \mathbb{C}^\times$ *such that the fixed field of the kernel is equal to* $\bar{K}^{\ker(\chi)} = K_{k,n}$, $k, n \geq 1$. *Then,* χ *has conductor* $\mathfrak{f}_\chi = \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$ *and we have (Kronecker's second limit formula)*

$$\frac{d}{ds}L_{\Sigma_f}(\chi, s)\mid_{s=0} = -\frac{1}{N\mathfrak{q} - \chi(\sigma_{\mathfrak{q}})} \cdot \frac{1}{12\omega_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}} \cdot \sum_{\sigma \in G(K_{k,n}/K)} \log \mid \sigma(e_{k,n}(\mathfrak{q})) \mid^2 \chi(\sigma), \tag{2.4.67}$$

where $e_{k,n}(\mathfrak{q}) = N_{F_{k,n}/K_{k,n}}(e'_{k,n}(\mathfrak{q})) \in \mathcal{O}^\times_{K_{k,n}}$ *so that* $u(\mathfrak{q})$ *is the image of* $(e_{k',n'}(\mathfrak{q}))_{k',n'}$ *in* $\mathcal{U}_\infty$ *and* $\omega_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}$ *denotes the number of roots of unity in* K *congruent to* 1 *modulo* $\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$.

Before we give a proof of the theorem let us make a remark about the interpolation property.

Remark 2.4.42. (i) The interpolation property is derived from a classical result known as Kronecker's second limit formula. For the connection to the rank one abelian Stark conjecture, we refer to Tate's book [Tat84], Stark's original paper [Sta80] and the course notes [DG11].

(ii) The requirement on χ that $\bar{K}^{\ker(\chi)} = K_{k,n}$, $k, n \geq 1$ is rather strong. We can relax the condition slightly by requiring only that χ has conductor $\mathfrak{f}_\chi = \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$ (which follows from the stronger requirement) and then get the interpolation property as in (2.4.74) with the units $e'_{k,n}(\mathfrak{q}) \in \mathcal{O}^\times_{F_{k,n}}$ instead of $e_{k,n}(\mathfrak{q}) \in \mathcal{O}^\times_{K_{k,n}}$.

(iii) A question that immediately arises from (2.4.67) is: when are both sides of the equation unequal to 0? An answer is provided by the following fact: In the course notes [DG11] there is a formula for the order of vanishing $r_\Sigma(\chi)$ of $L_{\Sigma_f}(\chi, s)$ at $s = 0$, see (loc. cit., equation (1.11)), it is given by

$$r_\Sigma(\chi) = \begin{cases} \#\{\nu \in \Sigma \mid \chi(G_\nu) = 1\} & \text{if } \chi \neq 1, \\ \#\Sigma - 1 & \text{if } \chi = 1, \end{cases}$$

where G_ν denotes the decomposition group at a place $\nu \in \Sigma = \Sigma_f \cup \Sigma_\infty$. In particular, since the complex archimedean place $\nu = \nu_\infty \in \Sigma_\infty$ of K has trivial decomposition group, i.e., $G(K_{k,n}/K)_{\nu_\infty} = 1$, we see that $r_\Sigma(\chi) \geq 1$ for all χ. On the other hand, if χ is ramified at the other primes, i.e., at the primes in Σ_f, then $r_\Sigma(\chi) = 1$. Moreover, we see that (2.4.67) always holds for the trivial character χ, since both sides are equal to 0; for the left hand side, note that $\#\Sigma = 4$ and for the right hand side note that $e_{k,n}(\mathfrak{q})$ is a unit so that

$$\sum_{\sigma \in G(K_{k,n}/K)} \log \mid \sigma(e_{k,n}(\mathfrak{a})) \mid^2 = \log \mid N_{K_{k,n}/K}\sigma(e_{k,n}(\mathfrak{a})) \mid^2 = 0$$

since $N_{K_{k,n}/K}\sigma(e_{k,n}(\mathfrak{a}))$ is a unit in K, i.e., a root of unit, and therefore has absolute value 1.

We also want to make a remark about some identifications that we will use without mentioning.

Remark 2.4.43. (i) For this remark let G be any profinite group and H any closed subgroup of G, not necessarily of finite index. Then we consider $\mathbb{Z}_p$ equipped with the trivial H action, which extends to an action of $\Lambda(H)$. Write $\operatorname{aug}_H : \Lambda(H) \to \mathbb{Z}_p$ for the augmentation map. The action of $\delta \in \Lambda(H)$ on $a \in \mathbb{Z}_p$ is then given by $\delta.a = \operatorname{aug}_H(\delta)a$. If H is normal in G, write $I(H)$ for the kernel of the map $pr : \Lambda(G) \twoheadrightarrow \Lambda(G/H)$. The ideal $I(H)$ is generated by elements of the form $1-h$, $h \in H$. For H normal in G we then have an isomorphism

$$\Lambda(G) \otimes_{\Lambda(H)} \mathbb{Z}_p \xrightarrow{\sim} \Lambda(G/H), \quad \lambda \otimes a \longmapsto pr(\lambda)a. \tag{2.4.68}$$

Indeed, first note that $\Lambda(G) \times \mathbb{Z}_p \to \Lambda(G/H)$ is $\Lambda(H)$-bilinear which follows from the fact that for $\delta \in \Lambda(H)$ we have $pr(\delta) = \operatorname{aug}_H(\delta)$. Secondly, note that the inverse of the map in (2.4.68) is induced by $\Lambda(G) \to \Lambda(G) \otimes_{\Lambda(H)} \mathbb{Z}_p$, $\lambda \mapsto \lambda \otimes 1$, which factors through $I(H)$.

(ii) Now, assume that $\Lambda(H)$ is Noetherian, which holds, e.g., if H is a p-adic Lie group. Then, we have

$$\text{c}-\operatorname{Ind}_G^H \mathbb{Z}_p \overset{\text{def}}{=} \Lambda(G) \hat{\otimes}_{\Lambda(H)} \mathbb{Z}_p \cong \Lambda(G) \otimes_{\Lambda(H)} \mathbb{Z}_p,$$

where the module on the left is the compact induction and the isomorphism follows from ([Wit03], Proposition 1.1.4 (2)) which says that for finitely presented modules the usual and the completed tensor product coincide, just note that $\mathbb{Z}_p$ is finitely presented as a $\Lambda(H)$-module since by the assumption that $\Lambda(H)$ is Noetherian, the kernel $I(H)$ of the augmentation map $\Lambda(H) \twoheadrightarrow \mathbb{Z}_p$ is finitely generated.

(iii) Lastly, we note that if H is of finite index and normal in G, then

$$\Lambda(G) \otimes_{\Lambda(H)} \mathbb{Z}_p \cong \Lambda(G/H) = \mathbb{Z}_p[G/H] \cong \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[H]} \mathbb{Z}_p = \operatorname{Ind}_G^H \mathbb{Z}_p,$$

where Ind_G^H is just the usual induction.

Proof (of theorem 2.4.41). We first consider the relations in $K_0(\mathfrak{M}_H(G))$. We will use repeatedly corollary 1.2.3 from section 1.2 stating that classes $[M] \in K_0(\mathfrak{M}_H(G))$ of modules M that are finitely generated as $\mathbb{Z}_p$-modules are equal to the zero class, compare remark 2.4.36. We fix an auxilliary prime ideal $\mathfrak{c}$ of K prime to $6p\mathfrak{f}$. Then $y_\mathfrak{c} := 1 - (\mathfrak{c}, K_\infty/K)$ is not a zero-divisor in Λ. In fact, $y_\mathfrak{c}$ even belongs to S, see lemma A.9.3. We then have

$$\begin{aligned}
[\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty] - [\bar{\mathcal{E}}_\infty/\Lambda y_\mathfrak{c} u(\mathfrak{q})] &= -[\mathcal{C}_\infty/\Lambda y_\mathfrak{c} u(\mathfrak{q})] \\
&= -[\mathcal{D}_\infty/\Lambda y_\mathfrak{c} u(\mathfrak{q})] - [\mathcal{C}_\infty/\mathcal{D}_\infty] \\
&= -[IJ\lambda/\Lambda y_\mathfrak{c} x_\mathfrak{q}\lambda] - [\Lambda(G/D_\mathfrak{l})] \\
&= -[IJ/\Lambda y_\mathfrak{c} x_\mathfrak{q}] - [\Lambda(G/D_\mathfrak{l})] \\
&= -[\Lambda/\Lambda y_\mathfrak{c} x_\mathfrak{q}] - [\Lambda(G/D_\mathfrak{l})],
\end{aligned} \tag{2.4.69}$$

where the first two equations follow from the exact sequences

$$0 \to \mathcal{C}_\infty/\Lambda y_{\mathfrak{c}} u(\mathfrak{q}) \to \bar{\mathcal{E}}_\infty/\Lambda y_{\mathfrak{c}} u(\mathfrak{q}) \to \bar{\mathcal{E}}_\infty/\mathcal{C}_\infty \to 0$$

and

$$0 \to \mathcal{D}_\infty/\Lambda y_{\mathfrak{c}} u(\mathfrak{q}) \to \mathcal{C}_\infty/\Lambda y_{\mathfrak{c}} u(\mathfrak{q}) \to \mathcal{C}_\infty/\mathcal{D}_\infty \to 0,$$

the third equation follows from corollary 2.4.26 and theorem 2.4.33, the fourth equation from the fact that λ is not a zero-divisor, see proposition 2.4.28, and the last equation from the fact that

$$[\Lambda/IJ] = [\Lambda/(I \cap J)] = 0,$$

where the first equality is lemma 2.4.39 and the second stems from the fact that $\Lambda/(I \cap J)$ embeds into the finitely generated $\mathbb{Z}_p$-module $\mathbb{Z}_p \oplus \mathbb{Z}_p(1)$.

Recall that $\mathbb{L}(u(\mathfrak{q})) = 12 x_{\mathfrak{q}} \lambda$. Then, using the isomorphism $\bar{\mathcal{E}}_\infty/\Lambda y_{\mathfrak{c}} u(\mathfrak{q}) \cong \mathbb{L}(\bar{\mathcal{E}}_\infty)/\Lambda y_{\mathfrak{c}} x_{\mathfrak{q}} \lambda$ and the fact that $x_{\mathfrak{q}}\lambda$ is not a zero-divisor one sees that

$$[\bar{\mathcal{E}}_\infty/\Lambda y_{\mathfrak{c}} u(\mathfrak{q})] = [\bar{\mathcal{E}}_\infty/\Lambda u(\mathfrak{q})] + [\Lambda/\Lambda y_{\mathfrak{c}}].$$

Similarly, using that $x_{\mathfrak{q}}$ is not a zero-divisor, we see that

$$[\Lambda/\Lambda y_{\mathfrak{c}} x_{\mathfrak{q}}] = [\Lambda/\Lambda x_{\mathfrak{q}}] + [\Lambda/\Lambda y_{\mathfrak{c}}].$$

It follows from (2.4.69) that we have an equation

$$[\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty] - [\bar{\mathcal{E}}_\infty/\Lambda u(\mathfrak{q})] = -[\Lambda/\Lambda x_{\mathfrak{q}}] - [\Lambda(G/D_{\mathfrak{l}})], \tag{2.4.70}$$

in which the auxilliary element $y_{\mathfrak{c}}$ no longer appears. Now, we use Rubin's main result on the two variable main conjecture, see ([Rub91], theorem 4.1 (i)), stating that

$$[\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty] = [\mathcal{A}_\infty], \tag{2.4.71}$$

where $A_\infty = \varprojlim_{k,n}(Cl(K_{k,n})\{p\})$ is the projective limit over the p-primary parts of the ideal class groups $Cl(K_{k,n})$. It follows that

$$-[\Lambda/\Lambda x_{\mathfrak{q}}] = [\mathcal{A}_\infty] + [\Lambda(G/D_{\mathfrak{l}})] - [\bar{\mathcal{E}}_\infty/\Lambda u(\mathfrak{q})]. \tag{2.4.72}$$

Note that Σ_f, the set of finite primes of K above p and those that ramify in K_∞/K, by our assumption on the conductor $\mathfrak{f}$, is given by $\{\mathfrak{p}, \bar{\mathfrak{p}}, \mathfrak{l}\}$. The decomposition groups of $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ have finite index in G. Therefore, the map from (A.3.26) has a kernel which is a finitely generated $\mathbb{Z}_p$-module, showing that

$$[\mathcal{A}_\infty] = [\varprojlim_{k,n}(\mathrm{Pic}(\mathcal{O}_{K_{k,n},\Sigma})\{p\})].$$

The modules $\varprojlim_{k,n}(\mathrm{Pic}(\mathcal{O}_{K_{k,n},\Sigma})\{p\})$ and $\Lambda(G/D_{\mathfrak{l}}) \cong \Lambda(G) \otimes_{\Lambda(D_{\mathfrak{l}})} \mathbb{Z}_p$ appear in the exact sequence (A.3.25), yielding

$$[\mathbb{H}^2_\Sigma] = [\varprojlim_{k,n}(\mathrm{Pic}(\mathcal{O}_{K_{k,n},\Sigma})\{p\})] + [\Lambda(G/D_{\mathfrak{l}})], \tag{2.4.73}$$

where we used that $\mathrm{Ind}_G^{D_{\mathfrak{p}}}\mathbb{Z}_p$ and $\mathrm{Ind}_G^{D_{\bar{\mathfrak{p}}}}\mathbb{Z}_p$ are finitely generated over $\mathbb{Z}_p$. Together with (2.2.3) (note that $\Sigma_{ur} = \varnothing$ since $\bar{\mathfrak{p}}$ (resp. $\mathfrak{p}$) is unramified in $\cup_{n\geq 1}K(E[\pi^n])$ (resp. $\cup_{k\geq 1}K(E[\bar{\pi}^k])$), we can rewrite (2.4.72) as

$$-[\Lambda/\Lambda x_{\mathfrak{q}}] = [\mathbb{H}^2_\Sigma] - [\mathbb{H}^1_\Sigma/\Lambda u(\mathfrak{q})],$$

which is what we wanted to prove.

Next, we determine the interpolation property of $x_{\mathfrak{a}}$ for $\mathfrak{a}$ prime to $6p\mathfrak{f}$, which, as noted above, is derived from Kronecker's (second) limit formula. The latter has already been stated in the form in which we want to use it in an article by Flach, see ([Fla09], Lemma 2.2 e), p. 265f). For a lattice $L \subset \mathbb{C}$, $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, Flach defines a Theta-function $\varphi(z,\tau)$, where $\tau = \frac{\omega_1}{\omega_2}$. In ([dS87], II, 2.1) De Shalit defines a Theta-function $\theta(z,L)$ and thanks to the product expansion of $\theta(z,L/\omega_2)$ for the normalized lattice L/ω_2 one immediately derives an equality

$$\theta(z,L/\omega_2) = \varphi(z,\tau)^{12}.$$

Using the monogeneity property of θ, one can now show for an integral ideal $\mathfrak{a}$ of K, $(\mathfrak{a},6)=1$, that the 12-th power of Flach's function $\psi(z,L,\mathfrak{a}^{-1}L)$ is given by

$$\psi(z,L,\mathfrak{a}^{-1}L)^{12} = \Theta(z,L,\mathfrak{a}).$$

For an integral ideal $\mathfrak{g}$ of K, considered as a lattice in $\mathbb{C}$ and generated over $\mathcal{O}_K$ by g, it follows that

$$\psi(1,\mathfrak{g},\mathfrak{a}^{-1}\mathfrak{g})^{12} = \Theta(1,\mathfrak{g},\mathfrak{a}) = \Theta\Big(\frac{\Omega}{g},L,\mathfrak{a}\Big)$$

and we see that Flach's element

$$ {}_{\mathfrak{a}}z_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n} := \psi(1,\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n,\mathfrak{a}^{-1}\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$$

is a twelfth root of our $e'_{k,n}(\mathfrak{a}) = \Theta\Big(\frac{\Omega}{f\bar{\pi}^k\pi^n},L,\mathfrak{a}\Big) \in \mathcal{O}^\times_{F_{k,n}}$, recall that we write $F_{k,n} = K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$.

Now, let χ be an Artin character as in the statement of the theorem. The claim that χ has conductor $\mathfrak{f}_\chi = \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$ follows from a fact from the theory of Artin conductors, see ([Neu07], VII, §11, (11.10) Satz), and the fact that $K_{k,n}$ has conductor $\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$, see lemma 2.4.17.

Racall that $F_{k,n} = K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$. Kronecker's second limit formula, as stated in ([Fla09], Lemma 2.2 e), p. 265f), says

$$\begin{aligned}\frac{d}{ds}L_{\Sigma_f}(\chi,s)\,|_{s=0} &= -\frac{1}{N\mathfrak{a}-\chi(\sigma_{\mathfrak{a}})}\cdot\frac{1}{\omega_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}}\cdot\sum_{\sigma\in G(F_{k,n}/K)}\log|\,\sigma({}_{\mathfrak{a}}z_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n})\,|^2\,\chi(\sigma)\\ &= -\frac{1}{N\mathfrak{a}-\chi(\sigma_{\mathfrak{a}})}\cdot\frac{1}{12\omega_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}}\cdot\sum_{\sigma\in G(F_{k,n}/K)}\log|\,\sigma(e'_{k,n}(\mathfrak{a}))\,|^2\,\chi(\sigma)\end{aligned} \tag{2.4.74}$$

where $\omega_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}$ denotes the number of roots of unity in K congruent to 1 modulo $\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$. Note that $\omega_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}$ divides 12. Since χ factors through $G(K_{k,n}/K)$, we immediately conclude that

$$\frac{d}{ds}L_{\Sigma_f}(\chi,s)\,|_{s=0} = -\frac{1}{N\mathfrak{a}-\chi(\sigma_{\mathfrak{a}})}\cdot\frac{1}{12\omega_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}}\cdot\sum_{\sigma\in G(K_{k,n}/K)}\log|\,\sigma(e_{k,n}(\mathfrak{a}))\,|^2\,\chi(\sigma), \tag{2.4.75}$$

where $e_{k,n}(\mathfrak{a}) = N_{F_{k,n}/K_{k,n}}(e'_{k,n}(\mathfrak{a})) \in \mathcal{O}^{\times}_{K_{k,n}}$. Compare also the limit formulas in ([dS87], II, §5, p. 88) and ([Kat04], section 15, p. 252). □

Chapter 3

Local Main Conjecture

In this chapter we study a local conjecture due to Kato that, as the global conjecture from the previous chapter, he stated during a talk in Cambridge on the occasion of John Coates' sixtieth birthday. The conjecture presented here concerns a p-adic Lie extensions $F_\infty/\mathbb{Q}_p$ and the *universal case* $T = \mathbb{Z}_p(1)$. The idea is to prove the universal case and then derive analogous results for more general representations T through twisting (and induction), compare corollary A.3.10. For general conjectures concerning local ϵ-isomorphisms see [Kat] and [FK06].

Venjakob's article [Ven13], based on Kato's work [Kat], contains a proof of the existence of ϵ-isomorphisms in certain abelian cases (arising from twists of the universal case). In the same article Venjakob shows that the existence of ϵ-isomorphisms implies the algebraic part of the (abelian version of the) local main conjecture studied in this thesis. The purpose of this chapter is to build on these results and prove the analytic part of the abelian local main conjecture, i.e., to determine the interpolation property of $\mathcal{E}_{u'} = \mathcal{E}_{p,u'}$, see conjecture 3.2.2 for the precise statement.

For basic facts about local fields that are used, see [Cas03] and [Ser95].

3.1 Setting

We fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and a generator $\epsilon = (\epsilon_n)_n = (\zeta_{p^n})_n$ of $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}$, where μ_{p^n}, $n \geq 1$, denotes the group of p^n-th roots of unities in $\overline{\mathbb{Q}}_p$. We note that this choice determines a unique homomorphism $\psi_\epsilon : \mathbb{Q}_p \longrightarrow \mathbb{C}_p^\times$ with kernel $\ker(\psi_\epsilon) = \mathbb{Z}_p$, such that $\psi_\epsilon(1/p^n) = \zeta_{p^n}$.

For an arbitrary, possibly infinite algebraic extension $L/\mathbb{Q}_p$ we set

$$\mathcal{U}'(L) = \varprojlim_{L',m} \mathcal{O}_{L'}^\times/(\mathcal{O}_{L'}^\times)^{p^m},$$

where the limit is taken over all finite subextensions $L'/\mathbb{Q}_p$ of $L/\mathbb{Q}_p$ with respect to norm maps and all $m \in \mathbb{N}$ with respect to the natural projections. Here, $\mathcal{O}_{L'}^\times$ is the unit group of the ring of integers $\mathcal{O}_{L'}$ of L'. For any extension F/L, there is a canonical projection map

$$\mathcal{U}'(F) \longrightarrow \mathcal{U}'(L).$$

Convention 3.1.1. *In general, unless specified otherwise, we use the notation $()'$ for objects related to a local setting.*

In this chapter we consider the cohomology groups

$$\mathbb{H}^i_{\text{loc}} = \mathrm{H}^i(\mathbb{Q}_p, \mathbb{T}_{un}), \quad i = 1, 2,$$

where the definition of $\mathbb{T}_{un} = \mathbb{T}_{un}(F_\infty)$ is as follows, compare [Ven13]. We write $\mathcal{G}'$ for the Galois group $\mathrm{Gal}(F_\infty/\mathbb{Q}_p)$ of a not necessarily abelian p-adic Lie extension $F_\infty/\mathbb{Q}_p$. Then, we define the universal module $\mathbb{T}_{un}$ by

$$\mathbb{T}_{un} = \Lambda(\mathcal{G}')^{\#}(1), \tag{3.1.1}$$

where (1) denotes the Tate twist and $\Lambda(\mathcal{G}')^{\#}$ is just $\Lambda(\mathcal{G}')$ as a $\Lambda(\mathcal{G}')$-module, but has the following action of $G_{\mathbb{Q}_p}$. An element $g \in G_{\mathbb{Q}_p}$ acts on $\lambda \in \Lambda(\mathcal{G}')$ by $g.\lambda = \lambda \overline{g}^{-1}$, where $\overline{g}$ is the image of g in $\mathcal{G}'$.

Using (A.3.12) and the Kummer sequence for local fields, we get isomorphisms

$$\mathbb{H}^1_{\text{loc}} \cong \varprojlim_{\mathbb{Q}_p \subset_f F \subset F_\infty} H^1(F, \mathbb{Z}_p(1)) \cong \varprojlim_{F,m} F^\times/(F^\times)^{p^m},$$

where $\subset_f$ means that $F/\mathbb{Q}_p$ is a finite extension. For extensions $F_\infty/\mathbb{Q}_p$ of infinite residue degree, compare ([Ven13], section 2.1), we have

$$\mathcal{U}'(F_\infty) \cong \mathbb{H}^1_{\text{loc}}.$$

Convention 3.1.2. *For the reciprocity map from local class field theory for a general non-archimedean local field F we assume that a prime element π_F of F corresponds to a geometric Frobenius element φ_{geo}, i.e. a map that, on an algebraic closure $\overline{k}_F$ of the residue field k_F of F, corresponds to $x \longmapsto x^{\frac{1}{q_F}}$ where q_F is the number of elements of k_F. Writing $W(\bar{F}/F)$ for the Weil group and I_F for the inertia group, as in [Del73], we then have a commutative diagram*

$$\begin{array}{ccccc} I_F & \longrightarrow & W(\bar{F}/F) & \longrightarrow & \mathbb{Z} \\ \big\downarrow & & \big\downarrow {\scriptstyle \varphi_{geo} \mapsto \pi_F} & & \big\downarrow {\scriptstyle \cdot(-1)} \\ \mathcal{O}_F^\times & \longrightarrow & F^\times & \xrightarrow{v_F} & \mathbb{Z} \end{array} \tag{3.1.2}$$

where v_F is the valuation of F and the upper horizontal map is defined as the composite $G_F \twoheadrightarrow G_{\overline{k}_F} \to \hat{\mathbb{Z}}$ where the second map sends the arithmetic Frobenius to 1.

Remark 3.1.3. Convention 3.1.2 is in line with the conventions in Deligne's article [Del73], compare ([Del73], p. 523), Tate's article [Tat79], compare ([Tat79], p. 6), and the conventions in the book [BH06] by Bushnell and Henniart, compare ([BH06], p. 186).

Recall that for any topological ring A, we write $\mathcal{PC}(A)$ for the category of pseudo-compact A-modules with continuous homomorphisms as morphisms, which is an abelian category, see ([Gab62], Chapitre IV, §3, Théorème 3) - as remarked in [Wit03], the proof in [Gab62] of this fact does not require A to be pseudo-compact. In proposition A.8.17 we prove in greater generality that the functor

$$\mathcal{PC}(\mathbb{Z}_p) \longrightarrow \mathcal{PC}(\hat{\mathbb{Z}}_p^{ur}), \quad N \longrightarrow \hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} N \tag{3.1.3}$$

is exact. Assume that the p-adic Lie group $\mathcal{G}' = G(F_\infty/\mathbb{Q}_p)$ contains a closed normal subgroup $\mathcal{H}'$ such that

$$\mathcal{G}'/\mathcal{H}' \cong \mathbb{Z}_p.$$

Let us write $\Lambda' = \Lambda(\mathcal{G}')$ and

$$\tilde{\Lambda}' = \Lambda(\mathcal{G}', \hat{\mathbb{Z}}_p^{ur})$$

for the Iwasawa algebra of $\mathcal{G}'$ with coefficients in $\hat{\mathbb{Z}}_p^{ur}$ and note that

$$\tilde{\Lambda}' \cong \hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} \Lambda'.$$

We recall our convention that any Λ'-module is a Hausdorff topological Λ'-module. Hence, any such compact Λ'-module M is the projective limit of finite Λ'-modules, see ([NSW08], (5.2.4) Proposition). Therefore, compact Λ'-modules M are *pseudo-compact* as Λ'-modules (and as $\mathbb{Z}_p$-modules) in the sense of [Wit03].

Remark 3.1.4. As explained in remark A.8.18 we have a natural isomorphism

$$\tilde{\Lambda}' \otimes_{\Lambda'} M \cong \hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} M \tag{3.1.4}$$

induced by the universal property of $- \otimes_{\Lambda'} -$.

As in (A.8.1) and (A.8.2) we define canonical Ore sets of Λ' and $\tilde{\Lambda}'$

$$\mathcal{S}' \subset \mathcal{S}'^* \subset \Lambda' \qquad \text{and} \qquad \tilde{\mathcal{S}}' \subset \tilde{\mathcal{S}}'^* \subset \tilde{\Lambda}'$$

and refer to section A.8 of the appendix for basic properties of these Ore sets.

Remark 3.1.5. Since $\hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} -$ is exact on $\mathcal{PC}(\mathbb{Z}_p)$ by (3.1.3) and since finitely generated Λ'-modules are pseudo-compact over $\mathbb{Z}_p$ we see from (A.8.12) that $\tilde{\Lambda}' \otimes_{\Lambda'} -$ is an exact functor from the category of finitely generated Λ'-modules to the category of finitely generated $\tilde{\Lambda}'$-modules. Lemma A.8.20 then shows that there is a map

$$K_0(\mathfrak{M}_{\mathcal{H}'}(\mathcal{G}')) \longrightarrow K_0(\mathfrak{M}_{\hat{\mathbb{Z}}_p^{ur}, \mathcal{H}'}(\mathcal{G}')), \quad [M] \longrightarrow [\tilde{\Lambda}' \otimes_{\Lambda'} M] = [\hat{\mathbb{Z}}_p^{ur} \hat{\otimes}_{\mathbb{Z}_p} M],$$

for which we also note that $\mathcal{S}' \subset \tilde{\mathcal{S}}'$ by lemma A.8.19.

3.2 Statement of the Local Main Conjecture

We make the following assumption, which is satisfied by the isomorphism from (3.3.8) in the setting considered in section 3.3, i.e., the setting considered by Venjakob in [Ven13].

Assumption 3.2.1. *There exists $u' \in \mathcal{U}'(F_\infty)$ such that*

$$\Lambda(\mathcal{G}')_{\mathcal{S}'} \to \mathcal{U}'(F_\infty)_{\mathcal{S}'}, \qquad 1 \longmapsto u',$$

is an isomorphism of $\Lambda(\mathcal{G}')_{\mathcal{S}'}$-modules. We will say that u is a local generator of $\mathcal{U}'(F_\infty)$.

As above we write $\tilde{\Lambda}' = \Lambda(\mathcal{G}', \hat{\mathbb{Z}}_p^{ur})$ and $\tilde{\mathcal{S}}'$ and $\tilde{\mathcal{S}}'^*$ for the Ore sets in $\tilde{\Lambda}'$. We now state the local main conjecture.

Conjecture 3.2.2 (Local Main Conjecture). *There exists $\mathcal{E}_{p,u'} \in K_1(\tilde{\Lambda}'_{\tilde{\mathcal{S}}'^*})$ such that*

(i) for any Artin representation $\rho : \mathcal{G}' \longrightarrow \mathrm{Aut}_{\mathbb{C}_p}(V)$,

$$\mathcal{E}_{p,u'}(\rho) = \frac{\epsilon_p(\rho)}{R_p(u', \rho)} \tag{3.2.1}$$

if $R_p(u', \rho) \neq 0$,

(ii) the image of $\mathcal{E}_{p,u'}$ under the connecting homomorphism from K-theory is given by

$$\partial(\mathcal{E}_{p,u'}) = \left[\tilde{\Lambda}' \otimes_{\Lambda'} \mathbb{H}^2_{\mathrm{loc}}\right] - \left[\tilde{\Lambda}' \otimes_{\Lambda'} \left(\mathbb{H}^1_{\mathrm{loc}}/\Lambda' u'\right)\right] \quad \text{in} \quad K_0(\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}}, \mathcal{H}'}(\mathcal{G}')). \tag{3.2.2}$$

We will also write $\mathcal{E}_{u'} = \mathcal{E}_{p,u'}$. In the above equation $\epsilon_p(\rho) = \epsilon_p(V)$ is the local constant attached to V and $R_p(u', \rho)$ is the p-adic regulator associated to ρ and u', see subsection 3.3.3. At the end of section 2 in [Ven13] an element $\mathcal{E}_{p,u'}$ satisfying (3.2.2) is given explicitly under the assumption that $F_\infty/\mathbb{Q}_p$ is an abelian p-adic Lie extension of the form $K'(\mu_{p^\infty})$, where K' is an infinite unramified extension of $\mathbb{Q}_p$. We will prove that in this case $\mathcal{E}_{p,u'}$ has the desired interpolation property (3.2.1) for Artin characters.

3.3 Interpolation Property

In order to determine the values of $\mathcal{E}_{p,u'}$ at Artin characters in the abelian setting, let us recall its construction. In particular, we need to review Coleman's interpolation theory for the multiplicative formal group, see Coleman's article [Col79] for general Lubin-Tate groups and also [Col83] for applications; there is also a summary contained in [dS87] and for the theory over $\mathbb{Q}_p$ compare [CS06].

3.3.1 Coleman map

For any $L/\mathbb{Q}_p$ we set $L_n = L(\mu_{p^n})$ and $L_\infty = \bigcup_n L_n$. We assume throughout the rest of this chapter that $K'/\mathbb{Q}_p$ is an unramified Galois extension of infinite degree and that $\mathcal{G}' = \mathrm{Gal}(K'_\infty/\mathbb{Q}_p)$ is a p-adic Lie group. As noted in [Ven13], these assumptions imply that $\mathcal{G}' \cong \mathbb{Z}_p^2 \times \Delta'$, where Δ' is a finite group of order prime to p. There is also a decomposition of $\mathcal{G}'$

$$\mathcal{G}' \cong \Gamma \times H \tag{3.3.1}$$

into the ramified part $\Gamma = G(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$ and the unramified part $H = G(K'/\mathbb{Q}_p)$. We will write Λ' for $\Lambda(\mathcal{G}')$ and

$$\tilde{\Lambda}' := \Lambda' \hat{\otimes}_{\mathbb{Z}_p} \widehat{\mathbb{Z}_p^{ur}} \cong \widehat{\mathbb{Z}_p^{ur}}[[\mathcal{G}']]$$

for the Iwasawa algebra of $\mathcal{G}'$ with $\widehat{\mathbb{Z}_p^{ur}}$-coefficients. We write ϕ for the arithmetic Frobenius (given by $a \mapsto a^p$ on residue fields) in $G(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$. Note that the action of ϕ extends to $\widehat{\mathbb{Z}_p^{ur}}$. We define an element $\varphi_p \in \mathcal{G}'$ that under the decomposition (3.3.1) corresonds to

$$\varphi_p = (id_\Gamma, \phi_{|K'}),$$

i.e., φ_p is the element that acts trivially on $\mathbb{Q}_p(\mu_{p^\infty})$ and as the arithmetic Frobenius on K'.

Let us recall the definition of $\mathcal{E}_{p,u'}$ which we will also denote by $\mathcal{E}_{u'}$. In order to do this we define a Λ' submodule of $\tilde{\Lambda}'$. We let ϕ act on $\tilde{\Lambda}'$ through its action on the coefficients and denote this action by $\phi(x)$, $x \in \tilde{\Lambda}'$. Now, we define

$$\Lambda'_{\varphi_p} := \{x \in \tilde{\Lambda}' \mid \phi(x) = \varphi_p \cdot x\},$$

where $\varphi_p \cdot x$ is multiplication in the Iwasawa algebra $\tilde{\Lambda}'$. Since ϕ acts trivially on the coefficients of any element in Λ' it is clear that Λ'_{φ_p} is a Λ'-module.

We note that for any quotient of $\mathcal{G}'$ of the form $(\Gamma/U) \times H_L$, where $H_L = G(L/\mathbb{Q}_p)$, $L \subset K'$, we can define a $\Lambda((\Gamma/U) \times H_L)$-submodule $\Lambda((\Gamma/U) \times H_L)_{\bar{\varphi}_p}$ of $\widehat{\mathbb{Z}_p^{ur}}[[(\Gamma/U) \times H_L]]$ in the same manner

$$\Lambda((\Gamma/U) \times H_L)_{\bar{\varphi}_p} := \{x \in \widehat{\mathbb{Z}_p^{ur}}[[(\Gamma/U) \times H_L]] \mid \phi(x) = \bar{\varphi}_p \cdot x\},$$

where $\bar{\varphi}_p$ denotes the image of φ_p in $\widehat{\mathbb{Z}_p^{ur}}[[(\Gamma/U) \times H_L]]$. If $(\Gamma/U) \times H_L$ is a finite quotient of $\mathcal{G}'$ then we have

$$\widehat{\mathbb{Z}_p^{ur}}[[(\Gamma/U) \times H_L]] = \widehat{\mathbb{Z}_p^{ur}}[(\Gamma/U) \times H_L] = \widehat{\mathbb{Z}_p^{ur}}[\Gamma/U][H_L]$$

and also write $\mathbb{Z}_p[\Gamma/U][H_L]_{\bar{\varphi}_p}$ for $\Lambda((\Gamma/U) \times H_L)_{\bar{\varphi}_p}$.

Next, we follow [Ven13] and explain that there is an exact sequence

$$0 \longrightarrow \mathcal{U}'(K'_\infty) \xrightarrow{\mathcal{L}_{K',\epsilon}} \mathbb{T}_{\mathrm{un}}(K'_\infty) \otimes_{\Lambda'} \Lambda'_{\varphi_p} \longrightarrow \mathbb{Z}_p(1) \longrightarrow 0 \tag{3.3.2}$$

which arises as the projective limit of the following compatible exact sequences (3.3.3). Let $L/\mathbb{Q}_p$ be a finite unramified extension contained in K', $L \subset K'$. Then, as in (3.3.1), we have a decomposition of the Galois group

$$G(L_\infty/\mathbb{Q}_p) \cong \Gamma \times H_L,$$

into a ramified and an unramified part, where $H_L = G(L/\mathbb{Q}_p)$. Writing $\Lambda'(L) = \Lambda\big(\Gamma \times H_L\big)$ there is an exact sequence

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \mathcal{U}'(L_\infty) \xrightarrow{\mathcal{L}_{L,\epsilon}} \mathbb{T}_{\mathrm{un}}(L_\infty) \otimes_{\Lambda'(L)} \Lambda'(L)_{\bar{\varphi}_p} \longrightarrow \mathbb{Z}_p(1) \longrightarrow 0, \tag{3.3.3}$$

where $\mathcal{L}_{L,\epsilon}$ is given by the composite map

$$\mathcal{U}'(L_\infty) \xrightarrow{\mathrm{Col}_{\epsilon,L}} \mathcal{O}_L[[\Gamma]] \xrightarrow{\sim} \Lambda'(L)_{\bar{\varphi}_p} \xrightarrow{\sim} \mathbb{T}_{\mathrm{un}}(L_\infty) \otimes_{\Lambda'(L)} \Lambda'(L)_{\bar{\varphi}_p}, \tag{3.3.4}$$

which we now want to explain. The third map is given by $x \longmapsto (1 \otimes \epsilon) \otimes x$, where $(1 \otimes \epsilon) \in \mathbb{T}_{un}(L_\infty) = \Lambda(\Gamma \times H_L)^{\#} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$. The second map in (3.3.4), which is an isomorphism of $\Lambda'(L)$-modules, not of algebras, is given as follows. If $d = [L : \mathbb{Q}_p]$ is the degree of L over $\mathbb{Q}_p$, then H_L is a cyclic group $H_L = \{\mathrm{id}, \bar{\varphi}_p, \dots, \bar{\varphi}_p{}^{d-1}\}$ generated by the image of φ_p in H_L. In ([Ven13], Proposition 2.1) Venjakob shows that for all open normal subgroups U of Γ there is an isomorphism given by

$$\mathcal{O}_L[\Gamma/U] \xrightarrow{\sim} \mathbb{Z}_p[\Gamma/U][H_L]_{\bar{\varphi}_p} \subset \widehat{\mathbb{Z}_p^{\mathrm{ur}}}[\Gamma/U][H_L], \quad a \longmapsto \sum_{i=0}^{d-1} \phi^{-i}(a)\bar{\varphi}_p{}^i.$$

Passing to the limit with respect to open normal subgroups U and the canonical projection maps one obtains the second map in (3.3.4).

The first map in (3.3.4) is the Coleman map, which we want to review in order to introduce some notation. First recall that the p-adic completion $\varprojlim_m \mathcal{O}_{L'}^\times/(\mathcal{O}_{L'}^\times)^{p^m}$ of the units $\mathcal{O}_{L'}^\times$ in a finite extension L' of $\mathbb{Q}_p$ can be naturally identified with the principal units $\mathcal{O}_{L'}^1$ in $\mathcal{O}_{L'}^\times$. In particular, we have

$$\mathcal{U}'(L_\infty) \stackrel{\mathrm{def}}{=} \varprojlim_{L',m} \mathcal{O}_{L'}^\times/(\mathcal{O}_{L'}^\times)^{p^m} \cong \varprojlim_{L'} \mathcal{O}_{L'}^1 \subset \varprojlim_{L'} \mathcal{O}_{L'}^\times,$$

where we let L' range through the finite subextensions of $L_\infty/\mathbb{Q}_p$, or, equivalently, through the (cofinal subsystem of) finite subextensions of L_∞/L, note that we still assume $[L : \mathbb{Q}_p] < \infty$. For our fixed generator $\epsilon = (\zeta_{p^n})_n$ of the Tate module $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}$ Coleman's theory gives a map

$$\varprojlim_n \mathcal{O}_{L_n}^\times \hookrightarrow \mathcal{O}_L[[T]]^\times, \quad u = (u_n)_n \longrightarrow f_u$$

such that

$$(f_u^{\phi^{-n}})(\zeta_{p^n} - 1) = u_n, \qquad \forall n \geq 1,$$

where ϕ acts on the coefficients of f_u. The elements $\zeta_{p^n} - 1$ are the p^n-torsion points in $\hat{\mathbb{G}}_m(\mathfrak{m})$, where $\mathfrak{m}$ is the valuation ideal of $\mathbb{C}_p$, since multiplication by p^n on the formal multiplicative group $\hat{\mathbb{G}}_m$ is given by

$$[p^n]_{\hat{\mathbb{G}}_m}(X) = (1 + X)^{p^n} - 1.$$

One may think of $[p]_{\hat{\mathbb{G}}_m}(X)$ as an endomorphism of the formal group $\hat{\mathbb{G}}_m$ lifting Frobenius, see ([dS87], I, section 1.2, 1.3). We define a $\mathbb{Z}_p$-algebra homomorphism φ by

$$\varphi : \mathcal{O}_L[[T]] \longrightarrow \mathcal{O}_L[[T]], \quad f(T) \longmapsto f^{\phi}((1+T)^p - 1),$$

where f^{ϕ} means that ϕ acts on the coefficients of f. Let us fix the topological generator $\gamma = 1_{\mathbb{Z}_p}$ of $\mathbb{Z}_p$ considered as an additive profinite group. Then, there is an isomorphism

$$\mathcal{M} : \mathcal{O}_L[[\mathbb{Z}_p]] \xrightarrow{\sim} \mathcal{O}_L[[T]], \quad 1_{\mathbb{Z}_p} \longmapsto 1 + T,$$

which is non-canonical in the sense that it depends on the choice of γ, see ([Was97], Theorem 7.1). Here, $\mathcal{M}$ stands for Mahler transform, compare ([CS06], §3.3) and Mahler's article [Mah58]. We note that there is a multiplicative norm operator $\mathcal{N}$ on $\mathcal{O}_L[[T]]$, see [dS87], such that for $f_u \in \mathcal{O}_L[[T]]^\times$, $u \in \varprojlim_n \mathcal{O}_{L_n}^\times$, we have $\mathcal{N} f_u = f_u^{\phi}$. Using property (loc. cit., I, §2.1, equation (1)) of $\mathcal{N}$ one gets an equality

$$\varphi(f_u) = (\mathcal{N} f_u)((1+T)^p - 1) = \prod_{\zeta \in \mu_p} f_u\big(T\ [+]_{\hat{\mathbb{G}}_m}(\zeta - 1)\big) = \prod_{\zeta \in \mu_p} f_u(\zeta(1+T) - 1).$$

Let $u \in \varprojlim_{L'} \mathcal{O}_{L'}^1$ now be a norm-compatible system of principal units. One can then show that $\frac{1}{p}\log\Big(\frac{f_u^p}{\varphi(f_u)}\Big)$ has integral coefficients, see (loc. cit., I, §3.3 Lemma). The integral measure $\mu_u \in \mathcal{O}_L[[\mathbb{Z}_p]]$ satisfying $\mathcal{M}(\mu_u) = \frac{1}{p}\log\Big(\frac{f_u^p}{\varphi(f_u)}\Big)$ is supported on $\mathbb{Z}_p^\times$, by which we mean that μ_u belongs to the image of the map

$$\iota : \mathcal{O}_L[[\mathbb{Z}_p^\times]] \hookrightarrow \mathcal{O}_L[[\mathbb{Z}_p]], \tag{3.3.5}$$

which sends a measure λ on $\mathbb{Z}_p^\times$ to the measure $\iota(\lambda) = \tilde{\lambda}$ extended by 0 to $p\mathbb{Z}_p$, see (loc. cit., §3.3).

As before we write $\kappa : \Gamma \xrightarrow{\sim} \mathbb{Z}_p^\times$ for the cyclotomic character. We define

$$\kappa_* : \mathcal{O}_L[[\Gamma]] \longrightarrow \mathcal{O}_L[[\mathbb{Z}_p^\times]]$$

to be the isomorphism of Iwasawa algebras induced by κ. Finally we can define the first map in (3.3.4)

$$\mathcal{U}'(L_\infty) \cong \varprojlim_{L'} \mathcal{O}_{L'}^1 \xrightarrow{\mathrm{Col}_{\epsilon,L}} \mathcal{O}_L[[\Gamma]], \quad u \longmapsto \kappa_*^{-1}\iota^{-1}\mathcal{M}^{-1}\Big(\frac{1}{p}\log\Big(\frac{f_u^p}{\varphi(f_u)}\Big)\Big), \tag{3.3.6}$$

where we note that only the element f_u depends on the choice of ϵ. We have now defined the map $\mathcal{L}_{L,\epsilon}$ from (3.3.3). The first non-trivial map of (3.3.3) is just the inclusion and the last non-trivial map (via the identifications from (3.3.4)) is given by the composite of $\mathcal{O}_L[[\Gamma]] \to \mathcal{O}_L(1)$ (induced by mapping $\gamma \in \Gamma$ to $\kappa(\gamma)$) and $\mathrm{Tr}_{L/\mathbb{Q}_p} \otimes \mathrm{id} : \mathcal{O}_L \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1) \longrightarrow \mathbb{Z}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$. It is explained in [Ven13] that, with respect to the norm maps and the natural projection maps, the sequences from (3.3.3) are compatible for extensions $\mathbb{Q}_p \subset_f L \subset_f L' \subset K'$. Passing to the projective limit one gets the sequence from (3.3.2).

Remark 3.3.1. We note that starting with the generator $\epsilon^{-1} = (\zeta_{p^n}^{-1})_n$ of $\mathbb{Z}_p(1)$ we get in an entirely similar fashion a map $\mathrm{Col}_{\epsilon^{-1},L}$ and an exact sequence

$$0 \longrightarrow \mathcal{U}'(K'_\infty) \overset{-\mathcal{L}_{K',\epsilon^{-1}}}{\longrightarrow} \mathbb{T}_{\mathrm{un}}(K'_\infty) \otimes_{\Lambda'} \Lambda'_{\varphi_p} \longrightarrow \mathbb{Z}_p(1) \longrightarrow 0 \tag{3.3.7}$$

as in (3.3.2) for ϵ^{-1} and $-\mathcal{L}_{K',\epsilon^{-1}}$.

We fix a Λ'-basis of $\mathbb{T}_{\mathrm{un}}(K'_\infty) \otimes_{\Lambda'} \Lambda'_{\varphi_p}$ which free of rank 1, i.e., an isomorphism $\delta : \mathbb{T}_{\mathrm{un}}(K'_\infty) \otimes_{\Lambda'} \Lambda'_{\varphi_p} \cong \Lambda'$. Since $\mathbb{Z}_p(1)$ is $\mathcal{S}'$-torsion, the exact sequence from (3.3.7) induces an isomorphism

$$\mathcal{U}'(K'_\infty)_{\mathcal{S}'} \overset{-\mathcal{L}_{K',\epsilon^{-1}}}{\longrightarrow} \left(\mathbb{T}_{\mathrm{un}}(K'_\infty) \otimes_{\Lambda'} \Lambda'_{\varphi_p}\right)_{\mathcal{S}'} \overset{\delta}{\cong} \Lambda'_{\mathcal{S}'}, \tag{3.3.8}$$

showing that assumption 3.2.1 is satisfied. In fact, let $u' \in \mathcal{U}'(K'_\infty)$, $s \in \mathcal{S}'$ be such that

$$-\mathcal{L}_{K',\epsilon^{-1}}^{-1}(\delta^{-1}(1)) = \frac{u'}{s}. \tag{3.3.9}$$

Then, u'/s is a $\Lambda'_{\mathcal{S}'}$-generator of $\mathcal{U}'(K'_\infty)_{\mathcal{S}'}$ and it follows that u' is also a $\Lambda'_{\mathcal{S}'}$-generator of $\mathcal{U}'(K'_\infty)_{\mathcal{S}'}$. The map $1 \longmapsto u'$ then gives a map as required for assumption 3.2.1.

Let us remark that the map $-\mathcal{L}_{K',\epsilon^{-1}}$ from (3.3.7) canonically induces a map

$$-\mathcal{L}_{K',\epsilon^{-1}} : \mathcal{U}'(K'_\infty) \otimes_{\Lambda'} \tilde{\Lambda}' \longrightarrow \mathbb{T}_{\mathrm{un}}(K'_\infty) \otimes_{\Lambda'} \tilde{\Lambda}'$$

of $\tilde{\Lambda}'$-modules, where the $\tilde{\Lambda}'$-module on the right is of rank 1 and generated by $(1 \otimes \epsilon) \otimes 1$. The existence of this map is based on the fact that the intersection

$$\Lambda'_{\varphi_p} \cap (\tilde{\Lambda}')^\times \neq \varnothing$$

is non-empty, see ([Ven13], §2.2) or ([FK06], Proposition 3.4.5), where we note that $K_1(\tilde{\Lambda}') \cong (\tilde{\Lambda}')^\times$ for our abelian p-adic Lie group $\mathcal{G}'$. Let c be an element belonging to $\Lambda'_{\varphi_p} \cap (\tilde{\Lambda}')^\times$. Then, we have a canonical isomorphism

$$\Lambda'_{\varphi_p} \otimes_{\Lambda'} \tilde{\Lambda}' \cong \tilde{\Lambda}', \quad a \otimes b \mapsto a \cdot b \tag{3.3.10}$$

as in ([Ven13], explanation preceding equation (2.18)) with inverse $x \mapsto c \otimes c^{-1}x$, which does not depend on c (recall Λ'_{φ_p} is free of rank 1 as a Λ'-module). Now, tensoring the exact sequence (3.3.7) with $\otimes_{\Lambda'}\tilde{\Lambda}'$ and using the isomorphism from (3.3.10), we get the exact sequence

$$0 \longrightarrow \mathcal{U}'(K'_\infty) \otimes_{\Lambda'} \tilde{\Lambda}' \overset{-\mathcal{L}_{K',\epsilon^{-1}}}{\longrightarrow} \mathbb{T}_{\mathrm{un}}(K'_\infty) \otimes_{\Lambda'} \tilde{\Lambda}' \longrightarrow \hat{\mathbb{Z}}_p^{ur}(1) \longrightarrow 0, \tag{3.3.11}$$

see proposition A.8.17 and remark 3.1.4 for the fact that $\otimes_{\Lambda'}\tilde{\Lambda}'$ is an exact functor.

3.3.2 Definition of $\mathcal{E}_{p,u'}$

We now define $\mathcal{E}_{p,u'} = \mathcal{E}_{u'} \in (\tilde{\Lambda}'_{\tilde{\mathcal{S}}'})^\times$ by the equation

$$-\mathcal{L}_{K',\epsilon^{-1}}(u' \otimes 1) = \mathcal{E}_{u'}^{-1} \cdot ((1 \otimes \epsilon) \otimes 1). \tag{3.3.12}$$

Let us introduce some notation and then make a remark about $\mathcal{E}_{u'}$. For $L \subseteq K'$, $[L : \mathbb{Q}_p] < \infty$, we will write u_{L_∞} and u_{L_n} for the images of any $u \in \mathcal{U}'(K'_\infty)$ under the maps $\mathcal{U}'(K'_\infty) \longrightarrow \mathcal{U}'(L_\infty)$ and $\mathcal{U}'(K'_\infty) \longrightarrow \mathcal{U}'(L_n) \cong \varprojlim_m \mathcal{O}_{L_n}^\times/(\mathcal{O}_{L_n}^\times)^{p^m} = \hat{\mathcal{O}}_{L_n}^\times$, respectively. Moreover, we will write $\Gamma_n = G(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$, $n \geq 1$, and for an element $\lambda \in \mathcal{O}_L[[\Gamma]] \cong \varprojlim_n \mathcal{O}_L[\Gamma_n]$ we write $\lambda = (\lambda_n)_n$ where the λ_n belong to the group rings $\mathcal{O}_L[\Gamma_n]$. For example, we will write $\big(\mathrm{Col}_{\epsilon^{-1},L}(u_{L_\infty})_n\big)_n$. Let us write $\mathcal{O}_{K'} = \bigcup_L \mathcal{O}_L$ for the valuation ring of K', where L ranges through all finite subextensions of $K'/\mathbb{Q}_p$.

Remark 3.3.2. First note that $\mathcal{E}_{u'}$ is actually a unit in $\tilde{\Lambda}'_{\tilde{\mathcal{S}}'}$ since both $-\mathcal{L}_{K',-\epsilon}(u' \otimes 1)$ and $(1 \otimes \epsilon) \otimes 1$ are generators of $\mathbb{T}_{\mathrm{un}}(K'_\infty) \otimes_{\Lambda'} \tilde{\Lambda}'_{\tilde{\mathcal{S}}'}$. Moreover, $\mathcal{E}_{u'}^{-1}$ even belongs to $\mathcal{O}_{K'}[[\mathcal{G}']] \bigcap (\tilde{\Lambda}'_{\tilde{\mathcal{S}}'})^\times$ since for $L \subset K'$ a finite extension of $\mathbb{Q}_p$ of degree d_L we have

$$-\mathcal{L}_{L,\epsilon^{-1}}(u'_{L_\infty}) = (1 \otimes \epsilon) \otimes \Big(- \sum_{i=0}^{d_L-1} \phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n\big)\bar{\varphi}_p^i\Big)_n \quad \in \ \mathbb{T}_{\mathrm{un}}(L_\infty) \otimes \varprojlim_n \mathbb{Z}_p[\Gamma_n][H_L]_{\bar{\varphi}_p},$$

where the elements $\phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n\big)$ belong to $\mathcal{O}_L[\Gamma_n]$, i.e., have coefficients in $\mathcal{O}_L$. It follows that we get a compatible system of elements

$$\mathcal{E}_{u'_{L_\infty}}^{-1} := \Big(- \sum_{i=0}^{d_L-1} \phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n\big)\bar{\varphi}_p^i\Big)_n \quad \in \ \varprojlim_n \mathbb{Z}_p[\Gamma_n][H_L]_{\bar{\varphi}_p} \subset \varprojlim_n \mathcal{O}_L[\Gamma_n][H_L]$$

for L ranging through all finite extensions of $\mathbb{Q}_p$ contained in K'. For the inclusion $\mathbb{Z}_p[\Gamma_n][H_L]_{\bar{\varphi}_p} \subset \mathcal{O}_L[\Gamma_n][H_L]$ see the proof of ([Ven13], Proposition 2.1). This system gives $\mathcal{E}_{u'}^{-1} = (\mathcal{E}_{u'_{L_\infty}}^{-1})_L$ which has coefficients in $\mathcal{O}_{K'}$.

3.3.3 Local constants and p-adic regulators

Let $\chi : \mathcal{G}' = H \times \Gamma \longrightarrow \mathbb{C}_p^\times$ be an Artin character, i.e., a character with finite image. We fix χ for the rest of this section. Restrict χ to H and define L to be the fixed field of the kernel of $\chi_{|H}$, i.e., such that

$$\chi : H_L = G(L/\mathbb{Q}_p) \hookrightarrow \mathbb{C}_p^\times$$

is injective. Note that $L/\mathbb{Q}_p$ is a finite extension since we assumed χ to be an Artin character. We write $H_L = G(L/\mathbb{Q}_p)$. Let d be the degree of L over $\mathbb{Q}_p$. Likewise, restrict χ to Γ and let n be the smallest integer such that $\chi_{|\Gamma}$ factors through $\Gamma_n = G(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$ but not through Γ_{n-1}. We will consider χ as a character of the finite group $H_L \times \Gamma_n \cong G(L(\zeta_{p^n})/\mathbb{Q}_p)$. When we restrict χ to $\Gamma_n \cong (\mathbb{Z}_p/p^n)^\times$ we can also interpret it as a primitive Dirichlet-character modulo p^n.

Definition 3.3.3 (Local constants). *Let $\epsilon^{-1} = (\zeta_{p^m}^{-1})_m$ be the inverse of our fixed generator of $\mathbb{Z}_p(1)$. We write*

$$\psi_{\epsilon^{-1}} : \mathbb{Q}_p \longrightarrow \mathbb{C}_p^\times$$

for the map with kernel equal to $\mathbb{Z}_p$ and $\psi_{\epsilon^{-1}}(1/p^m) = \zeta_{p^m}^{-1}$. Moreover, let $dx = dx_1$ be the Haar measure on $\mathbb{Q}_p$ assigning the value 1 to $\mathbb{Z}_p$, see the discussion in ([Tat79], section (3.6)) for consequences of this convention. Let us write $a_{\mathbb{Q}_p} : \mathbb{Q}_p^\times \to W(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ for the reciprocity map satisfying our sign convention 3.1.2. Then, we also interpret χ as a character

$$\chi : \mathbb{Q}_p^\times \xrightarrow{a_{\mathbb{Q}_p}} W(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow G_{\mathbb{Q}_p} \twoheadrightarrow \mathcal{G}' \to \mathbb{C}_p^\times$$

of $\mathbb{Q}_p^\times$ and the element $n \geq 0$ (which is the smallest integer $m \geq 0$ such that $\chi_{|\Gamma}$ factors through Γ_m) is then its conductor. We now define the local constant attached to χ by

$$\varepsilon_p(\chi, \psi_{\epsilon^{-1}}, dx) = \begin{cases} \sum_{m\in\mathbb{Z}} \int_{p^m\mathbb{Z}_p^\times} \chi(x)^{-1}\psi_{\epsilon^{-1}}(x)\ dx & \text{if } n \geq 1, \quad \text{(ramified case)} \\ 1 & \text{if } n = 0, \quad \text{(unramified case)}, \end{cases} \tag{3.3.13}$$

which is in line with [Del73] and [Tat79].

Remark 3.3.4. In the ramified case, $n \geq 1$, the local constant $\varepsilon(\chi, \psi_{\epsilon^{-1}}, dx)$ can be expressed as a Gauß sum. In fact, first note that our Haar measure $\mu = dx$ assigns to each residue class $a(1+(p)^n) = a + (p^n)$ of $\mathbb{Z}_p^\times$ modulo (the n-th principal units) $(1+(p)^n)$, $a \in \mathbb{Z}_p^\times$, the value $\mu(a + (p^n)) = \mu((p^n)) = 1/p^n$, see ([Bou04], INT VII.18). Also recall the explicit description of the local reciprocity map for Γ_n, see ([Mil13a], I, §3, Example 3.13) or ([Ser10], §3.1, Theorem 2, p.146), but note that the sign convention there is opposite to ours. Then, using the change of variables $x \mapsto x/p^n$ we get as in ([Hid93], §8.5, Example of integrals, *Gauß sum*, p. 259) that

$$\begin{aligned} \varepsilon_p(\chi, \psi_{\epsilon^{-1}}, dx) &= \int_{p^{-n}\mathbb{Z}_p^\times} \chi(x)^{-1}\psi_{\epsilon^{-1}}(x)\ dx \\ &= \chi(\bar{\varphi}_p^n)^{-1} \sum_{\gamma\in\Gamma_n} \chi(\gamma)^{-1}\psi_{\epsilon^{-1}}(\kappa(\gamma)/p^n) \\ &= \chi(\bar{\varphi}_p^n)^{-1} \sum_{\gamma\in\Gamma_n} \chi(\gamma)^{-1}\gamma(\zeta_{p^n}^{-1}), \end{aligned} \tag{3.3.14}$$

where the for the first equation see (loc. cit., (4b), p. 259). See also the discussion in ([Ven13], Appendix A, p. 33, footnote 2) regarding the conventions made in [FK06].

We will now define the p-adic regulator associated to a character χ as above and a norm-compatible sequence of principle units $u \in \mathcal{U}'(K'_\infty)$.

Definition 3.3.5 (p-adic regulator). *Let χ be an Artin character as above and let $u \in \mathcal{U}'(K'_\infty)$. Write u_{L_n} for the image of u under the projection $\mathcal{U}'(K'_\infty) \to \mathcal{O}_{L_n}^1$ to the principal units of $\mathcal{O}_{L_n}$. Then, we define the p-adic regulator of χ and u by*

$$R_p(u, \chi) = \sum_{g\in\Gamma_n\times H_L} \chi(g^{-1}) \cdot \log(g(u_{L_n}))$$

and note that this is equal to $\sum_{g\in\Gamma_n\times H_L}\chi(g^{-1})\cdot g\big(\log(u_{L_n})\big)$ *since every Galois automorphism* $g\in\Gamma_n\times H_L$ *is continuous.*

3.3.4 The values of $\mathcal{E}_{u'}$ at Artin characters

Let $\mathcal{G}'=G(K'_\infty/\mathbb{Q}_p)$ be as in subsection 3.3.1. Moreover, let $\chi:\mathcal{G}'=H\times\Gamma\longrightarrow\mathbb{C}_p^\times$ be an Artin character and adopt the notation from the previous subsection 3.3.3, i.e., so that L is the fixed field of the kernel of the restriction $\chi_{|H}$ of χ to H and χ restricted to Γ factors through Γ_n, but not through Γ_{n-1}. Moreover, let $u'\in\mathcal{U}'(K'_\infty)$ be an element as in assumption 3.2.1, which exists as we have explained after equation (3.3.9).

Remark 3.3.6. While we work under the assumption that $K'/\mathbb{Q}_p$ is of infinite degree, we note that this is not necessary. The proof of theorem 3.3.7 shows that the same interpolation property holds for finite unramified extensions $L'/\mathbb{Q}_p$, the corresponding extension $L'_\infty/\mathbb{Q}_p$ and elements $\mathcal{E}^{-1}_{u,L'}\in\mathcal{O}_{L'}[[\Gamma\times H_{L'}]]$ defined by

$$-\mathcal{L}_{L',\epsilon^{-1}}(u\otimes 1)=\mathcal{E}^{-1}_{u,L'}((1\otimes\epsilon)\otimes 1),\quad u\in\mathcal{U}'(L'_\infty). \tag{3.3.15}$$

In fact, the value of $\mathcal{E}_{u'}$ at χ only depends on $\mathcal{E}^{-1}_{u'_{L_\infty}}\in\mathcal{O}_L[[\Gamma\times H_L]]$, the image of $\mathcal{E}^{-1}_{u'}$ under the projection $\mathcal{O}_{K'}[[\mathcal{G}']]\to\mathcal{O}_{K'}[[\Gamma\times H_L]]$, compare remark 3.3.2.

We now want to determine the value of $\mathcal{E}_{u'}$ at χ, which, by definition, is given by

$$\int_{\mathcal{G}'}\chi\ d\mathcal{E}_{u'}:=\Big(\int_{\mathcal{G}'}\chi\ d(\mathcal{E}^{-1}_{u'})\Big)^{-1},$$

recall that $\mathcal{E}^{-1}_{u'}\in\mathcal{O}_{K'}[[\mathcal{G}']]\bigcap(\tilde{\Lambda}'_{\tilde{\mathcal{S}}'})^\times$ so that $\mathcal{E}_{u'}$ is of the form $\frac{1}{\mathcal{E}^{-1}_{u'}}\in(\tilde{\Lambda}'_{\tilde{\mathcal{S}}'})^\times$. That means we interpret $\mathcal{E}^{-1}_{u'}$ as an $\mathcal{O}_{K'}$-integral measure on $\mathcal{G}'$. Compare the interpolation property given in the next theorem 3.3.7 with the formula in ([FK06], §3.6.1) for the extension $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$ which is stated without proof.

Let us make the convention that elements of H_L will be denoted h or h' and elements of Γ_n will be denoted γ or γ'. We identify h with $(h,1)$ in $H_L\times\Gamma_n$ and likewise we identify γ with $(1,\gamma)$. Moreover, as before, we will write u_{L_∞} and u_{L_n} for the images of any $u\in\mathcal{U}'(K'_\infty)$ under the maps $\mathcal{U}'(K'_\infty)\longrightarrow\mathcal{U}'(L_\infty)$ and $\mathcal{U}'(K'_\infty)\longrightarrow\mathcal{U}'(L_n)\cong\varprojlim_m\mathcal{O}^\times_{L_n}/(\mathcal{O}^\times_{L_n})^{p^m}=\hat{\mathcal{O}}^\times_{L_n}$, respectively.

Theorem 3.3.7 (Interpolation property of $\mathcal{E}_{u'}$). *The value of $\mathcal{E}_{u'}$ at an Artin character χ is given by*

$$\int_{\mathcal{G}'}\chi\ d\mathcal{E}_{u'}\overset{\text{def}}{=}\Big(\int_{\mathcal{G}'}\chi\ d(\mathcal{E}^{-1}_{u'})\Big)^{-1}=-\frac{\varepsilon_p(\chi,\psi_{\epsilon^{-1}},dx)}{R_p(u',\chi)}$$

whenever $R_p(u',\chi)\neq 0$. In fact, we always have

$$\Big(\int_{\mathcal{G}'}\chi\ d(\mathcal{E}^{-1}_{u'})\Big)\cdot\varepsilon_p(\chi,\psi_{\epsilon^{-1}},dx)=-R_p(u',\chi),$$

regardless of whether $R_p(u',\chi)\neq 0$.

Proof. We adopt the same notation for χ as at the beginning of this subsection. In particular, χ factors through $\Gamma_n \times H_L$ and n is the smallest integer with this property. We know from remark 3.3.2 that $\mathcal{E}_{u'}^{-1}$ belongs to $\mathcal{O}_{K'}[[\mathcal{G}']]$ and that it is given by the compatible system $\mathcal{E}_{u'}^{-1} = (\mathcal{E}_{u'_{L'_\infty}}^{-1})_{L'}$, where $\mathcal{E}_{u'_{L'_\infty}}^{-1}$ was defined in the same remark. Recall that under the canonical projection

$$\mathcal{O}_{K'}[[\mathcal{G}']] \to \mathcal{O}_{K'}[\Gamma_n \times H_L], \quad \mathcal{E}_{u'}^{-1} \longmapsto -\sum_{i=0}^{d_L-1} \phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n\big)\bar{\varphi}_p^i \ \in \ \mathcal{O}_L[\Gamma_n \times H_L],$$

where $\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n$ is the image of $\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})$ under the projection $\mathcal{O}_L[[\Gamma]] \to \mathcal{O}_L[\Gamma_n]$. Elements of $\mathcal{O}_L[\Gamma_n \times H_L]$ have the form $\sum_{(\gamma,i)} \alpha[\gamma,i](\gamma,\bar{\varphi}_p^i)$ with $\alpha[\gamma,i] \in \mathcal{O}_L$, $(\gamma,\bar{\varphi}_p^i) \in \Gamma_n \times H_L$ and where we sum over $\Gamma_n \times \{0,\dots,d_L-1\}$. Using this notation, and an analogous notation for elements $\sum_{\gamma\in\Gamma_n} \beta[\gamma]\gamma$ in $\mathcal{O}_L[\Gamma_n]$, we have

$$-\sum_{i=0}^{d_L-1} \phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n\big)\bar{\varphi}_p^i = -\sum_{(\gamma,i)} \phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma]\big)(\gamma,\bar{\varphi}_p^i) \ \in \ \mathcal{O}_L[\Gamma_n \times H_L],$$

so the coefficient of $(\gamma,\bar{\varphi}_p^i)$ is the coefficient $\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma] \in \mathcal{O}_L$ acted upon by ϕ^{-i}. We can now start with the calculations. Since χ factors through $\Gamma_n \times H_L$, by definition of the integral we get

$$\int_{\mathcal{G}'} \chi \ d(\mathcal{E}_{u'}^{-1}) = -\sum_{(\gamma',i)} \Big(\phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\big)\cdot\chi(\gamma',\bar{\varphi}_p^i)\Big). \tag{3.3.16}$$

Multiplying this expression with $\chi(\bar{\varphi}_p^n)\cdot\varepsilon_p(\chi,\psi_{\epsilon^{-1}},dx)$, in view of (3.3.14) we get

$$\begin{aligned}
&\Big(\int_{\mathcal{G}'} \chi \ d(\mathcal{E}_{u'}^{-1})\Big)\cdot\big(\chi(\bar{\varphi}_p^n)\cdot\varepsilon_p(\chi,\psi_{\epsilon^{-1}},dx)\big)\\
&= -\Big(\sum_{(\gamma',i)} \Big(\phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\big)\cdot\chi(\gamma',\bar{\varphi}_p^i)\Big)\Big)\cdot\Big(\sum_{\gamma\in\Gamma_n}\chi(\gamma)^{-1}\gamma(\zeta_{p^n}^{-1})\Big) && \text{(by definition)}\\
&= -\sum_{(\gamma',i)}\sum_{\gamma\in\Gamma_n}\Big(\phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\big)\cdot\chi(\gamma'\gamma^{-1},\bar{\varphi}_p^i)\cdot\gamma(\zeta_{p^n}^{-1})\Big) && \text{(multiplying)}\\
&= -\sum_{(\gamma',i)}\sum_{\gamma\in\Gamma_n}\Big(\phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\big)\cdot\chi(\gamma^{-1},\bar{\varphi}_p^i)\cdot\gamma\gamma'(\zeta_{p^n}^{-1})\Big) && (\gamma \overset{\text{subst.}}{\longmapsto} \gamma\gamma')\\
&= -\sum_i\sum_\gamma\sum_{\gamma'}\Big(\chi(\gamma^{-1},\bar{\varphi}_p^i)\cdot\gamma\gamma'(\zeta_{p^n}^{-1})\cdot\phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\big)\Big) && \text{(rearrange).}
\end{aligned} \tag{3.3.17}$$

Let us consider the summands of the last sum; ϕ^{-i} acts on $\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma'] \in \mathcal{O}_L$ and γ acts on $\gamma'(\zeta_{p^n}^{-1})$. Since $\bar{\varphi}_p$ is the restriction of ϕ to L, we may also write $\phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\big) = \bar{\varphi}_p^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\big)$. Since $(\gamma,\bar{\varphi}_p^{-i}) \in G(L(\zeta_{p^n})/\mathbb{Q}_p)$ acts on L through $\bar{\varphi}_p^{-i}$ and on $\mathbb{Q}_p(\zeta_{p^n})$ through γ, we have

$$\gamma\gamma'(\zeta_{p^n}^{-1})\cdot\phi^{-i}\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\big) = (\gamma,\bar{\varphi}_p^{-i})\Big(\gamma'(\zeta_{p^n}^{-1})\cdot\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\Big). \tag{3.3.18}$$

Therefore, the last sum in (3.3.17) is equal to

$$
\begin{aligned}
&-\sum_i\sum_\gamma\sum_{\gamma'}\Big(\chi(\gamma^{-1},\bar{\varphi}_p^i)\cdot(\gamma,\bar{\varphi}_p^{-i})\big(\gamma'(\zeta_{p^n}^{-1})\cdot \mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\big)\Big) && \text{(use (3.3.18))}\\
&=-\sum_i\sum_\gamma\Big[\chi(\gamma^{-1},\bar{\varphi}_p^i)\cdot(\gamma,\bar{\varphi}_p^{-i})\Big(\sum_{\gamma'}\gamma'(\zeta_{p^n}^{-1})\cdot \mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']\Big)\Big] && \text{(factor out).} \quad (3.3.19)
\end{aligned}
$$

The element $\sum_{\gamma'}\gamma'(\zeta_{p^n}^{-1})\cdot\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma']$ from the last sum looks familiar. Note that the function $\Gamma\to\mu_{p^n}$ defined by $\gamma\mapsto\gamma(\zeta_{p^n}^{-1})$ is locally constant modulo $G(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p(\mu_{p^n}))$. Therefore, considering $\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})\in\mathcal{O}_L[[\Gamma]]$ as a measure on Γ, we get

$$
\begin{aligned}
\sum_{\gamma'}\gamma'(\zeta_{p^n}^{-1})\cdot\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma'] &= \int_\Gamma \gamma'(\zeta_{p^n}^{-1})\, d\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})\big)(\gamma')\\
&= \int_\Gamma \zeta_{p^n}^{-\kappa(\gamma')}\, d\big(\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})\big)(\gamma') && \text{(def. of } \kappa)\\
&= \int_{\mathbb{Z}_p^\times} \zeta_{p^n}^{-x}\, d\big(\kappa_*\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})\big)(x) && \text{(use } \mathcal{O}_L[[\Gamma]]\xrightarrow{\kappa_*}\mathcal{O}_L[[\mathbb{Z}_p^\times]])\\
&= \int_{\mathbb{Z}_p} \zeta_{p^n}^{-x}\, d\big(\iota\kappa_*\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})\big)(x) && \text{(extend measure by 0 to } p\mathbb{Z}_p),
\end{aligned}
\tag{3.3.20}
$$

where $\iota:\mathcal{O}_L[[\mathbb{Z}_p^\times]]\hookrightarrow\mathcal{O}_L[[\mathbb{Z}_p]]$ is defined as in (3.3.5). By definition of the Coleman map $\mathrm{Col}_{\epsilon^{-1},L}$, see (3.3.6), the measure appearing in the last term of (3.3.20) is given by

$$
\iota\kappa_*\mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty}) = \mathcal{M}^{-1}\Big(\frac{1}{p}\log\Big(\frac{f^p_{u'_{L_\infty}}}{\varphi(f_{u'_{L_\infty}})}\Big)\Big),
$$

where $f_{u'_{L_\infty}}\in\mathcal{O}_L[[T]]^\times$ is the Coleman power series attached to $u'_{L_\infty}\in\mathcal{U}'(L_\infty)$ (and with respect to the generator ϵ^{-1} of $\mathbb{Z}_p$). Using lemma 3.3.9 that we prove after this theorem, we see that the last term of (3.3.20) is equal to

$$
\frac{1}{p}\log\Big(\frac{f^p_{u'_{L_\infty}}(\zeta_{p^n}^{-1}-1)}{\varphi(f_{u'_{L_\infty}})(\zeta_{p^n}^{-1}-1)}\Big) = \log\big(f_{u'_{L_\infty}}(\zeta_{p^n}^{-1}-1)\big) - \frac{1}{p}\log\big(f^\phi_{u'_{L_\infty}}(\zeta_{p^{n-1}}^{-1}-1)\big), \tag{3.3.21}
$$

where, we recall that for $f(T)\in\mathcal{O}_L[[T]]$ we defined $\varphi(f)(T)=f^\phi((1+T)^p-1)$. Note also that the evaluation map $ev_{\zeta_{p^n}^{-1}}:\mathcal{O}_L[[T]]\longrightarrow\mathcal{O}_{L_n},\ T\longmapsto\zeta_{p^n}^{-1}-1$, from lemma 3.3.9 is continuous. Hence, for a power series $f(T)\in\mathcal{O}_L[[T]]$ congruent to 1 modulo $(\mathfrak{m}_L,T)$, where $\mathfrak{m}_L$ is the maximal ideal of $\mathcal{O}_L$, evaluating $\log(f(T))$ at $\zeta_{p^n}^{-1}-1$ yields the same as evaluating log at $f(\zeta_{p^n}^{-1}-1)$.

Since u'_{L_∞} is a norm-coherent series of principal units, the Coleman power series $f_{u'_{L_\infty}}(T)$ and also $f^\phi_{u'_{L_\infty}}(T)$ are congruent to 1 modulo $(\mathfrak{m}_L,T)$, see ([dS87], I, §3.3, p. 18). Let us write

$\mathfrak{m}_{L_n}$ for the maximal ideal of $\mathcal{O}_{L_n}$, $L_n = L(\zeta_{p^n})$. Then, since $\zeta_{p^n}^{-1} - 1$ and $\zeta_{p^{n-1}}^{-1} - 1$ are uniformizers for $\mathbb{Q}_p(\zeta_{p^n})$ and $\mathbb{Q}_p(\zeta_{p^{n-1}})$, respectively, they also belong to $\mathfrak{m}_{L_n}$ and $\mathfrak{m}_{L_{n-1}}$, respectively, and we conclude that $f_{u'_{L_\infty}}(\zeta_{p^n}^{-1} - 1)$ and $f^{\phi}_{u'_{L_\infty}}(\zeta_{p^{n-1}}^{-1} - 1)$ are principal units in $\mathcal{O}_{L_n}^{\times}$ and $\mathcal{O}_{L_{n-1}}^{\times}$, respectively. Hence, their logarithms are given by the usual formula. Since $(1, \phi_{|L}) = (1, \bar{\varphi}_p) \in \Gamma_n \times H_L$ is a continuous automorphism of L_n (and acts trivially on $\mathbb{Q}_p(\zeta_{p^n})$ and the coefficients of log), we have

$$\begin{aligned}
&\log\big(f_{u'_{L_\infty}}(\zeta_{p^n}^{-1} - 1)\big) \;-\; \frac{1}{p}\log\big(f^{\phi}_{u'_{L_\infty}}(\zeta_{p^{n-1}}^{-1} - 1)\big) \\
&= (1, \bar{\varphi}_p)^n \Big(\log\big(f^{\phi^{-n}}_{u'_{L_\infty}}(\zeta_{p^n}^{-1} - 1)\big) \;-\; \frac{1}{p}\log\big(f^{\phi^{-(n-1)}}_{u'_{L_\infty}}(\zeta_{p^{n-1}}^{-1} - 1)\big)\Big) \\
&= (1, \bar{\varphi}_p)^n \big(\log(u'_{L_n}) - \frac{1}{p}\log(u'_{L_{n-1}})\big), \qquad (3.3.22)
\end{aligned}$$

by definition of the Coleman power series (note we considered the maps constructed with respect to ϵ^{-1}). From (3.3.20) until now we have shown that

$$\sum_{\gamma'} \gamma'(\zeta_{p^n}^{-1}) \cdot \mathrm{Col}_{\epsilon^{-1},L}(u'_{L_\infty})_n[\gamma'] = (1, \bar{\varphi}_p)^n \big(\log(u'_{L_n}) - \frac{1}{p}\log(u'_{L_{n-1}})\big).$$

We get that the last term of (3.3.19) is equal to

$$\begin{aligned}
&-\sum_i \sum_\gamma \Big[\chi(\gamma^{-1}, \bar{\varphi}_p^i) \cdot (\gamma, \bar{\varphi}_p^{-i})\Big((1, \bar{\varphi}_p)^n \big(\log(u'_{L_n}) - \frac{1}{p}\log(u'_{L_{n-1}})\big)\Big)\Big] \\
&= -\sum_i \sum_\gamma \Big[\chi(\gamma^{-1}, \bar{\varphi}_p^i) \cdot (\gamma, \bar{\varphi}_p^{-i+n})\Big(\log(u'_{L_n}) - \frac{1}{p}\log(u'_{L_{n-1}})\Big)\Big] \qquad \text{(associativity)} \\
&= -\sum_i \sum_\gamma \Big[\chi(\gamma^{-1}, \bar{\varphi}_p^{i+n}) \cdot (\gamma, \bar{\varphi}_p^{-i})\Big(\log(u'_{L_n}) - \frac{1}{p}\log(u'_{L_{n-1}})\Big)\Big] \qquad (i \overset{\text{subst.}}{\longmapsto} i + n) \\
&= -\chi(\bar{\varphi}_p^n) \sum_i \sum_\gamma \Big[\chi(\gamma^{-1}, \bar{\varphi}_p^i) \cdot (\gamma, \bar{\varphi}_p^{-i})\Big(\log(u'_{L_n}) - \frac{1}{p}\log(u'_{L_{n-1}})\Big)\Big] \qquad \text{(factor out)}, \quad (3.3.23)
\end{aligned}$$

where we note that we may make the substitution $i \mapsto i + n$ since this just permutes H_L through multiplication by $\bar{\varphi}_p^n$. Since $-\frac{1}{p}\log(u'_{L_{n-1}})$ belongs to L_{n-1} ($u'_{L_{n-1}}$ is a principal unit in $\mathcal{O}_{L_{n-1}}^{\times}$), it follows from lemma 3.3.8, which we prove after this theorem, that the last term of (3.3.23) is equal to

$$-\chi(\bar{\varphi}_p^n) \sum_i \sum_\gamma \Big[\chi(\gamma^{-1}, \bar{\varphi}_p^i) \cdot (\gamma, \bar{\varphi}_p^{-i})\big(\log(u'_{L_n})\big)\Big] = -\chi(\bar{\varphi}_p^n) R_p(u', \chi).$$

So we have shown that

$$\Big(\int_{\mathcal{G}'} \chi \; d(\mathcal{E}_{u'}^{-1})\Big) \cdot \big(\chi(\bar{\varphi}_p^n) \cdot \varepsilon_p(\chi, \psi_{\epsilon^{-1}}, dx)\big) = -\chi(\bar{\varphi}_p^n) R_p(u', \chi),$$

which concludes the proof upon cancelling out the factor $\chi(\bar{\varphi}_p^n) \neq 0$. □

We prove two lemmata that we used in the above proof.

Lemma 3.3.8. *Let L be a finite unramified extension of $\mathbb{Q}_p$ as before and let $\tilde{\chi}: H_L \times \Gamma_n \longrightarrow \mathbb{C}_p^\times$ be character such that $\tilde{\chi}_{|H_L}$ is injective and $\tilde{\chi}_{|\Gamma_n}$ does not factor through Γ_{n-1} for n, $n \geq 1$. If $n = 1$, then assume that $p > 2$. Then for any $x \in L(\zeta_{p^{n-1}})$ the identity*

$$\sum_{(\sigma,g)\in H_L\times\Gamma_n} \left(\tilde{\chi}(\sigma,g)^{-1}(\sigma,g)(x)\right) = 0$$

holds.

Proof. By assumption we have $\tilde{\chi}\big(G\big(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_{p^{n-1}})\big)\big) \neq 1$. In case $n \geq 2$, the Galois group $G\big(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_{p^{n-1}})\big)$ is cyclic of order p and in case $n = 1$ it is cyclic of order $p-1$. In any case fix a generator g_0 of $G\big(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_{p^{n-1}})\big)$. We then have $\tilde{\chi}(g_0) \neq 1$. In $G(L_n/\mathbb{Q}_p) \cong H_L \times \Gamma_n$ the element g_0 corresponds to (id_{H_L}, g_0), hence it acts trivially on L and $\mathbb{Q}_p(\zeta_{p^{n-1}})$, i.e., on L_{n-1}. Write $\tilde{p}$ for the order of $G\big(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_{p^{n-1}})\big)$, so $\tilde{p} = p$ if $n \geq 2$ and $\tilde{p} = p-1$ if $n = 1$.

Now, for any $\overline{\gamma} \in \Gamma_{n-1}$ fix an element $\gamma \in \Gamma_n$ mapping to $\overline{\gamma}$ under the projection $\Gamma_n \longrightarrow \Gamma_{n-1}$. Then $\{\gamma, \gamma g_0, \gamma g_0^2, \ldots, \gamma g_0^{\tilde{p}-1}\}$ is the preimage of $\{\overline{\gamma}\}$ under the projection and we get

$$\begin{aligned}
\sum_{(\sigma,\gamma')\in H_L\times\Gamma_n} \tilde{\chi}(\sigma,\gamma')^{-1}(\sigma,\gamma')(x) &= \sum_{\sigma\in H_L}\sum_{\overline{\gamma}\in\Gamma_{n-1}}\sum_{i=0}^{\tilde{p}-1} \tilde{\chi}(\sigma,\gamma g_0^i)^{-1}(\sigma,\gamma g_0^i)(x) \\
&= \sum_{\sigma\in H_L}\sum_{\overline{\gamma}\in\Gamma_{n-1}}\sum_{i=0}^{\tilde{p}-1} \tilde{\chi}(\sigma,\gamma g_0^i)^{-1}(\sigma,\gamma)(x) && (g_{0|L_{n-1}} = \mathrm{id}_{L_{n-1}}) \\
&= \sum_{\sigma\in H_L}\sum_{\overline{\gamma}\in\Gamma_{n-1}} \left[\tilde{\chi}(\sigma,\gamma)(\sigma,\gamma)(x)\Big(\sum_{i=0}^{\tilde{p}-1}\tilde{\chi}(g_0^i)^{-1}\Big)\right] && (\text{factor out}) \\
&= 0
\end{aligned}$$

where the last equality follows because $\tilde{\chi}(g_0^{-1})$ is a $\tilde{p}$-th root of unity and not equal to 1 and hence it is a root of the polynomial

$$(X^{\tilde{p}} - 1)\big/(X-1) = X^{\tilde{p}-1} + X^{\tilde{p}-2} + \cdots + 1,$$

showing that $\sum_{i=0}^{\tilde{p}-1}\tilde{\chi}(g_0^{-1})^i = 0$. □

For the next lemma, let L be a finite unramified extension of $\mathbb{Q}_p$ and consider $L_n = L(\zeta_{p^n})$, where ζ_{p^n} is our (or any) fixed primitive p^n-th root of unity. The element $\zeta_{p^n}^{-1} - 1$ belongs to the maximal ideal $\mathfrak{m}_{\mathcal{O}_{L_n}}$ of $\mathcal{O}_{L_n}$, which is complete with respect to the $\mathfrak{m}_{\mathcal{O}_{L_n}}$-adic topology. By the universal property of the ring of power series we get a map

$$ev_{\zeta_{p^n}^{-1}}: \mathcal{O}_L[[T]] \longrightarrow \mathcal{O}_{L_n}, \quad T \longmapsto \zeta_{p^n}^{-1} - 1,$$

which is a continuous $\mathcal{O}_L$-algebra homomorphism. Recall that we have a topological algebra isomorphism $\mathcal{M}: \mathcal{O}_L[[\mathbb{Z}_p]] \xrightarrow{\sim} \mathcal{O}_L[[T]], \quad 1_{\mathbb{Z}_p} \longmapsto 1 + T$.

Lemma 3.3.9. *For every $n \geq 1$ and every $\mu \in \mathcal{O}_L[[\mathbb{Z}_p]]$ we have the equality*

$$\int_{\mathbb{Z}_p} (\zeta_{p^n}^{-1})^x d\mu(x) = ev_{\zeta_{p^n}^{-1}} \circ \mathcal{M}(\mu).$$

Proof. First let $a \in \mathbb{Z} \subset \mathbb{Z}_p \subset \mathcal{O}_L[[\mathbb{Z}_p]]^\times$. Then, we can consider the measure da on $\mathbb{Z}_p$ associated to a, which is the Dirac measure, and get

$$\int_{\mathbb{Z}_p} (\zeta_{p^n}^{-1})^x da(x) = (\zeta_{p^n}^{-1})^a.$$

On the other hand we have

$$ev_{\zeta_{p^n}^{-1}} \circ \mathcal{M}(a) = ev_{\zeta_{p^n}^{-1}}((1+T)^a) = (\zeta_{p^n}^{-1})^a.$$

By continuity the same holds for $a \in \mathbb{Z}_p \subset \mathcal{O}_L[[\mathbb{Z}_p]]^\times$ so that, as maps $\mathbb{Z}_p \longrightarrow \mathcal{O}_{L_n}^\times$, the above two agree. Now, the result follows by the universal property of the completed group ring, see, for example, ([Wit04], Satz 2.5.2), which says that the maps extend uniquely to continuous $\mathcal{O}_L$-algebra homomorphisms. Only note that $ev_{\zeta_{p^n}^{-1}} \circ \mathcal{M}$ is a continuous algebra homomorphism (since $ev_{\zeta_{p^n}^{-1}}$ and $\mathcal{M}$ are) and $\mathcal{O}_L[[\mathbb{Z}_p]] \ni \mu \longrightarrow \int_{\mathbb{Z}_p} (\zeta_{p^n}^{-1})^x d\mu(x)$ is, too, it factors through $\mathcal{O}_L[\mathbb{Z}_p/p^n]$. □

Chapter 4

Selmer Groups of p-adic Galois Representations

4.1 Definition

Let p be an odd prime and let us consider a number field F, a finite set of places Σ of F containing Σ_p and Σ_∞, and a finitely generated free $\mathbb{Z}_p$-module T endowed with a continuous action of G_F which is unramified outside Σ. We note that such T give rise to compact p-adic Lie extensions. In fact, if F_∞ denotes the fixed field of the kernel of the representation and r denotes the $\mathbb{Z}_p$-rank of T, then $G(F_\infty/F)$ is isomorphic to a closed subgroup of the compact p-adic Lie Group $GL_r(\mathbb{Z}_p)$ and therefore a compact p-adic Lie group itself, compare ([OV02], section 4.2, p. 561). Note that by general topology the image of $G(F_\infty/F)$ in $GL_r(\mathbb{Z}_p)$ is compact (since the representation is continuous) and since $GL_r(\mathbb{Z}_p)$ is Hausdorff it is then also closed, see ([Bre93], I, 7.5. Theorem). Likewise, if $\bar{\nu}$ is a non-archimedean prime of F_∞ above a prime ν of F, then the decomposition group of $\bar{\nu}$ in $G(F_\infty/F)$ is closed in $G(F_\infty/F)$ and therefore a compact p-adic Lie group.

Before we define a Selmer group for the Galois representation T we recall that $H^1_f(F_\nu, T\otimes\mathbb{Q}_p)$ is defined as follows; compare $([\text{Kat04}], 14.1, p.\ 235)$. For a finitely generated $\mathbb{Q}_p$ vector space V with an action of G_{F_ν} for some $\nu\in\Sigma$ we define $H^1_f(F_\nu, V)$ to be

$$H^1_f(F_\nu,V)=\begin{cases}\ker\big(H^1(F_\nu,V)\longrightarrow H^1(F_\nu^{\text{ur}},V)\big) & \text{if } \nu\in\Sigma_f\smallsetminus\Sigma_p,\\ \ker\big(H^1(F_\nu,V)\longrightarrow H^1(F_\nu,B_{\text{crys}}\otimes_{\mathbb{Q}_p}V)\big) & \text{if } \nu\in\Sigma_p,\\ 0 & \text{if } \nu\in\Sigma_\infty,\end{cases}$$

where B_{crys} is the ring defined by Fontaine (and Messing) in [FM87], see also [Fon82], [Fon94] or the more recent [FO]. We remark that in the literature the space $H^1_f(F_\nu,V)$ for $\nu\in\Sigma_f\smallsetminus\Sigma_p$ is often denoted $H^1_{ur}(F_\nu,V)$ and called the subgroup of $H^1(F_\nu,V)$ of unramified cohomology classes.

We will also need the notion of finite cohomology groups for finitely generated free $\mathbb{Z}_p$-modules T and discrete modules $T\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p$ with an action of G_{F_ν} and define these to be the inverse image and image of $H^1_f(F_\nu, T\otimes\mathbb{Q}_p)$, respectively, under the natural maps

$$H^1(F_\nu, T) \xrightarrow{\iota_*} H^1(F_\nu, T\otimes\mathbb{Q}_p) \xrightarrow{pr_*} H^1(F_\nu, T\otimes\mathbb{Q}_p/\mathbb{Z}_p),$$

i.e., for any place $\nu\in\Sigma$ we define

$$H^1_f(F_\nu, T) := \iota_*^{-1}\big(H^1_f(F_\nu, T\otimes\mathbb{Q}_p)\big)$$

and

$$H^1_f(F_\nu, T\otimes\mathbb{Q}_p/\mathbb{Z}_p) := pr_*\big(H^1_f(F_\nu, T\otimes\mathbb{Q}_p)\big).$$

We note that, p being odd, the first cohomology groups $H^1(F_\nu, V)$ vanish for archimedean places $\nu\in\Sigma_\infty$. Accordingly, we have $H^1_f(F_\nu, T) = H^1(F_\nu, T)$ and $H^1_f(F_\nu, T\otimes\mathbb{Q}_p/\mathbb{Z}_p) = 0$ for $\nu\in\Sigma_\infty$.

We make the following definition, similar to ([Kat04], 14.1, p. 234).

Definition 4.1.1 (Selmer group). *(i) For a number field F, a finite set of places Σ containing $\Sigma_p\cup\Sigma_\infty$, and a finitely generated free $\mathbb{Z}_p$-module T endowed with an action of G_F that is unramified outside Σ we define*

$$\mathrm{Sel}(F,T) = \ker\Big(H^1\big(G_\Sigma, T\otimes\mathbb{Q}_p/\mathbb{Z}_p\big) \longrightarrow \bigoplus_{\nu\in\Sigma} H^1(F_\nu, T\otimes\mathbb{Q}_p/\mathbb{Z}_p)/H^1_f(F_\nu, T\otimes\mathbb{Q}_p/\mathbb{Z}_p)\Big),$$

where ν runs through all places of F in Σ.

(ii) For an infinite algebraic extension F_∞/F with finite subextensions $\ldots F_n\subset F_{n+1}\cdots\subset F_\infty$ such that $F_\infty = \cup_n F_n$, we define

$$\mathrm{Sel}(F_\infty, T^*(1)) := \varinjlim_n \mathrm{Sel}(F_n, T^*(1)),$$

which is a subgroup of $H^1(G_{\infty,\Sigma}, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)$, the Pontryagin dual of which appears in the Poitou-Tate sequence (A.4.10).

4.2 Connection with the sequence of Poitou-Tate

We want to show that the map

$$H^1(G_{\infty,\Sigma}, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee \longrightarrow \varprojlim_n H^2(G_{n,\Sigma}, T)$$

from the Poitou-Tate sequence (A.4.10) factors through the canonical epimorphism

$$H^1(G_{\infty,\Sigma}, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee \twoheadrightarrow \mathrm{Sel}(F_\infty, T^*(1))^\vee.$$

We show this at the level of each F_n for $\mathrm{Sel}(F_n, T^*(1))^\vee$ and then pass to the limit. Let F and Σ be as before. We extract from (A.4.2) the exact sequence

$$\bigoplus_{\nu\in\Sigma} H^1(F_\nu, T) \longrightarrow H^1(G_\Sigma, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee \longrightarrow H^2(G_\Sigma, T)$$

and consider its dual

$$H^2(G_\Sigma, T)^\vee \longrightarrow H^1(G_\Sigma, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\lambda^1} \bigoplus_{\nu\in\Sigma} H^1(F_\nu, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p),$$

where we use local Tate duality $\bigoplus_{\nu\in\Sigma} H^1(F_\nu, T)^\vee \cong \bigoplus_{\nu\in\Sigma} H^1(F_\nu, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)$ (note that for H^1 local Tate duality also holds for archimedean places, see ([Rub00], Theorem 1.4.1)). By exactness, $H^2(G_\Sigma, T)^\vee$ maps onto $\ker(\lambda^1)$ which certainly is contained in $\mathrm{Sel}(F, T^*(1))$. But this implies that $H^1(G_\Sigma, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee \longrightarrow H^2(G_\Sigma, T)$ factors through $\mathrm{Sel}(F, T^*(1))^\vee$. This holds for each fields F_n, $n \geq 1$. Passing to the projective limit we get a commutative diagram

$$\begin{array}{ccc} H^1(G_{\infty,\Sigma}, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee & \longrightarrow & \varprojlim_n H^2(G_{n,\Sigma}, T), \\ \downarrow\!\!\downarrow & \nearrow & \\ \mathrm{Sel}(F_\infty, T^*(1))^\vee & & \end{array} \tag{4.2.1}$$

where we note that the vertical limit map is surjective as the dual of the injection $\mathrm{Sel}(F_\infty, T^*(1)) \hookrightarrow H^1(G_{\infty,\Sigma}, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)$. Substituting $\mathrm{Sel}(F_\infty, T^*(1))^\vee$ for $H^1(G_{\infty,\Sigma}, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee$ into the Poitou-Tate sequence (A.4.10) we preserve exactness at $\mathrm{Sel}(F_\infty, T^*(1))^\vee$ and all the following terms, but lose exactness at $\varprojlim_n \bigoplus_{\nu\in\Sigma_{n,f}} H^1(F_{n,\nu}, T)$ because the kernel of the composite map

$$\varprojlim_n \bigoplus_{\nu\in\Sigma_{n,f}} H^1(F_{n,\nu}, T) \longrightarrow H^1(G_{\infty,\Sigma}, T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee \twoheadrightarrow \mathrm{Sel}(F_\infty, T^*(1))^\vee$$

is, in general, larger than the kernel of just the first map. In order to remedy this failure of exactness, we need to introduce the finite parts of cohomology for compact modules T and discrete modules $T\otimes\mathbb{Q}_p/\mathbb{Z}_p$ that we defined at the beginning of this chapter.

We remark that our definition of $H^1_f(F_\nu, T\otimes\mathbb{Q}_p/\mathbb{Z}_p)$ coincides with the definition of $H_{f,(2)}(F_\nu, W)$ for discrete modules W of the form $(\mathbb{Q}_p/\mathbb{Z}_p)^k$ given in ([FK06], 4.2.28). We now recall an important duality result. We will write $H^i_{/f}(\dots)$ for the quotient $H^i(\dots)/H^i_f(\dots)$ both in local and in global settings.

Proposition 4.2.1. *Let F be a number field, Σ a finite set of places containing Σ_p, and T a finitely generated free $\mathbb{Z}_p$-module endowed with a $\mathbb{Z}_p$-linear continuous action of G_F that is unramified outside Σ. Assume for $\nu\in\Sigma_p$ that $T\otimes\mathbb{Q}_p$ is de Rham as a representation of G_{F_ν}. Then, for any $\nu\in\Sigma$ (archimedean primes included) the subgroups*

$$H^1_f(F_\nu, T) \qquad \text{and} \qquad H^1_f(F_\nu, T^*(1)\otimes\mathbb{Q}/\mathbb{Z})$$

are exact annihilators of each other with respect to the perfect pairing

$$H^1(F_\nu, T) \times H^1(F_\nu, T^*(1) \otimes \mathbb{Q}/\mathbb{Z}) \longrightarrow H^1(F_\nu, \mathbb{Q}_p/\mathbb{Z}_p(1)) \cong \mathbb{Q}_p/\mathbb{Z}_p$$

that induces local Tate duality. See section A.2 for our definition of perfect pairing.

Proof. A full proof of this duality result is obtained as follows. Combine ([BK90], Proposition 3.8) for the case $\nu \in \Sigma_p$ and de Rham $V = T \otimes \mathbb{Q}_p$ with ([Rub00], chapter 1, propositions 1.4.2 and 1.4.3) to see that

$$H^1_f(F_\nu, T) = H^1_f(F_\nu, T^*(1) \otimes \mathbb{Q}/\mathbb{Z})^\perp,$$

for any $\nu \in \Sigma$, i.e., that $H^1_f(F_\nu, T)$ is the exact annihilator of $H^1_f(F_\nu, T^*(1) \otimes \mathbb{Q}/\mathbb{Z})$. The identity $H^1_f(F_\nu, T)^\perp = H^1_f(F_\nu, T^*(1) \otimes \mathbb{Q}/\mathbb{Z})$ then follows from proposition A.2.1 for $\nu \in \Sigma_f$, compare also example A.2.2. We note that the statement is trivially true for archimedean primes $\nu \in \Sigma_\infty$, since, by definition,

$$H^1_f(F_\nu, T) = H^1(F_\nu, T) \qquad \text{and} \qquad H^1_f(F_\nu, T \otimes \mathbb{Q}_p/\mathbb{Z}_p) = 0$$

for $\nu \in \Sigma_\infty$. □

Moreover, proposition A.2.1 shows that we get an isomorphism

$$H^1_f(F_\nu, T) \cong H^1_{/f}(F_\nu, T^*(1) \otimes \mathbb{Q}/\mathbb{Z})^\vee,$$

for any $\nu \in \Sigma$. For T as in the proposition we have

$$\begin{aligned}
&\mathrm{Sel}(F, T^*(1))^\vee \\
&= \ker\Big(H^1(G_\Sigma, T^*(1) \otimes \mathbb{Q}/\mathbb{Z}) \longrightarrow \bigoplus_{\nu \in \Sigma} H^1_{/f}(F_\nu, T^*(1) \otimes \mathbb{Q}/\mathbb{Z})\Big)^\vee \\
&\cong \mathrm{coker}\Big(\bigoplus_{\nu \in \Sigma} H^1_f(F_\nu, T) \longrightarrow H^1(\mathcal{O}_F[1/\Sigma], T^*(1) \otimes \mathbb{Q}/\mathbb{Z})^\vee\Big).
\end{aligned}$$

It is now clear that we have to pass to the quotient $\oplus_{\nu \in \Sigma} H^1(F_\nu, T)/H^1_f(F_\nu, T)$ in order to preserve exactness when substituting $\mathrm{Sel}(F, T^*(1))^\vee$ for $H^1(G_\Sigma, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ in the Poitou-Tate sequence (A.4.10). In order to guarantee exactness at $H^1(G_\Sigma(F), T)$ (when cutting off the sequence (A.4.10) before this term), we define $H^1_f(G_\Sigma(F), T)$ to be the preimage of $\oplus_{\nu \in \Sigma} H^1_f(F_\nu, T)$ under the map

$$H^1(G_\Sigma(F), T) \longrightarrow \bigoplus_{\nu \in \Sigma} H^1(F_\nu, T).$$

We conclude this section with the result of the above considerations, which is analogous to the exact sequences Kato considers for the set Σ_p in ([Kat04], (14.9.3)) and which Perrin-Riou considers in both ([PR00], Appendix A.3.) and ([PR92], chapters 3 and 4).

Corollary 4.2.2. *In the setting and under the assumptions of Proposition 4.2.1, the Poitou-Tate sequence from (A.4.2) yields a six term exact sequence*

$$0 \to H^1_{/f}(G_\Sigma, T) \to \bigoplus_{\Sigma_f} H^1_{/f}(F_\nu, T) \longrightarrow \mathrm{Sel}(F, T^*(1))^\vee \to H^2(G_\Sigma, T) \to \prod_{\nu \in \Sigma_f} H^2(F_\nu, T) \to H^0(G_\Sigma, T^\vee(1))^\vee \to 0, \tag{4.2.2}$$

where we note that for $\nu \in \Sigma_\infty$ we have $H^1_{/f}(F_\nu, T) = 0$ by definition of $H^1_f(F_\nu, T)$. Likewise, the dual Poitou-Tate sequence from (A.4.3) gives an exact sequence

$$0 \to H^1_{/f}(G_\Sigma, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \to \bigoplus_{\Sigma} H^1_{/f}(F_\nu, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \to H^1_f(G_\Sigma, T)^\vee \to H^2(G_\Sigma, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \prod_{\nu \in \Sigma_f} H^0(F_\nu, T)^\vee \longrightarrow H^0(G_\Sigma, T)^\vee \to 0. \tag{4.2.3}$$

Later we will use projective limits (passing through finite subextensions of a p-adic Lie extension F_∞/F) of the above sequences in order to derive relations in the group $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$. However, in order to get exact sequences in $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$ we will have to pass to quotients of the corresponding modules by appropriate submodules related to our fixed global and local units $u \in \mathcal{U}$ and $u' \in \mathcal{U}'$.

4.3 Tate Module of an abelian variety

In this subsection we consider an abelian variety A of dimension d defined over a number field F with good reduction at all primes above a fixed prime p. We will separately study (projective limits of) the modules appearing in the exact sequence (4.2.2) for $T = T_pA$.

We are particularly interested in the following case. We fix algebraic closures $\overline{\mathbb{Q}}$, $\overline{\mathbb{Q}}_p$ and an embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$. All algebraic extensions of $\mathbb{Q}$ are considered inside $\overline{\mathbb{Q}}$. Now, let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and good ordinary reduction at p. Consider the extension $K_\infty = \cup_n K_n$, where $K_n = K(E[p^n])$ (inside $\overline{\mathbb{Q}}$). We write $\mathfrak{p}$ (resp. ν) for the prime of K (resp. K_∞) above p that is determined by the embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$. Moreover, we set $\Sigma_f = \{p\} \cup \Sigma_{\mathrm{bad}}$, where Σ_{bad} is the finite set of primes where E has bad reduction.

Under the assumption that p splits in $\mathcal{O}_K$ we are able to prove that $\varprojlim_n H^1_f(G_{n,\Sigma}, T) = 0$ so that (as we will see) passing to the projective limit of the general exact sequence (4.2.2) with respect to the K_n and the corestriction and dual restriction maps yields an exact sequence isomorphic to

$$\begin{aligned}
0 \longrightarrow H^1(G_\Sigma(\mathbb{Q}), \Lambda(\mathcal{G})^\# \otimes T) &\longrightarrow \operatorname{Ind}_{\mathcal{G}}^{\mathcal{G}'} H^1(\mathbb{Q}_p, \Lambda(\mathcal{G}')^\# \otimes T/T^0) \longrightarrow \\
\operatorname{Sel}(K_\infty, T^*(1))^\vee &\longrightarrow H^2(G_\Sigma(\mathbb{Q}), \Lambda^\# \otimes T) \longrightarrow \\
\bigoplus_{q \in \Sigma_f} \operatorname{Ind}_{\mathcal{G}}^{\mathcal{G}_{\nu_q}} T(-1) &\longrightarrow T(-1) \longrightarrow 0.
\end{aligned} \tag{4.3.1}$$

where $\mathcal{G} = \operatorname{Gal}(K_\infty/\mathbb{Q})$, $\mathcal{G}' = \operatorname{Gal}(K_{\infty,\nu}/\mathbb{Q}_p)$, $\mathcal{G}_{\nu_q} = \operatorname{Gal}(K_{\infty,\nu_q}/\mathbb{Q}_q)$, where for every $q \in \Sigma_f$ we fix a prime ν_q of K_∞ above q, $T = T_pE$ and $T^0 = T_pE \cap M_p^0(p)$. The $\mathbb{Q}_p$-vector space $M_p^0(p)$ is defined as follows.

Let us denote the other prime of K above p by $\bar{\mathfrak{p}}$, $\bar{\mathfrak{p}} \neq \mathfrak{p}$. Since K has class number one, we may fix an $\mathcal{O}_K$-generator π of $\mathfrak{p}$ and a generator $\bar{\pi}$ of $\bar{\mathfrak{p}}$. We have $\mathbb{Q}_p = K_{\mathfrak{p}}$ and π is a uniformizer for $\mathcal{O}_{K_{\mathfrak{p}}}$, i.e., a generator of the maximal ideal of $\mathcal{O}_{K_{\mathfrak{p}}}$. Note that $\bar{\pi}$ is a unit in $\mathcal{O}_{K_{\mathfrak{p}}}$, i.e., belongs to $\mathcal{O}_{K_{\mathfrak{p}}}^\times$.

For any finite extension L of K in $\overline{\mathbb{Q}}$ we write $\nu = \nu_L$ for the prime of L above $\mathfrak{p}$ determined by the embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ and L_ν, which is a finite extension of $K_{\mathfrak{p}}$, for the completion at ν. Moreover, we write $\mathfrak{m}_{L_\nu}$ for the maximal ideal of the ring of integers $\mathcal{O}_{L_\nu}$ of L_ν. Note that $\bar{\pi}$ belongs to the units $\mathcal{O}_{L_\nu}^\times$. Let us write $\mathfrak{m}$ for $\mathfrak{m} = \bigcup_L \mathfrak{m}_{L_\nu}$ in $\bigcup_L L_\nu$, where the union is taken over all finite subextensions $L/\mathbb{Q}$ of $\overline{\mathbb{Q}}/K$. Considering E as an elliptic curve over $K_{\mathfrak{p}}$, we then have exact sequences

$$0 \longrightarrow \widehat{E}(\mathfrak{m}_{L_\nu}) \longrightarrow E(L_\nu) \xrightarrow{red_{\mathfrak{p}}} \tilde{E}(k_{L_\nu}) \longrightarrow 0, \qquad K \subset L \subset \overline{\mathbb{Q}},\ [L:K] < \infty,$$

where $\widehat{E}$ is the formal group law associated to E, k_{L_ν} denotes the residue field of L_ν and $red_{\mathfrak{p}}$ is the reduction map to the elliptic curve $\tilde{E}$ with coefficients in $\mathbb{F}_p$. Passing to the inductive limit gives

$$0 \longrightarrow \widehat{E}(\mathfrak{m}) \longrightarrow E(\overline{\mathbb{Q}}_p) \xrightarrow{red_{\mathfrak{p}}} \tilde{E}(\overline{\mathbb{F}}_p) \longrightarrow 0,$$

which induces an injection of Galois modules

$$T_pE/T_p\widehat{E} \hookrightarrow T_p\tilde{E}. \tag{4.3.2}$$

Note that the p-power division points in $\widehat{E}(\mathfrak{m})$ are actually π-power division points since the element $\bar{\pi}$ is a unit in $\mathcal{O}_{K_{\mathfrak{p}}}^\times$ and therefore defines an isomorphism of the formal group $\widehat{E}/\mathcal{O}_{K_{\mathfrak{p}}}$ (and hence of $\widehat{E}(\mathfrak{m})$), see ([Ser10], section 3.3, proposition 3). We define

$$M_p^0(p) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(\widehat{E})$$

and recall that we defined $T^0 = T_pE \cap M_p^0(p)$, so clearly $T_p(\widehat{E}) \subset T^0$. Recall that due to our ordinary good reduction assumption $T_p\tilde{E}$ and $T_p\widehat{E}$ are both free of rank 1 as $\mathbb{Z}_p$-modules. Since $T_pE/T_p\widehat{E} \neq 0$ embeds into the free $\mathbb{Z}_p$-module $T_p\tilde{E} \cong \mathbb{Z}_p$, it is itself free of rank 1. The module T/T^0 is a natural quotient of $T_pE/T_p\widehat{E}$ such that $\mathbb{Q}_p \otimes T/T^0$ has $\mathbb{Q}_p$-dimension 1. Therefore, T/T^0 must be free of rank 1 as a $\mathbb{Z}_p$-module and it follows that $T_pE/T_p\widehat{E} \cong T/T^0$. Therefore and since $T_p(\widehat{E}) \subset T^0$ we have

$$T_p\widehat{E} = T^0.$$

We recall that the action of $G_{\mathbb{Q}_p}$ on $T_p\tilde{E}$ factors through $G_{\mathbb{F}_p}$, i.e., is unramified. Therefore, the action on $T/T_p\widehat{E} = T/T^0$ is unramified.

4.3.1 First local cohomology groups for $\nu \in \Sigma_f \smallsetminus \Sigma_p$

Assume that the abelian variety A/F has good reduction at all places of F above p. We will prove the following proposition for primes belonging to $\Sigma_f \smallsetminus \Sigma_p = \Sigma_{\text{bad}}$, the finite places where A/F has bad reduction.

Proposition 4.3.1. *For $T = T_pA$ and a finite place ν of F where A has bad reduction, we have*

$$H^1(F_\nu, T)/H^1_f(F_\nu, T) = 0$$

for the modules $H^1(F_\nu, T)/H^1_f(F_\nu, T)$ from the sequence (4.2.2).

We write V_pA for $T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Let $A^\vee$ be the dual abelian variety of A and recall that there is a non-degenerate $\mathbb{Z}_p$-bilinear (Weil) pairing

$$T_pA \times T_p(A^\vee) \longrightarrow \mathbb{Z}_p(1)$$

that commutes with the action of G_F, see, for example, ([Mum85], section 20. Riemann forms). This pairing induces a G_F-isomorphism $(V_pA)^*(1) \cong V_p(A^\vee)$.

We recall a well-known theorem proven by Lutz (in the case of an elliptic curve) und Mattuck (in the general case), describing the structure of rational points over local fields. Let ν be a finite place of F above the prime l of $\mathbb{Q}$. A proof of the theorem can be found in Mattuck's paper ([Mat55], VI, 13., Theorem 7, p. 114).

Theorem 4.3.2. *The group $A(F_\nu)$ of F_ν-rational points of A contains a subgroup of finite index that is isomorphic to $d = \dim(A)$ copies of $\mathcal{O}_{F_\nu}$, the ring of integers of F_ν. In symbols, there is an isomorphism*

$$A(F_\nu) \cong \mathcal{O}_{F_\nu}^d \times (\text{a finite group}).$$

In particular, for a prime p, $p \neq l$, $A(F_\nu)$ does not contain an element of order a power of p that is infinitely divisible by p, i.e., in terms of the Tate module of $A(F_\nu)$, $T_pA(F_\nu) = 0$.

Now, let the setting be as in Proposition 4.2.1, in particular we consider a free $\mathbb{Z}_p$-module T with a continuous $\mathbb{Z}_p$-linear Galois action. Propositions 4.2.1 and A.2.1 imply that for any $\nu \in \Sigma_f$ we have

$$\left(H^1(F_\nu, T)/H^1_f(F_\nu, T)\right)^\vee \cong H^1_f(F_\nu, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p), \tag{4.3.3}$$

which holds without any restriction for $\nu \in \Sigma_f \smallsetminus \Sigma_p$, while for $\nu \in \Sigma_p$, in general, one has to assume that the G_{F_ν}-representation $T \otimes \mathbb{Q}_p$ is de Rham.

We now give a proof of proposition 4.3.1, which is rather lengthy (but gives more information on the Galois actions invloved). After this proof we give another, shorter one, so the reader may skip the following one and proceed with the other proof that uses Mattuck's theorem.

Proof (of Proposition 4.3.1). We use equation (4.3.3) for $T = T_pA$ and $\nu \in \Sigma_{\mathrm{bad}}$, a place of F where A has bad reduction. So we have to show that

$$H^1_f(F_\nu, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = 0.$$

By definition, $H^1_f(F_\nu, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ is the image of $H^1_f(F_\nu, T^*(1) \otimes \mathbb{Q}_p)$ under the canonical map

$$H^1(F_\nu, T^*(1) \otimes \mathbb{Q}_p) \longrightarrow H^1(F_\nu, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p).$$

Hence it is sufficient to prove that $H^1_f(F_\nu, T^*(1) \otimes \mathbb{Q}_p)$ vanishes for $T = T_pA$ and a finite place ν of Σ not above p. We have remarked above that the Weil pairing induces an isomorphism $T^*(1) \otimes \mathbb{Q}_p \cong (V_pA)^*(1) \cong V_p(A^\vee)$. Using this isomorphism and the inflation-restriction exact sequence, we get

$$H^1_f(F_\nu, T^*(1) \otimes \mathbb{Q}_p) \cong H^1\left(G(F_\nu^{\mathrm{ur}}/F_\nu), H^0(G_{F_\nu^{\mathrm{ur}}}, V_p(A^\vee))\right),$$

but the group on the right vanishes, see ([BK90], Example 3.11), which we want to show next for elliptic curves. If A is an elliptic curve then $A^\vee = A$.

As for the vanishing of $H^1\left(G(F_\nu^{\mathrm{ur}}/F_\nu), H^0(G_{F_\nu^{\mathrm{ur}}}, V_pE)\right)$, Malte Witte explained to me a proof that works for elliptic curves E and places ν of bad reduction. We sketch this proof. So let E be an elliptic curve defined over F and let ν be a place of F where E has bad reduction. Write $l \in \mathbb{Z}$ for the prime below ν. Let p be a prime different from l. We write $k_\nu \cong \mathbb{F}_{l^r}$ for the residue field of ν and $\overline{k_\nu}$ for an algebraic closure. We consider the two exact sequences found in ([Sil86], VII. proof of Theorem 7.1). Firstly, consider

$$0 \longrightarrow E_0(F_\nu^{\mathrm{ur}}) \longrightarrow E(F_\nu^{\mathrm{ur}}) \longrightarrow E(F_\nu^{\mathrm{ur}})/E_0(F_\nu^{\mathrm{ur}}) \longrightarrow 0,$$

where $E_0(F_\nu^{\mathrm{ur}})$ is the subset of points of $E(F_\nu^{\mathrm{ur}})$ that under the reduction map $E(F_\nu^{\mathrm{ur}}) \longrightarrow \tilde{E}(\overline{k_\nu})$ map to a nonsingular point in $\tilde{E}_{\mathrm{ns}}(\overline{k_\nu}) \subset \tilde{E}(\overline{k_\nu})$, and, secondly, we have,

$$0 \longrightarrow E_1(F_\nu^{\mathrm{ur}}) \longrightarrow E_0(F_\nu^{\mathrm{ur}}) \longrightarrow \tilde{E}_{\mathrm{ns}}(\overline{k_\nu}) \longrightarrow 0, \tag{4.3.4}$$

where $E_1(F_\nu^{\mathrm{ur}})$ is the kernel of the reduction map, and, by a fact about formal groups, does not have any non-trivial p-torsion. Now, assume that $H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE \otimes \mathbb{Q}_p)$ is non-trivial (if it is trivial then there is nothing to show). By proposition A.3.12 we have $H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE \otimes \mathbb{Q}_p) \cong H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE) \otimes \mathbb{Q}_p$ and, hence, the Tate module for F_ν^{ur}-rational points $\varprojlim_n E(F_\nu^{\mathrm{ur}})[p^n]$ has positive $\mathbb{Z}_p$-rank. But $E(F_\nu^{\mathrm{ur}})/E_0(F_\nu^{\mathrm{ur}})$ is finite, due to Kodaira and Néron, see ([Sil86], VII. Theorem 6.1), and hence $\varprojlim_n E_0(F_\nu^{\mathrm{ur}})[p^n]$ is non-trivial. In fact, if p^r is the maximal power of p that divides the cardinality of $E(F_\nu^{\mathrm{ur}})/E_0(F_\nu^{\mathrm{ur}})$ and $(t_n)_{n\geq 1}$ is a non-trivial element that belongs to $\varprojlim_n E(F_\nu^{\mathrm{ur}})[p^n]$, then $p^r t_{n+r} = t_n$ belongs to $E_0(F_\nu^{\mathrm{ur}})$ for all $n \in \mathbb{N}$. Hence, $(t_n)_{n\geq 1}$ also belongs to $\varprojlim_n E_0(F_\nu^{\mathrm{ur}})[p^n]$. We have just seen that $H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE) = \varprojlim_n E(F_\nu^{\mathrm{ur}})[p^n]$ is equal to $\varprojlim_n E_0(F_\nu^{\mathrm{ur}})[p^n]$. Now, by the exact sequence (4.3.4), and since $E_1(F_\nu^{\mathrm{ur}})$ does not contain any non-trivial p-torsion, we have an embedding

$$\varprojlim_n E_0(F_\nu^{\mathrm{ur}})[p^n] \hookrightarrow \varprojlim_n \tilde{E}_{\mathrm{ns}}(\overline{k_\nu})[p^n]. \tag{4.3.5}$$

Recall that the reduction type of E over F_ν is the same as the reduction type of E over F_ν^{ur}, compare ([Sil86], VII. Proposition 5.4 (a)). Now, if E had additive reduction over F_ν^{ur}, then, we would have an equality $\tilde{E}_{\mathrm{ns}}(\overline{k_\nu}) \cong \overline{k_\nu}$, which is impossible, because $\overline{k_\nu}$ does not have any p-torsion. So E must have multiplicative reduction over F_ν^{ur} (and therefore over F_ν), which implies $\tilde{E}_{\mathrm{ns}}(\overline{k_\nu}) \cong (\overline{k_\nu})^\times$ (as abelian groups), see ([Sil86], VII, §5, proposition 5.1 (b)). In case the reduction is non-split multiplicative, then the isomorphism of abelian groups $\tilde{E}_{\mathrm{ns}}(\overline{k_\nu}) \cong (\overline{k_\nu})^\times$ need not be $G(F_\nu^{\mathrm{ur}}/F_\nu)$-linear. However, if $P \in \tilde{E}(\overline{k_\nu})$ denotes the node, i.e., the singular point of the reduced curve, let us write k_ν' for the finite extension of k_ν obtained by adjoining the coefficients of the two distinct tangent lines at P. Then, write L for the finite extension of F_ν inside F_ν^{ur} corresponding to k_ν' such that we have canonically $G(F_\nu^{\mathrm{ur}}/L) \cong G(\overline{k_\nu}/k_\nu')$. It now follows from the explicit description of the isomorphism $\tilde{E}_{\mathrm{ns}}(\overline{k_\nu}) \cong (\overline{k_\nu})^\times$ that it is $G(F_\nu^{\mathrm{ur}}/L)$-linear, see (loc. cit., III, §2, proposition 2.5 (a)). In particular, we have a $G(F_\nu^{\mathrm{ur}}/L)$-isomorphism

$$\varprojlim_n \tilde{E}_{\mathrm{ns}}(\overline{k_\nu})[p^n] \cong \mathbb{Z}_p(1).$$

We conclude from this and from (4.3.5) that $H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE) \cong \varprojlim_n E_0(F_\nu^{\mathrm{ur}})[p^n]$ is a free $\mathbb{Z}_p$-module of rank 1 and that we have an isomorphism

$$H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE) \otimes \mathbb{Q}_p \cong \big(\varprojlim_n E_0(F_\nu^{\mathrm{ur}})[p^n]\big) \otimes \mathbb{Q}_p \cong \big(\varprojlim_n \tilde{E}_{\mathrm{ns}}(\overline{k_\nu})[p^n]\big) \otimes \mathbb{Q}_p \cong \mathbb{Q}_p(1)$$

of $G(F_\nu^{\mathrm{ur}}/L)$-modules. In particular, the Frobenius in $G(F_\nu^{\mathrm{ur}}/L)$, and therefore the Frobenius in $G(F_\nu^{\mathrm{ur}}/F_\nu)$, do not act trivially on $H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE)$. Let us write $\chi : G(F_\nu^{\mathrm{ur}}/F_\nu) \longrightarrow \mathbb{Z}_p^\times$ for the character giving the action on $H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE)$ (restricted to $G(F_\nu^{\mathrm{ur}}/L)$ this is the cyclotomic character).

Then, we have $H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE \otimes \mathbb{Q}_p) \cong \mathbb{Q}_p(\chi)$. The first cohomology group of the Prüfer ring $\hat{\mathbb{Z}} \cong G(F_\nu^{\mathrm{ur}}/F_\nu)$ for modules as in our situation is well-known, see ([Rub00], Appendix B, Lemma B.2.8) or ([Ser95], XIII, §1), and given by

$$H^1\big(G(F_\nu^{\mathrm{ur}}/F_\nu), \mathbb{Q}_p(\chi)\big) = \mathbb{Q}_p(\chi)\big/\big(1 - \chi(\mathrm{Frob}_\nu)\big)\mathbb{Q}_p(\chi) = 0,$$

which holds, since the Frobenius does not act trivially on $\mathbb{Q}_p(\chi)$. This completes the proof. □

Of course, in the last step, we could have also used the inflation-restriction sequence to conclude that

$$H^1\big(G(F_\nu^{\mathrm{ur}}/F_\nu), H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE \otimes \mathbb{Q}_p)\big) = 0$$

using the facts that $H^1\big(G(F_\nu^{\mathrm{ur}}/L), \mathbb{Q}_p(1)\big) = 0$ and that $H^0(G_L, T_pE \otimes \mathbb{Q}_p) \cong H^0(G_L, T_pE) \otimes \mathbb{Q}_p = 0$ by Mattuck's theorem.

After writing up the above proof, the author found a similar, but shorter one using Mattuck's theorem as suggested in ([BK90], Example 3.11).

Proof (of Proposition 4.3.1, second version). As in the first proof one reduces to showing that $H^1\big(G(F_\nu^{\mathrm{ur}}/F_\nu), H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE \otimes \mathbb{Q}_p)\big) = 0$. Since E/F has bad reduction at $\nu \in \Sigma_{\mathrm{bad}}$, $G_{F_\nu^{\mathrm{ur}}}$ does not act trivially on the Tate-module T_pE. Therefore, $\dim_{\mathbb{Q}_p}\big((T_pE \otimes \mathbb{Q}_p)^{G_{F_\nu^{\mathrm{ur}}}}\big) < 2$. If $\dim_{\mathbb{Q}_p}\big((T_pE \otimes \mathbb{Q}_p)^{G_{F_\nu^{\mathrm{ur}}}}\big) = 0$ we are done, so assume $\dim_{\mathbb{Q}_p}\big((T_pE \otimes \mathbb{Q}_p)^{G_{F_\nu^{\mathrm{ur}}}}\big) = 1$. If the Frobenius of $G(F_\nu^{\mathrm{ur}}/F_\nu)$ acted trivially on $(T_pE \otimes \mathbb{Q}_p)^{G_{F_\nu^{\mathrm{ur}}}}$ then we would have $\dim_{\mathbb{Q}_p}\big((T_pE \otimes \mathbb{Q}_p)^{G_{F_\nu}}\big) = 1$, which is a contradiction by Mattuck's theorem (using that taking cohomology commutes with $- \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$). Therefore, the Frobenius does not act trivially, and we have

$$H^1\big(G(F_\nu^{\mathrm{ur}}/F_\nu), H^0(G_{F_\nu^{\mathrm{ur}}}, T_pE \otimes \mathbb{Q}_p)\big) \cong (T_pE \otimes \mathbb{Q}_p)^{G_{F_\nu^{\mathrm{ur}}}} \big/ \big((1 - \chi(\mathrm{Frob}_\nu))(T_pE \otimes \mathbb{Q}_p)^{G_{F_\nu^{\mathrm{ur}}}}\big) = 0$$

by the well-known formula for the first cohomology groups of $\hat{\mathbb{Z}}$, where $\chi(\mathrm{Frob}_\nu) \in \mathbb{Q}_p^\times \smallsetminus \{1\}$ is the element that gives the action of the Frobenius on $(T_pE \otimes \mathbb{Q}_p)^{G_{F_\nu^{\mathrm{ur}}}}$. □

4.3.2 First local cohomology groups for $\nu \in \Sigma_p$

We write $A^\vee$ for the dual abelian variety of A. We will now study the groups $H^1(F_\nu, T)/H^1_f(F_\nu, T)$ for $T = T_pA$ and places $\nu \in \Sigma_p$. Recall the non-degenerate $\mathbb{Z}_p$-bilinear Weil pairing

$$T_pA \times T_p(A^\vee) \longrightarrow \mathbb{Z}_p(1),$$

see ([Mum85], section 20. Riemann forms), which induces an isomorphism $T_pA \cong T_p(A^\vee)^*(1)$, see example A.2.1. Propositions 4.2.1 and A.2.1 imply that

$$\big(H^1(F_\nu, T)/H^1_f(F_\nu, T)\big)^\vee \cong H^1_f(F_\nu, T^\vee(1)), \tag{4.3.6}$$

for which we note that the Tate module of an abelian variety is de Rham as a representation of G_{F_ν} for $\nu \in \Sigma_p$, see the work of Fontaine [Fon82]. Recall that $T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong T^\vee(1)$ is isomorphic to the p-primary part $A^\vee(\overline{F}_\nu)\{p\} = \bigcup_n A^\vee(\overline{F}_\nu)[p^n]$ of $\overline{F}_\nu$-rational points $A^\vee(\overline{F}_\nu)$ of $A^\vee$; note that there is a natural isomorphism $A \cong (A^\vee)^\vee$, see ([Mum85], p. 81) or ([Mil08], I, section 8). In order to avoid confusion, note that our T is isomorphic to Fukaya and Kato's module T_0, a Galois stable $\mathbb{Z}_p$-lattice of the p-adic realization of the motive $h^1(A^\vee)(1)$.

We have already noted that our definition of H^1_f for discrete modules like $T^\vee(1)$ coincides with the definition of $H^1_{f,(2)}$ found in ([FK06], 4.2.28) and goes back originally to the paper [BK90] of Bloch and Kato. However, there is a second definition due to Greenberg of a finite part of the first local cohomology group given in [Gre89]. In our setting of an abelian variety and a place ν above p one uses the unique G_{F_ν}-stable $\mathbb{Q}_p$-subspace of $M_p = V_p(A) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(A)$, denoted by $M_p^0(\nu)$ in ([FK06], 4.2.3), that satisfies

$$D_{dR}(F_v, M_p^0(\nu)) \cong D_{dR}(F_v, M_p)/D^0_{dR}(F_v, M_p).$$

The existence of this subspace (for a general motive M and its p-adic realization) is called the condition of Dabrowski-Panchishkin. In ([Ven05], Chapter 6, p. 25) Venjakob explains that for the motive $M = h(A^\vee)(1)$, where $A^\vee/\mathbb{Q}$ is an abelian variety with good ordinary reduction at $\nu = p$, $M_p^0(\nu)$ is given by $V_p(\widehat{A}) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(\widehat{A})$, where $\widehat{A}$ is the formal group associated to A (the $\mathfrak{m}$-valued points of which give the kernel of the reduction map at ν, $\mathfrak{m}$ is the valuation ideal of $\overline{\mathbb{Q}}_p$). See also the article [Nek93] by Nekovář, in particular, 1.28 - 1.31, which includes the definition of an ordinary p-adic Galois representation and ([Nek06], (9.6.7.2)) by the same author. For more information on the theory of ordinary representations see also [PR94] and [Gre89].

Now, we come to the definition of Greenberg's finite cohomology group which is denoted by $H^1_{f,(1)}(F_v, T^\vee(1))$ in the paper of Fukaya and Kato.

Definition 4.3.3 (Greenberg's H^1_f). *We write*

$$T^0(\nu) = T \cap M_p^0(\nu) \tag{4.3.7}$$

for a G_{F_ν}-stable $\mathbb{Z}_p$-lattice of $V_p(\widehat{A})$ and define $H^1_{f,(1)}(F_v, T^\vee(1))$ to be the kernel of the natural map

$$H^1(F_\nu, T^\vee(1)) \longrightarrow H^1(F_\nu, (T^0(\nu))^\vee(1))$$

induced by the embedding $T^0(\nu) \subset T$.

We now specialize to $A = E$, an elliptic curve defined over F with good ordinary reduction above p, so that $A = A^\vee$. For a place ν above p Fukaya and Kato then show, see ([FK06], Lemma 4.2.32), that

$$H^1_{f,(2)}(F_v, T^\vee(1)) = H^1_{f,(1)}(F_v, T^\vee(1))(\mathrm{div}),$$

where the right hand side denotes the divisible part of $H^1_{f,(1)}(F_v, T^\vee(1))$. In order to be able to apply the quoted Lemma we note that $H^0(F_\nu, M_p/M_p^0(\nu)) = 0 = H^0(F_\nu, (M_p^0(\nu))^*(1))$, see ([FK06], 4.2.31).

For our purposes it is important to consider the situation for the whole tower $F \subset F_n \subset F_\infty$, where $F_n = F(E[p^n])$, $F_\infty = \cup_n F_n$. We will write $F_n F_\nu$ for the composite field of F_n and F_ν inside a fixed algebraic closure $\overline{F}_\nu$, $\overline{F} \subset \overline{F}_\nu$. The proof of ([FK06], proposition 4.2.30), the conditions of which are met by E/F with good ordinary reduction at every place above p and the extension F_∞/F, see (loc. cit., 4.2.31), shows the following proposition.

Proposition 4.3.4. *Passing to the inductive limit with respect to $n \in \mathbb{N}$ we get an equality*

$$\varinjlim_n H^1_{f,(1)}(F_\nu F_n, T^\vee(1)) = \varinjlim_n H^1_{f,(2)}(F_\nu F_n, T^\vee(1))$$

as subgroups of $H^1(F_\nu F_\infty, T^\vee(1))$.

From this proposition and the duality result (4.3.6) we conclude that for a prime ν of F above p we have

$$\begin{aligned}\varprojlim_n H^1(F_\nu F_n, T)/H^1_f(F_\nu F_n, T) &\cong \big(\varinjlim_n H^1_{f,(2)}(F_\nu F_n, T^\vee(1))\big)^\vee \\ &\cong \big(\varinjlim_n H^1_{f,(1)}(F_\nu F_n, T^\vee(1))\big)^\vee \\ &\cong \varprojlim_n \operatorname{coker}\big(H^1(F_\nu F_n, T^0(\nu)) \longrightarrow H^1(F_\nu F_n, T)\big),\end{aligned} \tag{4.3.8}$$

where, in the last equation, we use local Tate duality and the fact that for a map $\varphi : M \longrightarrow N$, we have $\ker(\varphi)^\vee = \operatorname{coker}(\varphi^\vee)$. Let us write $\operatorname{Coker}(\nu, n) = \operatorname{coker}\big(H^1(F_\nu F_n, T^0(\nu)) \longrightarrow H^1(F_\nu F_n, T)\big)$. By the long exact cohomology sequences attached to

$$0 \longrightarrow T^0(\nu) \longrightarrow T \longrightarrow T/T^0(\nu) \longrightarrow 0$$

we have exact sequences for all $n \geq 1$

$$0 \to \operatorname{Coker}(\nu, n) \to H^1(F_\nu F_n, T/T^0(\nu)) \to H^2(F_\nu F_n, T^0(\nu)) \to H^2(F_\nu F_n, T) \to \dots$$

in which all modules are projective limits of finite modules and therefore compact, compare propositions A.3.2 and A.3.4. Passing to the projective limit with respect to $n \geq 1$, we get an exact sequence and we want to show that the map

$$\varprojlim_n \operatorname{Coker}(\nu, n) \to \varprojlim_n H^1(F_\nu F_n, T/T^0(\nu)) \tag{4.3.9}$$

is an isomorphism. By exactness of the sequence, this amounts to showing that the image of the map $\varprojlim_n H^1(F_\nu F_n, T/T^0(\nu)) \to \varprojlim_n H^2(F_\nu F_n, T^0(\nu))$ is equal to 0. But the image of the latter map is equal to the kernel of $\varprojlim_n H^2(F_\nu F_n, T^0(\nu)) \to \varprojlim_n H^2(F_\nu F_n, T)$, which, we will now show, is injective.

By local Tate duality we have

$$\varprojlim_n H^2(F_\nu F_n, T) \cong \big(\varinjlim_n H^0(F_\nu F_n, T^\vee(1))\big)^\vee \cong H^0(F_\nu F_\infty, T^\vee(1))^\vee \cong T(-1),$$

where the last equation holds since $G_{F_\nu F_\infty}$ acts trivially on $T^\vee(1)$ (remember F_∞ is precisely the trivializing extension for T and it contains $F(\mu_{p^\infty})$). Likewise we have

$$\varprojlim_n H^2(F_\nu F_n, T^0(\nu)) \cong T^0(\nu)(-1)$$

and we see that $\varprojlim_n H^2(F_\nu F_n, T^0(\nu)) \to \varprojlim_n H^2(F_\nu F_n, T)$ is just the embedding $T^0(\nu)(-1) \hookrightarrow T(-1)$. We conclude that the map from (4.3.9) is an isomorphism. The next proposition is the main result of this subsection and summarizes the above observations.

Proposition 4.3.5. *Let E be an elliptic curve defined over a number field F with good ordinary reduction at all primes above p. Then, for all $\nu \in \Sigma_p$ we have an isomorphism*

$$\varprojlim_n H^1(F_\nu F_n, T)/H^1_f(F_\nu F_n, T) \cong \varprojlim_n H^1(F_\nu F_n, T/T^0(\nu)),$$

where $T = T_pE$ and $T^0(\nu)$ is as in (4.3.7).

Remark 4.3.6. We want to remark that the results in this subsection are easily generalized to Galois-stable $\mathbb{Z}_p$-lattices T of M_p for motives M over F and extensions F_∞/F such that

(i) the p-adic realization M_p is ordinary as a representation of G_{F_ν} for all places ν above p,

(ii) F_∞/F is a trivializing extension for M_p, i.e., G_{F_∞} acts trivially on M_p, and $F_{cyc} \subset F_\infty$,

(iii) M/F satisfies the assumptions of ([FK06], proposition 4.2.30).

Note that when M_p is ordinary as a representation of G_{F_ν}, $\nu \in \Sigma_p$, then it is semistable, see ([Nek93], 1.30 Theorem), and therefore de Rham, so we may apply the duality result of Bloch and Kato for the finite parts of the local cohomology groups. Moreover, if M_p is ordinary at each prime above ν, then the condition of Dabrowski-Panchishkin is satisfied, see ([Nek93], 6.7).

We conclude this subsection by giving a more concrete description of the finite part $H^1_f(F_\nu, V_pA)$ for the Tate module $V_pA = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_pA$ of an abelian variety A/F with scalars extended to $\mathbb{Q}_p$. By ([BK90], Example 3.11, p. 361) we have an isomorphism

$$A(F_\nu) \otimes \mathbb{Q} \cong H^1_f(F_\nu, V_pA),$$

which is induced by the limit of the boundary maps of the Kummer sequences

$$A(F_\nu) \hookrightarrow \varprojlim_m A(F_\nu)/p^m A(F_\nu) \hookrightarrow H^1(F_\nu, T_pA).$$

We note that $A(F_\nu) \otimes \mathbb{Q}$ is actually a finitely generated $\mathbb{Q}_p$-vector space by Mattuck's theorem.

4.3.3 Second local cohomology groups

Assume we are given a p-adic Lie extension F_∞/F such that $F(\mu_{p^\infty}) \subset F_\infty$ and $\cup_n F_n = F_\infty$, where each F_n is a finite Galois extension of F. Also T is a free finitely generated $\mathbb{Z}_p$-module with G_F-action. Moreover, assume that F_∞ trivializes T, i.e., G_{F_∞} acts trivially on T. We consider the groups $\bigoplus_{\nu\in\Sigma_n} H^2(F_{n,\nu},T)$, where $\Sigma_{n,f}$ denotes the set of primes of F_n above Σ_f. Using local Tate duality, we have

$$\begin{aligned}\varprojlim_n \bigoplus_{\nu\in\Sigma_{n,f}} H^2(F_{n,\nu},T) &= \varprojlim_n \bigoplus_{\nu\in\Sigma_{n,f}} H^0(F_{n,\nu},T^\vee(1))^\vee \\ &= \big(\varinjlim_n \bigoplus_{\nu\in\Sigma_{n,f}} H^0(F_{n,\nu},T^\vee(1))\big)^\vee \\ &= \big(\bigoplus_{\nu\in\Sigma_f} \mathrm{Coind}_G^{G_\nu} H^0(F_{\infty,\bar\nu},T^\vee(1))\big)^\vee \\ &= \bigoplus_{\nu\in\Sigma_f} \mathrm{c\text{-}Ind}_G^{G_\nu} T(-1).\end{aligned}$$

4.3.4 First global cohomology groups

We now consider the groups $H^1(G_\Sigma,T)/H^1_f(G_\Sigma,T)$. For a more detailed study of the finite parts $H^1_{f,\Sigma}(F,T)$ for general T see the work of Bloch and Kato ([BK90], chapter 5) and of Perrin-Riou and Fontaine ([FPR91], Chapitre II, 1.3, p. 643f). The notation used in these sources differs slightly from ours. With our notation, for a representation V unramified outside a finite set of places Σ

$$H^1_f(G_\Sigma(F),V) = \ker\big(H^1(G_\Sigma,V) \longrightarrow \bigoplus_{\nu\in\Sigma} H^1_{/f}(F_\nu,V)\big)$$

and $H^1_f(G_\Sigma(F),T)$ is the inverse image of $H^1_f(G_\Sigma(F),V)$ in $H^1(G_\Sigma(F),T)$. In the notation of [FPR91] Σ is not mentioned explicitly and our $H^1_f(G_\Sigma(F),V)$ is denoted $H^1_f(F,V)$.

Conjecturally, see Perrin-Riou's work ([PR92], p. 137f), for the motive $M = h^1(A)(1)$ associated to an abelian variety A defined over a number field F, we have an isomorphism

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} H^1_f(F,M) \cong H^1_f(G_\Sigma(F),V_pA),$$

where $H^1_f(F,M)$ denotes the first motivic cohomology group. In our case $H^1_f(F,M) \cong \mathbb{Q}\otimes_{\mathbb{Z}} A(F)$, see, for example, Flach's survey article [Fla04].

In the next subsection we study the example of an elliptic curve $E/\mathbb{Q}$ with complex multiplication and good ordinary reduction at p and show that $\varprojlim_n H^1_f(G_{n,\Sigma},T) = 0$ for $T = T_pE$.

4.3.5 Vanishing of $\varprojlim_n H^1_f(G_{n,\Sigma},T_pE)$ for $E/\mathbb{Q}$ with CM and good ordinary reduction at split p

Fix a prime number $p \in \mathbb{Z}_p$, $p \neq 2$, and embeddings $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ and $\overline{\mathbb{Q}} \subset \mathbb{C}$. Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and good reduction at p and set $K_\infty = \cup_n K_n$, where $K_n = K(E[p^n])$. We assume that p splits in K, i.e., $\mathcal{O}_K p = \mathfrak{p}\bar{\mathfrak{p}}$, $\bar{\mathfrak{p}} \neq \mathfrak{p}$, which implies that E has good ordinary reduction at $\mathfrak{p}$, see proposition A.6.2.

We will use the same notation as at the beginning of section 4.3. In particular, we write $\mathfrak{p}$ (resp. $\bar\nu$) for the prime of K (resp. K_∞) above p that is determined by the embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$.

Moreover, we set $\mathcal{G} = G(K_\infty/\mathbb{Q})$, $G = G(K_\infty/K)$ and $\mathcal{G}' = G(K_{\infty,\bar{\nu}}/\mathbb{Q}_p)$. We identify $G(K_{\infty,\bar{\nu}}/\mathbb{Q}_p)$ with the decomposition group of $\bar{\nu}$ in $\mathcal{G}$.

Recall that we have $T_0 = T_p\hat{E}$. In this subsection we will study the first map appearing in the Poitou-Tate sequence (4.3.1)

$$H^1(G_\Sigma(\mathbb{Q}), \Lambda(\mathcal{G})^\# \otimes T) \longrightarrow \mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'} H^1(\mathbb{Q}_p, \Lambda(\mathcal{G}')^\# \otimes (T/T^0)), \tag{4.3.10}$$

the kernel of which is precisely $\varprojlim_n H^1_f(G_{n,\Sigma}, T)$. We want to show that this kernel vanishes when p splits in $\mathcal{O}_K$. For any Galois-module M we write $M(-1) = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(-1)$ for the -1-Tate twist. We recall that we have an isomorphism

$$T(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma \cong H^1(G_\Sigma(\mathbb{Q}), \Lambda(\mathcal{G})^\# \otimes T)$$

of $\Lambda(\mathcal{G})$-modules and an isomorphism

$$(T/T^0)(-1) \otimes H^1(\mathbb{Q}_p, \Lambda(\mathcal{G}')^\#(1)) \cong H^1(\mathbb{Q}_p, \Lambda(\mathcal{G}')^\# \otimes (T/T^0)),$$

of $\Lambda(\mathcal{G}')$-modules, which both follow from corollary A.3.10. Therefore, we have to study the induced map

$$T(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma \longrightarrow \mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'} \Big((T/T^0)(-1) \otimes H^1(\mathbb{Q}_p, \Lambda(\mathcal{G}')^\#(1)) \Big) \tag{4.3.11}$$

and show that it is injective; recall that $\mathbb{H}^1_\Sigma \cong \varprojlim_n H^1(G_\Sigma(K_n), \mathbb{Z}_p(1))$. The map (4.3.11) is given by

$$(t \otimes \epsilon_0) \otimes f \longmapsto \sum_{\sigma \in \mathcal{G}/\mathcal{G}'} \sigma \otimes [\sigma^{-1} t] \otimes \sigma^{-1}\epsilon_0 \otimes loc_{\bar{\nu}}(\sigma^{-1} f), \tag{4.3.12}$$

where we write ϵ_0 for some fixed generator of $\mathbb{Z}_p(-1)$, $[\tilde{t}]$ for the image of $\tilde{t} \in T$ in T/T_0 and $loc_{\bar{\nu}}$ for the following composition. We compose the localization map λ^1 from the Poitou-Tate sequence (A.4.13) with the projection to the $\mathfrak{p}$-part, compare diagram (4.3.14) below, and we compose this composition with the natural map $\mathrm{Ind}M \cong \mathrm{Coind}M \to M$ that exists for any M. The resulting map $\mathbb{H}^1_\Sigma \to H^1(\mathbb{Q}_p, \Lambda(\mathcal{G}')^\#(1))$ is denoted by $loc_{\bar{\nu}}$ (in terms of units this is the natural map $\bar{\mathcal{E}}_\infty \longrightarrow \mathcal{U}'(K_{\infty,\bar{\nu}})$ from global to principal local units).

Let us consider the isomorphism between T_pE and $\mathrm{Ind}_{G_\mathbb{Q}}^{G_K} T_\pi E$, as described in subsection A.6.4. ψ_E, the Größencharacter attached to E, gives the action of G on $T_\pi E$. Recall that we write $\bar{\nu}$ for the prime of K_∞ above $\mathfrak{p}$ determined by the embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ and defined $\mathcal{G}' = G(K_{\infty,\bar{\nu}}/\mathbb{Q}_p)$. We note that due to the splitting assumption the decomposition groups of $\bar{\nu}$ in G and $\mathcal{G}$ coincide, i.e., if we write $G' = G(K_{\infty,\bar{\nu}}/K_\mathfrak{p})$, then $G' = \mathcal{G}'$. In particular, $H^1(\mathbb{Q}_p, \Lambda(\mathcal{G}')^\#(1)) = H^1(K_\mathfrak{p}, \Lambda(G')^\#(1))$. The map $[\iota_{\bar{\pi}}] : T_{\bar{\pi}}E \xrightarrow{\sim} T_pE/T_p\hat{E}$ from (A.6.19) is G'-equivariant. We get a G'-equivariant map

$$T_{\bar{\pi}}E(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma \longrightarrow (T/T^0)(-1) \otimes_{\mathbb{Z}_p} H^1(K_\mathfrak{p}, \Lambda(G')^\#(1))$$

given by

$$t \otimes \epsilon_0 \otimes f \longmapsto [\iota_{\bar{\pi}}](t) \otimes \epsilon_0 \otimes loc_{\bar{\nu}}(f). \tag{4.3.13}$$

For every $\mathfrak{q} \in \Sigma_f$ fix a prime $\bar{\nu}_{\mathfrak{q}}$ of K_∞ above $\mathfrak{q}$ (of course, we choose $\bar{\nu}$ above $\mathfrak{p}$). We then have the following commutative diagram

$$\begin{array}{ccc} \mathbb{H}^1_\Sigma & \xhookrightarrow{\lambda^1} \bigoplus_{\mathfrak{q}\in\Sigma_f(K)} \mathrm{Ind}_G^{G_\mathfrak{q}} \varprojlim_n H^1(K_{n,\bar{\nu}_\mathfrak{q}}, \mathbb{Z}_p(1)) \twoheadrightarrow & \mathrm{Ind}_G^{G'} H^1(K_\mathfrak{p}, \Lambda(G')^\#(1)) \\ \uparrow \cong & & \uparrow = \\ \varprojlim_n (\mathcal{O}^\times_{K_n} \otimes_\mathbb{Z} \mathbb{Z}_p) & \hookrightarrow & \mathrm{Ind}_G^{G'} \varprojlim_n \hat{\mathcal{O}}^\times_{K_{n,\bar{\nu}}} \end{array} \tag{4.3.14}$$

where the vertical map on the left, by (2.2.3), is an isomorphism since K_∞/K contains a $\mathbb{Z}_p$-extension of K unramified at $\mathfrak{p}$ (which is the one in $K(E[\bar{\pi}^\infty])/K$) and another one unramified at $\bar{\mathfrak{p}}$, (the one in $K(E[\pi^\infty])/K$). Moreover, the vertical map on the right is an isomorphism since $K_{\infty,\bar{\nu}}/K_\mathfrak{p}$ contains an unramified $\mathbb{Z}_p$-extension (the one contained in the compositum $K(E[\bar{\pi}^\infty])K_\mathfrak{p}$), compare ([Ven13], section 2.1). The lower horizontal map is injective since we have seen that the Leopoldt conjecture (which is a theorem for the abelian extensions K_n/K) implies that for each n, $n \geq 1$, $\mathcal{O}^\times_{K_n} \otimes_\mathbb{Z} \mathbb{Z}_p \hookrightarrow \bigoplus_{\omega|\mathfrak{p}} \hat{\mathcal{O}}^\times_{K_{n,\omega}}$ is injective, where we only sum over the primes ω of K_n that lie above $\mathfrak{p}$ and not over all that lie above p, i.e., we omit the ones lying above $\bar{\mathfrak{p}}$, see subsection 2.4.2. We conclude that the composite of the upper horizontal maps in (4.3.14) is injective.

Remark 4.3.7. That the map $\mathbb{H}^1_\Sigma \longrightarrow \mathrm{Ind}_\mathcal{G}^{\mathcal{G}'} H^1(\mathbb{Q}_p, \Lambda(\mathcal{G}')^\#(1)) = \mathrm{Ind}_\mathcal{G}^{G'} H^1(K_\mathfrak{p}, \Lambda(G')^\#(1))$, where we induce up to $\mathcal{G}$, is injective we already knew from the usual (or even weak) Leopoldt conjecture. For the injectivity of the composite of the upper horizontal maps in (4.3.14), however, we needed the stronger version of Leopoldt's conjecture that we stated in subsection 2.4.2.

Now, note that since G' is of finite index in G, there is an isomorphism of functors between $\mathrm{Ind}_G^{G'}$ and $\mathrm{Coind}_G^{G'}$. The map $loc_{\bar{\nu}}$ appearing in (4.3.13) is the map

$$loc_{\bar{\nu}} : \mathbb{H}^1_\Sigma \longrightarrow H^1(K_\mathfrak{p}, \Lambda(G')^\#(1))$$

that induces, by the universal property of $\mathrm{Coind}_G^{G'} \cong \mathrm{Ind}_G^{G'}$, the composite of the upper horizontal maps in (4.3.14), i.e., so that this composite is given by

$$\mathbb{H}^1_\Sigma \ni f \longmapsto \sum_{\bar{\sigma}\in G/G'} \left(\sigma \otimes loc_{\bar{\nu}}(\sigma^{-1} f)\right) \in \mathrm{Ind}_G^{G'} H^1(K_\mathfrak{p}, \Lambda(G')^\#(1)). \tag{4.3.15}$$

By the universal property of $\mathrm{Coind}_G^{G'} \cong \mathrm{Ind}_G^{G'}$ the map (4.3.13) induces the following G-equivariant map

$$T_{\bar{\pi}} E(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma \longrightarrow \mathrm{Ind}_G^{G'}\Big((T/T^0)(-1) \otimes_{\mathbb{Z}_p} H^1(K_\mathfrak{p}, \Lambda(G')^\#(1))\Big) \tag{4.3.16}$$

given by

$$t \otimes \epsilon_0 \otimes f \longmapsto \sum_{\bar\sigma \in G/G'} \sigma \otimes [\iota_{\bar\pi}](\sigma^{-1}t) \otimes \sigma^{-1}\epsilon_0 \otimes loc_{\bar\nu}(\sigma^{-1}f).$$

Note that $\sigma^{-1}\epsilon_0 = \kappa(\sigma)\epsilon_0$, where κ denotes the cyclotomic character. We claim that the map (4.3.16) is injective. Indeed, fixing a $\mathbb{Z}_p$-generator t of the free $\mathbb{Z}_p$-module $T_{\bar\pi}E$ of rank 1, we first see that any element of $T_{\bar\pi}E(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma$ can be written in the form $t \otimes \epsilon_0 \otimes f$ for some $f \in \mathbb{H}^1_\Sigma$.

Recall that G' is of finite index in G and note that for any $\mathbb{Z}_p[G']$-module M we have an isomorphism

$$\bigoplus_{\bar\sigma \in G/G'} \sigma M \cong \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[G']} M = \mathrm{Ind}_G^{G'} M, \qquad (\sigma m_{\bar\sigma})_{\bar\sigma} \longmapsto \sum_{\bar\sigma \in G/G'} \sigma \otimes m_{\bar\sigma},$$

where σM is just M as a $\mathbb{Z}_p$-module. Hence, for the injectivity of (4.3.16) it is sufficient to show that if $(t \otimes \epsilon_0 \otimes f) \neq 0$, then there is at least one coset $\bar\sigma \in G/G'$ such that $[\iota_{\bar\pi}](\sigma^{-1}t) \otimes \kappa(\sigma)\epsilon_0 \otimes loc_{\bar\nu}(\sigma^{-1}f) \neq 0$.

So let $(t \otimes \epsilon_0 \otimes f) \neq 0$. By the injectivity of the composite of the upper horizontal maps in (4.3.14) which is given explicitly by (4.3.15) we must have $loc_{\bar\nu}(\sigma^{-1}f) \neq 0$ for at least one $\bar\sigma \in G/G'$. Let $\bar\sigma$ be such a coset. Since $t \neq 0$ we have $\kappa(\sigma)\sigma^{-1}t \neq 0$ and therefore the image $[\iota_{\bar\pi}](\kappa(\sigma)\sigma^{-1}t)$ under the injective map $[\iota_{\bar\pi}]$ from (A.6.19) is non-zero in the free $\mathbb{Z}_p$-module $T_pE/T_p\widehat{E} \cong T/T^0$ of rank 1, (recall that due to our ordinary reduction assumption $T_pE/T_p\widehat{E} \neq 0$ embeds into $T_p\tilde{E} \cong \mathbb{Z}_p$, see (4.3.2)). Fixing a $\mathbb{Z}_p$-generator t' of $T_pE/T_p\widehat{E}$ we can write

$$[\iota_{\bar\pi}](\kappa(\sigma)\sigma^{-1}t) = at'$$

for some $a \in \mathbb{Z}_p$, $a \neq 0$. Noting that

$$(T/T^0)(-1) \otimes_{\mathbb{Z}_p} H^1(K_{\mathfrak{p}}, \Lambda(G')^{\#}(1)) \cong H^1(K_{\mathfrak{p}}, \Lambda(G')^{\#}(1)), \quad bt' \otimes \epsilon_0 \otimes g \longmapsto b \cdot g,$$

defines a $\mathbb{Z}_p$-linear isomorphism, we can conclude our proof that (4.3.16) is injective by observing that under the isomorphism just defined $[\iota_{\bar\pi}](\sigma^{-1}t) \otimes \kappa(\sigma)\epsilon_0 \otimes loc_{\bar\nu}(\sigma^{-1}f)$ maps to

$$a \cdot loc_{\bar\nu}(\sigma^{-1}f) \neq 0$$

which is not zero since $H^1(K_{\mathfrak{p}}, \Lambda(G')^{\#}(1))$ has no non-trivial p-torsion. For the last fact we quote Wintenberger's result ([Win80], section 4, Théorème (i)), see also Yager's ([Yag82], section 8, Lemma 23, p.436) or Rubin ([Rub91], Theorem 5.1 (ii)). Recall that $\bar\nu$ is the prime of F_∞ above $\mathfrak{p}$ determined by $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$. Wintenberger's result says that $H^1(K_{\mathfrak{p}}, \Lambda(G')^{\#}(1)) \cong \varprojlim_n \widehat{K}^\times_{n,\bar\nu}$ embeds into a free $\Lambda(G')$-module of rank 1, and hence it does not have any p-torsion. Recall that $\widehat{K}^\times_{n,\bar\nu}$ is the p-adic completion of $K^\times_{n,\bar\nu}$. Let us note that we may actually apply Winternberger's result since G', as a subgroup of finite index in $G \cong \mathbb{Z}_p^2 \times (\mathbb{Z}_p/(p-1))^2$, is itself of the form $\mathbb{Z}_p^2 \times \Delta'$, with Δ' finite and $p \nmid \#\Delta'$.

To conclude, we have shown that the map from (4.3.16) is injective. Now, note that in (4.3.16) we considered $\mathbb{H}^1_\Sigma$ as a G-module, which it is by restriction from its $\mathcal{G}$-action. Therefore, using the identification

$$T_pE(-1) \otimes \mathbb{H}^1_\Sigma \cong \operatorname{Ind}^G_{\mathcal{G}}\big(T_{\bar\pi}E(-1) \otimes \mathbb{H}^1_\Sigma\big),$$

compare remark 4.3.8, and applying the exact functor $\operatorname{Ind}^G_{\mathcal{G}}$ to (4.3.16) yields the map from (4.3.11) and shows that it is injective. Since it is not entirely obvious (one has to be careful when using the identifications of Ind and Coind) that applying $\operatorname{Ind}^G_{\mathcal{G}}$ to (4.3.16) yields the map from (4.3.11), we show that it does in the following remark.

Remark 4.3.8. First recall that for a general G-module M and a $\mathcal{G}$-module N one has the canonical $\mathcal{G}$-isomorphism

$$\operatorname{Ind}^G_{\mathcal{G}}(M \otimes \operatorname{Res}^{\mathcal{G}}_G N) \cong (\operatorname{Ind}^G_{\mathcal{G}} M) \otimes N, \tag{4.3.17}$$

given by

$$1 \otimes (m_1 \otimes n_1) + c \otimes (m_2 \otimes n_2) \longmapsto (1 \otimes m_1) \otimes n_1 + (c \otimes m_2) \otimes cn_2,$$

where $c \in \mathcal{G}$ denotes the complex conjugation isomorphism, compare ([Lan05] XVIII, Theorem 7.11). We will use this isomorphism twice below. Recall the isomorphism $T_pE \to T_\pi E \times T_{\bar\pi}E$, $t \mapsto (t_\pi, t_{\bar\pi})$ from (A.6.12) and also the isomorphism $T_\pi E \times T_{\bar\pi}E \cong \operatorname{Ind}^G_{\mathcal{G}} T_{\bar\pi}E$ given by

$$(y, z) \longmapsto (c \otimes c^{-1}y) + (1 \otimes z),$$

the inverse of which is the natural map induced by $T_{\bar\pi}E \hookrightarrow T_\pi E \times T_{\bar\pi}E$.

We will use the following identifications

$$\begin{aligned}
\big[T_pE \otimes \mathbb{Z}_p(-1)\big] \otimes \mathbb{H}^1_\Sigma &\cong \big[(T_\pi E \times T_{\bar\pi}E) \otimes \mathbb{Z}_p(-1)\big] \otimes \mathbb{H}^1_\Sigma \\
&\cong \big[(\operatorname{Ind}^G_{\mathcal{G}} T_{\bar\pi}E) \otimes \mathbb{Z}_p(-1)\big] \otimes \mathbb{H}^1_\Sigma \\
&\cong \big[\operatorname{Ind}^G_{\mathcal{G}}\big(T_{\bar\pi}E \otimes \mathbb{Z}_p(-1)\big)\big] \otimes \mathbb{H}^1_\Sigma && \text{use (4.3.17)} \\
&\cong \operatorname{Ind}^G_{\mathcal{G}}\big[T_{\bar\pi}E \otimes \mathbb{Z}_p(-1) \otimes \mathbb{H}^1_\Sigma\big] && \text{use (4.3.17)}
\end{aligned}$$

under which an element of the form $t \otimes \epsilon_0 \otimes f$ in $\big[T_pE \otimes \mathbb{Z}_p(-1)\big] \otimes \mathbb{H}^1_\Sigma$ maps to

$$\begin{aligned}
(t \otimes \epsilon_0) \otimes f &\longmapsto \Big((t_\pi, t_{\bar\pi}) \otimes \epsilon_0\Big) \otimes f \\
&\longmapsto \Big(\big((c \otimes c^{-1}t_\pi) + (1 \otimes t_{\bar\pi})\big) \otimes \epsilon_0\Big) \otimes f \\
&\longmapsto \Big(\big(c \otimes (c^{-1}t_\pi \otimes c^{-1}\epsilon_0)\big) + \big(1 \otimes (t_{\bar\pi} \otimes \epsilon_0)\big)\Big) \otimes f \\
&\longmapsto \Big(c \otimes \big(c^{-1}t_\pi \otimes c^{-1}\epsilon_0 \otimes c^{-1}f\big)\Big) + \Big(1 \otimes \big(t_{\bar\pi} \otimes \epsilon_0 \otimes f\big)\Big).
\end{aligned} \tag{4.3.18}$$

Under the map

$$\operatorname{Ind}^G_{\mathcal{G}}\big[T_{\bar\pi}E(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma\big] \longrightarrow \operatorname{Ind}^G_{\mathcal{G}}\Big[\operatorname{Ind}^{G'}_G\Big((T/T^0)(-1) \otimes_{\mathbb{Z}_p} H^1(K_{\mathfrak{p}}, \Lambda(G')^\#(1))\Big)\Big]$$

induced by (4.3.16), the element from (4.3.18) maps to

$$c \otimes \Big(\sum_{\bar\sigma \in G/G'} \sigma \otimes [\iota_{\bar\pi}](\sigma^{-1}c^{-1}t_\pi) \otimes \sigma^{-1}c^{-1}\epsilon_0 \otimes loc_{\bar\nu}(\sigma^{-1}c^{-1}f)\Big)$$
$$+ 1 \otimes \Big(\sum_{\bar\sigma \in G/G'} \sigma \otimes [\iota_{\bar\pi}](\sigma^{-1}t_{\bar\pi}) \otimes \sigma^{-1}\epsilon_0 \otimes loc_{\bar\nu}(\sigma^{-1}f)\Big). \quad (4.3.19)$$

We know by remark A.6.14 that $[\iota_{\bar\pi}](\sigma^{-1}c^{-1}t_\pi) = [\sigma^{-1}c^{-1}t]$ and $[\iota_{\bar\pi}](\sigma^{-1}t_{\bar\pi}) = [\sigma^{-1}t]$ in $T_pE/T_p\hat{E}$ for any $\sigma \in G$, where we use the brackets $[-]$ to denote the residue classes modulo $T_p\hat{E}$. Hence, the element from (4.3.19), under the canonical map $\mathrm{Ind}_{\mathcal{G}}^{G}\mathrm{Ind}_{G}^{G'} \cdots \cong \mathrm{Ind}_{\mathcal{G}}^{G'} \ldots$ maps to

$$\Big(\sum_{\bar\sigma \in G/G'} c\sigma \otimes [\sigma^{-1}c^{-1}t] \otimes \sigma^{-1}c^{-1}\epsilon_0 \otimes loc_{\bar\nu}(\sigma^{-1}c^{-1}f)\Big)$$
$$+ \Big(\sum_{\bar\sigma \in G/G'} \sigma \otimes [\sigma^{-1}t] \otimes \sigma^{-1}\epsilon_0 \otimes loc_{\bar\nu}(\sigma^{-1}f)\Big)$$
$$= \sum_{\bar\sigma \in \mathcal{G}/G'} \sigma \otimes [\sigma^{-1}t] \otimes \sigma^{-1}\epsilon_0 \otimes loc_{\bar\nu}(\sigma^{-1}f),$$

which, since elements of the form $t \otimes \epsilon_0 \otimes f$ generate $\big[T_pE \otimes \mathbb{Z}_p(-1)\big] \otimes \mathbb{H}^1_\Sigma$, shows that applying $\mathrm{Ind}_{\mathcal{G}}^{G}$ to (4.3.16) and using the above standard identifications indeed yields the map from (4.3.11).

4.3.6 Second global cohomology group

Let the setting be as in the last subsection, i.e., we are given a p-adic Lie extension F_∞/F such that $F(\mu_{p^\infty}) \subset F_\infty$ and $\cup_n F_n = F_\infty$, where each F_n is a finite Galois extension of F. As above, T is a free finitely generated $\mathbb{Z}_p$-module with continuous G_Σ-action which factors through G. We then have isomorphisms, see section A.3,

$$\varprojlim_n H^2(G_{n,\Sigma}, T) = H^2(G_\Sigma, \Lambda^\# \otimes T)$$
$$= T(-1) \otimes_{\mathbb{Z}_p} H^2(G_\Sigma, \Lambda^\#(1)).$$

Now, we also assume that only finitely many primes ramify in F_∞/F. We then have a short exact sequence, see ([Kat06], p. 555),

$$0 \longrightarrow H^2(G_{\Sigma_p}, \Lambda^\#(1)) \longrightarrow H^2(G_\Sigma, \Lambda^\#(1)) \longrightarrow \bigoplus_{\nu \in \Sigma_f \smallsetminus \Sigma_p} \mathrm{c{-}Ind}_G^{G_\nu}\mathbb{Z}_p \longrightarrow 0.$$

Having studied (the projective limits of) the terms appearing in (4.2.2), we conclude that passing to the projective limit of (4.2.2) for the various F_n yields an exact sequence isomorphic to (4.3.1).

Chapter 5

The element $\Omega_{p,u,u'}$

We will see in this chapter that a choice of global unit u as in assumption 2.3.1 and a choice of local unit u' as in assumption 3.2.1 each canonically determine a generator of $\big(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\big(T_pE/T^0(-1)\otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}}\big)\big)_{\mathcal{S}^*}$ which is a free $\Lambda(\mathcal{G})_{\mathcal{S}^*}$-module of rank 1. The element $\Omega_{p,u,u'}\in\Lambda(\mathcal{G})^\times_{\mathcal{S}^*}$ is then defined to be the *base change* of these two bases. In (5.4.1) we will determine its image in $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$ under the connecting homomorphism from K-theory, which will be an important ingredient in the proof the main theorem 6.2.3 in chapter 6.

5.1 Setting

Fix a prime number $p\in\mathbb{Z}_p$, $p\neq 2$, and embeddings $\overline{\mathbb{Q}}\subset\overline{\mathbb{Q}}_p$ and $\overline{\mathbb{Q}}\subset\mathbb{C}$. Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and good ordinary reduction at p, which we assume to split in the quadratic imaginary number field K.

As before, we set $K_\infty=\cup_n K_n$, where $K_n=K(E[p^n])$. We write $\mathfrak{p}=(\pi)$ (resp. $\bar\nu$) for the prime of K (resp. K_∞) above p that is determined by the embedding $\overline{\mathbb{Q}}\subset\overline{\mathbb{Q}}_p$. The other, complex conjugate prime of K above p we denote by $\bar{\mathfrak{p}}=(\bar\pi)$. Moreover, we set

$$\mathcal{G}=G(K_\infty/\mathbb{Q}),\quad G=G(K_\infty/K)\quad\text{and}\quad \mathcal{G}'=G(K_{\infty,\bar\nu}/\mathbb{Q}_p)=G(K_{\infty,\bar\nu}/K_{\mathfrak{p}})$$

and define subgroups

$$\mathcal{H}=G(K_\infty/\mathbb{Q}^{\mathrm{cyc}}),\quad H=G(K_\infty/K^{\mathrm{cyc}})\quad\text{and}\quad \mathcal{H}'=G(K_{\infty,\bar\nu}/\mathbb{Q}_p^{\mathrm{cyc}})$$

of $\mathcal{G}$, G and $\mathcal{G}'$ respectively. By the splitting assumption we have $G(K_{\infty,\bar\nu}/\mathbb{Q}_p)=G(K_{\infty,\bar\nu}/K_{\mathfrak{p}})$ and we also write G' for $\mathcal{G}'$. This makes sense since when we identify $\mathcal{G}'$ with the decomposition group of $\bar\nu$ in $\mathcal{G}$ (which we will do without further mentioning) it is already a subgroup of G. Note that the extension $K_{\infty,\bar\nu}/\mathbb{Q}_p$ meets all requirements of the setting that we studied in chapter 3. In fact, $G(K_{\infty,\bar\nu}/\mathbb{Q}_p)\subset G$ is abelian, $\cup_n K(E[\bar\pi^n])$ contains a $\mathbb{Z}_p$-extension of K in which $\mathfrak{p}$ is unramified and $\mu_{p^\infty}\subset K_\infty$ by the Weil pairing so that the abelian extension $K_{\infty,\bar\nu}/K_{\mathfrak{p}}$ is indeed of the form $K'(\mu_{p^\infty})/\mathbb{Q}_p$ for some infinite unramified extension $K'/\mathbb{Q}_p$. Let us write Λ' for $\Lambda(\mathcal{G}') = \Lambda(G')$. For the Ore sets as defined in chapters 2 and 3 we write

$$S \subset S^* \subset \Lambda(G), \quad \mathcal{S} \subset \mathcal{S}^* \subset \Lambda(\mathcal{G}) \quad \text{and} \quad \mathcal{S}' \subset \mathcal{S}'^* \subset \Lambda'.$$

Remark 5.1.1. We recall that the discriminant $-D$ of any quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$ as above is divisible by one (positive) prime number in $\mathbb{Z}$ only, which we will denote by l_K, compare ([Sil99], Appendix A, §3) or see subsection A.6.3. In the following we will write Σ for the set of places of K consisting of the places $\Sigma_p = \{\mathfrak{p}, \bar{\mathfrak{p}}\}$ above p, of the complex archimedean place $\Sigma_\infty = \{\nu_\infty\}$ and the places $\Sigma_{\text{bad},K}$ where E/K has bad reduction, i.e.,

$$\Sigma = \Sigma_p \cup \Sigma_\infty \cup \Sigma_{\text{bad},K}$$

Then, we write $\Sigma_{\mathbb{Q}}$ for the places of $\mathbb{Q}$ below those in Σ and *assume* that

$$\mathbb{Q}_{\Sigma_{\mathbb{Q}}} = K_\Sigma, \tag{5.1.1}$$

so that, in particular, $G_\Sigma(K) \subset G_{\Sigma_{\mathbb{Q}}}(\mathbb{Q})$. This condition is satisfied if we choose one of the representatives $E/\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$ with minimal discriminant listed in Appendix A, §3 of Silverman's book [Sil99]. In fact, writing $\mathfrak{f} = \mathfrak{f}_\psi$ for the conductor of the Größencharacter ψ attached to E/K (considered as a curve over K), we know by theorem A.6.8 and proposition A.6.9 that for such a curve

$$\mathfrak{f} = \mathfrak{l}^r, \quad r \geq 1,$$

is a prime power of the unique (l_K ramifies in K) prime ideal $\mathfrak{l}$ lying above $\mathbb{Z}l_K$. Hence, $\Sigma_{\text{bad},K} = \{\mathfrak{l}\}$ so that $\Sigma_{\mathbb{Q}} = \{p\} \cup \{l_K\} \cup \{\nu_{\infty|_{\mathbb{Q}}}\}$ and $\{l_K\}$ coincides with the set $\Sigma_{\text{bad},\mathbb{Q}}$ consisting of the unique prime of $\mathbb{Z}$ at which $E/\mathbb{Q}$ has bad reduction. We conclude that Σ is precisely the set of primes of K above the primes of $\Sigma_{\mathbb{Q}}$ and, since $\Sigma_{\mathbb{Q}}$ contains the unique prime $\mathbb{Z}l_K$ which ramifies in $K/\mathbb{Q}$, that (5.1.1) holds.

Recall that for $m \geq 0$ we defined the global universal cohomology groups

$$\mathbb{H}^m_\Sigma \cong \varprojlim_n H^m(G_\Sigma(K_n), \mathbb{Z}_p(1)) \cong H^m(G_\Sigma(\mathbb{Q}), \Lambda(\mathcal{G})^\#(1)) \cong H^m(G_\Sigma(K), \Lambda(G)^\#(1))$$

Note that, since $G_\Sigma(K) \subset G_{\Sigma_{\mathbb{Q}}}(\mathbb{Q})$, each module $H^m(G_\Sigma(K_n), \mathbb{Z}_p(1))$ naturally carries an action of $G(K_n/\mathbb{Q}) = G_{\Sigma_{\mathbb{Q}}}(\mathbb{Q})/G_\Sigma(K_n)$ and, by restriction, a $G(K_n/K)$-action, just note that K_n, as the composite of K and $\mathbb{Q}(E[p^n])$, is Galois over $\mathbb{Q}$ and see ([NSW08], (1.6.3) Proposition). For $m \geq 0$ we also define local universal cohomology groups

$$\mathbb{H}^m_{\text{loc}} \cong \varprojlim_n H^m(K_{n,\bar{\nu}}, \mathbb{Z}_p(1)) \cong H^m(\mathbb{Q}_p, \Lambda(\mathcal{G}')^\#(1)),$$

where we write $\bar{\nu}$ also for the prime of K_n below the prime $\bar{\nu}$ of K_∞. We set

$$\bar{\mathcal{E}}_\infty = \varprojlim_n (\mathcal{O}_{K_n}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p),$$

for the projective limit of the p-adic completions of the units of K_n, which, for all practical purposes, we identify via the Kummer sequence with $\mathbb{H}_\Sigma^m$

$$\bar{\mathcal{E}}_\infty \cong \mathbb{H}_\Sigma^1,$$

compare (2.2.3). For the principal semi-local units we will write

$$\mathcal{U}_\infty = \varprojlim_n \prod_{\omega|\mathfrak{p}} \mathcal{O}_{K_{n,\omega}}^1 \cong \varprojlim_n \prod_{\omega|\mathfrak{p}} \hat{\mathcal{O}}_{K_{n,\omega}}^\times,$$

where $K_{n,\omega}$ denotes the completion of K_n at the some prime ω of K_n above $\mathfrak{p}$. Note that since the (strong) version of the Leopoldt conjecture holds for the fields K_n, see (2.4.4), we have an embedding $\bar{\mathcal{E}}_\infty \hookrightarrow \mathcal{U}_\infty$. For the local principal units in the extension $K_{\infty,\nu}/\mathbb{Q}_p$ we write

$$\mathcal{U}'(K_{\infty,\bar{\nu}}) = \varprojlim_n \hat{\mathcal{O}}_{K_{n,\bar{\nu}}}^\times.$$

Note that $G' = \mathcal{G}'$ is of finite index in G and that we have an isomorphism

$$\mathrm{Ind}_G^{G'} \mathcal{U}'(K_{\infty,\bar{\nu}}) \;\cong\; \mathcal{U}_\infty$$

induced by the natural embedding $\mathcal{U}'(K_{\infty,\nu}) \hookrightarrow \mathcal{U}_\infty$. Since $K_{\infty,\nu}/\mathbb{Q}_p$ is of infinite residue degree, the Kummer sequence identifies $\mathcal{U}'(K_{\infty,\bar{\nu}})$ with $\mathbb{H}_{\mathrm{loc}}^1$

$$\mathcal{U}'(K_{\infty,\bar{\nu}}) \;\cong\; \mathbb{H}_{\mathrm{loc}}^1.$$

5.2 Choices of u and u'

Recall the assumption 2.3.1 that there exists $u \in \varprojlim_n \mathcal{O}_{K_n}^\times$ such that

$$\Lambda(G)_{S^*} \longrightarrow (\bar{\mathcal{E}}_\infty)_{S^*} \cong (\mathbb{H}_\Sigma^1)_{S^*}, \quad 1 \longmapsto u$$

is an isomorphism of $\Lambda(G)_{S^*}$-modules. Also recall assumption 3.2.1 that there exists $u' \in \mathcal{U}'(K_{\infty,\bar{\nu}})$ such that

$$\Lambda'_{\mathcal{S}'^*} \longrightarrow (\mathcal{U}'(K_{\infty,\bar{\nu}}))_{\mathcal{S}'^*} \cong (\mathbb{H}_{\mathrm{loc}}^1)_{\mathcal{S}'^*}, \quad 1 \longmapsto u'$$

is an isomorphism of $\Lambda'_{\mathcal{S}'^*}$-modules. These assumptions guarantee that the quotients

$$\mathbb{H}_\Sigma^1/\Lambda(G)u \quad \text{and} \quad \mathbb{H}_{\mathrm{loc}}^1/\Lambda(\mathcal{G}')u',$$

are S^*- and $\mathcal{S}'^*$-torsion, i.e., they belong to the categories $S^* - \mathrm{tor} = \mathfrak{M}_H(G)$ and $\mathcal{S}'^* - \mathrm{tor} = \mathfrak{M}_{\mathcal{H}'}(\mathcal{G}')$, respectively. We want to recall the choices of u and u'.

5.2.1 Local Case

Fix a generator ϵ of $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}$ and write K' for the intersection $K_{\infty,\bar{\nu}} \cap \mathbb{Q}_p^{ur}$ in $\overline{\mathbb{Q}}_p$. We defined $\Lambda'_{\varphi_p} := \{x \in \tilde{\Lambda}' \mid \phi(x) = \varphi_p \cdot x\}$, where the arithmetic Frobenius $\phi \in G(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$ acts on the coefficients of $\tilde{\Lambda}' = \widehat{\mathbb{Z}_p^{ur}} \hat{\otimes}_{\mathbb{Z}_p} \Lambda'$ and $\varphi_p \cdot x$ is multiplication of x with the element $\varphi_p = (1, \phi_{|K'}) \in G(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \times G(K'/\mathbb{Q}_p) \cong \mathcal{G}'$. Recall the exact sequence from (3.3.7)

$$0 \longrightarrow \mathcal{U}'(K_{\infty,\bar{\nu}}) \xrightarrow{-\mathcal{L}_{\epsilon^{-1}}} \mathbb{T}_{\mathrm{un}}(K_{\infty,\bar{\nu}}) \otimes_{\Lambda'} \Lambda'_{\varphi_p} \longrightarrow \mathbb{Z}_p(1) \longrightarrow 0 \tag{5.2.1}$$

which, as in [Ven13], was constructed by passing to the limit of Coleman's exact sequences for $\hat{\mathbb{G}}_m$ and the finite unramified subextensions in $K_{\infty,\bar{\nu}}/\mathbb{Q}_p$. The module $\mathbb{T}_{\mathrm{un}}(K_{\infty,\bar{\nu}}) \otimes_{\Lambda'} \Lambda'_{\varphi_p}$ in the middle of (5.2.1) is non-canonically isomorphic to Λ', see (loc. cit. Proposition 2.1 and its proof). Fixing a Λ'-generator λ' of Λ'_{φ_p}, we get an isomorphism

$$\Lambda'_{\mathcal{S}'} \xrightarrow{1 \mapsto 1 \otimes \lambda'} \left(\mathbb{T}_{\mathrm{un}}(K_{\infty,\bar{\nu}}) \otimes_{\Lambda'} \Lambda'_{\varphi_p}\right)_{\mathcal{S}'} \xrightarrow{(-\mathcal{L}_{\epsilon^{-1}})^{-1}_{\mathcal{S}'}} \mathcal{U}'(K_{\infty,\bar{\nu}})_{\mathcal{S}'} \tag{5.2.2}$$

and define the element $u_{\lambda'}/s_{\lambda'} \in \mathcal{U}'(K_{\infty,\bar{\nu}})_{\mathcal{S}'}$ as the image of 1 under this isomorphism. Then $u_{\lambda'}$ is an element satisfying the condition for assumption 3.2.1. Note that for any $\lambda \in \Lambda' \cap (\Lambda'_{\mathcal{S}'})^\times$, the element $\lambda u_{\lambda'}$ also satisfies the condition for assumption 3.2.1.

The annihilator of $u_{\lambda'}$ in Λ' is trivial. Indeed, if $a \in \Lambda'$ annihilates $u_{\lambda'}$, then it annihilates $u_{\lambda'}/s_{\lambda'} \in \mathcal{U}'(K_{\infty,\bar{\nu}})_{\mathcal{S}'}$ and hence also $1 = 1/1 \in \Lambda'_{\mathcal{S}'}$ which means that $a/1 = 0$ in $\Lambda'_{\mathcal{S}'}$ which implies that $a = 0$ since $\mathcal{S}'$ does not contain any zero-divisors, see ([CFK+05], Theorem 2.4).

5.2.2 Global Case

In the global setting we considered compatible systems of elliptic units $e(\mathfrak{a}) \in \varprojlim_n \mathcal{O}^\times_{K_n}$ for an integral ideal $\mathfrak{a}$ of K prime to $6p\mathfrak{f}$, see definition 2.4.24 (we used two variables there to distinguish between π- and $\bar{\pi}$-power torsion points, which is not necessary for our purposes in this chapter). We write $u(\mathfrak{a})$ for the image of $e(\mathfrak{a})$ in $\bar{\mathcal{E}}_\infty \subset \mathcal{U}_\infty$. For the commutative main theorem 2.4.41 we then restricted to a prime ideal $\mathfrak{q}$ of K that, in addition to being prime to $6p\mathfrak{f}$ has norm $N\mathfrak{q}$ congruent to 1 modulo (p). Let us assume that $\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty$ is S^*-torsion, which implies that $\mathbb{H}^1_\Sigma/\Lambda(G)u(\mathfrak{q})$ is S^*-torsion, see remark 2.4.40.

We know from proposition 2.4.28 that λ is a non-zero divisor in $\Lambda(G, \widehat{\mathbb{Z}_p^{ur}})$. Since neither $x_\mathfrak{q} = N(\mathfrak{q}) - \sigma_\mathfrak{q}$ nor $12 \in \mathbb{Z}_p^\times$ are zero divisors, it follows that $12x_\mathfrak{q}\lambda = \mathbb{L}(u(\mathfrak{q}))$ is not a zero divisor in $\Lambda(G, \widehat{\mathbb{Z}_p^{ur}})$. In particular, $\mathrm{ann}_{\Lambda(G)} u(\mathfrak{q}) = 0$. We conclude that $u(\mathfrak{q})$ (or, strictly speaking, $e(\mathfrak{q})$) satisfies the above global assumption under the assumption that $\bar{\mathcal{E}}_\infty/\mathcal{C}_\infty$ is S^*-torsion.

5.3 Definition

Using corollary A.3.10 we extract from the Poitou-Tate sequence (4.3.1) an exact sequence

$$0 \to T(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma \xrightarrow{\text{loc}} \operatorname{Ind}^{\mathcal{G}'}_{\mathcal{G}}\big(T/T^0(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\text{loc}}\big) \to \operatorname{Sel}(K_\infty, T^*(1))^\vee, \tag{5.3.1}$$

where $T = T_pE$ and $T^0 = T_pE \cap V_p(\hat{E})$. As before, we write

$$S \subset S^* \subset \Lambda(G), \quad \mathcal{S} \subset \mathcal{S}^* \subset \Lambda(\mathcal{G}) \quad \text{and} \quad \mathcal{S}' \subset \mathcal{S}'^* \subset \Lambda'.$$

for the canonical Ore sets in $\Lambda(G)$, $\Lambda(\mathcal{G})$ and $\Lambda' = \Lambda(\mathcal{G}') = \Lambda(G')$, respectively, as in (A.8.1) and (A.8.2). Let $u \in \varprojlim_n \mathcal{O}^\times_{K_n}$ and $u' \in \mathcal{U}'(K_{\infty,\bar{\nu}})$ be any global and local units satisfying assumptions 2.3.1 (for G) and 3.2.1, respectively. We also write u and u' for the images in $\mathbb{H}^1_\Sigma$ and $\mathbb{H}^1_{\text{loc}}$, respectively.

5.3.1 Global contribution

Since S^* contains no non-trivial zero divisors by ([CFK+05], Theorem 2.4) we have $\operatorname{ann}_{\Lambda(G)} u = 0$. Hence, we get an exact sequence

$$0 \to \Lambda(G) \xrightarrow{1 \mapsto u} \operatorname{Res}^{\mathcal{G}}_G \mathbb{H}^1_\Sigma \to \mathbb{H}^1_\Sigma / \Lambda(G)u \to 0,$$

where we write $\operatorname{Res}^{\mathcal{G}}_G \mathbb{H}^1_\Sigma$ for $\mathbb{H}^1_\Sigma$ to emphasize that the $\Lambda(G)$ action on $\mathbb{H}^1_\Sigma$ is the restriction of a $\Lambda(\mathcal{G})$-action. We twist this sequence with $T_{\bar{\pi}}(-1) = T_{\bar{\pi}}(E)(-1)$ and get

$$0 \to T_{\bar{\pi}}(-1) \otimes_{\mathbb{Z}_p} \Lambda(G) \to T_{\bar{\pi}}(-1) \otimes_{\mathbb{Z}_p} \operatorname{Res}^{\mathcal{G}}_G \mathbb{H}^1_\Sigma \to T_{\bar{\pi}}(-1) \otimes_{\mathbb{Z}_p} \big(\mathbb{H}^1_\Sigma / \Lambda(G)u\big) \to 0, \tag{5.3.2}$$

where each modules is equipped with the $\Lambda(G)$-action induced by the diagonal G-action. We now fix a basis $t_{\bar{\pi}}$ of $T_{\bar{\pi}} \cong \mathbb{Z}_p$ and, as before, a basis ϵ of $\mathbb{Z}_p(1)$, which determines a basis of $\mathbb{Z}_p(-1)$. Together, $t_{\bar{\pi}}$ and ϵ determine a basis $t = t_{\bar{\pi},\epsilon}$ of $T_{\bar{\pi}}(-1)$, which, in turn, determines an isomorphism

$$\phi_t = \phi_{t_{\bar{\pi},\epsilon}} : T_{\bar{\pi}}(-1) \otimes_{\mathbb{Z}_p} \Lambda(G) \cong \Lambda(G)$$

of left $\Lambda(G)$-modules as in lemma 1.1.1. Using this isomorphism and applying $\operatorname{Ind}^G_{\mathcal{G}}$ to (5.3.2) we get an exact sequence

$$0 \to \Lambda(\mathcal{G}) \xrightarrow{\phi_{t,u}} T_p(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma \to \operatorname{Ind}^G_{\mathcal{G}}\Big(T_{\bar{\pi}}(-1) \otimes_{\mathbb{Z}_p} \big(\mathbb{H}^1_\Sigma / \Lambda(G)u\big)\Big) \to 0, \tag{5.3.3}$$

where we used the isomorphism $\operatorname{Ind}^G_{\mathcal{G}}\big(T_{\bar{\pi}}(-1) \otimes_{\mathbb{Z}_p} \operatorname{Res}^{\mathcal{G}}_G \mathbb{H}^1_\Sigma\big) \cong T_p(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma$.

Remark 5.3.1. We note that for a finitely generated $\Lambda(G)$-module M we canonically have $\operatorname{Ind}^G_{\mathcal{G}} M \cong \Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M$, compare corollary A.8.9.

Since $\mathbb{H}^1_\Sigma/\Lambda(G)u$ is S^*-torsion, lemma 1.1.14 shows that $T_{\tilde{\pi}}(-1)\otimes_{\mathbb{Z}_p}\left(\mathbb{H}^1_\Sigma/\Lambda(G)u\right)$ is S^*-torsion. $T_{\tilde{\pi}}(-1)\otimes_{\mathbb{Z}_p}\left(\mathbb{H}^1_\Sigma/\Lambda(G)u\right)$ is also finitely generated over $\Lambda(G)$, which follows from lemma 1.1.1. Therefore, we may apply corollary A.8.16 stating that $\mathrm{Ind}^G_{\mathcal{G}}\Big(T_{\tilde{\pi}}(-1)\otimes_{\mathbb{Z}_p}\left(\mathbb{H}^1_\Sigma/\Lambda(G)u\right)\Big)$ is then $\mathcal{S}^*$-torsion.

We conclude that the image of 1 under the map $\phi_{t,u}$ from (5.3.3), which is given by

$$\phi_{t,u}(1) = t\otimes u,$$

generates $\left(T_p(-1)\otimes_{\mathbb{Z}_p}\mathbb{H}^1_\Sigma\right)_{\mathcal{S}^*}$ as a $\Lambda(\mathcal{G})_{\mathcal{S}^*}$-module. It also follows from (5.3.3) that in $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$ we have

$$\Big[\left(T_p(-1)\otimes_{\mathbb{Z}_p}\mathbb{H}^1_\Sigma\right)/\Lambda(\mathcal{G})\phi_{t,u}(1)\Big] = \Big[\mathrm{Ind}^G_{\mathcal{G}}\Big(T_{\tilde{\pi}}(-1)\otimes_{\mathbb{Z}_p}\left(\mathbb{H}^1_\Sigma/\Lambda(G)u\right)\Big)\Big]. \tag{5.3.4}$$

5.3.2 Local contribution

In the local situation we proceed similarly and note that while $\mathcal{G}'$ is, in general, not a normal subgroup of $\mathcal{G}$, it still holds that for a finitely generated Λ'-module M we canonically have $\mathrm{Ind}^{\mathcal{G}'}_{\mathcal{G}} M \cong \Lambda(\mathcal{G})\otimes_{\Lambda'} M$, compare corollary A.8.9.

Since S'^* contains no non-trivial zero divisors $\mathrm{ann}_{\Lambda'}(u') = 0$, see ([CFK+05], Theorem 2.4), and we get an exact sequence

$$0\to\Lambda'\xrightarrow{1\mapsto u'}\mathbb{H}^1_{\mathrm{loc}}\to\mathbb{H}^1_{\mathrm{loc}}/\Lambda'u'\to 0.$$

Recall the definition of T^0 from section 4.3 and let us write T for T_pE considered as a G'-module. We twist the above exact sequence with $T' := (T/T^0)(-1)$, which is free as a $\mathbb{Z}_p$-module of rank 1 (it always embedds into $T_p\tilde{E}$, which is free of rank one by our ordinary reduction assumption) and get

$$0\to T'\otimes_{\mathbb{Z}_p}\Lambda'\to T'\otimes_{\mathbb{Z}_p}\mathbb{H}^1_{\mathrm{loc}}\to T'\otimes_{\mathbb{Z}_p}\left(\mathbb{H}^1_{\mathrm{loc}}/\Lambda'u'\right)\to 0. \tag{5.3.5}$$

Fixing a basis t_0 of T/T^0 and a basis ϵ of $\mathbb{Z}_p(1)$ as above (the one induced by the global choice and the fixed embedding $\overline{\mathbb{Q}}\subset\overline{\mathbb{Q}}_p$) we get a basis $t' = t'_{0,\epsilon}$ of T'. This choice determines an isomorphism

$$\phi_{t'} : T'\otimes_{\mathbb{Z}_p}\Lambda'\cong\Lambda'$$

of left Λ'-modules as in lemma 1.1.1. Using this isomorphism and applying $\mathrm{Ind}^{\mathcal{G}'}_{\mathcal{G}}$ to (5.3.5) we get an exact sequence

$$0\to\Lambda(\mathcal{G})\xrightarrow{\phi_{t',u'}}\mathrm{Ind}^{\mathcal{G}'}_{\mathcal{G}}\left(T'\otimes_{\mathbb{Z}_p}\mathbb{H}^1_{\mathrm{loc}}\right)\to\mathrm{Ind}^{\mathcal{G}'}_{\mathcal{G}}\Big(T'\otimes_{\mathbb{Z}_p}\left(\mathbb{H}^1_{\mathrm{loc}}/\Lambda'u'\right)\Big)\to 0. \tag{5.3.6}$$

As in the global case, using ([CFK+05], Proposition 2.3), lemma 1.1.1 and corollary A.8.16, one can show that $\mathrm{Ind}^{\mathcal{G}'}_{\mathcal{G}}\Big(T'\otimes_{\mathbb{Z}_p}\left(\mathbb{H}^1_{\mathrm{loc}}/\Lambda'u'\right)\Big)$ is $\mathcal{S}^*$-torsion.

We conclude that the image of 1 under the map $\phi_{t',u'}$ from (5.3.6), which is given by

$$\phi_{t',u'}(1) = 1\otimes t'\otimes u' \;\in\; \Lambda(\mathcal{G})\otimes_{\Lambda'}\left(T'\otimes_{\mathbb{Z}_p}\mathbb{H}^1_{\mathrm{loc}}\right),$$

generates $\left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T' \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}}\right)\right)_{\mathcal{S}^*}$ as a $\Lambda(\mathcal{G})_{\mathcal{S}^*}$-module. Moreover, it follows from (5.3.6) that in $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$ we have the equality

$$\left[\left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T' \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}}\right)\right)/\Lambda(\mathcal{G})\phi_{t',u'}(1)\right] = \left[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T' \otimes_{\mathbb{Z}_p} \left(\mathbb{H}^1_{\mathrm{loc}}/\Lambda' u'\right)\right)\right] \tag{5.3.7}$$

From now on we assume the following fundamental conjecture.

Conjecture 5.3.2 (Torsion Conjecture). *The dual* $\mathrm{Sel}(F_\infty, T^*(1))^\vee$ *of the Selmer group is* $\mathcal{S}^*$*-torsion.*

This assumption implies that the first two terms of (5.3.1) become isomorphic after extending scalars to $\Lambda(G)_{\mathcal{S}^*}$. In particular, we now have two generators

$$\phi_{t',u'}(1) \quad \text{and} \quad \mathrm{loc}(\phi_{t,u}(1))$$

of $\left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T/T^0(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}}\right)\right)_{\mathcal{S}^*}$ as a $\Lambda(\mathcal{G})_{\mathcal{S}^*}$-module.

Definition 5.3.3 (of $\boldsymbol{\Omega_{p,u,u'}}$). *We define the element* $\Omega_{p,u,t,u',t'} \in \Lambda(\mathcal{G})_{\mathcal{S}^*}$ *by the equation*

$$\Omega_{p,u,t,u',t'} \cdot \phi_{t',u'}(1) = \mathrm{loc}(\phi_{t,u}(1))$$

and note that $\Omega_{p,u,t,u',t'}$ *actually belongs to* $\Lambda(\mathcal{G})^\times_{\mathcal{S}^*}$ *since* $\phi_{t',u'}(1)$ *and* $\mathrm{loc}(\phi_{t,u}(1))$ *are both generators of* $\left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T/T^0(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}}\right)\right)_{\mathcal{S}^*}$*. We will show next that a choice of* t *determines* t' *canonically and that* $\Omega_{p,u,t,u',t'}$ *is then independent of* t *and* t'*.*

Remark 5.3.4 (Independence of $\boldsymbol{t, t'}$). In the local setting we fixed a generator t_0 of $T_pE/T_p\hat{E}$ and in the global setting we fixed a generator $t_{\bar{\pi}}$ of $T_{\bar{\pi}}E$. It follows from (A.6.14) and proposition A.6.13 that we have a canonical isomorphism

$$T_{\bar{\pi}}E \cong T_pE/T_p\hat{E} \cong T_p\tilde{E}, \tag{5.3.8}$$

which means that a global choice, i.e., a generator of $T_{\bar{\pi}}E$, canonically determines a local choice, and vice versa.

Let us choose a generator $t_{\bar{\pi}}$ of $T_{\bar{\pi}}E$ and write t_0 for the image of $t_{\bar{\pi}}$ under $T_{\bar{\pi}}E \cong T_pE/T_p\hat{E}$. Moreover, for a fixed generator ϵ of $\varprojlim_n \mu_{p^n}(\bar{\mathbb{Q}})$ let us also write ϵ for the generator of $\varprojlim_n \mu_{p^n}(\bar{\mathbb{Q}}_p)$ induced by $\bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_p$. With these choices we have

$$T_{\bar{\pi}}E(-1) \cong (T_pE/T_p\hat{E})(-1), \quad t \longmapsto t'.$$

Any other choice of generator of $T_{\bar{\pi}}E(-1)$ is of the form at for $a \in \mathbb{Z}_p^\times$ and at determines at' via ι. Since $\phi_{at',u'}(1) = 1 \otimes at' \otimes u'$ and $\phi_{at,u}(1) = at \otimes u$ for any $a \in \mathbb{Z}_p^\times$ we have

$$\mathrm{loc}(\phi_{at,u}(1)) = a \cdot \mathrm{loc}(\phi_{t,u}(1)) \qquad \text{and} \qquad a\phi_{t',u'}(1) = \phi_{at',u'}(1)$$

and therefore

$$\Omega_{p,u,t,u',t'} = \Omega_{p,u,at,u',at'}$$

for any $a \in \mathbb{Z}_p^\times$. We conclude that $\Omega_{p,u,t,u',t'}$ is independent of t and t' as long as we let t determine t' canonically via ι. We shall henceforth let t determine t' and simply write $\Omega_{p,u,u'}$ for $\Omega_{p,u,t,u',t'}$.

5.4 Relations in $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$

Next we derive the relation for which we introduced the element $\Omega_{p,u,u'}$. Let us write

$$\begin{aligned}
&\frac{\lambda_\Omega}{s_\Omega} = \Omega_{p,u,u'}\\
&x = \phi_{t',u'}(1)\\
&y = \mathrm{loc}(\phi_{t,u}(1))\\
&M = \mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\big((T_pE/T^0)(-1)\otimes_{\mathbb{Z}_p}\mathbb{H}^1_{\mathrm{loc}}\big)\\
&\Lambda = \Lambda(\mathcal{G}).
\end{aligned}$$

By definition and since $\mathcal{S}^*$ does not contain any non-trivial zero divisors, we have

$$\lambda_\Omega \cdot x = s_\Omega \cdot y$$

in Λ. We get the two exact sequences

$$0 \to \Lambda x/\Lambda(\lambda_\Omega\cdot x) \to M/\Lambda(\lambda_\Omega\cdot x) \to M/\Lambda x \to 0$$

and

$$0 \to \Lambda y/\Lambda(s_\Omega\cdot y) \to M/\Lambda(s_\Omega\cdot y) \to M/\Lambda y \to 0.$$

Since x and y are generators of $M_{\mathcal{S}^*} \cong \Lambda_{\mathcal{S}^*}$ and since $\mathcal{S}^*$ does not contain any non-trivial zero divisors we have $\mathrm{ann}_\Lambda(x) = 0 = \mathrm{ann}_\Lambda(y)$. It follows that

$$\Lambda x/\Lambda(\lambda_\Omega\cdot x) \cong \Lambda/\Lambda\lambda_\Omega \quad \text{and} \quad \Lambda y/\Lambda(s_\Omega\cdot y) \cong \Lambda/\Lambda s_\Omega.$$

In $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$ we get

$$\begin{aligned}
[M/\Lambda x] &= [M/\Lambda(\lambda_\Omega\cdot x)] - [\Lambda x/\Lambda(\lambda_\Omega\cdot x)]\\
&= [M/\Lambda(s_\Omega\cdot y)] - [\Lambda/\Lambda\lambda_\Omega]\\
&= [M/\Lambda y] + [\Lambda y/\Lambda(s_\Omega\cdot y)] - [\Lambda/\Lambda\lambda_\Omega]\\
&= [M/\Lambda y] + [\Lambda/\Lambda s_\Omega] - [\Lambda/\Lambda\lambda_\Omega]
\end{aligned}$$

Rewriting this reads

$$\begin{aligned}
&[\Lambda/\Lambda\lambda_\Omega] - [\Lambda/\Lambda s_\Omega] + \big[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\big((T_pE/T^0)(-1)\otimes_{\mathbb{Z}_p}\mathbb{H}^1_{\mathrm{loc}}\big)/\Lambda\phi_{t',u'}(1)\big]\\
&= \big[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\big((T_pE/T^0)(-1)\otimes_{\mathbb{Z}_p}\mathbb{H}^1_{\mathrm{loc}}\big)/\Lambda\mathrm{loc}(\phi_{t,u}(1))\big]
\end{aligned} \tag{5.4.1}$$

and we note that $\partial([\Omega_{p,u,u'}]) = [\Lambda/\Lambda\lambda_\Omega] - [\Lambda/\Lambda s_\Omega]$ where $\partial : K_1(\Lambda(\mathcal{G})_{\mathcal{S}^*}) \to K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$ is the connecting homomorphism from K-theory and $[\Omega_{p,u,u'}]$ denotes the image of $\Omega_{p,u,u'}$ in $K_1(\Lambda(\mathcal{G})_{\mathcal{S}^*})$.

Chapter 6

Twist conjecture for Elliptic Curves $E/\mathbb{Q}$ with CM

In this chapter, we study the third and last of Kato's conjectures which were mentioned in the introduction of this thesis. This last conjecture, in some sense, is the culmination of the work we have done so far. While the study of $L_{p,u} \in K_1(\mathbb{Z}_p[[G]]_{S^*})$ and $\mathcal{E}_{p,u'} \in K_1(\widehat{\mathbb{Z}}_p^{ur}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*})$ from the previous chapters is certainly interesting in its own right, it is strongly motivated by the following question: Is it possible to express p-adic L-functions of motives M (satisfying, at the minimum, conditions (C1) and (C2) from [FK06]), up to elements of the form $\Omega_{p,u,u'}$, as twists of universal elements such as $L_{p,u}$ and $\mathcal{E}_{p,u'}$ by p-adic representations associated to M? Moreover, is such an element a characteristic element of the Pontryagin dual of the Selmer group (or Selmer complex as in loc. cit.)?

Since (in his talk in Cambridge) Kato did not give a precise interpolation formula for the element starring in his third conjecture, we do not aim to state the conjecture in the greatest generality and simply restrict to the setting in which we can prove it. Therefore, let us consider an elliptic curve E defined over $\mathbb{Q}$ with complex mutliplication by $\mathcal{O}_K$, the conductor of which is a prime power (in K). In this setting we will define an element $\mathcal{L}_{p,u,u',E} \in K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*})$ in terms of twists of the elements $L_{p,u}$ and $\mathcal{E}_{p,u'}$ studied in chapters 2 and 3, respectively, and in terms of $\Omega_{p,u,u'}$ defined in section 5.3. We will then prove that $\mathcal{L}_{p,u,u',E}$ (up to an Euler factor) is a characteristic element of the dual Selmer group, see theorem 6.2.3. Moreover, we show in corollary 6.2.6 that $\mathcal{L}_{p,u,u',E}$ coincides with $\tau_{\psi^{-1}}(\lambda)$, the twist of de Shalit's element λ (from definition 2.4.24) by the inverse ψ^{-1} of the Größencharacter ψ attached to E/K which gives the action of $G = G(K([p^\infty])/K)$ on $T_\pi E$. For $\tau_{\psi^{-1}}(\lambda)$ an interpolation property is immediately derived from ([dS87], Theorem 4.14, p. 80) and ([BV10], Lemma 2.10, p. 394).

6.1 Setting

Let $E/\mathbb{Q}$ be one of the elliptic curves listed in Appendix A, §3 of Silverman's book [Sil99] with complex multiplication by $\mathcal{O}_K$, which are representatives of their $\bar{\mathbb{Q}}$-isomorphism classes with minimal discriminant. Such a curve has bad reduction at precisely one prime number $l = l_K$ in $\mathbb{Z}$, which coincides with the unique prime dividing the discriminant of K as we explain in subsection A.6.3.

Remark 6.1.1. Instead of restricting to one of the above curves, we could take any elliptic curve $E/\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$ that has bad reduction at precisely one prime l of $\mathbb{Z}$ such that l is the only prime of $\mathbb{Z}$ that ramifies in K. The conductor over K of such a curve is then a non-trivial prime power by the fact that E cannot have good reduction everywhere over K, which was proven by Stroeker ([Str83], (1.7) Main Theorem).

We fix a prime number $p \in \mathbb{Z}$, $p \geq 5$, at which E has good reduction and which splits in K. Recall from proposition A.6.2 that E has then good ordinary reduction at the primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ of K above p. We fix an embedding $\bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_p$ and assume that restricted to K this embedding determines the valuation corresponding to $\mathfrak{p}$. We assume that the torsion conjecture 5.3.2 holds, i.e., that $\mathrm{Sel}(F_\infty, T_pE^*(1))^\vee$ is $\mathcal{S}^*$-torsion.

Remark 6.1.2. Assuming that $\mathrm{Sel}(F_\infty, T_pE^*(1))^\vee$ is $\mathcal{S}^*$-torsion implies, by the Poitou-Tate sequence from (4.3.1), and corollary 2.4.34 that $H^2(G_\Sigma(\mathbb{Q}), \Lambda(\mathcal{G})^\# \otimes T_pE) \cong T_pE(-1) \otimes \mathbb{H}^2_\Sigma$ is $\mathcal{S}^*$-torsion. Since G is of finite index in $\mathcal{G}$ it follows that $T_pE(-1) \otimes \mathbb{H}^2_\Sigma$ is S^*-torsion. But as G-modules we have an injection $T_\pi E(-1) \otimes \mathbb{H}^2_\Sigma \hookrightarrow T_pE(-1) \otimes \mathbb{H}^2_\Sigma$, which shows that $T_\pi E(-1) \otimes \mathbb{H}^2_\Sigma$ is S^*-torsion. Since $T_\pi E(-1)$ is of $\mathbb{Z}_p$-rank 1 we can twist this module by the inverse of the character giving the action of G on $T_\pi E(-1)$ and, hence, conclude that $\mathbb{H}^2_\Sigma$ must be S^*-torsion. It follows now from remark 2.3.5 that $\mathcal{A}_\infty = \varprojlim_{k,n}(Cl(K_{k,n})\{p\})$ is S^*-torsion. Hence, the $\mathrm{Sel}(F_\infty, T_pE^*(1))^\vee$-torsion assumption implies the torsion assumption from the commutative main theorem 2.4.41.

Let us fix a complex period Ω such that for the period lattice L of E we have $L = \mathcal{O}_K\Omega$. We also fix a generator ϵ of $\mathbb{Z}_p(1)$ as in [dS87] and let these choices determine the period Ω_p as in (loc. cit., p. 67f), which determines an isomorphism $\theta = \theta_{\Omega_p} : \mathbb{G}_m \cong \hat{E}$ of formal groups.

As before we write ψ for the Größencharacter attached to E/K and set $\pi = \psi(\mathfrak{p})$ and $\bar{\pi} = \overline{\psi(\mathfrak{p})} = \psi(\bar{\mathfrak{p}})$ (where the last equation holds by ([Kat76], p. 559)) for the generators of $\mathfrak{p}$ and $\bar{\mathfrak{p}}$, respectively. Recall that we write

$$S \subset S^* \subset \Lambda(G), \quad \mathcal{S} \subset \mathcal{S}^* \subset \Lambda(\mathcal{G}) \quad \text{and} \quad \mathcal{S}' \subset \mathcal{S}'^* \subset \Lambda(\mathcal{G}').$$

for the canonical Ore sets in $\Lambda(G)$, $\Lambda(\mathcal{G})$ and $\Lambda(\mathcal{G}')$, respectively, as in [CFK+05]. For the Ore sets in the Iwasawa algebras with $\hat{\mathbb{Z}}_p^{ur}$-coefficients $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[G]]$, $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]$ and $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]$ we will write

$$\tilde{S}^* \subset \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[G]], \quad \tilde{\mathcal{S}}^* \subset \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]] \quad \text{and} \quad \tilde{\mathcal{S}}'^* \subset \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']].$$

Let us make a remark linking the setting considered in this chapter to some of the previous chapters. We write $K_n = K(E[p^n])$, $n \geq 1$, and $\Lambda' = \Lambda(\mathcal{G}') = \Lambda(G')$.

Remark 6.1.3. (i) If we consider the curve $E/\mathbb{Q}$ as a curve over K all the assumptions from the setting of subsection 2.4.6 are satisfied, including assumption 2.4.29 that

$$\mathfrak{f} = \mathfrak{l}^r, \quad r \geq 1,$$

where $\mathfrak{f}$ denotes the conductor of the Größencharacter ψ attached to E/K and $\mathfrak{l}$ is a prime ideal of $\mathcal{O}_K$, compare remark 5.1.1. Hence, up to the assumption that $\varprojlim_n(Cl(K_n)\{p\})$ is S^*-torsion, the commutative main theorem 2.4.41 holds. Moreover, when we consider the decomposition group $\mathcal{G}' \cong G(K_{\infty,\bar{\nu}}/\mathbb{Q}_p)$ of a fixed prime $\bar{\nu}$ of $K_\infty = K(E[p^\infty])$ above $\mathfrak{p}$, then we are in the setting of section 3.3. In particular, the local main conjecture holds in this case. Furthermore, since we assume that the torsion conjecture 5.3.2 holds (which was used to define $\Omega_{p,u,u'}$), our present setting satisfies all conditions of the setting considered in section 5.1 where we studied $\Omega_{p,u,u'}$, including the assumption from (5.1.1), compare also remark 5.1.1.

(ii) We note that the compact p-adic Lie group $\mathcal{G}'$ and its closed normal subgroup $\mathcal{H}' = \mathrm{Gal}(K_{\infty,\bar{\nu}}/\mathbb{Q}_p^{cyc})$ satisfy the conditions (i), (ii) and (iii) from subsection 1.2.1, for which we recall the decomposition from (3.3.1), that $\mathcal{G}'$ embedds into G, which has no elements of order p, and the fact that $K_{\infty,\bar{\nu}}$ contains an unramified $\mathbb{Z}_p$-extension of $K_\mathfrak{p} \cong \mathbb{Q}_p$ generated by the coordinates of points in $E[\bar{\pi}^\infty]$, where $\bar{\pi}$ denotes a fixed generator of $\bar{\mathfrak{p}}$ implying that the abelian group $\mathcal{H}'$ also has dimension 1 as a p-adic Lie group. Therefore, the classes of modules that are finitely generated over $\mathbb{Z}_p$ vanish in $K_0(\mathfrak{M}_{\mathcal{H}'}(\mathcal{G}'))$ by corollary 1.2.3. Recall from remark 2.4.36 that a similar statement holds for G and H. Moreover, corollary 1.2.4 applies to $G \subset \mathcal{G}$ and $H = G \cap \mathcal{H}$ and to $\mathcal{G}' \subset \mathcal{G}$ and $\mathcal{H}' = \mathcal{G}' \cap \mathcal{H}$, respectively (here we identify $\mathcal{G}'$ and $\mathcal{H}'$ with their images in $\mathcal{G}$, compare example A.8.7 in the appendix).

(iii) Recall from (1.1.2) that in order to define the twist operators on K_1-groups, we fixed a $\mathbb{Z}_p$-basis of the representation space. Throughout this chapter we fix the same basis $t_{\bar{\pi}}$ of $T_{\bar{\pi}}E$ as in section 5.3 where we defined $\Omega_{p,u,u'}$. We also identify $T_{\bar{\pi}}E$ with $T_{\bar{\pi},\cdot p}E$ (the $\bar{\pi}$-adic Tate module with transition maps given by multiplication with p) as in remark A.6.12 and recall from the same remark that $T_{\bar{\pi},\cdot p}E$ naturally embedds into T_pE. Let us write $[-] : T_pE \longrightarrow T_pE/T_p\hat{E}$ for the canonical projection and recall from remark 5.3.4 that it restricts to an isomorphism $[-] : T_{\bar{\pi}}E \overset{\sim}{\longrightarrow} T_pE/T_p\hat{E}$. Hence, $t_{\bar{\pi}}$ canonically determines a basis $t_0 = [t_{\bar{\pi}}]$ of $T_pE/T_p\hat{E}$. Together with our fixed generator ϵ of $\mathbb{Z}_p(1)$ which determines a basis ϵ_0 of $\mathbb{Z}_p(-1)$, these determine bases $t = t_{\bar{\pi}} \otimes \epsilon_0$ and $t' = [t_{\bar{\pi}}] \otimes \epsilon_0$ of $T_{\bar{\pi}}E(-1)$ and $(T_pE/T_p\hat{E})(-1)$, respectively, such that under the natural map $\iota_1 : T_pE(-1) \longrightarrow (T_pE/T_p\hat{E})(-1)$ induced by $[-]$ we have $t \mapsto t'$. We also write ι_1 for the restriction of ι_1 to $T_{\bar{\pi}}E(-1)$.

6.2 Main theorems

Our first task is to define the element $\mathcal{L}_{p,u,u',E} \in K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*})$ in terms of twists of the elements $L_{p,u}$ and $\mathcal{E}_{p,u'}$ and in terms of $\Omega_{p,u,u'}$. The element $\mathcal{E}_{p,u'}$ from the local main conjecture (which is a theorem in the setting considered in the present chapter) will be twisted by the $\mathcal{G}'$-representation $(T_pE/T_p\hat{E})(-1)$, which is of $\mathbb{Z}_p$-rank 1. We will write $\tau_{E/\hat{E}(-1)}$ for the twist operator from corollary 1.1.10 on $K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*})$ induced by $(T_pE/T_p\hat{E})(-1)$. The element $L_{p,u} := \frac{1}{x_{\mathfrak{q}}}$ from the commutative global theorem 2.4.41 will be twisted by the G-representation $T_{\bar{\pi}}E(-1)$, which is also of $\mathbb{Z}_p$-rank 1. We will write $\tau_{E_{\bar{\pi}}(-1)}$ for the twist operator from corollary 1.1.10 on $K_1(\Lambda(G)_{S^*})$ induced by $T_{\bar{\pi}}E(-1)$. We want to consider the elements

$$\tau_{E_{\bar{\pi}}(-1)}(L_{p,u}) \in K_1(\Lambda(G)_{S^*}), \quad \tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'}) \in K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*}), \quad \Omega_{p,u,u'} \in K_1(\Lambda(\mathcal{G})_{\mathcal{S}^*}) \tag{6.2.1}$$

in one common K_1-group. By corollary A.8.15 and remark 3.1.5 we have inclusions

$$S^* \subset \mathcal{S}^* \subset \tilde{\mathcal{S}}^* \quad \text{and} \quad \tilde{\mathcal{S}}'^* \subset \tilde{\mathcal{S}}^*$$

and therefore we have natural inclusions of rings (via which we consider all of the following rings as subrings of $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*}$)

$$\begin{array}{ccccc} \Lambda(G)_{S^*} & \hookrightarrow & \Lambda(\mathcal{G})_{\mathcal{S}^*} & \hookrightarrow & \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*} \\ & & & & \uparrow \\ & & & & \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*} \end{array} \tag{6.2.2}$$

which induce maps

$$\begin{array}{ccccc} K_1(\Lambda(G)_{S^*}) & \longrightarrow & K_1(\Lambda(\mathcal{G})_{\mathcal{S}^*}) & \longrightarrow & K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*}) \\ & & & & \uparrow \\ & & & & K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*}). \end{array} \tag{6.2.3}$$

It is through these maps that we consider the images of the elements from (6.2.1) in the group $K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*})$. We are now in a position to make the following

Definition 6.2.1 (of $\mathcal{L}_{p,u,E}$). *We define an element $\mathcal{L}_{p,u,E}$ in $K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*})$ by*

$$\mathcal{L}_{p,u,E} = \frac{\tau_{E_{\bar{\pi}}(-1)}(L_{p,u})}{\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})} \cdot \Omega_{p,u,u'} \cdot \frac{1}{12},$$

which is independent of u' as we show in theorem 6.2.5 and note that $12 \in \mathbb{Z}_p^{\times}$ since $p \geq 5$ by assumption.

Remark 6.2.2. We could have also defined $\mathcal{L}_{p,u,E}$ as an element in the intersection of Iwasawa algebras

$$\left(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*}\right)^{\times} \bigcap \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\mathcal{S}^*}$$

since the representations by which we twist have $\mathbb{Z}_p$-rank 1. In fact, $\tau_{E_{\bar{\pi}}(-1)}(L_{p,u})$ comes from $\tau_{E_{\bar{\pi}}(-1)}(1/x_{\mathfrak{q}}) \in \Lambda(G)_S^{\times}$ with $x_{\mathfrak{q}} = N\mathfrak{q} - \mathrm{Frob}_{\mathfrak{q}} \in \Lambda(G)_S^{\times}$, where we also write $\tau_{E_{\bar{\pi}}(-1)}$ for the ring homomorphism $\Lambda(G)_{S^*} \to \Lambda(G)_{S^*}$ from proposition 1.1.9 corresponding to $T_{\bar{\pi}}E(-1)$. Likewise, recall from (3.3.12) that $\mathcal{E}_{p,u'}$ was originally defined as an element in $\left(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*}\right)^{\times}$ and $\mathcal{E}_{p,u'}^{-1} \in \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]$, so that we can interpret $\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})$ as an element of $\left(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*}\right)^{\times}$, where, as above, we consider $\tau_{E/\hat{E}(-1)}$ also as the ring homomorphism $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*} \to \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*}$ from proposition 1.1.9 induced by $(T_pE/T_p\hat{E})(-1)$. Lastly, $\Omega_{p,u,u'}$ is, by definition 5.3.3, an element in $\Lambda(\mathcal{G})_{\mathcal{S}^*}^{\times}$.

Before stating our first theorem let us recall some more facts from K-theory. First, recall the definition of the torsion categories $\mathfrak{M}_H(G)$, $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$, $\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}}(\mathcal{G})$ and $\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}'}(\mathcal{G}')$ from definiton 1.1.18. Moreover, recall from lemma A.8.8 that $\Lambda(\mathcal{G})$ is free of rank $[\mathcal{G}:G]$ over $\Lambda(G)$ (in particular flat over $\Lambda(G)$) and $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]$ is free over $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]$ of rank $[\mathcal{G}:\mathcal{G}']$. Moreover, for a finitely generated $\Lambda(\mathcal{G})$-module M we have $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]] \otimes_{\Lambda(\mathcal{G})} M \cong \hat{\mathbb{Z}}_p^{\mathrm{ur}}\hat{\otimes}_{\mathbb{Z}_p} M$, see remark 3.1.4, and $\hat{\mathbb{Z}}_p^{\mathrm{ur}}\hat{\otimes}_{\mathbb{Z}_p}-$ is exact on pseudo-compact $\mathbb{Z}_p$-modules, see proposition A.8.17 (finitely generated $\Lambda(\mathcal{G})$-modules are pseodo-compact as $\mathbb{Z}_p$-modules). Corollary A.8.16 and lemma A.8.20 therefore imply that we have maps

$$\begin{aligned}
&K_0(\mathfrak{M}_H(G)) \longrightarrow K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G})), && [M] \longmapsto [\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M] = [\mathrm{Ind}_{\mathcal{G}}^{G} M]\\
&K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G})) \longrightarrow K_0(\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}}(\mathcal{G})), && [M] \longmapsto [\hat{\mathbb{Z}}_p^{\mathrm{ur}}\hat{\otimes}_{\mathbb{Z}_p} M] = [\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]] \otimes_{\Lambda(\mathcal{G})} M]\\
&K_0(\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}'}(\mathcal{G}')) \longrightarrow K_0(\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}}(\mathcal{G})), && [M] \longmapsto [\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]] \otimes_{\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]} M] = [\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'} M],
\end{aligned}$$

see also corollary A.8.9. Lastly, let us recall the following exact sequence from K-theory

$$K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]) \longrightarrow K_1(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*}) \xrightarrow{\partial} K_0(\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}}(\mathcal{G})) \longrightarrow K_0(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]) \twoheadrightarrow K_0(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*}).$$

We now prove one of the main theorems of this thesis.

Theorem 6.2.3. *Let the setting be as above. Assume that* $\mathrm{Sel}(K_\infty, T^*(1))^\vee$ *is* $\mathcal{S}^*$*-torsion. Then, up to a twisted Euler factor,* $\mathcal{L}_{p,u,E}$ *is a characteristic element of* $\hat{\mathbb{Z}}_p^{\mathrm{ur}}\hat{\otimes}_{\mathbb{Z}_p}\mathrm{Sel}(K_\infty, T_pE^*(1))^\vee$*, i.e., we have*

$$\partial(\mathcal{L}_{p,u,E}) = [\mathrm{Sel}(K_\infty, T_pE^*(1))^\vee]_{\tilde{\Lambda}} + [\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_{\nu_l}} T_pE(-1)]_{\tilde{\Lambda}},$$

where l *is the unique prime at which* $E/\mathbb{Q}$ *has bad reduction,* $\mathcal{G}_{\nu_l}$ *is the decomposition group of some place of* K_∞ *above* l *and the notation* $[-]_{\tilde{\Lambda}}$ *is defined in (6.2.4).*

Proof. Let us write $\tilde{\Lambda} = \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]$. For any finitely generated $\Lambda(\mathcal{G})$-module M that is $\mathcal{S}^*$-torsion let us write

$$[M]_{\tilde{\Lambda}} := [\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]] \otimes_{\Lambda(\mathcal{G})} M] = [\hat{\mathbb{Z}}_p^{\mathrm{ur}} \hat{\otimes}_{\mathbb{Z}_p} M] \tag{6.2.4}$$

for its class in $K_0(\mathfrak{M}_{\hat{\mathbb{Z}}_p^{\mathrm{ur}},\mathcal{H}}(\mathcal{G}))$. We will adopt a similar notation

$$[M]_{\tilde{\Lambda}} := [\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]] \otimes_{\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]} M]$$

for a finitely generated $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]$-module M that is $\tilde{\mathcal{S}}'^*$-torsion. We will use repeatedly the diagram (1.1.9) which states that twisting on K_1-groups corresponds to taking the tensor product with the representation on K_0-groups. The contribution of $\tau_{E_{\bar{\pi}}(-1)}(L_{p,u})$, by the defining property (2.4.66) of $L_{p,u} = \frac{1}{x_{\mathfrak{q}}}$, is given by

$$\begin{aligned}\partial(\tau_{E_{\bar{\pi}}(-1)}(L_{p,u})) &= \left[\mathrm{Ind}_{\mathcal{G}}^{G}(T_{\bar{\pi}}E(-1) \otimes_{\mathbb{Z}_p} \mathrm{Res}_{G}^{\mathcal{G}} \mathbb{H}_{\Sigma}^2)\right]_{\tilde{\Lambda}} - \left[\mathrm{Ind}_{\mathcal{G}}^{G}(T_{\bar{\pi}}E(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}_{\Sigma}^1/\Lambda(G)u)\right]_{\tilde{\Lambda}} \\ &= \left[T_pE(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}_{\Sigma}^2)\right]_{\tilde{\Lambda}} - \left[\left(T_pE(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}_{\Sigma}^1\right)/\Lambda(\mathcal{G})\phi_{t,u}(1)\right]_{\tilde{\Lambda}}\end{aligned} \tag{6.2.5}$$

where the second equality follows from (5.3.4).

We write $\tilde{\Lambda}' = \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]$ and $T' = (T_pE/T_p\hat{E})(-1)$ as before. The element $\mathcal{E}_{p,u'}$ from the local main theorem, by the defining property (3.2.2) of $\mathcal{E}_{p,u'}$, maps to

$$\begin{aligned}\partial(\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})) &= \left[T' \otimes_{\mathbb{Z}_p} \left(\tilde{\Lambda}' \otimes_{\Lambda'} \mathbb{H}_{\mathrm{loc}}^2\right)\right]_{\tilde{\Lambda}} - \left[T' \otimes_{\mathbb{Z}_p} \left(\tilde{\Lambda}' \otimes_{\Lambda'} \left(\mathbb{H}_{\mathrm{loc}}^1/\Lambda' u'\right)\right)\right]_{\tilde{\Lambda}} \\ &= \left[\tilde{\Lambda}' \otimes_{\Lambda'} \left(T' \otimes_{\mathbb{Z}_p} \mathbb{H}_{\mathrm{loc}}^2\right)\right]_{\tilde{\Lambda}} - \left[\tilde{\Lambda}' \otimes_{\Lambda'} \left(T' \otimes_{\mathbb{Z}_p} \left(\mathbb{H}_{\mathrm{loc}}^1/\Lambda' u'\right)\right)\right]_{\tilde{\Lambda}} \\ &= \left[\tilde{\Lambda} \otimes_{\Lambda'} \left(T' \otimes_{\mathbb{Z}_p} \mathbb{H}_{\mathrm{loc}}^2\right)\right] - \left[\tilde{\Lambda} \otimes_{\Lambda'} \left(T' \otimes_{\mathbb{Z}_p} \left(\mathbb{H}_{\mathrm{loc}}^1/\Lambda' u'\right)\right)\right] \\ &= \left[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T' \otimes_{\mathbb{Z}_p} \mathbb{H}_{\mathrm{loc}}^2\right)\right]_{\tilde{\Lambda}} - \left[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T' \otimes_{\mathbb{Z}_p} \left(\mathbb{H}_{\mathrm{loc}}^1/\Lambda' u'\right)\right)\right]_{\tilde{\Lambda}} \\ &= \left[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T' \otimes_{\mathbb{Z}_p} \mathbb{H}_{\mathrm{loc}}^2\right)\right]_{\tilde{\Lambda}} - \left[\left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T' \otimes_{\mathbb{Z}_p} \mathbb{H}_{\mathrm{loc}}^1\right)\right)/\Lambda(\mathcal{G})\phi_{t',u'}(1)\right]_{\tilde{\Lambda}}\end{aligned} \tag{6.2.6}$$

where the second equality follows from corollary 1.1.7 (twisting commutes with extension of scalars to $\hat{\mathbb{Z}}_p^{\mathrm{ur}}$), the last equality from (5.3.7) and in the third and fourth equation we use the isomorphisms

$$\tilde{\Lambda} \otimes_{\tilde{\Lambda}'} \tilde{\Lambda}' \otimes_{\Lambda'} M \cong \tilde{\Lambda} \otimes_{\Lambda'} M \cong \tilde{\Lambda} \otimes_{\Lambda(\mathcal{G})} \Lambda(\mathcal{G}) \otimes_{\Lambda'} M$$

for a finitely generate Λ'-module M.

Let us write $\Lambda = \Lambda(\mathcal{G})$. The element $\Omega_{p,u,u'}$, by (5.4.1), maps to

$$\begin{aligned}\partial(\Omega_{p,u,u'}) = &\quad [\Lambda/\Lambda\lambda_{\Omega}]_{\tilde{\Lambda}} - [\Lambda/\Lambda s_{\Omega}]_{\tilde{\Lambda}} \\ = &\quad \left[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T' \otimes_{\mathbb{Z}_p} \mathbb{H}_{\mathrm{loc}}^1\right)/\Lambda \mathrm{loc}(\phi_{t,u}(1))\right]_{\tilde{\Lambda}} \\ &\quad - \left[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\left(T' \otimes_{\mathbb{Z}_p} \mathbb{H}_{\mathrm{loc}}^1\right)/\Lambda\phi_{t',u'}(1)\right]_{\tilde{\Lambda}}.\end{aligned} \tag{6.2.7}$$

We conclude from (6.2.5), (6.2.6) and (6.2.7) that the element $\mathcal{L}_{p,u,E}$ (the term $1/12 \in \mathbb{Z}_p^\times$ does not alter the image) maps to

$$\begin{aligned}
\partial(\mathcal{L}_{p,u,E}) = \quad & \partial(\tau_{E_{\tilde{\pi}}(-1)}(L_{p,u})) - \partial(\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})) + \partial(\Omega_{p,u,u'}) \\
= \quad & \big[T_pE(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^2_\Sigma)\big]_{\tilde{\Lambda}} - \big[\big(T_pE(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma\big)/\Lambda(\mathcal{G})\phi_{t,u}(1)\big]_{\tilde{\Lambda}} \\
& - \big[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\big(T' \otimes_{\mathbb{Z}_p} \mathbb{H}^2_{\mathrm{loc}}\big)\big]_{\tilde{\Lambda}} + \big[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\big(T' \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}}\big)/\Lambda\mathrm{loc}(\phi_{t,u}(1))\big]_{\tilde{\Lambda}}.
\end{aligned} \tag{6.2.8}$$

Using corollary A.3.10 we can write the Poitou-Tate sequence from (4.3.1) as

$$\begin{aligned}
0 \longrightarrow T_pE(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma \xrightarrow{\ \mathrm{loc}\ } \mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\big(T' \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}}\big) \\
\longrightarrow \mathrm{Sel}(K_\infty, T_pE^*(1))^\vee \longrightarrow T_pE(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^2_\Sigma \\
\longrightarrow \bigoplus_{q \in \Sigma_f} \mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_{\nu_q}} T_pE(-1) \longrightarrow T_pE(-1) \longrightarrow 0.
\end{aligned} \tag{6.2.9}$$

where we recall $\Sigma_f = \{p, l\}$ where l is the unique prime at which $E/\mathbb{Q}$ has bad reduction. In the above sequence we may pass to the quotients $\big(T_pE(-1) \otimes_{\mathbb{Z}_p} \mathbb{H}^1_\Sigma\big)/\Lambda(\mathcal{G})\phi_{t,u}(1)$ and $\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\big(T' \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}}\big)/\Lambda\mathrm{loc}(\phi_{t,u}(1))$ and still get an exact sequence as $\Lambda\mathrm{loc}(\phi_{t,u}(1))$ lies in the kernel of the map to the dual selmer group. By assumption $\mathrm{Sel}(F_\infty, T^*(1))^\vee$ is $\mathcal{S}^*$-torsion. Moreover, corollary 2.4.34 implies that

$$\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_{\nu_l}} T_pE(-1) \cong (\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_{\nu_l}} \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} T_pE(-1)$$

is $\mathcal{S}^*$-torsion. It follows from corollary 1.2.4, which we may use by remark 6.1.3 (ii), that

$$[\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'} T_pE(-1)] = 0, \quad [T_pE(-1)] = [\mathrm{Ind}_{\mathcal{G}}^{G} T_\pi E] = 0, \quad [\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}\big(T' \otimes_{\mathbb{Z}_p} \mathbb{H}^2_{\mathrm{loc}}\big)] = 0$$

in $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$. Hence, their images in $K_0(\mathfrak{M}_{\mathbb{Z}_p^{\mathrm{ur}},\mathcal{H}}(\mathcal{G}))$ vanish. It follows from (6.2.8) and the above Poitou-Tate sequence that

$$\partial(\mathcal{L}_{p,u,u'}) = [\mathrm{Sel}(K_\infty, T_pE^*(1))^\vee]_{\tilde{\Lambda}} + [\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_{\nu_l}} T_pE(-1)]_{\tilde{\Lambda}},$$

which concludes the proof. □

Next, we want to study the interpolation property of $\mathcal{L}_{p,u,E}$ and make a preparatory

Remark 6.2.4. (i) It is well-known that the Weil pairing (compare subsection A.2.1) induces an isomorphism $\bigwedge^2(T_pE) \cong \mathbb{Z}_p(1)$. Hence, the determinant of $\rho_E : G \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_pE)$ is given by the cyclotomic character κ, i.e., we have

$$\psi \cdot \bar{\psi} = \det(\rho_E) = \kappa,$$

where $\bar{\psi}$ is the Größencharacter of infinity type $(0,1)$ attached to E. Since the action of G on $T_{\bar{\pi}}E$ is given by $\bar{\psi}$ we see that $T_{\bar{\pi}}E(-1)$ corresponds to $\bar{\psi}\cdot\kappa^{-1} = \psi^{-1}$. In particular, under the ring homomorphism $\tau_{E_{\bar{\pi}}(-1)} : \Lambda(G) \to \Lambda(G)$ we have for any $g \in G$

$$\tau_{E_{\bar{\pi}}(-1)}(g) \overset{\text{def}}{=} \psi^{-1}(g^{-1})g = \psi(g)g.$$

(ii) Recall from proposition 1.1.9 that the twist operators $\tau_{E/\hat{E}(-1)}$ and $\tau_{E_{\bar{\pi}}(-1)}$ are induced by ring homomorphisms between the respective localized Iwasawa algebras and note by the isomorphism from (5.3.8) that these fit into a commutative diagram

$$\begin{array}{ccccc} \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*} & \xrightarrow{\tau_{E/\hat{E}(-1)}} & \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]_{\tilde{\mathcal{S}}'^*} & \hookrightarrow & \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\tilde{\mathcal{S}}^*} \\ \downarrow & & \downarrow & \nearrow & \\ \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[G]]_{\tilde{S}^*} & \xrightarrow{\tau_{E_{\bar{\pi}}(-1)}} & \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[G]]_{\tilde{S}^*}, & & \end{array} \tag{6.2.10}$$

where the vertical injections and the maps on the right are induced by the natural embeddings $\mathcal{G}' \subset G \subset \mathcal{G}$ and the inclusions $\tilde{\mathcal{S}}'^* \subset \tilde{S}^* \subset \tilde{\mathcal{S}}^*$ which hold by corollary A.8.15.

The second main theorem of this chapter, which we prove next, will enable us to derive as a corollary an expression of $\mathcal{L}_{p,u,E}$ for which an interpolation property has been established. Let us first recall that in theorem 2.4.25 we explained de Shalit's construction of the semi-local version $\mathbb{L} : \mathcal{U}_\infty \hat{\otimes}_{\mathbb{Z}_p} \hat{\mathbb{Z}}_p^{ur} \longrightarrow \hat{\mathbb{Z}}_p^{ur}[[G]]$ of the Coleman map associated to $\hat{E}$, where $\mathcal{U}_\infty = \varprojlim_n \prod_{\omega|\mathfrak{p}} \mathcal{O}^1_{K_{n,\omega}}$ denote that semi-local principal units for the tower $K_n = K(E[p^n])$, $n \geq 1$ (earlier we considered the fields $K_{k,n} = K(E[\bar{\pi}^k\pi^n])$ in order to distinguish between the $\bar{\pi}$- and the π-variable, so that with this notation $K_n = K_{n,n}$). One can proceed in an entirely similar fashion for the formal group $\mathbb{G}_m$. In fact, as we explain in the proof of theorem 6.2.5 below, the (local) Coleman map $-\mathcal{L}_{\epsilon^{-1}}$ for $\mathbb{G}_m$ from (5.2.1) may be viewed as a map $-\mathcal{L}_{\epsilon^{-1}} : \mathcal{U}'(K_{\infty,\bar{\nu}}) \longrightarrow \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]$ of $\Lambda(\mathcal{G}')$-modules, where $\mathcal{U}'(K_{\infty,\bar{\nu}}) = \varprojlim_n \mathcal{O}^1_{K_{n,\bar{\nu}}}$ are the local principal units for the extension $K_{\infty,\nu}/\mathbb{Q}_p$. Considering the induced map of G-modules and using the natural isomorphism $\mathcal{U}_\infty \cong \mathrm{Ind}_G^{\mathcal{G}'}\mathcal{U}'(K_{\infty,\bar{\nu}})$ we obtain the map

$$\mathcal{L}_{semi-loc} :\ \mathcal{U}_\infty \cong \mathrm{Ind}_G^{\mathcal{G}'}\mathcal{U}'(K_{\infty,\bar{\nu}}) \xrightarrow{\mathrm{Ind}_G^{\mathcal{G}'}(-\mathcal{L}_{\epsilon^{-1}})} \mathrm{Ind}_G^{\mathcal{G}'}\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']] \cong \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[G]], \tag{6.2.11}$$

which is the semi-local version of the Coleman map for $\mathbb{G}_m$. Note that via the natural (diagonal) map $\bar{\mathcal{E}}_\infty = \varprojlim_n (\mathcal{O}_{K_n}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p) \hookrightarrow \mathcal{U}_\infty$, which is an embedding by (2.4.4), we can also evaluate $\mathcal{L}_{semi-loc}$ at global units. We also consider the natural map

$$loc_{\bar{\nu}} : \bar{\mathcal{E}}_\infty \longrightarrow \mathcal{U}'(K_{\infty,\bar{\nu}})$$

from global to local principal units, which we also interpret as a map $loc_{\bar{\nu}} : \mathbb{H}^1_{\Sigma} \to \mathbb{H}^1_{\mathrm{loc}}$ as we explain after (4.3.12) via the isomorphisms $\bar{\mathcal{E}}_\infty \cong \mathbb{H}^1_\Sigma$ and $\mathcal{U}'(K_{\infty,\bar{\nu}}) \cong \mathbb{H}^1_{\mathrm{loc}}$ from Kummer theory.

We will intepret the elements $\Omega_{p,u,u'}$ and $\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})^{-1} = \tau_{E/\hat{E}(-1)}(\mathcal{E}^{-1}_{p,u'})$ as elements in $\left(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]\right)_{\mathcal{S}^*}$ which is possible as we have explained in remark 6.2.2. Here and in the following proof, when we localize with respect to $\mathcal{S}^*$ we always consider the modules in question as $\Lambda(\mathcal{G})$-modules.

Theorem 6.2.5. *The element $\frac{\Omega_{p,u,u'}}{\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})}$ is equal to the $\tau_{E_{\bar{\pi}}(-1)}$-twist of the image of u under the semi-local version $\mathcal{L}_{semi-loc}$ of the Coleman map for $\mathbb{G}_m$, i.e.,*

$$\frac{\Omega_{p,u,u'}}{\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})} = \tau_{E_{\bar{\pi}}(-1)}(\mathcal{L}_{semi-loc}(u)) = \tau_{E_{\bar{\pi}}(-1)}\Big(\sum_{\sigma\in G/\mathcal{G}'} \sigma \cdot \big(-\mathcal{L}_{\epsilon^{-1}}(loc_{\bar{\nu}}(\sigma^{-1}u))\big)\Big)$$

in $\left(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]\right)_{\mathcal{S}^*}$, which shows that the element on the left side does not depend on u'. In particular, $\mathcal{L}_{p,u,E}$ is independent of u'.

Proof. Let us write $\tilde{\Lambda}' = \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}']]$ and recall that $\mathcal{U}'(K_{\infty,\bar{\nu}}) \cong \mathbb{H}^1_{\mathrm{loc}}$. By abuse of notation let us also write $-\mathcal{L}_{\epsilon^{-1}}$ for the composition of the map $-\mathcal{L}_{\epsilon^{-1}}$ from (5.2.1) with the isomorphism $\mathbb{T}_{\mathrm{un}}(K_{\infty,\bar{\nu}}) \otimes_{\Lambda'} \Lambda'_{\varphi_p} \cong \Lambda'_{\varphi_p}$ and the natural embedding $\Lambda'_{\varphi_p} \subset \tilde{\Lambda}'$, i.e., for the map

$$-\mathcal{L}_{\epsilon^{-1}} : \mathcal{U}'(K_{\infty,\bar{\nu}}) \longrightarrow \tilde{\Lambda}' \tag{6.2.12}$$

of Λ'-modules. By definition of $\mathcal{E}_{p,u'}$ from (3.3.12) we have $-\mathcal{L}_{\epsilon^{-1}}(u') = \mathcal{E}^{-1}_{p,u'}$. Let us write $T' = (T_pE/T_p\hat{E})(-1)$, which is free of $\mathbb{Z}_p$-rank 1. Tensoring (6.2.12) with $T' \otimes_{\mathbb{Z}_p} -$, using lemma 1.1.5, applying $\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}$ and applying $(-)_{\mathcal{S}^*}$ (viewing all modules as $\Lambda(\mathcal{G})$-modules) yields the composite map

$$\left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}(T' \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}})\right)_{\mathcal{S}^*} \xrightarrow{(I)} \left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}(T' \otimes_{\mathbb{Z}_p} \tilde{\Lambda}')\right)_{\mathcal{S}^*} \xrightarrow{(II)} \left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'} \tilde{\Lambda}'\right)_{\mathcal{S}^*} \xrightarrow{(III)} \left(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]\right)_{\mathcal{S}^*}. \tag{6.2.13}$$

We note that our fixed basis t' of T' (compare remark 6.1.3 (iii)) determines the isomorphism $T' \otimes_{\mathbb{Z}_p} \tilde{\Lambda}' \cong \tilde{\Lambda}'$ from lemma 1.1.5 and under this isomorphism we have

$$t' \otimes \lambda \longmapsto \tau_{E/\hat{E}(-1)}(\lambda), \qquad \lambda \in \tilde{\Lambda}', \tag{6.2.14}$$

which follows from lemma 1.1.11. By the defining property of $\Omega_{p,u,u'} = \frac{\lambda_\Omega}{s_\Omega} \in \Lambda(\mathcal{G})_{\mathcal{S}^*}$ we have an equality

$$\lambda_\Omega \cdot \phi_{t',u'}(1) = s_\Omega \cdot \mathrm{loc}(\phi_{t,u}(1))$$

in $\left(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}(T' \otimes_{\mathbb{Z}_p} \mathbb{H}^1_{\mathrm{loc}})\right)_{\mathcal{S}^*}$. Recall that $\phi_{t',u'}(1) = 1 \otimes t' \otimes u'$ and

$$\mathrm{loc}(\phi_{t,u}(1)) = \mathrm{loc}(t \otimes u) = \sum_{\sigma \in \mathcal{G}/\mathcal{G}'} \sigma \otimes \iota_1(\sigma^{-1}t) \otimes loc_{\bar{\nu}}(\sigma^{-1}u),$$

where ι_1 is the natural projection $T_pE(-1) \longrightarrow (T_pE/T_p\hat{E})(-1)$ mentioned in remark 6.1.3 (iii). Now, we make the important observation that for $g \in \mathcal{G} \smallsetminus G$, i.e., for an element that can be written as $g = g_0 c$ where c is complex conjugation and g_0 belongs to G, the element $g.t_{\bar{\pi}}$ belongs to $T_{\pi,\cdot p}E$ (see remark A.6.12 for the definition of $T_{\pi,\cdot p}E$ and $T_{\bar{\pi},\cdot p}E$ and remark 6.1.3 for our convention that we identify $T_{\bar{\pi}}E$ with $T_{\bar{\pi},\cdot p}E$). This is true since by definition $t_{\bar{\pi}} \in T_{\bar{\pi},\cdot p}E$ and the action of complex conjugation turns $\bar{\pi}$-power divisions into π-power division points, compare (A.6.17). It follows from proposition A.6.13 that $T_pE/T_p\hat{E} = T_pE/T_{\pi,\cdot p}E$ and hence that $[g^{-1}.t_{\bar{\pi}}] = 0$ in $T_pE/T_p\hat{E}$ and $\iota_1(g^{-1}t) = 0$ in T' for all $g \in \mathcal{G} \smallsetminus G$. We conclude that

$$\sum_{\sigma \in \mathcal{G}/\mathcal{G}'} \sigma \otimes \iota_1(\sigma^{-1}t) \otimes loc_{\bar{\nu}}(\sigma^{-1}u) = \sum_{\sigma \in G/\mathcal{G}'} \sigma \otimes \iota_1(\sigma^{-1}t) \otimes loc_{\bar{\nu}}(\sigma^{-1}u),$$

where on the right we sum only over representatives of $G/\mathcal{G}'$. We have noted in remark 6.2.4 (i) that G acts on $t \in T_{\bar{\pi}}(-1)$ through $\bar{\psi} \cdot \kappa^{-1}$ and hence we can rewrite the last sum as

$$\begin{aligned}\sum_{\sigma \in G/\mathcal{G}'} \sigma \otimes \iota_1(\sigma^{-1}t) \otimes loc_{\bar{\nu}}(\sigma^{-1}u) &= \sum_{\sigma \in G/\mathcal{G}'} \big((\bar{\psi} \cdot \kappa^{-1})(\sigma^{-1}) \cdot \sigma\big) \otimes \iota_1(t) \otimes loc_{\bar{\nu}}(\sigma^{-1}u) \\ &= \sum_{\sigma \in G/\mathcal{G}'} \tau_{E_{\bar{\pi}}(-1)}(\sigma) \otimes t' \otimes loc_{\bar{\nu}}(\sigma^{-1}u), \end{aligned} \tag{6.2.15}$$

where the last equation holds by definition of $\tau_{E_{\bar{\pi}}(-1)}$ and t'.

Now, we compare the images of $\lambda_\Omega \cdot \phi_{t',u'}(1)$ and $s_\Omega \cdot \mathrm{loc}(\phi_{t,u}(1))$ under the composite map from (6.2.13) using (6.2.14). On the one hand we have

$$\begin{aligned}\lambda_\Omega \cdot \phi_{t',u'}(1) &\overset{(I)}{\longmapsto} \lambda_\Omega \cdot \big(1 \otimes t' \otimes -\mathcal{L}_{\epsilon^{-1}}(u')\big) && \text{in} \quad \big(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'}(T' \otimes_{\mathbb{Z}_p} \tilde{\Lambda}')\big)_{\mathcal{S}^*} \\ &\overset{(II)}{\longmapsto} \lambda_\Omega \cdot \big(1 \otimes \tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'}^{-1})\big) && \text{in} \quad \big(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}'} \tilde{\Lambda}'\big)_{\mathcal{S}^*} \\ &\overset{(III)}{\longmapsto} \frac{\lambda_\Omega}{\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})} && \text{in} \quad \big(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]\big)_{\mathcal{S}^*}.\end{aligned} \tag{6.2.16}$$

On the other hand we have

$$\begin{aligned} s_\Omega \cdot \mathrm{loc}(\phi_{t,u}(1)) &\overset{(I)}{\longmapsto} s_\Omega \cdot \Big(\sum_{\sigma \in G/\mathcal{G}'} \tau_{E_{\bar{\pi}}(-1)}(\sigma) \otimes t' \otimes -\mathcal{L}_{\epsilon^{-1}}(loc_{\bar{\nu}}(\sigma^{-1}u))\Big) \\ &\overset{(II)}{\longmapsto} s_\Omega \cdot \Big(\sum_{\sigma \in G/\mathcal{G}'} \tau_{E_{\bar{\pi}}(-1)}(\sigma) \otimes \tau_{E/\hat{E}(-1)}\big(-\mathcal{L}_{\epsilon^{-1}}(loc_{\bar{\nu}}(\sigma^{-1}u))\big)\Big) \\ &\overset{(III)}{\longmapsto} s_\Omega \cdot \Big(\sum_{\sigma \in G/\mathcal{G}'} \tau_{E_{\bar{\pi}}(-1)}(\sigma) \cdot \tau_{E/\hat{E}(-1)}\big(-\mathcal{L}_{\epsilon^{-1}}(loc_{\bar{\nu}}(\sigma^{-1}u))\big)\Big) \\ &= s_\Omega \cdot \tau_{E_{\bar{\pi}}(-1)}\Big(\sum_{\sigma \in G/\mathcal{G}'} \sigma \cdot \big(-\mathcal{L}_{\epsilon^{-1}}(loc_{\bar{\nu}}(\sigma^{-1}u))\big)\Big), \end{aligned} \tag{6.2.17}$$

where the last equality follows from the commutativity of (6.2.10). We conclude so far that

$$\frac{\Omega_{p,u,u'}}{\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})} = \tau_{E_{\bar{\pi}}(-1)}\Big(\sum_{\sigma\in G/\mathcal{G}'} \sigma\cdot\big(-\mathcal{L}_{\epsilon^{-1}}(loc_{\bar{\nu}}(\sigma^{-1}u))\big)\Big) \quad \text{in} \quad \big(\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]\big)_{\mathcal{S}^*}, \tag{6.2.18}$$

which shows, in particular, that the left side does not depend on u'. Next, let us consider the composite map

$$\bar{\mathcal{E}}_\infty \xrightarrow{\mathrm{Coind}_G^{\mathcal{G}'}(loc_{\bar{\nu}})} \mathrm{Coind}_G^{\mathcal{G}'}\mathcal{U}'(K_{\infty,\bar{\nu}}) \cong \mathrm{Ind}_G^{\mathcal{G}'}\mathcal{U}'(K_{\infty,\bar{\nu}}) \xrightarrow{\mathrm{Ind}_G^{\mathcal{G}'}(-\mathcal{L}_{\epsilon^{-1}})} \mathrm{Ind}_G^{\mathcal{G}'}\tilde{\Lambda}' \cong \hat{\mathbb{Z}}_p^{\mathrm{ur}}[[G]] \tag{6.2.19}$$

under which u maps to $\sum_{\sigma\in G/\mathcal{G}'}\sigma\cdot\big(-\mathcal{L}_{\epsilon^{-1}}(loc_{\bar{\nu}}(\sigma^{-1}u))\big)$, the argument of $\tau_{E_{\bar{\pi}}(-1)}$ on the right side of (6.2.18).

Now, in order to conclude the proof, we only have to note that the composite map from (6.2.19) coincides with the composite of the embedding $\bar{\mathcal{E}}_\infty \hookrightarrow \mathcal{U}_\infty$ with $\mathcal{L}_{semi-loc}$. □

As above, compare remark 6.2.2, we consider $\Omega_{p,u,u'}$, $\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})^{-1}$ and $\tau_{E_{\bar{\pi}}(-1)}(L_{p,u})$ (and, hence, also $\mathcal{L}_{p,u,E}$) as elements in $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\mathcal{S}^*}$ and get the following

Corollary 6.2.6. *We have an equality of elements in* $\hat{\mathbb{Z}}_p^{\mathrm{ur}}[[\mathcal{G}]]_{\mathcal{S}^*}$

$$\mathcal{L}_{p,u,E} = \tau_{\psi^{-1}}(\lambda),$$

where $\tau_{\psi^{-1}}(\lambda)$ *denotes the twist of de Shalit's element* $\lambda\in\Lambda(G)$ *(from definition 2.4.24) by the* G*-module* $(T_\pi E)^*$*. The action of* G *on* $(T_\pi E)^*$ *is given by* ψ^{-1}*. For an Artin character* χ *of* $\mathcal{G}$ *we have*

$$\frac{1}{\Omega_p}\cdot\int_G \mathrm{Res}_G^{\mathcal{G}}\chi\, d\mathcal{L}_{p,u,E} = \frac{1}{\Omega}\cdot G\big(\psi\cdot\mathrm{Res}\chi\big)\cdot\Big(1-\frac{(\psi\cdot\mathrm{Res}\chi)(\mathfrak{p})}{p}\Big)\cdot L_{\mathfrak{f}\bar{\mathfrak{p}}}((\psi\cdot\mathrm{Res}\chi)^{-1},0), \tag{6.2.20}$$

where we refer to ([dS87], p. 80) for the definition of $G\big(\psi\cdot\mathrm{Res}\chi\big)$ *which is related to a local constant and in the expression* $(\psi\cdot\mathrm{Res}\chi)(\mathfrak{p})$ *we consider* $\psi\cdot\mathrm{Res}\chi$ *as a map on ideals of* K *prime to* $\mathfrak{f}$*. The periods* Ω *and* Ω_p *are defined at the beginning of this chapter.*

Proof. By the previous theorem 6.2.5 we know that

$$\frac{\Omega_{p,u,u'}}{\tau_{E/\hat{E}(-1)}(\mathcal{E}_{p,u'})} = \tau_{E_{\bar{\pi}}(-1)}(\mathcal{L}_{semi-loc}(u)).$$

But for *large enough* (unramified) abelian extensions the Coleman maps (composed with an integral logarithm and an isomorphism to $\mathbb{G}_m$ and then extended to measures) induced by two formal groups (in our case $\hat{E}$ and $\mathbb{G}_m$) coincide, which is proven in ([dS87], Proposition 3.9, p.

23) for the maximal abelian extension. The arguments in loc. cit. also work in our case using the fact that for any $n \geq 1$ we have

$$K_{\mathfrak{p}}(E[\bar{\pi}^n], E[\pi^n]) = K(E[\bar{\pi}^n], \mu_{p^n}),$$

i.e., adjoining to the local field $K_{\mathfrak{p}}(E[\bar{\pi}^n])$ the p^n division points of $\hat{E}$ or $\mathbb{G}_m$ yields the same extension, which follows from the Weil pairing. Hence, we have an equality

$$\mathcal{L}_{semi-loc}(u) = \mathbb{L}(u), \tag{6.2.21}$$

where $\mathcal{L}_{semi-loc}$ is the semi-local Coleman map for $\mathbb{G}_m$ and $\mathbb{L}$ is the one for $\hat{E}$. By definition 2.4.24, $u = u(\mathfrak{q})$ is the the compatible system of elliptic units attached to $\mathfrak{q} \subset \mathcal{O}_K$ and $L_{p,u} = \frac{1}{(N\mathfrak{q} - \mathrm{Frob}_{\mathfrak{q}})}$. By definition of λ and since $\tau_{E_{\bar{\pi}}(-1)}(12) = 12$ we get

$$\begin{aligned}
\mathcal{L}_{p,u,E} &\overset{\text{thm } 6.2.5}{=} \tau_{E_{\bar{\pi}}(-1)}(L_{p,u}) \cdot \tau_{E_{\bar{\pi}}(-1)}(\mathcal{L}_{semi-loc}(u)) \cdot \frac{1}{12} \\
&\overset{(6.2.21)}{=} \tau_{E_{\bar{\pi}}(-1)}\Big(\frac{\mathbb{L}(u(\mathfrak{q}))}{12 \cdot (N\mathfrak{q} - \mathrm{Frob}_{\mathfrak{q}})}\Big) \\
&\overset{\text{def.}\lambda}{=} \tau_{E_{\bar{\pi}}(-1)}(\lambda).
\end{aligned}$$

Now, we only have to note that $\psi^{-1} = \bar{\psi} \cdot \kappa^{-1}$ as was explained in remark 6.2.4 (i) and that $\bar{\psi} \cdot \kappa^{-1}$ gives the action on $T_{\bar{\pi}}E(-1)$, i.e., $\tau_{E_{\bar{\pi}}(-1)} = \tau_{\psi^{-1}}$.

Now we note that for an element $g \in G$, by definition of the twist operator, we have $\tau_{\psi^{-1}}(g) = \psi^{-1}(g^{-1})g = \psi(g)g$, which shows that for an Artin character δ of G and any measure μ we have

$$\int_G \delta \; d(\tau_{\psi^{-1}}(\mu)) = \int_G \delta \cdot \psi \; d\mu. \tag{6.2.22}$$

But $\delta \cdot \psi$ is a Größencharacter of type $(1,0)$ and for such Größencharacters de Shalit ([dS87], Theorem 4.14, p. 80) determines the interpolation property for λ. The interpolation property for $\tau_{\psi^{-1}}(\lambda)$ is now derived from ([BV10], Lemma 2.10, p. 394) and (6.2.22). □

Appendix A

Appendix

A.1 Some Galois Isomorphisms

Let T be a finitely generated free $\mathbb{Z}_p$-module with continuous $\mathbb{Z}_p$-linear action of $G_F = G(\bar{F}/F)$, where F is a perfect field and $\bar{F}$ an algebraic closure. We write $T^* := \mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p)$ for the $\mathbb{Z}_p$-dual representation and $T^\vee := \mathrm{Hom}_{cts}(T, \mathbb{Q}_p/\mathbb{Z}_p)$ for the Pontryagin dual, the discrete $\mathbb{Z}_p$-module of continuous homomorphisms of abelian groups where $\mathbb{Q}_p/\mathbb{Z}_p$ is equipped with the discrete topology. By continuity, the maps in $T^\vee$ are also $\mathbb{Z}_p$-linear. Now, there is a canonical isomorphism

$$T^*(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \cong T^\vee(1), \tag{A.1.1}$$

which can be seen by applying $()^\vee$ to both sides. In fact, we have

$$\begin{aligned}
(T^*(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee &= \mathrm{Hom}_{cts}(T^*(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \\
&\cong \mathrm{Hom}_{\mathbb{Z}_p}(T^*(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \\
&\cong \mathrm{Hom}_{\mathbb{Z}_p}(T^*(1), (\mathbb{Q}_p/\mathbb{Z}_p)^\vee) \\
&\cong (T^*(1))^* \\
&\cong T(-1)
\end{aligned}$$

where the second equation holds since $T^*(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ is discrete (and therefore any map from it is continuous), compare also the following remark. On the other hand, we have $(T^\vee(1))^\vee \cong T(-1)$, so there is an isomorphism as in (A.1.1), indeed.

Remark A.1.1. (i) Every $\mathbb{Z}$-linear map $B \to A$ between abelian groups, where B is a $\mathbb{Z}_p$-module that coincides with its p-primary part $B = B\{p\}$, and A is an arbitrary $\mathbb{Z}_p$-module, is also $\mathbb{Z}_p$-linear. In particular, for any discrete module D such that $D = D\{p\}$ we have

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

(ii) If T is a finitely generated $\mathbb{Z}_p$-module (which we always equip with the p-adic topology), then it is compact. Hence, any continuous $\mathbb{Z}$-linear map $T \to \mathbb{Q}_p/\mathbb{Z}_p$ factors through a finite quotient of of the form T/p^nT, $n \geq 1$. By (i) we see that $T \to T/p^nT \to \mathbb{Q}_p/\mathbb{Z}_p$ is $\mathbb{Z}_p$-linear. On the other hand, any $\mathbb{Z}_p$-linear map $T \to \mathbb{Q}_p/\mathbb{Z}_p$ factors through T/p^nT for some $n \geq 1$ (simply choose a basis $t_1, \dots, t_r$ of T, the image of each t_i will be annihilated by some power of p). Since T/p^nT is equipped with the discrete topology the composite $T \to T/p^nT \to \mathbb{Q}_p/\mathbb{Z}_p$ is then continuous. We have shown that

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

Now, let W be a discrete $\mathbb{Z}_p$-module of the form $W \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$, $r \geq 1$, with a continuous $\mathbb{Z}_p$-linear action of G_F. Then, we have a G_F-linear isomorphism

$$\mathrm{Hom}_{cts}(\mathbb{Q}_p, W) \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} (\varprojlim_n W[p^n]), \tag{A.1.2}$$

of $\mathbb{Q}_p$-vector spaces, where $\varprojlim_n W[p^n]$ denotes the Tate-module of W, $W[p^n]$ denotes the p^n-torsion subgroup of W and the transition maps in the limit are multiplication by p. The $\mathbb{Q}_p$-vector space structure for the module on the left is defined by $(y.\varphi)(x) := \varphi(yx)$, $\varphi \in \mathrm{Hom}_{cts}(\mathbb{Q}_p, W)$, $x, y \in \mathbb{Q}_p$.

The isomorphism (A.1.2) is given as follows. Let $\varphi \neq 0$ belong to $\mathrm{Hom}_{cts}(\mathbb{Q}_p, W)$ and let $k \in \mathbb{Z}$ be the largest integer such that there exists a unit $u \in \mathbb{Z}_p^\times$ satisfying $\varphi(up^k) \neq 0$. By continuity, φ is $\mathbb{Z}_p$-linear and, hence, we must have $\varphi(p^k) \neq 0$. Now, let us write

$$x_n := \varphi(p^{k-n+1}) \in W[p^n]$$

and define one direction of (A.1.2) by

$$\varphi \longmapsto p^{-k} \otimes (x_n)_n,$$

which is easily seen to be $\mathbb{Q}_p$-linear. The inverse of (A.1.2) is defined as follows. A non-trivial element of the form $z \otimes (y_n)_n$ belonging to $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} (\varprojlim_n W[p^n])$ can be written as $z \otimes (y_n)_n = p^t \otimes (x_n)_n$ with $t \in \mathbb{Z}$ and $x_1 \neq 0$, since if $y_1 = \cdots = y_m = 0$ for $m \geq 1$, then $p^m(y_{n+m})_n = (y_n)_n$. Note that a continuous linear map $\psi : \mathbb{Q}_p \longrightarrow W$ is determined by its values at powers of p. We define the inverse of (A.1.2) by mapping $p^t \otimes (x_n)_n$ to the continuous map induced by

$$\psi : \mathbb{Q}_p \longrightarrow W, \quad p^l \longmapsto \begin{cases} 0 & \text{if} \quad l > -t \\ x_{1-t-l} & \text{if} \quad l \leq -t \end{cases}$$

which satisfies $p\psi(p^l) = \psi(p^{l+1})$ and can therefore be extended to $\mathbb{Q}_p$ by defining $\psi(up^l) := u\psi(p^l)$, $u \in \mathbb{Z}_p^\times$.

A.2 Non-degenerate and perfect Pairings

In this section we recall some isomorphisms induced by non-degenerate pairings that we will need. Let A, B and C be R-modules. Then, we say that an R-bilinear pairing

$$A \times B \longrightarrow C$$

is *nondegenerate* if it induces R-linear injections

$$A \hookrightarrow \mathrm{Hom}_R(B, C) \qquad \text{and} \qquad B \hookrightarrow \mathrm{Hom}_R(A, C).$$

It is called *perfect* if both of these two maps are isomorphisms.

A.2.1 Weil pairing

Let A be an abelian variety defined over a a field F of characteristic 0 and write $A^\vee$ for its dual abelian variety. We write $A[p^n]$ for the p^n-torsion points of $A(\overline{F})$. Moreover, we write

$$e_n : A[p^n] \times A^\vee[p^n] \longrightarrow \mu_{p^n}$$

for the Weil pairing $e_n = e_{p^n}$, see [Lan83] or ([Mum85], section 20. Riemann forms), compare also [Mil86a]. This pairing is non-degenerate in both variables, see ([Lan83], VII, §2 Proposition 4 and its proof, p.189f). Moreover, it commutes with the action of G_F.

For a finite abelian group B we write $B' = \mathrm{Hom}(B, \mu)$ where $\mu = \bigcup_m \mu_m$ denotes the union of all roots of unity in $\overline{F}$. One has $B \cong (B')'$. Moreover B has the same cardinality as B' (this is clear for cyclic groups and then follows for general finite abelian B). By the non-degeneracy, the maps e_n induce injective maps

$$A[p^n] \hookrightarrow A^\vee[p^n]' \qquad \text{and} \qquad A^\vee[p^n] \hookrightarrow A[p^n]', \tag{A.2.1}$$

which must already be bijections since all groups have the same cardinality. Alternatively, write C for the cokernel of $A[p^n] \hookrightarrow A^\vee[p^n]'$. Dualizing, one gets

$$0 \to C' \to (A^\vee[p^n]')' \to A[p^n]'$$

and checks immediately that the composite $A^\vee[p^n] \cong (A^\vee[p^n]')' \to A[p^n]'$ is the map from (A.2.1), which is injective. Hence, $C' = 0$ and therefore $C \cong (C')' = 0$. We see that the maps from (A.2.1) are bijections. Note that $A[p^n]' \cong \mathrm{Hom}(A[p^n], \mu_{p^n})$ and that any $\mathbb{Z}$-linear map in $\mathrm{Hom}(A[p^n], \mu_{p^n})$ is automatically $\mathbb{Z}_p$-linear. Using the canonical identification $T_pA/p^n \cong A[p^n]$ and noting that any linear map $T_pA \to \mu_{p^n}$ factors through T_pA/p^n, the right map from (A.2.1) induces an isomorphism

$$A^\vee[p^n] \to A[p^n]' \cong \mathrm{Hom}_{\mathbb{Z}_p}(A[p^n], \mu_{p^n}) \cong \mathrm{Hom}_{\mathbb{Z}_p}(T_pA, \mu_{p^n}) \tag{A.2.2}$$

which maps $a \in A^\vee[p^n]$ to the map in $\mathrm{Hom}_{\mathbb{Z}_p}(T_pA, \mu_{p^n})$ given by $t = (t_k)_k \longmapsto e_n(t_n, a)$, where $(t_k)_k \in \varprojlim_k A[p^k]$. The maps form a projective system of maps with repect to the natural maps $A^\vee[p^n] \overset{\cdot p}{\to} A^\vee[p^{n-1}]$ and the maps $\mathrm{Hom}_{\mathbb{Z}_p}(T_pA, \mu_{p^n}) \to \mathrm{Hom}_{\mathbb{Z}_p}(T_pA, \mu_{p^{n-1}})$ induced by $\mu_{p^n} \overset{()^p}{\to} \mu_{p^{n-1}}$, which follows from the fact that the Weil pairing satisfies

$$e_n(t_n, a)^p = e_{n-1}(p \cdot t_n, p \cdot a) = e_{n-1}(t_{n-1}, p \cdot a), \qquad (t_k)_k \in \varprojlim_k A[p^k],\ a \in A^\vee[p^n].$$

Passing to the limit of the maps from (A.2.2) we get an isomorphism

$$T_p(A^\vee) \longrightarrow \varprojlim_n \mathrm{Hom}_{\mathbb{Z}_p}(T_pA, \mu_{p^n}) \cong \mathrm{Hom}_{\mathbb{Z}_p}(T_pA, \mathbb{Z}_p(1)) = (T_pA)^*(1).$$

Likewise, we get $T_p(A^\vee)^*(1) \cong T_pA$.

A.2.2 $\mathbb{Q}_p/\mathbb{Z}_p$-valued pairings

Now let A and B be $\mathbb{Z}_p$-modules and consider a non-degenerate $\mathbb{Z}_p$-bilinear pairing

$$< -,- >: A \times B \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

Let $A_f \subset A$ and $B_f \subset B$ be two $\mathbb{Z}_p$-submodules. We define the *orthogonal complements*

$$B_f^\perp = \{a \in A \mid < a, b >= 0\ \forall b \in B_f\} \qquad \text{and} \qquad A_f^\perp = \{b \in B \mid < a, b >= 0\ \forall a \in A_f\}.$$

of B_f in A and of A_f in B, respectively. The non-degenerate pairing $< -,- >$ induces two more pairings

$$A_f \times (B/A_f^\perp) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \qquad \text{and} \qquad (A/B_f^\perp) \times B_f \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p, \tag{A.2.3}$$

which are both non-degenerate. We say that A_f and B_f are *exact annihilators* or orthogonal complements of each other if

$$A_f = B_f^\perp \qquad \text{and} \qquad B_f = A_f^\perp.$$

From the theory of finite (and equi-) dimensional k-vector spaces V, W and perfect pairings $V \times W \to k$ we know that if $V_f \subset V$ is the orthogonal complement of $W_f \subset W$, then W_f is also the orthogonal complement of V_f. We want to show that this also holds in the following setting using that $\mathbb{Q}_p/\mathbb{Z}_p$ is $\mathbb{Z}_p$-divisible, hence injective as a $\mathbb{Z}_p$-module. Consider the conditions:

(i) One of A, B is finitely generated as a $\mathbb{Z}_p$-module and the other is a discrete abelian p-primary torsion group, i.e., each element is annihilated by some power of p. Compare remark A.1.1 for the fact that then $A^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ and $B^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p)$.

(ii) Assume (i) holds. The $\mathbb{Z}_p$-linear maps $A \to \mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p)$ and $B \to \mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ induced by $< -,- >$ are continuous, where the Hom-sets are each equipped with the compact-open topology.

Proposition A.2.1. *Assume that the above (i) and (ii) hold, that* $< -, - >: A \times B \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$ *is perfect and that* $A_f = B_f^{\perp}$. *Then, we also have* $B_f = A_f^{\perp}$, *i.e.,* A_f *and* B_f *are exact annihilators of each other. Moreover, the two pairings from* $(A.2.3)$ *are perfect.*

Proof. By assumption $A_f = B_f^{\perp}$, so we have a non-degenerate pairing $(A/A_f) \times B_f \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$. Moreover, the image of the map $A_f \hookrightarrow \mathrm{Hom}(B, \mathbb{Q}_p/\mathbb{Z}_p)$ is contained in $\mathrm{Hom}(B/B_f, \mathbb{Q}_p/\mathbb{Z}_p) \subset \mathrm{Hom}(B, \mathbb{Q}_p/\mathbb{Z}_p)$. Now, since $\mathbb{Q}_p/\mathbb{Z}_p$ is injective as a $\mathbb{Z}_p$-module, see ([Rot09], chapter 3, Corollary 3.35), we get a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_f & \longrightarrow & A & \longrightarrow & A/A_f & \longrightarrow & 0 \\ & & \big\downarrow \iota_1 & & \big\downarrow \cong & & \big\downarrow \iota_2 & & \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}_p}(B/B_f, \mathbb{Q}_p/\mathbb{Z}_p) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}_p}(B_f, \mathbb{Q}_p/\mathbb{Z}_p) & \longrightarrow & 0 \end{array} \tag{A.2.4}$$

where ι_1 and ι_2 are injective and the vertical map in the middle is an isomorphism, by assumption (all vertical maps are induced by the pairing). It follows that ι_2 is surjective and a diagram chase (or the five lemma) then shows that ι_1 is also surjective, so that both ι_1 and ι_2 are isomorphisms.

Now, by condition (ii) the isomorphism $A \to \mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p)$ is a topological isomorphism. This is clear if A is discrete and if A is finitely generated as a $\mathbb{Z}_p$-module, hence compact, then it follows from general topology since the map is continuous and $\mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p)$ is Hausdorff. It follows that ι_1 and ι_2 are topological isomorphisms. We get an isomorphism

$$B/B_f \cong \mathrm{Hom}_{\mathbb{Z}_p}(B/B_f, \mathbb{Q}_p/\mathbb{Z}_p)^{\vee} \xrightarrow{(\iota_1)^{\vee}} A_f^{\vee}$$

which is immediately verified to be the map induced by $< -, - >$ and see that $B_f = A_f^{\perp}$. Likewise we can apply $(-)^{\vee}$ to ι_2 and see that the pairings from $(A.2.3)$ are perfect. □

Example A.2.2. For a local non-archimedean field F of characteristic 0 and a finitely generated free $\mathbb{Z}_p$-module T with continuous $\mathbb{Z}_p$-linear action of G_F the cup product and the local invariant map induce perfect pairings

$$H^i(F, T) \times H^{2-i}(F, T^{\vee}(1)) \longrightarrow H^2(F, \mathbb{Q}_p/\mathbb{Z}_p(1)) \cong \mathbb{Q}_p/\mathbb{Z}_p$$

for $i = 0, 1, 2$ which are known as local Tate duality, see ([Rub00], Chapter 1, Theorem 1.4.1) and ([Ser97], Chapter II, §5.2, Theorem 2, p.91). The group $H^{2-i}(F, T^{\vee}(1))$ is a discrete torsion group and $H^i(F, T)$ is finitely generated as a $\mathbb{Z}_p$-module, see ([PR00], Appendix A.1). Moreover, the discussion following lemma A.3.5, see (A.3.5) and (A.3.6), shows that condition (ii) is satisfied.

We will later define finite parts of cohomology $H^1_f(F, T) \subset H^1(F, T)$ and $H^1_f(F, T^{\vee}(1)) \subset H^1(F, T^{\vee}(1))$ and then quote results stating that $H^1_f(F, T) = H^1_f(F, T^{\vee}(1))^{\perp}$ with respect to the above pairing (under the assumption that $T \otimes \mathbb{Q}_p$ is de Rham in case F is a finite extension of $\mathbb{Q}_p$). Proposition A.2.1 then shows that $H^1_f(F, T)$ and $H^1_f(F, T^{\vee}(1))$ are exact annihilators of each other and that the induced pairings as in (A.2.3) are perfect.

A.3 Galois Cohomology

Let us review some basic facts about Galois cohomology. Unless stated otherwise group actions are assumed to be left actions. We will consider continuous cochain cohomology as defined in ([NSW08], section 2.7). Whenever F is a field (we will only consider perfect fields), we write $\bar{F}$ for an algebraic closure of F and $G_F = G(\bar{F}/F)$ for its absolute Galois group. If F is a number field and Σ a set of places of F we write F_Σ for the maximal extension of F inside $\bar{F}$ that is unramified outside Σ and $G_\Sigma(F) = G(F_\Sigma/F)$ for the Galois group of F_Σ/F. We recall the following results (loc. cit., Proposition (8.3.18), Theorem (8.3.20) (i)). Let $p \in \mathbb{Z}$ be a prime number and write cd_pG for the cohomological p-dimension of a profinite group G.

Proposition A.3.1. *Let F be a number field and Σ a finite set of places of F containing all infinite places and Σ_p, the set of places above p. Then,*

$$cd_pG_\Sigma(F) \leq 2.$$

Moreover, for a finite $G_\Sigma(F)$-module T of order a power of p, $\mathrm{H}^n(G_\Sigma(F), T)$ is finite for all $n \geq 0$.

For non-archimedean local fields we recall ([NSW08], Theorem (7.1.8) (i), (iii)).

Proposition A.3.2. *Let L be a finite extension of $\mathbb{Q}_l$. For the cohomological p-dimension of the absolute Galois group G_L of L we have*

$$cd_p(G_L) = 2.$$

Moreover, for a finite G_L-module T of order a power of p, the groups $\mathrm{H}^n(G_L, T)$ are finite for all $n \geq 0$.

Remark A.3.3. In particular, profinite groups of the form G_L and $G_\Sigma(F)$, L a finite extension of $\mathbb{Q}_p$, F a number field and $\Sigma_p \subseteq \Sigma$, satisfy the finitetess conditions (i) and (ii) of Case 1 of ([FK06], Proposition 1.6.5), which states that, for certain modules, Galois cohomology of such groups commutes with the tensor product; see the next subsection for details.

For finitely generated free $\mathbb{Z}_p$-modules T with a continuous action of a profinite group G one can often reduce questions concerning $H^i(G, T)$ to questions regarding cohomology groups of the finite discrete groups T/p^n, $n \geq 1$. Let us quote a result of Tate as stated in ([Rub00], Appendix B, Proposition B.2.3) (see also ([Jan88], section 2)).

Proposition A.3.4. *Let $i \geq 1$ and $T = \varprojlim_n T_n$ where each T_n is a finite module with a continuous action of a profinite group G. Assume that $H^{i-1}(G, T_n)$ is finite for every n. Then we have an isomorphism*

$$H^i(G, T) \cong \varprojlim_n H^i(G, T_n). \tag{A.3.1}$$

A.3.1 Functoriality of local Tate duality

Let F be a finite extension of $\mathbb{Q}_l$ for some prime l, fix an algebraic closure $\bar{F}$ and write μ for the group of all roots of unity in $\bar{F}$ and G_F for the absolute Galois group. For a finite G_F-module A write $A' = \operatorname{Hom}_{\mathbb{Z}}(A, \mu)$. Recall Tate's local duality result, for example from ([NSW08], (7.2.6) Theorem). For lack of a reference we state the following lemma that we need for duality results for finitely generated free $\mathbb{Z}_p$-modules.

Lemma A.3.5. *Let $\pi : A \to B$ be a homomorphism of finite G_F-modules. Then, for $i = 0, 1, 2$ we have the following diagram*

$$\begin{array}{ccccc} H^i(F,B) & \times & H^{2-i}(F,B') & \xrightarrow{\cup} & H^2(F,\mu) \cong \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \pi_*}\uparrow & & \downarrow{\scriptstyle (\pi^*)_*} & & \| \\ H^i(F,A) & \times & H^{2-i}(F,A') & \xrightarrow{\cup} & H^2(F,\mu) \cong \mathbb{Q}/\mathbb{Z}, \end{array} \tag{A.3.2}$$

which commutes in the sense that for $f \in H^i(F,A)$ and $g \in H^{2-i}(F,B')$ we have $f \cup (\pi^*)_*(g) = \pi_*(f) \cup g$. Here we write $\pi^* : B' \to A'$ for the map induced by π and we write $(-)_*$ for the maps induced on cohomology groups.

Proof. This is immediately verified at the level of cochains. □

Given a finitely generated free $\mathbb{Z}_p$-module T with continuous $\mathbb{Z}_p$-linear G_F-action, we may apply the lemma to the canonical maps $T/p^{n+1} \to T/p^n$, $n \geq 1$. This means that the induced bijections

$$H^i(F, T/p^n) \to \operatorname{Hom}_{\mathbb{Z}}\big(H^{2-i}(F, (T/p^n)'), \mathbb{Q}/\mathbb{Z}\big), \qquad n \geq 1, \tag{A.3.3}$$

form a projective system of maps and the induced bijections

$$H^i(F, (T/p^n)') \to \operatorname{Hom}_{\mathbb{Z}}\big(H^{2-i}(F, T/p^n), \mathbb{Q}/\mathbb{Z}\big), \qquad n \geq 1, \tag{A.3.4}$$

form a direct system of maps. The groups $H^i(F, T/p^n)$ and $H^i(F, (T/p^n)')$, $i = 0, 1, 2$, are finite discrete torsion groups annihilated by p^n. They naturally are $\mathbb{Z}_p$-modules. If, in (A.3.3) and (A.3.4) we replace $\mathbb{Q}/\mathbb{Z}$ by $\mathbb{Q}_p/\mathbb{Z}_p$ (which we may) then the above $\operatorname{Hom}_{\mathbb{Z}}$-sets become $\operatorname{Hom}_{\mathbb{Z}_p}$-sets and the bijections from (A.3.3) and (A.3.4) become $\mathbb{Z}_p$-linear bijections. The modules on the right of (A.3.3) and (A.3.4) are the Pontryagin duals of the finite discrete torsion modules $H^{2-i}(F, (T/p^n)')$ and $H^{2-i}(F, T/p^n)$, compare remark A.1.1. Hence, passing to the projective and direct limit, respectively, we get a $\mathbb{Z}_p$-linear topological (see the following remark) isomorphism

$$H^i(F,T) \to \varprojlim_n \operatorname{Hom}_{\mathbb{Z}_p}\big(H^{2-i}(F, (T/p^n)'), \mathbb{Q}_p/\mathbb{Z}_p\big) \cong \operatorname{Hom}_{\mathbb{Z}_p}\big(H^{2-i}(F, T^\vee(1)), \mathbb{Q}_p/\mathbb{Z}_p\big) \tag{A.3.5}$$

of compact modules, where the module on the right is equipped with the compact-open topology, and a $\mathbb{Z}_p$-linear topological isomorphism

$$H^i(F, T^\vee(1)) \to \operatorname{Hom}_{\mathbb{Z}_p}\big(H^{2-i}(F,T), \mathbb{Q}_p/\mathbb{Z}_p\big) \tag{A.3.6}$$

of discrete modules.

Remark A.3.6. Let $(D_i)_{i\in I}$ be a direct system of abelian discrete groups. The natural maps $D_j \to \varinjlim_i D_i$, $j \in I$, induce compatible continuous maps $(\varinjlim_i D_i)^\vee \to D_j^\vee$ where $(\varinjlim_i D_i)^\vee$ and $D_j^\vee$ are equipped with the compact-open topology. We get a continuous map $(\varinjlim_i D_i)^\vee \to \varprojlim_j (D_j^\vee)$, which is a bijection and where $\varprojlim_j (D_j^\vee)$ is equipped with the projective limit topology. It follows that this must be a topological isomorphism since it is a continous map from a compact space to a Hausdorff space.

A.3.2 Connection with étale Cohomology and the Kummer sequence

In this subsection we want to recall that for a number field F, a finite set of places Σ of F containing the infinite places Σ_∞ and a finite discrete $G_\Sigma(F)$-module A such that the order $\#A$ of A is a unit in $\mathcal{O}_{F,\Sigma}$, continuous cochain cohomology coincides with the étale cohomology of the sheaf determined by A on $\mathrm{Spec}(\mathcal{O}_{F,\Sigma})_{\text{ét}}$, i.e., we have canonical isomorphisms

$$H^i(G_\Sigma(F), A) \cong H^i_{\text{ét}}(\mathrm{Spec}(\mathcal{O}_{F,\Sigma}), A), \qquad i \geq 0,$$

see ([Nek06], section (9.2.1)). Let us briefly recall the connection between the category $\mathrm{Spec}(F)_{\text{ét}}$ of étale F-schemes (resp., $\mathrm{Spec}(F)_{\text{f,ét}}$ of finite étale F-schemes) and the category $G_F - \mathrm{Set}^d$ of discrete left G_F-sets, (resp., $G_F - \mathrm{Set}^d_f$, the subcategory of finite discrete left G_F-sets).

For a scheme S, let us write $S_{\text{ét}}$ for the category of étale S-schemes and $S_{f,\text{ét}}$ for the subcategory of finite étale S-schemes. Moreover, we write $\text{Ét}(S)$ for the category of sheaves of sets on $S_{\text{ét}}$, i.e., the étale topos on $S_{\text{ét}}$, and $\mathrm{lcc} - \text{Ét}(S)$ for the subcategory of locally constant constructible sheaves.

The following diagram summarizes several well-known results, which we quote from Conrad's notes [Cona], see also Milne's [Mil13b] and [Mil80]. We write $\underline{X}_S(-) \coloneqq Mor_S(-, X)$ for the sheaf on $S_{\text{ét}}$ associated to an étale S-scheme $X \in S_{\text{ét}}$ and for a sheaf $\mathcal{F} \in \text{Ét}(\mathrm{Spec}(F))$ we write $M_{\mathcal{F}} \coloneqq \varinjlim_L \mathcal{F}(\mathrm{Spec}(L))$ for the associated discrete G_F-set, where the limit ranges over all finite subextensions L/F of $F \subset \overline{F}$. As a localisation of the Dedekind domain $\mathcal{O}_F$, $\mathcal{O}_{F,\Sigma}$ is a Dedekind domain and we write $\iota : \mathrm{Spec}(F) \to \mathrm{Spec}(\mathcal{O}_{F,\Sigma})$ for the inclusion of the generic point.

$X(\bar{F})$ for $Mor_F(\mathrm{Spec}(F), X)$.

$$\begin{array}{ccccc}
\mathrm{Spec}(F)_{\text{ét}} & \xrightarrow{X \mapsto \underline{X}_F} & \text{Ét}(\mathrm{Spec}(F)) & \xrightarrow{\mathcal{F} \mapsto M_{\mathcal{F}}} & G_F - \mathrm{Set}^d \\
\uparrow \subseteq & & \uparrow \subseteq & & \uparrow \subseteq \\
\mathrm{Spec}(F)_{\text{f,ét}} & \xrightarrow{X \mapsto \underline{X}_F} & \mathrm{lcc} - \text{Ét}(\mathrm{Spec}(F)) & \xrightarrow{\mathcal{F} \mapsto M_{\mathcal{F}}} & G_F - \mathrm{Set}^d_f \\
{\scriptstyle (-) \times_{\mathcal{O}_{F,\Sigma}} F} \uparrow & & \uparrow {\scriptstyle \mathcal{F} \mapsto \iota^* \mathcal{F}} & & \\
\mathrm{Spec}(\mathcal{O}_{F,\Sigma})_{\text{f,ét}} & \xrightarrow{X \mapsto \underline{X}_{\mathcal{O}_{F,\Sigma}}} & \mathrm{lcc} - \text{Ét}(\mathrm{Spec}(\mathcal{O}_{F,\Sigma})) & &
\end{array} \tag{A.3.7}$$

where the lower diagram commutes up to isomorphism, which can be shown using the Yoneda Lemma, see ([Cona], Example 1.1.6.1). The functor $(-)\times_{\mathcal{O}_{F,\Sigma}} F$ denotes base change and $\mathcal{F} \mapsto \iota^* \mathcal{F}$ is the pullback. Both of the arrows in the top row define equivalences of categories, see (loc. cit., Theorem 1.1.4.3 and Corollary 1.1.4.6). Moreover, the other two horizontal arrows on the left ($X \mapsto \underline{X}_F$, $X \in \mathrm{Spec}(F)_{\mathrm{f,\acute{e}t}}$ and $X \mapsto \underline{X}_{\mathcal{O}_{F,\Sigma}}$, $X \in \mathrm{Spec}(\mathcal{O}_{F,\Sigma})_{\mathrm{f,\acute{e}t}}$) also define equivalences of categories, see (loc. cit., Theorem 1.1.7.2). The pullback functor $\mathcal{F} \mapsto \iota^* \mathcal{F}$ is fully faithful with essential image equal to the category of finite discrete G_F-sets unramified at the closed points of $\mathrm{Spec}(\mathcal{O}_{F,\Sigma}) \cong \mathrm{Spec}(\mathcal{O}_F) \setminus \Sigma_f$, see (loc. cit., Corollary 1.1.7.3).

In the top row, group schemes over F correspond to sheaves of abelian groups, which correspond to discrete G_F-modules. Under the functor $\acute{\mathrm{E}}\mathrm{t}(\mathrm{Spec}(F)) \to G_F - \mathrm{Set}^d$, the global sections functor corresponds to taking Galois invariants, which explains the relation between Galois cohomology (for discrete G_F-modules) and étale cohomology (for the corresponding sheaf of abelian groups), see ([Cona], Corollary 1.1.45 and the discussion preceding it). We also note that if X is an étale F-scheme, then $M_{\underline{X}_F}$ is given by the discrete G_F-set $X_F(\bar{F}) = Mor_F(\mathrm{Spec}(\overline{F}), X)$.

Let us now look at the sequence of sheaves of abelian groups on $\mathrm{Spec}(\mathcal{O}_{F,\Sigma})_{\acute{\mathrm{e}}\mathrm{t}}$ known as the Kummer sequence

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \overset{x\mapsto x^n}{\longrightarrow} \mathbb{G}_m \longrightarrow 0, \qquad n \in \mathbb{N}_{\geq 1}, \tag{A.3.8}$$

where $\mathbb{G}_m$ is the sheaf of points of the group scheme $\mathbb{G}_m$ (note the abuse of notation, in (A.3.8) we should write $\underline{\mathbb{G}_m}_{\mathcal{O}_{F,\Sigma}}$ instead of $\mathbb{G}_m$ for the sheaf associated to $\mathbb{G}_m$ to be in line with our notation), $x \mapsto x^n$ is the map that, on points, is given by raising to the n-th power and μ_n is the kernel. We just quote as a fact that if n is unit in $\mathcal{O}_{F,\Sigma}$, then the sequence (A.3.8) is exact in the category of sheaves of abelian groups on $\mathrm{Spec}(\mathcal{O}_{F,\Sigma})_{\acute{\mathrm{e}}\mathrm{t}}$ ($0 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m$ is always exact). Let us assume that $n \in \mathcal{O}_{F,\Sigma}^{\times}$ from now on. The sheaf μ_n is represented by the finite étale $\mathcal{O}_{F,\Sigma}$-group scheme $\mathrm{Spec}\big(\mathbb{Z}[T]/(T^n-1)\big)\times_{\mathbb{Z}} \mathcal{O}_{F,\Sigma} \cong \mathrm{Spec}\big(\mathcal{O}_{F,\Sigma}[T]/(T^n-1)\big)$. We have noted already that for $X \in \mathrm{Spec}(F)_{\acute{\mathrm{e}}\mathrm{t}}$, $M_{\underline{X}_F}$ is given by the discrete G_F-set $X_F(\bar{F})$. Hence, the finite discrete G_F-module that, through (A.3.7), corresponds to $\mathrm{Spec}\big(\mathcal{O}_{F,\Sigma}[T]/(T^n - 1)\big)$ is given by $Mor_F\big(\overline{F}, \mathrm{Spec}(F[T]/(T^n-1))\big)$ which is just the finite G_F-module $\mu_n(\bar{F})$ of n-th roots of unity in the algebraic closure $\bar{F}$, which is unramified outside Σ.

A.3.3 Tensor products and cohomology

Next we turn to the behaviour of Galois cohomology with respect to twisting. We recall the result ([FK06], Proposition 1.6.5 (3)) of Fukaya and Kato and explain how we want to use it later on. We will not work in the greatest generality, but restrict to the following setting. Fix a prime number $p \in \mathbb{Z}$. Let F_∞/F be a p-adic Lie extension inside a fixed algebraic closure $\overline{F}$ of F, where F is either a number field or a finite extension $F/\mathbb{Q}_p$ for some fixed prime $p \in \mathbb{Z}$. In case F is a number field, assume that F_∞/F is unramified outside a finite set of primes Σ containing Σ_p. Also in the number field case we assume that F is totally imaginary if $p = 2$. Then, define a field

$$\tilde{F} = \begin{cases} F_\Sigma & \text{if } F \text{ is a number field,} \\ \overline{F} & \text{if } F \text{ is a finite extension of } \mathbb{Q}_p. \end{cases} \tag{A.3.9}$$

We will write

$$G = G(\tilde{F}/F) \tag{A.3.10}$$

and note that by propositions A.3.1 and A.3.2 the Galois group G, for both cases, F a number field and a local field, satisfies the conditions (i) and (ii) of Case 1 of (loc. cit., Proposition 1.6.5). By definition, we have a canonical projection

$$G \twoheadrightarrow G(F_\infty/F),$$

in both, the global and the local case. Let us briefly recall some isomorphisms. Let L/F be a finite Galois extension inside $\tilde{F}/F$ and write $H = G(\tilde{F}/L)$, $H \subseteq G$. Moreover, let T be a finitely generated $\mathbb{Z}_p$-module with a continuous $\mathbb{Z}_p$-linear action of G and write $\mathbb{Z}_p(0)$ for $\mathbb{Z}_p$ equipped with the trivial H-action from the right. More generally, whenever it makes sense, we write $T(k)$, $k \in \mathbb{Z}$, for the k-th Tate twist of T. Using a standard result for induced modules ([Lan05] XVIII, Theorem 7.11), we then have

$$\mathrm{Ind}_G^H \mathrm{Res}_H^G T \cong \mathrm{Ind}_G^H(\mathbb{Z}_p(0) \otimes_{\mathbb{Z}_p} \mathrm{Res}_H^G T) \cong \left(\mathrm{Ind}_G^H \mathbb{Z}_p(0)\right) \otimes_{\mathbb{Z}_p} T \cong \mathbb{Z}_p[G(L/F)]^\# \otimes_{\mathbb{Z}_p} T, \tag{A.3.11}$$

where G acts on $\mathbb{Z}_p[G(L/F)]^\#$ (which is just $\mathbb{Z}_p[G(L/F)]$ as a left $\mathbb{Z}_p[G(L/F)]$-module) from the left via $g.x = x \cdot \overline{g}^{-1}$, where $\overline{g}$ denotes the image of $g \in G$ in $G(L/F)$ and the tensor product on the right carries the diagonal action $g.(x \otimes t) = x \cdot \overline{g}^{-1} \otimes g.t$.

Now, assume we are given an, in general, infinite Galois extension $F_\infty = \cup_n F_n$ of F as above, with Galois group $G(F_\infty/F)$, where the F_n, $n \geq 1$, form an increasing chain of finite Galois extensions of F. Moreover, assume we are given a finitely generated $\mathbb{Z}_p$-module T with a continuous action of $G = G(\tilde{F}/F)$. For $\Lambda = \Lambda(G(F_\infty/F))$ we then have

$$\Lambda^\# \otimes_{\mathbb{Z}_p} T \cong \varprojlim_n \left(\mathbb{Z}_p/(p^n)[G(F_n/F)]^\# \otimes_{\mathbb{Z}_p} T/p^n T\right),$$

since for finitely generated $\mathbb{Z}_p$-modules T the completed tensor product agrees with the usual tensor product, see ([Bru66], Lemma 2.1 (ii)).

We note that by propositions A.3.1 and A.3.2 we may apply proposition A.3.4 to G, $H_n := G(\tilde{F}/F_n)$, $n \geq 1$, and projective limits of finite modules of p-power order. In particular, we may apply it to the projective limits of the finite modules $T_n = \mathbb{Z}_p/(p^n)[G(F_n/F)]^\# \otimes T/p^n T$ and $T'_m = \mathrm{Res}_{H_n}^G T/p^m T$. Note that $T_n \cong \mathrm{Ind}_G^{H_n} \mathrm{Res}_{H_n}^G T/p^n T$. Then, using Shapiro's Lemma and the isomorphism (A.3.11) we have

$$\begin{aligned} H^i(G(\tilde{F}/F), \Lambda^\# \otimes T) &\cong \varprojlim_n H^i(G, T_n) \\ &\cong \varprojlim_{n,m} H^i(H_n, \mathrm{Res}_{H_n}^G T/p^m T) \\ &\cong \varprojlim_n H^i(G(\tilde{F}/F_n), \mathrm{Res}_{H_n}^G T). \end{aligned} \tag{A.3.12}$$

Les us now discuss Fukaya and Kato's result about the behaviour of Galois cohomology with respect to twisting. Note that $\Lambda = \Lambda(G(F_\infty/F))$ satisfies the condition $(*)$ of ([FK06], 1.4.1), saying that there exists a two-sided ideal I of Λ such that Λ/I^n is finite of p-power order for all $n \geq 1$ and such that

$$\Lambda \cong \varprojlim_n \Lambda/I^n.$$

Let $\Lambda' \cong \varprojlim_n \Lambda'/(I')^n$, where I' is a two-sided ideal of Λ' such that $\Lambda'/(I')^n$, for all $n \geq 1$, is finite of p-power order, be another such ring. The example we have in mind is $\Lambda' = \Lambda(G(F_\infty/K))$, where K is a subfield of F such that F/K is a finite extension and such that F_∞/K is also a p-adic Lie extension.

Now, let M be a finitely generated projective left Λ-module equipped with a continuous Λ-linear action of G. Moreover, let Y be a (Λ', Λ)-bimodule (i.e., a left Λ'-module and a right Λ-module such that the actions commute) such that

(i) as a left Λ'-module Y is finitely generated and projective,

(ii) Y has a topology such that the right Λ-action is continuous.

Then, the above-mentioned result from (loc. cit.) states that there is an isomorphism in the derived category of Λ'-modules

$$Y \otimes^L_\Lambda R\Gamma(G, M) \cong R\Gamma(G, Y \otimes_\Lambda M), \tag{A.3.13}$$

where the action of G on $Y \otimes_\Lambda M$ is defined by $g.(y \otimes m) = y \otimes g.m$, $g \in G, y \in Y, m \in M$, and where for any G-module N we write $R\Gamma(G, N)$ for $C(G, N)$, the complex of continuous cochains of G with values in N, regarded as an object in the derived category.

In fact, Fukaya and Kato prove in (loc. cit., Lemma 1.6.8), that there exists a bounded complex $L^\bullet$ of finitely generated projective Λ-modules and a homomorphism of complexes of Λ-modules $L^\bullet \longrightarrow C(G, M)$ such that for any pair (Λ', Y) as above, the induced map

$$Y \otimes_\Lambda L^\bullet \to C(G, Y \otimes_\Lambda M) \tag{A.3.14}$$

is a quasi-isomorphism, where $Y \otimes_\Lambda L^\bullet$ denotes the complex induced by tensoring each term L^n of $L^\bullet$ with Y. By the induced map we mean the composite map

$$Y \otimes_\Lambda L^\bullet \to Y \otimes_\Lambda C(G, M) \to C(G, Y \otimes_\Lambda M), \tag{A.3.15}$$

where the first map is induced by $L^\bullet \longrightarrow C(G, M)$ and the second map is defined in the obvious way. In particular, from the case $Y = \Lambda$ considered as a (Λ, Λ)-bimodule, we see that the map

$$L^\bullet \to C(G, M) \tag{A.3.16}$$

itself is a quasi-isomorphism. Now assume that Y is also flat as a right Λ-module. By the flatness of Y the map $Y \otimes_\Lambda L^\bullet \to Y \otimes_\Lambda C(G, M)$ is then also a quasi-isomorphism. In fact, we have

$$H^n(Y \otimes_\Lambda L^\bullet) \cong Y \otimes_\Lambda H^n(L^\bullet) \cong Y \otimes_\Lambda H^n(G, M) \cong H^n(Y \otimes_\Lambda C(G, M)),$$

where the first and the last isomorphism hold by the flatness of Y and the middle one since (A.3.16) is a quasi-isomorphism. Now, consider the composite map from (A.3.15) again. Since both, the composite and the first map of the composite are quasi-isomorphisms, so must be the second map of the composite and we record this in the following

Proposition A.3.7. *Let the setting be as in the preceding discussion. In addition, assume that Y is flat as a right Λ-module. Then, the map*

$$Y \otimes_\Lambda C(G, M) \to C(G, Y \otimes_\Lambda M)$$

is a quasi-isomorphism. In particular, we have $Y \otimes_\Lambda H^n(G, M) \cong H^n(G, Y \otimes_\Lambda M)$, for all $n \geq 0$. We recall that the G-action on $Y \otimes_\Lambda M$ is given by the action on M, i.e., by $1 \otimes g$, $g \in G$, on the tensor product.

We will now discuss some examples for Y arising from p-adic Galois representations T, by which we mean finitely generated free $\mathbb{Z}_p$-modules T with a continuous $\mathbb{Z}_p$-linear action of G that factors through $G(F_\infty/F)$. We fix such a Galois representation T and assume, as before, that F_∞/F is a p-adic Lie-extension (this is automatically satisfied if F_∞ is the trivializing extension, i.e., the fixed field of the kernel). Recall definition (A.3.9) of $\tilde{F}$, and that for $G = G(\tilde{F}/F)$ we have a natural projection $G \twoheadrightarrow G(F_\infty/F)$, for which we shall write $g \mapsto \bar{g}$. Let us write $\kappa : G \longrightarrow \mathbb{Z}_p^\times$ for the p-cyclotomic character; note that $\tilde{F}$ always contains the p-power roots of unity, since we assumed that $\Sigma_p \subset \Sigma$ in the global case. Writing, as before, $\Lambda = \Lambda(G(F_\infty/F))$ we define the following objects

$$M = \Lambda^\#(1),$$

which is just Λ as a left Λ-module (i.e., free of Λ-rank 1 and, in particular, projective) and $g \in G$ acts (Λ-linearly!) on $\lambda \in \Lambda^\#(1)$ by $g.\lambda := \lambda \bar{g}^{-1}\kappa(g)$,

$$\Lambda' = \Lambda,$$

and

$$Y = \Lambda \otimes_{\mathbb{Z}_p} T,$$

which is a left Λ-module by the action on the first factor $\lambda'.(\lambda \otimes t) := (\lambda'\lambda) \otimes t$ for $\lambda', \lambda \in \Lambda$, $t \in T$, and a right Λ-module via the action induced by $(\lambda \otimes t).h := (\lambda h) \otimes (h^{-1}.t)$ for $\lambda \in \Lambda$, $t \in T$, $h \in G(F_\infty/F)$. Note that the left and right action of Λ on $\Lambda \otimes_{\mathbb{Z}_p} T$ are compatible and that, as a left-module (!), $\Lambda \otimes_{\mathbb{Z}_p} T$ is free and isomorphic to Λ^r, where $r := \mathrm{rk}_{\mathbb{Z}_p} T$ is the $\mathbb{Z}_p$-rank of T. In particular, it is finitely generated and projective as a left-module. The continuity of the right action follows since we assumed that the action of $G(F_\infty/F)$ on T is continuous.

We claim that $\Lambda \otimes_{\mathbb{Z}_p} T$ is also free of rank r as a right Λ-module. In a slightly different form, this has been proved by Venjakob in ([Ven03], Lemma 7.2). Let us fix an isomorphism $\phi : T \cong \mathbb{Z}_p^r$ of $\mathbb{Z}_p$-modules. Next, consider the map

$$\Lambda \otimes_{\mathbb{Z}_p} T \to \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Z}_p^r \cong \Lambda^r, \tag{A.3.17}$$

induced by $g \otimes t \mapsto g \otimes \phi(gt) \mapsto g\phi(gt)$. As we will explain below, it follows as in (loc. cit., Lemma 7.2) that this map is an isomorphism of right Λ-modules (Λ^r is equipped with the canonical right Λ-module structure). In order to avoid confusion, we note that if we write $\phi(gt) = (\phi(gt)_1, \dots, \phi(gt)_r)$ for the image of gt under ϕ in $\mathbb{Z}_p^r$, then $g\phi(gt)$ is given by $(g\phi(gt)_1, \dots, g\phi(gt)_r)) \in \Lambda^r$.

Remark A.3.8. Our definition of $(A.3.17)$ is different from Venjakob's, who defines a map $g \otimes t \mapsto g \otimes \phi(g^{-1}t) \mapsto g\phi(g^{-1}t)$, with the inverse of g acting on t, which makes the map left Λ-linear, with Λ-action induced by $h.(\lambda \otimes t) = (h\lambda) \otimes (ht)$, $h \in G(F_\infty/F)$ (and the canonical left Λ-structure on Λ^r). However, our map (A.3.17), with respect to our right Λ-structure (and the canonical right Λ-structure on Λ^r), is right Λ-linear

$$(g \otimes t).h \overset{\text{def}}{=} gh \otimes h^{-1}t \longmapsto gh\phi(ghh^{-1}t) = gh\phi(gt) = (g\phi(gt))h, \quad g, h \in G(F_\infty/F), t \in T.$$

We do not claim that our map (A.3.17) is left Λ-linear with respect to our left Λ-structure (and the canonical left Λ-structure on Λ^r). In fact, it is not unless the Galois action on T is trivial.

As for the existence of the map (A.3.17), i.e., that it actually extends from (the group ring tensored with T) $\mathbb{Z}_p[G(F_\infty/F)] \otimes_{\mathbb{Z}_p} T$ to $\Lambda \otimes_{\mathbb{Z}_p} T$, one proceeds as in the proof of ([Ven03], Lemma 7.2). Consider pairs (U, n) where $n \geq 1$ is an integer and U is an open normal subgroup of $G(F_\infty/F)$ such that U acts trivially on the discrete space T/p^nT. Then, for each such pair, one can define a map $\mathbb{Z}_p[G(F_\infty/F)/U] \otimes_{\mathbb{Z}_p} T/p^nT \to \mathbb{Z}_p/(p^n)[G(F_\infty/F)/U]^r$ by the same formula as above just for cosets $\bar{g} \otimes \bar{t} \mapsto \bar{g} \otimes \overline{\phi(gt)} \mapsto \bar{g}\overline{\phi(gt)}$ and verify that it is an isomorphism. One then passes to the projective limit and gets the desired map upon noting that the completed tensor product coincides with the usual tensor product, since T is finitely generated as a $\mathbb{Z}_p$-module. We conclude that $\Lambda \otimes_{\mathbb{Z}_p} T$ is a free right Λ-module of rank r. In particular it is flat as right Λ-module and we may apply proposition A.3.7 to $\Lambda \otimes_{\mathbb{Z}_p} T$ and $\Lambda^{\#}(1)$. Before we do this let us record the following

Proposition A.3.9. *Let the setting be as at the beginning of this subsection and recall the definition (A.3.9) and (A.3.10) of $G = G(\tilde{F}/F)$. Then, the modules $H^n(G, \Lambda^{\#}(1))$ are 0 for $n \geq 3$ and for $n = 0$. In the global case, the modules $H^i(G_\Sigma(F), \Lambda^{\#}(1))$, $i = 1, 2$ are finitely generated over Λ. In the local case for $F/\mathbb{Q}_p$ a finite extension we have*

$$H^n(G_F, \Lambda^{\#}(1)) \cong \begin{cases} \varprojlim_{L,k} L^\times/(L^\times)^{p^k} & \text{if } n = 1, \\ \mathbb{Z}_p & \text{if } n = 2, \end{cases} \tag{A.3.18}$$

where L ranges through the finite subextensions of F_∞/F and the limit is taken with respect to norm maps $N_{L'/L}$, $L \subset L'$, and projection maps $L^\times/(L^\times)^{p^{k+1}} \twoheadrightarrow L^\times/(L^\times)^{p^k}$. Let us, in addition, assume that there exists a finite subextension K/F of F_∞/F such that F_∞/K is abelian and $G(F_\infty/K) \cong \mathbb{Z}_p^r \times \Delta$, where $r = 1, 2$ and Δ is finite of order prime to p, and that either the following (i) or the following (ii) hold *(i)* $\mu_{p^\infty}(\overline{F}) \subset F_\infty$ *and in case that* $p = 2$*, then also* $\mu_4 \subset K$*,*

(ii) $\mu_{p^\infty}(F_\infty) = \{1\}$*.*

Then, $H^1(G_F, \Lambda^\#(1))$ *is finitely generated over* $\Lambda(G(F_\infty/K))$ *(and hence over* $\Lambda(G(F_\infty/F))$*).*

Proof. The vanishing of $H^n(G, \Lambda^\#(1))$ for $n \geq 3$ follows since both, $cd_p G_F$ for F local non-archimedean and $cd_p G_\Sigma(F)$ for F a number field, are less than or equal to 2, see propositions A.3.1 and A.3.2. The vanishing of $H^0(G, \Lambda^\#(1))$ follows from the fact that neither a number field, nor a finite extension of $\mathbb{Q}_p$ contain infinitely many roots of unity.

In the global case, for the fact that $H^i(G_\Sigma(F), \Lambda^\#(1))$, $i = 1, 2$ are finitely generated, see [Kat06].

In the local case, the description of $H^1(G_F, \Lambda^\#(1))$ follows from Hilbert's Satz 90 and the Kummer sequence, while $H^2(G_F, \Lambda^\#(1)) \cong \mathbb{Z}_p$ follows from local Tate duality, compare remark A.4.6 (iii).

Now, assume the additional assumption on the existence of a finite subextension K/F of F_∞/F is satisfied. First consider the case $r = 2$. Note that since F_∞/F is a p-adic Lie extension, so is F_∞/K since $G(F_\infty/K) \subset G(F_\infty/F)$ is an open, hence closed, subgroup. It follows that $\Lambda(G(F_\infty/K))$ is Noetherian, see ([Laz65], V 2.2.4). Then, the fact that $H^1(G_F, \Lambda^\#(1))$ is finitely generated over $\Lambda(G(F_\infty/K))$ follows from a result of Wintenberger, see ([Win80], section 4, Théorèm). When applying the quoted result, one only has to note that if ϕ is a character of Δ and e_ϕ the associated idempotent, then $e_\phi \Lambda(G(F_\infty/K))^d$, $d \geq 1$, is Noetherian as a $\Lambda(G(F_\infty/K))$-module (indeed, it is finitely generated, just consider the natural $\Lambda(G(F_\infty/K))$-linear projection $\Lambda(G(F_\infty/K))^d \twoheadrightarrow e_\phi \Lambda(G(F_\infty/K))^d$, note that $G(F_\infty/K)$ is abelian!), so any $e_\phi \Lambda(G(F_\infty/K))$-submodule of $e_\phi \Lambda(G(F_\infty/K))^d$, $d \geq 1$, (which is then automatically a $\Lambda(G(F_\infty/K))$-submodule) is finitely generated over $\Lambda(G(F_\infty/K))$. Let us note that Wintenberger determines the structure of $\varprojlim_{L,k} L^\times/(L^\times)^{p^k}$ much more precisely, but for now, we are only interested in it being finitely generated.

The local case for $r = 1$ was treated by Iwasawa in ([Iwa73], §12, Theorem 25). In fact, if $r = 1$, let K' be the finite extension of K such that $G(F_\infty/K') \cong \mathbb{Z}_p$. Now, note that $H^1(G_F, \Lambda^\#(1))$ is a different guise of the Galois group of the maximal abelian p-extension of F_∞. Indeed, using local Tate duality, we have

$$H^1(G_F, \Lambda^\#(1)) \cong \varprojlim_{L,\mathrm{cor}} H^1(G_L, \mathbb{Z}_p(1)) \cong \varprojlim_{L,\mathrm{res}^\vee} (H^1(G_L, \mathbb{Q}_p/\mathbb{Z}_p)^\vee) \cong \mathrm{Hom}(G_{F_\infty}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee.$$

Since $\Lambda(G(F_\infty/K'))$ is Noetherian we can now derive the result for both cases (i) and (ii) from (loc. cit.), where it is stated for the Galois group of the maximal abelian p-extension of F_∞. □

For a more detailed description of the modules $H^n(G, \Lambda^\#(1))$, see ([Ven00], chapters 2 and 3). We note that there is a criterion due to Balister and Howson for a Hausdorff Λ-module X that is profinite to be finitely generated, see [BH03], it says the following. Let I be an ideal of Λ

such that $I^n \to 0$, $n \to \infty$, in Λ. Then, if X/IX is finitely generated as a Λ/I-module, then X is finitely generated as a Λ-module.

Let us deduce the following corollary from propositions A.3.7 and A.3.9.

Corollary A.3.10. *Let the assumptions be as in proposition A.3.9. Let T be a finitely generated free $\mathbb{Z}_p$-module with a continuous $\mathbb{Z}_p$-linear action of G factoring through $G(F_\infty/F)$. For every $n \geq 0$ we have an isomorphism of left Λ-modules*

$$T \otimes_{\mathbb{Z}_p} H^n(G, \Lambda^\#(1)) \to H^n(G, \Lambda^\#(1) \otimes_{\mathbb{Z}_p} T),$$

where the Λ-action on the left is induced by the diagonal action $h.(t \otimes f) = ht \otimes hf$, $h \in G(F_\infty/F)$, $t \in T$, $f \in H^n(G, \Lambda^\#(1))$ and G acts on $\Lambda^\#(1) \otimes_{\mathbb{Z}_p} T$ diagonally, i.e., as $g(\lambda \otimes t) = \lambda\kappa(g)\bar{g}^{-1} \otimes \bar{g}t$, $g \in G$, $\lambda \in \Lambda$, $t \in T$.

Proof. As we have explained above, we may apply proposition A.3.7 to $\Lambda \otimes_{\mathbb{Z}_p} T$ and $\Lambda^\#(1)$, which gives us an isomorphism

$$(\Lambda \otimes_{\mathbb{Z}_p} T) \otimes_\Lambda H^n(G, \Lambda^\#(1)) \cong H^n(G, (\Lambda \otimes_{\mathbb{Z}_p} T) \otimes_\Lambda \Lambda^\#(1)), \tag{A.3.19}$$

for any $n \geq 0$, where $g \in G$ acts on $(\lambda' \otimes t) \otimes \lambda \in (\Lambda \otimes_{\mathbb{Z}_p} T) \otimes_\Lambda \Lambda^\#(1)$ as $g\big((\lambda' \otimes t) \otimes \lambda\big) = (\lambda' \otimes t) \otimes (\lambda\bar{g}^{-1}\kappa(g))$, i.e., only on the $\Lambda^\#(1)$ factor. We will show that the two modules in (A.3.19) are isomorphic to $T \otimes_{\mathbb{Z}_p} H^n(G, \Lambda^\#(1))$ and $H^n(G, \Lambda^\#(1) \otimes_{\mathbb{Z}_p} T)$, respectively. Let us begin with $H^n(G, (\Lambda \otimes_{\mathbb{Z}_p} T) \otimes_\Lambda \Lambda^\#(1))$. Forgetting the G-actions for a moment, the map

$$\Lambda^\#(1) \otimes_{\mathbb{Z}_p} T \to (\Lambda \otimes_{\mathbb{Z}_p} T) \otimes_\Lambda \Lambda^\#(1), \quad \lambda \otimes t \mapsto (\lambda \otimes t) \otimes 1, \tag{A.3.20}$$

certainly defines an isomorphism of left Λ-modules (the left Λ-module structure is in both cases defined via the action on the first left factor). In fact, the map is even a (Λ, Λ)-bimodule isomorphism (using the correct actions), but we do not need this fact. Recall from the statement of the corollary that we let G act diagonally on $\Lambda^\#(1) \otimes_{\mathbb{Z}_p} T$. It follows that (A.3.20) is also G-equivariant. Indeed, let $g \in G$, then we have for $\lambda \otimes t \in \Lambda^\#(1) \otimes_{\mathbb{Z}_p} T$

$$g.(\lambda \otimes t) \overset{\text{def}}{=} \lambda\kappa(g)\bar{g}^{-1} \otimes \bar{g}t \longmapsto (\lambda\kappa(g)\bar{g}^{-1} \otimes \bar{g}t) \otimes 1 = (\lambda \otimes t) \otimes \bar{g}^{-1}\kappa(g) = g.\big((\lambda \otimes t) \otimes 1\big),$$

where on the right-hand side we used the definition of the right Λ-action on $\Lambda \otimes_{\mathbb{Z}_p} T$.

It remains to show that $T \otimes_{\mathbb{Z}_p} H^n(G, \Lambda^\#(1))$ is isomorphic to $(\Lambda \otimes_{\mathbb{Z}_p} T) \otimes_\Lambda H^n(G, \Lambda^\#(1))$, which follows from the following lemma, which we may apply since $H^n(G, \Lambda^\#(1))$ is finitely generated over Λ. □

Recall that any compact Λ-module N can be written as $N \cong \varprojlim_V N_V$, where N_V denote the coinvariants and the projective limit is taken over all open normal subgroups $V \subset G(F_\infty/F)$, see ([CS06], Appendix A.1). Clearly, if N is finitely generated over Λ, then N_V/p^n is finite for all open normal subgroups $V \subset G(F_\infty/F)$ and $n \geq 1$.

Lemma A.3.11. *Let T be a free $\mathbb{Z}_p$-module endowed with a continuous left $G(F_\infty/F)$-action and let N be a finitely generated left Λ-module. As above, we consider the right Λ-action on $\Lambda \otimes_{\mathbb{Z}_p} T$ induced by $(\lambda \otimes t).g = \lambda g \otimes g^{-1}t$, where $g \in G(F_\infty/F), \lambda \in \Lambda, t \in T$. We define a Λ-action on $T \otimes_{\mathbb{Z}_p} N$ induced by the diagonal action of $g \in G(F_\infty/F)$, that is $g.(t \otimes x) = gt \otimes gx$, $t \in T$, $x \in N$. Then there is an isomorphism*

$$\left(\Lambda \otimes_{\mathbb{Z}_p} T\right) \otimes_\Lambda N \longrightarrow T \otimes_{\mathbb{Z}_p} N, \qquad (\lambda \otimes t) \otimes x \longmapsto \lambda.(t \otimes x),$$

of left Λ-modules (for the Λ-action on the Λ-factor on the left and the diagonal action on the right).

Proof. One checks that for fixed $x \in N$, the map $\Lambda \times T \to T \otimes_{\mathbb{Z}_p} N$ defined by $(\lambda, t) \mapsto \lambda.(t \otimes x)$ is $\mathbb{Z}_p$-bilinear. Hence, one gets a map

$$\left(\Lambda \otimes_{\mathbb{Z}_p} T\right) \times N \longrightarrow T \otimes_{\mathbb{Z}_p} N, \qquad (\lambda \otimes t, x) \longmapsto \lambda.(t \otimes x),$$

which is easily seen to be $\mathbb{Z}_p[G(F_\infty/F)]$-bilinear. Now, consider pairs (n, U), where $n \geq 1$ is an integer, and U is an open normal subgroup of $G(F_\infty/F)$ acting trivially on T/p^n. Note that if V is any other open normal subgroup of $G(F_\infty/F)$, then $(n, U \cap V)$ is also such a pair. Let us write $G' = G(F_\infty/F)$. In an entirely similar fashion as above, for any pair (n, U) we get a map

$$(\mathbb{Z}_p[G'/U] \otimes_{\mathbb{Z}_p} T/p^n) \times (N_U/p^n) \longrightarrow T/p^n \otimes_{\mathbb{Z}_p} (N_U/p^n)$$

which is $\mathbb{Z}_p[G(F_\infty/F)]$-bilinear, and therefore Λ-bilinear (since the Λ-action factors through $\mathbb{Z}_p[G'/U]$). Hence, we get a map

$$(\mathbb{Z}_p[G'/U] \otimes_{\mathbb{Z}_p} T/p^n) \otimes_\Lambda (N_U/p^n) \longrightarrow T/p^n \otimes_{\mathbb{Z}_p} (N_U/p^n),$$

which is left $\mathbb{Z}_p[G'/U]$-linear with respect to the induced actions. One checks immediately (on generators) that $\bar{t} \otimes \bar{x} \mapsto (1 \otimes \bar{t}) \otimes \bar{x}$, where $\bar{x} \in (N_U/p^n)$, $\bar{t} \in T/p^r$, defines an inverse. Recall that $\Lambda \otimes_{\mathbb{Z}_p} T$ is free of rank r as a right Λ-module. Since for finitely presented modules (and compact modules in the other variable) the completed tensor product coincides with the usual tensor product, see ([Wit03], Proposition 1.14), we conclude

$$\begin{aligned}
\left(\Lambda \otimes_{\mathbb{Z}_p} T\right) \otimes_\Lambda N &\cong \left(\Lambda \otimes_{\mathbb{Z}_p} T\right) \hat{\otimes}_\Lambda N \\
&\cong \varprojlim_{(n,U)} \Big((\mathbb{Z}_p[G'/U] \otimes_{\mathbb{Z}_p} T/p^n) \otimes_\Lambda (N_U/p^n) \Big) \\
&\cong \varprojlim_{(n,U)} \left(T/p^n \otimes_{\mathbb{Z}_p} (N_U/p^n) \right) \\
&\cong T \hat{\otimes}_{\mathbb{Z}_p} N \\
&\cong T \otimes_{\mathbb{Z}_p} N,
\end{aligned}$$

which concludes the proof. □

We will also need the following standard result, see (the proof of) ([Tat76], proposition 2.3) in Tate's article or also ([Rub00], Appendix B, Proposition B.2.4). Had we worked in greater generality in this subsection we could have also deduced it from the result of Fukaya and Kato.

Proposition A.3.12. *Let T be a finitely generated free $\mathbb{Z}_p$-module with a continuous $\mathbb{Z}_p$-linear action of a profinite group G. Then, for all $i \geq 0$, the natural map*

$$H^i(G,T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \longrightarrow H^i(G, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$$

is an isomorphism.

Proof. One can proceed similarly as in the proof of ([Tat76], proposition 2.3). Tensor the exact sequence

$$0 \to \mathbb{Z}_p \to \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

with T, which is flat over $\mathbb{Z}_p$ by assumption, and look at the corresponding long exact cohomology sequence. The groups $H^i(G, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$ are torsion, which yields

$$H^i(G,T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong H^i(G, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong H^i(G, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$$

as desired, where the second isomorphism is given by $v \otimes x \mapsto vx$, $v \in H^i(G, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$, $x \in \mathbb{Q}_p$. □

A.3.4 Kummer sequence

Let the setting be as in section 2.2.

Remark A.3.13. We note that, by definition of Σ, each canonical morphism

$$\pi_n : \mathrm{Spec}(\mathcal{O}_{F_n,\Sigma}) \longrightarrow \mathrm{Spec}(\mathcal{O}_{F,\Sigma})$$

is étale. Therefore, compare ([Mil80], Remark 3.1 (a) Chapter 2, p. 68), if $\mathcal{F}$ is any sheaf on the small étale site $\mathrm{Spec}(\mathcal{O}_{F,\Sigma})_{\text{ét}}$, then the inverse image $\pi_n^*\mathcal{F}$ is just the restriction $\mathcal{F}\,|_{\mathrm{Spec}(\mathcal{O}_{F_n,\Sigma})}$. We will simply also write $\mathcal{F}$ for $\pi_n^*\mathcal{F}$.

We want to recall that $\mathbb{H}^1_\Sigma$ and $\mathbb{H}^2_\Sigma$, which were defined to be

$$\mathbb{H}^m_\Sigma := \varprojlim_n H^m_{\text{ét}}\big(\mathcal{O}_{F_n}\big[\frac{1}{\Sigma_f}\big], \mathbb{Z}_p(1)\big),$$

appear in the Kummer sequence. In fact, for every $n \geq 0$ and every $k \geq 1$ there is an exact sequence of sheaves

$$0 \longrightarrow \mu_{p^k} \longrightarrow \mathbb{G}_m \xrightarrow{p^k} \mathbb{G}_m \longrightarrow 0$$

on the site $\operatorname{Spec}(\mathcal{O}_{F_n}[\frac{1}{\Sigma_f}])_{\text{ét}}$ since p is different from the residue characteristic of every point of $\operatorname{Spec}(\mathcal{O}_{F_n}[\frac{1}{\Sigma_f}])$, compare ([Mil80], p.66) and recall $\Sigma_p \subset \Sigma_f$. We note that for $n \geq 1$ these sequences agree with

$$0 \longrightarrow \pi_n^*(\mu_{p^k,\mathcal{O}_{F,\Sigma}}) \longrightarrow \pi_n^*\mathbb{G}_{m,\mathcal{O}_{F,\Sigma}} \xrightarrow{p^k} \pi_n^*\mathbb{G}_{m,\mathcal{O}_{F,\Sigma}} \longrightarrow 0,$$

the sequences obtained by applying the inverse image functors π_n^* to the exact sequence on $\operatorname{Spec}(\mathcal{O}_{F,\Sigma})_{\text{ét}}$. For each $n \geq 0$ and every $k \geq 0$, we get a long exact sequence

$$\begin{array}{l} 1 \longrightarrow \mu_{p^k}(\mathcal{O}_{F_n,\Sigma}) \longrightarrow \mathcal{O}_{F_n,\Sigma}^\times \xrightarrow{p^k} \mathcal{O}_{F_n,\Sigma}^\times \longrightarrow \\ H^1_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mu_{p^k}) \longrightarrow \operatorname{Pic}(\mathcal{O}_{F_n,\Sigma}) \xrightarrow{p^k} \operatorname{Pic}(\mathcal{O}_{F_n,\Sigma}) \longrightarrow \\ H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mu_{p^k}) \longrightarrow H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{G}_m) \xrightarrow{p^k} H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{G}_m) \longrightarrow 1. \end{array} \tag{A.3.21}$$

For the last arrow we note that, since the p-cohomological dimension of $G_\Sigma(F_n)$ is less than or equal to 2, see proposition A.3.1, we have

$$H^3_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mu_{p^k}) = 0,$$

compare also ([FK06], section 1.6.3). The above sequence induces a short exact sequence

$$1 \longrightarrow \mathcal{O}_{F_n,\Sigma}^\times/(\mathcal{O}_{F_n,\Sigma}^\times)^{p^k} \longrightarrow H^1_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{Z}/p^k\mathbb{Z}(1)) \longrightarrow \operatorname{Pic}(\mathcal{O}_{F_n,\Sigma})[p^k] \longrightarrow 1.$$

Then, taking projective limits, first with respect to k and then with respect to n, we get an isomorphism

$$\varprojlim_n(\mathcal{O}_{F_n,\Sigma}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p) \xrightarrow{\sim} \mathbb{H}^1_\Sigma. \tag{A.3.22}$$

We note that since $\mathbb{Q}^{cyc} \subseteq F_\infty$ we have

$$\varprojlim_n(\mathcal{O}_{F_n,\Sigma}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p) \cong \varprojlim_n(\mathcal{O}_{F_n,\Sigma_p}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p),$$

see ([Kat06], section 2.5, p.554).

By a similar reasoning as above, for every $n \geq 0$, we can extract from (A.3.21) a short exact sequence

$$1 \longrightarrow \operatorname{Pic}(\mathcal{O}_{F_n,\Sigma})\{p\} \longrightarrow H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{Z}_p(1)) \longrightarrow \varprojlim_k H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{G}_m)[p^k] \longrightarrow 1, \tag{A.3.23}$$

where, for an abelian group A, we write $A\{p\}$ for the p-primary subgroup, i.e., the subgroup of elements of finite p-power order. The cohomology group $H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{G}_m)[p^k]\subseteq H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{G}_m)\{p\}$ can be described as follows. By ([NSW08], proof of (8.3.11) Proposition) there is a short exact sequence

$$0\longrightarrow H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{G}_m)\{p\}\longrightarrow \bigoplus_{\nu\in\Sigma_f(F_n)}\mathbb{Q}_p/\mathbb{Z}_p\overset{\text{sum}}{\longrightarrow}\mathbb{Q}_p/\mathbb{Z}_p\longrightarrow 0.$$

Note that the summation map $\bigoplus_{\nu\in\Sigma_f(F_n)}\mathbb{Q}_p/\mathbb{Z}_p\overset{\text{sum}}{\longrightarrow}\mathbb{Q}_p/\mathbb{Z}_p$ as a map of abelian groups has a section, i.e. a splitting homomorphism. The Snake Lemma applied to mupltiplication with p^k implies the existence of a short exact sequence

$$0\longrightarrow H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{G}_m)[p^k]\longrightarrow \bigoplus_{\nu\in\Sigma_f(F_n)}\frac{1}{p^k}\mathbb{Z}_p/\mathbb{Z}_p\overset{\text{sum}_{n,k}}{\longrightarrow}\frac{1}{p^k}\mathbb{Z}_p/\mathbb{Z}_p\longrightarrow 0,$$

where the exactness on the right is clear by definition of the sum map (or follows formally from the above splitting). Together with (A.3.23), passing to the projective limit, we get

$$1\longrightarrow \mathrm{Pic}(\mathcal{O}_{F_n,\Sigma})\{p\}\longrightarrow H^2_{\text{ét}}(\mathcal{O}_{F_n,\Sigma},\mathbb{Z}_p(1))\longrightarrow \bigoplus_{\nu\in\Sigma_f(F_n)}\mathbb{Z}_p\overset{\text{sum}_n}{\longrightarrow}\mathbb{Z}_p\longrightarrow 0. \tag{A.3.24}$$

Now, we can also pass to the projective limit with respect to the F_n, $n\geq 1$, and get

$$1\longrightarrow \varprojlim_n\big(\mathrm{Pic}(\mathcal{O}_{F_n,\Sigma})\{p\}\big)\longrightarrow \mathbb{H}^2_\Sigma\longrightarrow \bigoplus_{\nu\in\Sigma_f}\Lambda(\mathcal{G})\otimes_{\Lambda(\mathcal{G}_\nu)}\mathbb{Z}_p\longrightarrow\mathbb{Z}_p\longrightarrow 0. \tag{A.3.25}$$

We also have a surjective map

$$\mathrm{Pic}(\mathcal{O}_{F_n}[1/p])\{p\}\twoheadrightarrow \mathrm{Pic}(\mathcal{O}_{F_n,\Sigma})\{p\}$$

for every $n\geq 0$, see (A.5.2), which, due to our assumption that $\mathbb{Q}_{cyc}\subset F_\infty$, yields an isomorphism

$$\varprojlim_n\big(\mathrm{Pic}(\mathcal{O}_{F_n}[1/p])\{p\}\big)\cong\varprojlim_n\big(\mathrm{Pic}(\mathcal{O}_{F_n,\Sigma})\{p\}\big),$$

see ([Kat06], section 2.5). Now, since the primes above p are finitely decomposed in F_∞, we also see that the epimorphism (see (A.5.2) again)

$$\varprojlim_n\big(Cl(F_n)\{p\}\big)\twoheadrightarrow\varprojlim_n\big(\mathrm{Pic}(\mathcal{O}_{F_n}[1/p])\{p\}\big)$$

has a kernel that is finitely generated as a $\mathbb{Z}_p$-module. It follows that the composite map

$$\varprojlim_n\big(Cl(F_n)\{p\}\big)\twoheadrightarrow\varprojlim_n\big(\mathrm{Pic}(\mathcal{O}_{F_n,\Sigma})\{p\}\big) \tag{A.3.26}$$

has a kernel which is a finitely generated $\mathbb{Z}_p$-module.

A.4 The sequence of Poitou-Tate

Fix a prime $p \in \mathbb{Z}$, $p \neq 2$. Recall that in our global setting we have considered a tower of finite Galois extensions of number fields $F \subseteq F_n \subseteq F_{n+1} \cdots \subseteq F_\infty = \cup_n F_n$ such that $F(\mu_{p^\infty}) \subset F_\infty$. Assume that only finitely many primes ramify in F_∞/F and fix a finite set of places Σ of F containing the places above the fixed prime p, the infinite places of F and those that ramify in F_∞/F. We write F_Σ for the maximal extension unramified outside the primes of Σ and $G_\Sigma(F)$ for $\mathrm{Gal}(F_\Sigma/F)$ or simply G_Σ when F is clear from the context. Note that by assumption $F_\infty \subset F_\Sigma$. We also write $G_{n,\Sigma}$ for $G_{\Sigma_n}(F_n) = \mathrm{Gal}(F_{n,\Sigma_n}/F_n)$, where Σ_n is the set of places of F_n above those in Σ. Recall that we write $\mathcal{G}$ for $\mathrm{Gal}(F_\infty/F)$.

In the local setting we have considered $\mathrm{Gal}(K'(\mu_{p^\infty})/\mathbb{Q}_p)$, where $K'(\mu_{p^\infty})/\mathbb{Q}_p$ is a Galois extension that is obtained by adjoining all p-power roots of unity $\mu_{p^\infty} \subset \overline{\mathbb{Q}}_p$ to an infinite unramified extension K' of $\mathbb{Q}_p$. The prime example we have in mind is $\mathcal{G}_\nu = \mathrm{Gal}(F_{\infty,\nu}/\mathbb{Q}_p)$ where ν is a prime of F_∞ above p for $F_\infty = \mathbb{Q}(E[p^\infty])$, $E/\mathbb{Q}$ being an elliptic curve with complex multiplication by $\mathcal{O}_K$, K quadratic imaginary, and good, ordinary reduction at p. If E is only defined over K and p splits in K, $\mathcal{O}_K p = \mathfrak{p}\bar{\mathfrak{p}}$, then $K_\mathfrak{p} = \mathbb{Q}_p = K_{\bar{\mathfrak{p}}}$ and we are also in the setting just described.

We have encountered global and local cohomology groups in previous sections. To be precise, we examined

$$\mathbb{H}^i_\Sigma = \varprojlim_n \mathrm{H}^i_{\text{ét}}(\mathcal{O}_{F_n}\Big[\frac{1}{\Sigma_f}\Big], \mathbb{Z}_p(1)) = \varprojlim_n \mathrm{H}^i(G_{n,\Sigma}, \mathbb{Z}_p(1)),$$

$i = 1, 2$, in chapter 2.2 and

$$\mathbb{H}^i_{\text{loc}} = \mathrm{H}^i(\mathbb{Q}_p, \mathbb{T}_{un}) = \mathrm{H}^i(\mathbb{Q}_p, \Lambda(G)^\#(1)) = \varprojlim_{\mathbb{Q}_p \subseteq L \subset K_\infty} \mathrm{H}^i(L, \mathbb{Z}_p(1)),$$

$i = 1, 2$ where the limit is taken over all finite subextensions of $\mathbb{Q}_p$ in K_∞ in chapter 3. In this chapter we study the sequence of Poitou-Tate that relates the above global and local cohomology groups. We follow [NSW08] in our exposition. A modified version of the Poitou-Tate sequence will allow us to integrate a Selmer group, see definition 4.1.1, as one of its terms, which we will show in the next chapter.

A.4.1 Definition

We now quote the nine-term exact sequence of Poitou-Tate from ([NSW08], (8.6.10)) for number fields F and finite sets of primes Σ, $\Sigma_\infty \subset \Sigma$. For a finite $G_\Sigma(F)$-module B we write

$$T' = \mathrm{Hom}(B, \mathcal{O}_\Sigma^\times)$$

for the dual $G_\Sigma(F)$-module, where $\mathcal{O}_\Sigma^\times$ is the group of Σ-units of F_Σ and $\mathcal{O}_\Sigma = \bigcup_{F' \subset F_\Sigma} \mathcal{O}_{F',\Sigma}$, where the union is taken over all finite subextensions F' of F_Σ/F.

We adopt the convention of [NSW08] that for an archimedean prime $\nu \in \Sigma_\infty$ of F and a Galois-module B as in the following theorem, we write $H^0(F_\nu, B)$ for the modified cohomology group $\hat{H}^0(F_\nu, B) := B^{G_{F_\nu}} / N_{G_{F_\nu}} B$, where $N_{G_{F_\nu}} = \sum_{g \in G_{F_\nu}} g$ is the norm element in $\mathbb{Z}[G_{F_\nu}]$.

Theorem A.4.1 (Poitou-Tate). *Let Σ be a finite set of primes of a number field F containing all infinite primes. Let B be a finite $G_\Sigma(F)$-module the order of which is a unit in $\mathcal{O}_{F,\Sigma}$. Then, there is a long exact sequence of topological groups*

$$\begin{array}{l} 0 \longrightarrow H^0(G_\Sigma, B) \xrightarrow{\lambda^0} \bigoplus_{\nu\in\Sigma} H^0(F_\nu, B) \longrightarrow H^2(G_\Sigma, B')^\vee \\ \longrightarrow H^1(G_\Sigma, B) \xrightarrow{\lambda^1} \bigoplus_{\nu\in\Sigma} H^1(F_\nu, B) \longrightarrow H^1(G_\Sigma, B')^\vee \\ \longrightarrow H^2(G_\Sigma, B) \xrightarrow{\lambda^2} \bigoplus_{\nu\in\Sigma} H^2(F_\nu, B) \longrightarrow H^0(G_\Sigma, B')^\vee \longrightarrow 0, \end{array}$$

where we write $(-)^\vee$ for $\mathrm{Hom}_{cts}(-, \mathbb{R}/\mathbb{Z})$, which, for finite B of p-power order coincides with our usual $(-)^\vee$, compare remark A.4.3 (i). The maps λ^i, $i = 0, 1, 2$, are called localization maps.

For the definitions of the various maps appearing in the sequence, compare the proof of lemma A.4.5, where they are reviewed. We will refer to the above sequence as $PT(F, \Sigma, B)$.

Remark A.4.2. Let B be as in the theorem. Note that for a complex archimedean place $\nu \in \Sigma_\mathbb{C} \subset \Sigma_\infty$, the groups $H^0(F_\nu, B) = \hat{H}^0(F_\nu, B)$, $H^1(F_\nu, B)$ and $H^2(F_\nu, B)$ are trivial. In particular, if F has no real archimedean places (e.g., when F contains a non-trivial cyclotomic field), then

$$\prod_{\nu\in\Sigma} H^i(F_\nu, B) = \prod_{\nu\in\Sigma_f} H^i(F_\nu, B), \qquad i = 0, 1, 2,$$

where Σ_f denotes the set of non-archimedean places in Σ. By a non-trivial cyclotomic field we mean a field of the form $\mathbb{Q}(\zeta_{q^n})$ for a primitive q^n-th root of unity ζ_{q^n} such that $q \in \mathbb{Z}$ is a prime and either $q \neq 2$ or $n \geq 2$. Moreover, note that if $\nu \in \Sigma_\mathbb{R}$ is a real archimedean place and 2 does not divide the order of B, then we also have

$$\hat{H}^0(F_\nu, B) := B^{G_\mathbb{R}} / N_{G_\mathbb{R}} B = 0.$$

If 2 does not divide the order $\#B$ of B, then it does not divide the order of B' (since the latter divides $(\#B)^2$) and the local duality theorem for the group $G(\mathbb{C}/\mathbb{R})$, see ([NSW08], (7.2.17) Theorem), shows that for B, $2 \nmid \#B$, and a real archimedean place $\nu \in \Sigma_\mathbb{R}$ we also have $H^2(F_\nu, B) = 0$.

A.4.2 Functoriality

In this subsection, functoriality properties of the Poitou-Tate sequence (with respect to the ground field F and the module B) are reviewed. Most of them are well-known, but for lack of a reference some details are provided concerning the functoriality with respect to F. Throughout this section we always assume Σ to be a finite set of places of F containing Σ_∞, the set of archimedean places of F, and Σ_p, the set of finite primes above a fixed prime p. We will also assume that F is totally imaginary if $p = 2$, compare remark A.4.2.

Let us consider a finitely generated free $\mathbb{Z}_p$-module T with a continuous action of G_F that is unramified outside the finite set of primes Σ of F. Note that the units $\mathcal{O}_\Sigma^\times$ contain the p-power roots of unity, $\bigcup_n \mu_{p^n} \subset \mathcal{O}_\Sigma^\times$. Moreover, we have

$$(T/p^nT)' \overset{\text{def}}{=} \operatorname{Hom}(T/p^nT, \mathcal{O}_{F,\Sigma}^\times) \cong \operatorname{Hom}(T, \mu_{p^n}) \cong \operatorname{Hom}(T, \mathbb{Z}_p(1)) \otimes \Big(\big(\frac{1}{p^n}\mathbb{Z}_p\big)/\mathbb{Z}_p \Big),$$

where the last equation holds since T is projective as a $\mathbb{Z}_p$-module. Passing to the direct limit we get

$$\varinjlim_n \big((T/p^nT)' \big) \cong T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p, \tag{A.4.1}$$

where we recall that T^* is defined to be the dual $\mathbb{Z}_p$-representation $\operatorname{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p)$. It is time we made a remark about Pontryagin duals.

Remark A.4.3. (i) For a general Hausdorff, abelian locally compact topological group A, one defines $A^\vee = \operatorname{Hom}_{cts}(A, \mathbb{R}/\mathbb{Z})$, where $\mathbb{R}/\mathbb{Z}$ is equipped with the quotient topology induced by the usual topology on $\mathbb{R}$. If D is a discrete torsion group, then the embedding $\mathbb{Q}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z}$ induces an isomorphism $\operatorname{Hom}(D, \mathbb{Q}/\mathbb{Z}) \cong \operatorname{Hom}_{cts}(D, \mathbb{R}/\mathbb{Z})$. Moreover, if D is a discrete torsion group and coincides with its p-primary subgroup $D = D\{p\}$, then $\operatorname{Hom}(D, \mathbb{Q}/\mathbb{Z}) \cong \operatorname{Hom}_{cts}(D, \mathbb{Q}_p/\mathbb{Z}_p)$, since the p-primary parts of $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Q}_p/\mathbb{Z}_p$ coincide, $(\mathbb{Q}/\mathbb{Z})\{p\} = \bigcup_n (\frac{1}{p^n}\mathbb{Z})/\mathbb{Z} \cong \bigcup_m (\frac{1}{p^m}\mathbb{Z}_p)/\mathbb{Z}_p = (\mathbb{Q}_p/\mathbb{Z}_p)\{p\}$. Note that if T is finite discrete of p-power order, then T' and $H^i(G_\Sigma, T')$, $i = 0, 1, 2$, are too, compare proposition A.3.1.

(ii) Note that for finitely many discrete abelian groups $D_1, \dots, D_k$, the product topology on $\prod_{i=1}^k D_i$ coincides with the discrete topology on $\prod_{i=1}^k D_i$. Hence, we have a homeomorphism $(\prod_{i=1}^k D_i)^\vee \cong \prod_{i=1}^k (D_i^\vee)$. For finitely many Hausdorff compact abelian groups $T_1, \dots, T_k$ we therefore get $(\prod_{i=1}^k (T_i^\vee))^\vee \cong \prod_{i=1}^k ((T_i^\vee)^\vee) \cong \prod_{i=1}^k T_i$, i.e., we also have $(\prod_{i=1}^k T_i)^\vee \cong \prod_{i=1}^k (T_i^\vee)$.

(iii) Let $(D_i)_{i\in I}$ be a direct system of discrete abelian groups, then $\varinjlim_i D_i$ equipped with the final topology with respect to the canonical maps $D_j \to \varinjlim_i D_i$ is certainly also discrete. Hence, we get a homeomorphism $(\varinjlim_i D_i)^\vee \cong \varprojlim_i (D_i^\vee)$.

(iv) Let $(T_i)_{i\in I}$ be a projective system of Hausdorff compact abelian groups and consider the induced direct system of discrete groups $(T_i^\vee)_{i\in I}$. Using (iii) we get $(\varinjlim_i (T_i^\vee))^\vee \cong \varprojlim_i ((T_i^\vee)^\vee) \cong \varprojlim_i T_i$ and therefore, $\varinjlim_i (T_i^\vee) \cong (\varprojlim_i T_i)^\vee$.

Let us consider the Poitou-Tate sequences $PT(F, \Sigma, T/p^nT)$ for the finite modules T/p^nT, $n \geq 1$, where T is a finitely generated free $\mathbb{Z}_p$-module as above. Note that since we assumed Σ to be finite, all groups in the sequences $PT(F, \Sigma, T/p^nT)$, $n \geq 1$, are compact, in fact, they are even finite, see ([NSW08], (8.6.10)) and propositions A.3.1 and A.3.2. We state without proof

Lemma A.4.4. *The Poitou-Tate sequence is functorial in the second variable, i.e., if* $f : A \to B$ *is a morphism of finite* $G_\Sigma(F)$*-modules, the orders of which are both units in* $\mathcal{O}_{F,\Sigma}$*, then* f *induces a map* $f_* : PT(F,\Sigma,A) \longrightarrow PT(F,\Sigma,B)$.

The lemma allows us to pass to the projective limit of the sequences $PT(F,\Sigma,T/p^nT)$, $n \geq 1$, where the transition maps are induced by the canonical maps $T/p^{n+1}T \to T/p^nT$. Since Σ is finite, the groups appearing in $PT(F,\Sigma,T/p^nT)$ are compact and in view of (A.4.1) and proposition A.3.4, we then get an exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(G_\Sigma,T) \longrightarrow \textstyle\bigoplus_{\nu\in\Sigma_f} H^0(F_\nu,T) \longrightarrow H^2(G_\Sigma,T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee \\ \longrightarrow H^1(G_\Sigma,T) \longrightarrow \textstyle\bigoplus_{\nu\in\Sigma} H^1(F_\nu,T) \longrightarrow H^1(G_\Sigma,T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee \\ \longrightarrow H^2(G_\Sigma,T) \longrightarrow \textstyle\bigoplus_{\nu\in\Sigma_f} H^2(F_\nu,T) \longrightarrow H^0(G_\Sigma,T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee \longrightarrow 0, \end{aligned} \tag{A.4.2}$$

where, see remark A.4.2, the groups $H^i(F_\nu,T)$, $i = 0,1,2$, vanish for complex archimedean places $\nu \in \Sigma_\mathbb{C}$ and $H^0(F_\nu,T)$, $H^2(F_\nu,T)$ also vanishes for $\nu \in \Sigma_\mathbb{R}$ (since if there are real places, then $p \neq 2$ by assumption). We will denote the above exact sequence by $PT(F,\Sigma,T)$. We remark that there is a dual version of this sequence, which is given by

$$\begin{aligned} 0 \longrightarrow H^0(G_\Sigma,T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \textstyle\bigoplus_{\nu\in\Sigma_f} H^0(F_\nu,T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^2(G_\Sigma,T)^\vee \\ \longrightarrow H^1(G_\Sigma,T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \textstyle\bigoplus_{\nu\in\Sigma} H^1(F_\nu,T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(G_\Sigma,T)^\vee \\ \longrightarrow H^2(G_\Sigma,T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \textstyle\bigoplus_{\nu\in\Sigma_f} H^2(F_\nu,T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^0(G_\Sigma,T)^\vee \longrightarrow 0. \end{aligned} \tag{A.4.3}$$

Now, in our global setting, assume that $\mu_{p^\infty} \subset F_\infty$, which, e.g., holds in the case $F_n = F(E[p^n])$ by the Weil pairing. More generally, it is also sufficient for our purposes in this section to assume that F_n, for some $n \geq 1$, has only complex archimedean places, which is then true for all F_m, $m \geq n$. Let T be a finitely generated free $\mathbb{Z}_p$-module with a continuous action of G_F that is unramified outside Σ again, and recall that we write $T^* = \mathrm{Hom}_{\mathbb{Z}_p}(T,\mathbb{Z}_p)$. We then have for $i \geq 0$

$$\begin{aligned} \varinjlim_n \varinjlim_m H^i(G_{n,\Sigma},(T/p^m)') &\cong H^i(G_{\infty,\Sigma},T^*(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \\ &\cong H^i(G_{\infty,\Sigma},T^\vee(1)). \end{aligned}$$

For each number field F_n, $n \geq 1$, we get a long exact sequence as in (A.4.2). We want to show that these sequences form a projective system (with respect to corestriction maps and duals of restriction maps) of sequences in the following lemma. It has been remarked in ([Mil86b], Remark 4.19) that the dual statement is true, i.e., that with respect to restriction maps and duals of corestriction maps, the Poitou-Tate sequences form a direct system.

By a map $(\varphi_n)_n$ between sequences $((M_n)_n, d_n)$, where $d_n : M_n \to M_{n+1}$, and $((N_n)_n, d'_n)$, where $d'_n : N_n \to N_{n+1}$, we mean, of course, a map such that $\varphi_{n+1} \circ d_n = d'_n \circ \varphi_n$.

Lemma A.4.5. *Given F and Σ as above, let L/F be a finite Galois subextension of F_Σ/F and write Σ_L for the primes of L above those in Σ. Write $G_\Sigma(F) = G(F_\Sigma/F)$ and $G_\Sigma(L) = G(F_\Sigma/L) = G(L_{\Sigma_L}/L)$. Then, there is a map of exact sequences from the Poitou-Tate sequence (A.4.2) for L and Σ_L to the Poitou-Tate sequence (A.4.2) for F and Σ. The map is given by the maps*

(i) $\operatorname{cor}^{G_\Sigma(L)}_{G_\Sigma(F)} : H^m(G_\Sigma(L), T) \longrightarrow H^m(G_\Sigma(F), T), \quad m = 0, 1, 2,$

(ii) for each $\nu \in \Sigma$ and a fixed prime $\omega_0 \in \Sigma_L$ of L above ν, a map

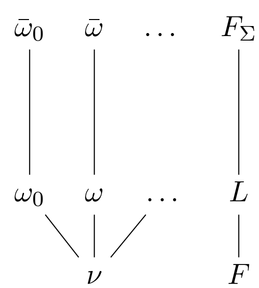
$$\sum_{\omega|\nu} \operatorname{cor}^{G_{L_{\omega_0}}}_{G_{F_\nu}} \circ (\sigma_\omega)_* : \bigoplus_{\omega|\nu} H^m(L_\omega, T) \longrightarrow H^m(F_\nu, T), \quad m = 0, 1, 2,$$

where $(\sigma_\omega)_*$ is the conjugation map $H^m(L_\omega, T) \to H^m(L_{\omega_0}, T)$ induced by certain Galois automorphisms σ_ω (fixing F) such that $\sigma_\omega G_{L_\omega} \sigma_\omega^{-1} = G_{L_{\omega_0}}$,

(iii) $\left(\operatorname{res}^{G_\Sigma(F)}_{G_\Sigma(L)}\right)^\vee : H^m(G_\Sigma(L), T^\vee(1))^\vee \longrightarrow H^m(G_\Sigma(F), T^\vee(1))^\vee, \quad m = 0, 1, 2.$

Proof. We divide the proof into three parts.

1. Part: We begin with the compatibility of the maps from the first to the second non-trivial column of (A.4.2). Let us fix a prime $\nu \in \Sigma$ of F, a prime $\bar\omega_0$ of F_Σ above ν and let us write $F_{\Sigma,\bar\omega_0}$ for the union of the completions at $\bar\omega_0$ of the finite subextensions of F_Σ/F. Let us write ω_0 for the prime of L below $\bar\omega_0$ and fix a prime $\overline{\omega}$ of F_Σ above each other prime ω of L above ν, so that we have



(A.4.4)

Moreover, for each ω above ν fix σ_ω in $G_\Sigma(F)$ so that $\bar\omega_0 \circ \sigma_\omega = \bar\omega$. For any ω above ν we write $G_\Sigma(F)_{\bar\omega} \cong G(F_{\Sigma,\bar\omega}/F_\nu)$ and $G_\Sigma(L)_{\bar\omega} \cong G(F_{\Sigma,\bar\omega}/L_\omega)$ for the decomposition groups of $\bar\omega$ in $G_\Sigma(F)$ and $G_\Sigma(L)$, respectively; when we write ω to mean any prime of L above ν, then, in particular,

ω could be ω_0. We have $\sigma_\omega(G_\Sigma(L)_{\bar\omega})\sigma_\omega^{-1} = G_\Sigma(L)_{\bar\omega_0}$ (note that $G_\Sigma(L)$ is normal in $G_\Sigma(F)$) and write

$$(\sigma_\omega)_* : H^m(G_\Sigma(L)_{\bar\omega}, T) \to H^m(G_\Sigma(L)_{\bar\omega_0}, T)$$

for the conjugation isomorphism, see ([NSW08], chapter I, §5) for a definition and note that $\sigma_\omega T = T$. Moreover, we set $G_{L_\omega} = G(\overline{F}_{\Sigma,\bar\omega}/L_\omega)$ for arbitrary $\omega \mid \nu$, and $G_{F_\nu} = G(\overline{F}_{\Sigma,\bar\omega_0}/F_\nu)$, where $\overline{F}_{\Sigma,\bar\omega}$ denote fixed algebraic closures. Then, we have surjections $G_{L_\omega} \twoheadrightarrow G_\Sigma(L)_{\bar\omega}$ and $G_{F_\nu} \twoheadrightarrow G_\Sigma(F)_{\bar\omega_0}$. Note that the induced embeddings $\sigma_\omega : F_{\Sigma,\bar\omega} \hookrightarrow \overline{F}_{\Sigma,\bar\omega_0}$ extend to isomorphisms $\sigma_\omega : \overline{F}_{\Sigma,\bar\omega} \cong \overline{F}_{\Sigma,\bar\omega_0}$ which we also denote by σ_ω. As before, we have conjugation isomorphisms $(\sigma_\omega)_* : H^m(L_\omega, T) \cong H^m(L_{\omega_0}, T)$. Then, consider the following diagram, where, by proposition A.3.1, A.3.2 and A.3.4, we may assume that T is of finite p-power order and therefore discrete,

$$\begin{array}{ccccc}
H^m(G_\Sigma(L),T) & \xrightarrow{\oplus_{\omega|\nu} \mathrm{res}^{G_\Sigma(L)}_{G_\Sigma(L)_{\bar\omega}}} & \bigoplus_{\omega|\nu} H^m(G_\Sigma(L)_{\bar\omega},T) & \xrightarrow{\oplus_{\omega|\nu} \inf^{G_\Sigma(L)_{\bar\omega}}_{G_{L_\omega}}} & \bigoplus_{\omega|\nu} H^m(L_\omega,T) \\
\downarrow \mathrm{cor}^{G_\Sigma(L)}_{G_\Sigma(F)} & & \downarrow \sum_{\omega|\nu} \mathrm{cor}^{G_\Sigma(L)_{\bar\omega_0}}_{G_\Sigma(F)_{\bar\omega_0}} \circ (\sigma_\omega)_* & & \downarrow \sum_{\omega|\nu} \mathrm{cor}^{G_{L_{\omega_0}}}_{G_{F_\nu}} \circ (\sigma_\omega)_* \\
H^m(G_\Sigma(F),T) & \xrightarrow[\mathrm{res}^{G_\Sigma(F)}_{G_\Sigma(F)_{\bar\omega_0}}]{} & H^m(G_\Sigma(F)_{\bar\omega_0},T) & \xrightarrow[\inf^{G_\Sigma(F)_{\bar\omega_0}}_{G_{F_\nu}}]{} & H^m(F_\nu,T)
\end{array} \tag{A.4.5}$$

the left diagram commutes by the double-coset formula for res and cor, see ([NSW08], (1.5.6) Proposition), and the right diagram commutes since conjugation commutes with inflation, see (loc. cit., (1.5.4) Proposition) and by (loc. cit., (1.5.5) proposition), which states that $\inf^{G/V}_G \circ \mathrm{cor}^{U/V}_{G/V} = \mathrm{cor}^U_G \circ \inf^{U/V}_U$ for V closed and normal and U open in a profinite group G. In our case $G = G_{F_\nu}$, $U = G_{L_{\omega_0}}$ and $V = G_{F_{\Sigma,\overline{\omega}_0}}$; V is equal to the kernel of $G_{L_{\omega_0}} \twoheadrightarrow G_\Sigma(L)_{\bar\omega_0}$.

<u>2. Part:</u> Next, using the same notation as before, we consider the maps from the second to the third non-trivial column of (A.4.2) and show that they are compatible. This is equivalent to showing that for any $\nu \in \Sigma$, $m = 0,1,2$, the dual diagram

$$\begin{array}{ccc}
\bigoplus_{\omega|\nu} \left(H^m(L_\omega,T)^\vee\right) & \longleftarrow & H^{2-m}(G_\Sigma(L),T^\vee(1)) \\
\uparrow \oplus_{\omega|\nu}\left(\left(\mathrm{cor}^{G_{L_{\omega_0}}}_{G_{F_\nu}} \circ (\sigma_\omega)_*\right)^\vee\right) & & \uparrow \mathrm{res}^{G_\Sigma(F)}_{G_\Sigma(L)} \\
H^m(F_\nu,T)^\vee & \longleftarrow & H^{2-m}(G_\Sigma(F),T^\vee(1))
\end{array} \tag{A.4.6}$$

commutes, compare remark A.4.3 (ii) for the fact that $(-)^\vee$ commutes with finite products for both discrete and compact modules. The horizontal arrows in (A.4.6) are defined via local Tate cohomology and the localization maps λ^{2-m} for $T^\vee(1)$, which we explain now. Assume we have already shown that the following diagram commutes

$$\begin{array}{ccc}
\bigoplus_{\omega|\nu}\left(H^m(L_\omega,T)^\vee\right) & \xleftarrow{\cong} & \bigoplus_{\omega|\nu} H^{2-m}(L_\omega,T^\vee(1)) \\
\Big\uparrow {\scriptstyle \bigoplus_{\omega|\nu}\left(\left(\mathrm{cor}^{G_{L_{\omega_0}}}_{G_{F_\nu}}\circ(\sigma_\omega)_*\right)^\vee\right)} & & \Big\uparrow {\scriptstyle \bigoplus_{\omega|\nu}(\sigma_\omega^{-1})_*\circ \mathrm{res}^{G_{F_\nu}}_{G_{L_{\omega_0}}}} \\
H^m(F_\nu,T)^\vee & \xleftarrow{\cong} & H^{2-m}(F_\nu,T^\vee(1)),
\end{array} \tag{A.4.7}$$

where the horizontal maps are induced by local Tate duality. Then, showing the commutativity of (A.4.6) is equivalent to showing that

$$\begin{array}{ccc}
\bigoplus_{\omega|\nu} H^{2-m}(L_\omega,T^\vee(1)) & \xleftarrow{\lambda^{2-m}} & H^{2-m}(G_\Sigma(L),T^\vee(1)) \\
\Big\uparrow {\scriptstyle \bigoplus_{\omega|\nu}(\sigma_\omega^{-1})_*\circ \mathrm{res}^{G_{F_\nu}}_{G_{L_{\omega_0}}}} & & \Big\uparrow {\scriptstyle \mathrm{res}^{G_\Sigma(F)}_{G_\Sigma(L)}} \\
H^{2-m}(F_\nu,T^\vee(1)) & \xleftarrow{\lambda^{2-m}} & H^{2-m}(G_\Sigma(F),T^\vee(1))
\end{array} \tag{A.4.8}$$

commutes, where, by abuse of notation, we use the same symbol λ^{2-m} for both of the horizontal localization maps, which, as before, are given by the restrictions to the decomposition groups in the extension F_Σ/F and F_Σ/L composed with the inflation maps to the absolute Galois groups of the local fields. In fact, (A.4.6) is, by definition, the diagram that arises by connecting (A.4.7) with (A.4.8). As in the first part of the proof, we divide the diagram (A.4.8) into two diagrams, one corresponding to the restriction maps and one to the inflation maps. The first commutes since conjugation commutes with restriction. The second diagram commutes since conjugation commutes with inflation and by ([NSW08], (1.5.5) Proposition) stating that for closed subgroups $V \subset U \subset G$ we have $\mathrm{inf}_U^{U/V}\circ \mathrm{res}^{G/V}_{U/V} = \mathrm{res}^G_U \circ \mathrm{inf}^{G/V}_G$. Use this result for $V = G_{F_{\Sigma,\bar\omega_0}}$, $U = G_{L_{\omega_0}}$ and $G = G_{F_\nu}$.

Now, it remains to prove that the diagram from (A.4.7) commutes. By the compatibility of conjugation with res and cor, this follows from the next diagram, where, for ease of notation, we write M/K for an arbitrary finite extension of non-archimedean local fields. Whenever we have a map $f : A \to B$, then $(f)^*$ denotes the induced map $\mathrm{Hom}(B,C) \to \mathrm{Hom}(A,C)$, $g \mapsto g\circ f$, while $(f)_*$ means $\mathrm{Hom}(D,A) \to \mathrm{Hom}(D,B)$, $h \mapsto f\circ h$. Let us write $H^2(M) = H^2(M,\mathbb{Q}_p/\mathbb{Z}_p(1))$ and

$H^2(K) = H^2(K, \mathbb{Q}_p/\mathbb{Z}_p(1))$ and consider the diagram

$$\begin{array}{ccccc}
 & & \mathrm{Hom}\big(H^m(M,T), H^2(M)\big) & & \\
 & \swarrow{\scriptstyle (\mathrm{inv}_M)_*} & \downarrow{\scriptstyle (\mathrm{cor}^{G_M}_{G_K})_*} & \nwarrow{\scriptstyle (x \longmapsto -\cup x)} & \\
\mathrm{Hom}\big(H^m(M,T), \mathbb{Q}_p/\mathbb{Z}_p\big) & \xleftarrow{(\mathrm{inv}_K)_*} & \mathrm{Hom}\big(H^m(M,T), H^2(K)\big) & & H^{2-m}(M, T^\vee(1)) \\
\uparrow{\scriptstyle (\mathrm{cor}^{G_M}_{G_K})^*} & & \uparrow{\scriptstyle (\mathrm{cor}^{G_M}_{G_K})^*} & & \uparrow{\scriptstyle \mathrm{res}^{G_K}_{G_M}} \\
\mathrm{Hom}\big(H^m(K,T), \mathbb{Q}_p/\mathbb{Z}_p\big) & \xleftarrow{(\mathrm{inv}_K)_*} & \mathrm{Hom}\big(H^m(K,T), H^2(K)\big) & \xleftarrow{(y \mapsto -\cup y)} & H^{2-m}(K, T^\vee(1))
\end{array} \tag{A.4.9}$$

where we write $H^m(K,T) \times H^{2-m}(K,T^\vee(1)) \xrightarrow{\cup} H^2(K)$ for the cup product and $\mathrm{inv}_K : H^2(K) \cong \mathbb{Q}_p/\mathbb{Z}_p$ for the local invariant map (and likewise for M), so that the composite of the two lowest (resp. diagonal) morphisms of the diagram gives the local Tate duality isomorphism for K (resp. M). The right part of the diagram commutes by a general result about the compatibility of restriction, corestriction and the cup product, see ([NSW08], (1.5.3) Proposition (iv)). The lower diagram on the left commutes by definition and the upper diagram on the left is just the property ([NSW08], (7.1.4) Corollary) satisfied by local invariant maps for extensions M/K.

<u>3. Part:</u> For the maps from the third to the first column one has to show the compatibility of global Poitou-Tate duality. We skip the proof of this part. □

In view of remark A.4.2 and our assumption that for some n, $n \geq 1$, F_n has only complex archimedean places, passing to the projective limit (with respect to the maps as in lemma A.4.5) yields a long exact sequence

$$\begin{array}{l}
0 \longrightarrow \varprojlim_n H^0(G_{n,\Sigma}, T) \longrightarrow \varprojlim_n \bigoplus_{\nu \in \Sigma_{n,f}} H^0(F_{n,\nu}, T) \longrightarrow H^2(G_{\infty,\Sigma}, T^\vee(1))^\vee \\
\varprojlim_n H^1(G_{n,\Sigma}, T) \longrightarrow \varprojlim_n \bigoplus_{\nu \in \Sigma_{n,f}} H^1(F_{n,\nu}, T) \longrightarrow H^1(G_{\infty,\Sigma}, T^\vee(1))^\vee \\
\varprojlim_n H^2(G_{n,\Sigma}, T) \longrightarrow \varprojlim_n \bigoplus_{\nu \in \Sigma_{n,f}} H^2(F_{n,\nu}, T) \longrightarrow H^0(G_{\infty,\Sigma}, T^\vee(1))^\vee \longrightarrow 0
\end{array} \tag{A.4.10}$$

where $\Sigma_{n,f}$ denotes the set of finite places of F_n above Σ_f.

For a prime $\nu \in \Sigma_f$ we write $\overline{F}_\nu$ for an algebraic closure of the completion of F at ν and fix an embedding $\overline{F} \subset \overline{F}_\nu$. This embedding determines a prime $\bar{\nu}$ of F_∞ above ν and we denote by $\mathcal{G}_\nu$ the correpsonding decomposition group in $\mathcal{G} = G(F_\infty/F)$. We have seen in the proof of lemma

A.4.5 that local Tate duality turns corestriction maps into duals of restriction maps, see (A.4.7) and (A.4.9). Hence, we get for $i = 0, 1, 2$

$$\begin{aligned}
\varprojlim_{n,\mathrm{cor}} \bigoplus_{\nu\in\Sigma_{n,f}} H^i(F_{n,\nu}, T) &\cong \varprojlim_{n,\mathrm{res}^\vee} \Big(\bigoplus_{\nu\in\Sigma_{n,f}} H^{2-i}(F_{n,\nu}, T^\vee(1))^\vee \Big) \\
&\cong \Big(\varinjlim_{n,\mathrm{res}} \bigoplus_{\nu\in\Sigma_{n,f}} H^{2-i}(F_{n,\nu}, T^\vee(1)) \Big)^\vee \\
&\cong \Big(\bigoplus_{\nu\in\Sigma_f} \mathrm{Coind}_{\mathcal{G}}^{\mathcal{G}_\nu} H^{2-i}(F_{\infty,\bar\nu}, T^\vee(1)) \Big)^\vee \\
&\cong \bigoplus_{\nu\in\Sigma_f} \mathrm{c\text{-}Ind}_{\mathcal{G}}^{\mathcal{G}_\nu} \big(H^{2-i}(F_{\infty,\bar\nu}, T^\vee(1))^\vee \big), \qquad \text{(A.4.11)}
\end{aligned}$$

and we refer to remark A.4.3 for the properties of $(-)^\vee$ that we used. Above, when we write $F_{\infty,\bar\nu}$ for a prime $\nu \in \Sigma_f$ we mean the union of the completions $F_{n,\bar\nu}$ of F_n at the (restriction of the) prime $\bar\nu$ of F_∞ above ν induced by the embedding $\overline{F} \subset \overline{F}_\nu$. For $i = 0, 1, 2$, the last term from (A.4.11) above is isomorphic to

$$\begin{aligned}
\bigoplus_{\nu\in\Sigma_f} \mathrm{c\text{-}Ind}_{\mathcal{G}}^{\mathcal{G}_\nu} \big(H^{2-i}(F_{\infty,\bar\nu}, T^\vee(1))^\vee \big) &\cong \bigoplus_{\nu\in\Sigma_f} \mathrm{c\text{-}Ind}_{\mathcal{G}}^{\mathcal{G}_\nu} \Big(\big(\varinjlim_{n,\mathrm{res}} H^{2-i}(F_{n,\bar\nu}, T^\vee(1)) \big)^\vee \Big) \\
&\cong \bigoplus_{\nu\in\Sigma_f} \mathrm{c\text{-}Ind}_{\mathcal{G}}^{\mathcal{G}_\nu} \varprojlim_{n,\mathrm{res}^\vee} \big(H^{2-i}(F_{n,\bar\nu}, T^\vee(1))^\vee \big) \\
&\cong \bigoplus_{\nu\in\Sigma_f} \mathrm{c\text{-}Ind}_{\mathcal{G}}^{\mathcal{G}_\nu} \varprojlim_{n,\mathrm{cor}} H^i(F_{n,\bar\nu}, T). \qquad \text{(A.4.12)}
\end{aligned}$$

Remark A.4.6. Consider the case $T = \mathbb{Z}_p(1)$. Then,

(i) we canonically have $T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Q}_p/\mathbb{Z}_p$ with trivial $G_{\mathbb{Q}}$-action on the right. It follows, compare ([NSW08], Theorem (2.6.9)) that for all $n \geq 1$

$$H^2(G_{n,\Sigma}, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = H_2(G_{n,\Sigma}, \mathbb{Z}_p)^\vee.$$

Hence, if Leopoldt's conjecture is true for p and all F_n, i.e., if $H_2(G_{n,\Sigma}, \mathbb{Z}_p)$ vanishes, then the Poitou-Tate sequence as in (A.4.2) gives us a six term exact sequence consisting of the lower two lines. This will be the case when $F_n = K(E[p^n])$ for an elliptic curve with complex multiplication by $\mathcal{O}_K$, since F_n is then abelian over the quadratic imaginary number field K, compare ([NSW08], Theorem (10.3.16)).

Regardless of whether the Leopoldt conjecture holds for each F_n, the weak Leopoldt conjecture holds for F_∞ and $\mathbb{Q}_p/\mathbb{Z}_p$ whenever $F^{cyc} \subset F_\infty$. In fact, it holds for each cyclotomic extension F_n^{cyc}/F_n, $n \geq 1$, see ([NSW08], (10.3.25) Theorem) and compare also Iwasawa's article [Iwa73]. We may therefore conclude

$$H^2(G_{\infty,\Sigma}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \varinjlim_{n} H^2(G(F_\Sigma/F_n^{cyc}), \mathbb{Q}_p/\mathbb{Z}_p) = 0,$$

which shows that for $T = \mathbb{Z}_p(1)$ the sequence (A.4.10) always restricts to an exact sequence consisting of the lower two lines. We remark that the statement about the weak Leopoldt conjecture holds for more general modules T as long as F_∞/F contains the cyclotomic extension of F and the trivializing extension for $T^\vee(1)$, compare ([Ven00], remark 3.0.4). For more information on weak Leopoldt conjectures see ([PR00], appendix B) and [Sch85] for some results concerning elliptic curves.

(ii) we have $H^1(G_{\infty,\Sigma}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee = \mathrm{Hom}_{cts}(G_{\infty,\Sigma}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong G(F_\Sigma/F_\infty)^{ab}(p)$.

(iii) by (A.4.11) for $i = 2$ we have

$$\varprojlim_n \bigoplus_{\nu\in\Sigma_{n,f}} H^2(F_{n,\nu}, T) \cong \bigoplus_{\nu\in\Sigma_f} \text{c--Ind}_{\mathcal{G}}^{\mathcal{G}_\nu} \mathbb{Z}_p.$$

(iv) lastly, we also have

$$H^0(G_{\infty,\Sigma}, T^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee = \mathbb{Z}_p.$$

(v) assuming that $F^{cyc} \subset F_\infty$, in view of (A.4.12), the Poitou-Tate sequences (A.4.10) reduces to

$$\begin{array}{l} 0 \to \varprojlim_n H^1(G_{n,\Sigma}, \mathbb{Z}_p(1)) \xrightarrow{\lambda^1} \bigoplus_{\nu\in\Sigma_f} \text{c--Ind}_{\mathcal{G}}^{\mathcal{G}_\nu} \varprojlim_n H^1(F_{n,\bar\nu}, \mathbb{Z}_p(1)) \to H^1(G_{\infty,\Sigma}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \\ \to \varprojlim_n H^2(G_{n,\Sigma}, \mathbb{Z}_p(1)) \xrightarrow{\lambda^2} \bigoplus_{\nu\in\Sigma_f} \text{c--Ind}_{\mathcal{G}}^{\mathcal{G}_\nu} \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow 0, \end{array} \tag{A.4.13}$$

where we recognise $\mathbb{H}^i_\Sigma = \varprojlim_n H^i(G_{n,\Sigma}, \mathbb{Z}_p(1))$, $i = 1, 2$, from the global theory and for $\nu \in \Sigma_p$, $\mathbb{H}^1_{\mathrm{loc}} = \varprojlim_n H^1(F_{n,\bar\nu}, \mathbb{Z}_p(1))$ and $\mathbb{H}^2_{\mathrm{loc}} = \mathbb{Z}_p$ from the local theory.

A.5 Σ-units and Σ-ideal class groups

Let F be a number field and $\Sigma' \subset \Sigma$ be finite sets of places containing the infinite places Σ_∞ of F. We write Σ'_f and Σ_f for the finite primes in Σ' and Σ, respectively. Denote by J_F the ideal group of F, the free abelian group generated by all non-zero prime ideals of F (i.e., by the non-archimedean primes). Then, by the Snake Lemma we have the following diagram

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & \mathcal{O}^{\times}_{F,\Sigma'} & \longrightarrow & \mathcal{O}^{\times}_{F,\Sigma} & \dashrightarrow & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & \longrightarrow & F^{\times} & = & F^{\times} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bigoplus_{\nu\in\Sigma_f\smallsetminus\Sigma'_f}\mathbb{Z}\nu & \longrightarrow & J_F/<\nu\in\Sigma'_f> & \longrightarrow & J_F/<\nu\in\Sigma_f> & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & \dashrightarrow & \bigoplus_{\nu\in\Sigma_f\smallsetminus\Sigma'_f}\mathbb{Z}\nu & \longrightarrow & Cl_{\Sigma'}(F) & \longrightarrow & Cl_{\Sigma}(F) & \longrightarrow & 0
\end{array} \tag{A.5.1}$$

In particular, tensoring with $\mathbb{Z}_p$ yields an exact sequence

$$0 \to \mathcal{O}^{\times}_{F,\Sigma'} \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathcal{O}^{\times}_{F,\Sigma} \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \bigoplus_{\nu\in\Sigma_f\smallsetminus\Sigma'_f} \mathbb{Z}_p\nu \to Cl_{\Sigma'}(F)\{p\} \to Cl_{\Sigma}(F)\{p\} \to 0. \tag{A.5.2}$$

A.6 Elliptic curves with complex multiplication

In this section we gather some known facts about elliptic curves defined over a quadratic imaginary number field K with complex multiplication by an order in K. We write $\bar{K}$ for an algebraic closure of K and G_K for $\mathrm{Gal}(\bar{K}/K)$. If one is interested in curves already defined over $\mathbb{Q}$, one can find a complete list of the finitely many $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over $\mathbb{Q}$ with complex multiplication in ([Sil99], Appendix A, §3).

As a special case of ([Sil99], Chapter II, Theorem 4.3) we have the following proposition.

Proposition A.6.1. *Let E/K be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then, K coincides with its Hilbert class field.*

In the above proposition by Hilbert class field we mean the big Hilbert class field, i.e., the ray class field of K modulo the unit ideal (1), which coincides with the maximal abelian extension of K that is unramified at all primes. The proof, in a more general situation, shows that the j-invariant $j(E)$ of E generates the Hilbert class field. In our situation, since E is defined over K, $j(E)$ also belongs to K, which implies what we claimed.

We also note that for an elliptic curves E/K with complex multiplication, as Shimura remarks in ([Shi71], (5.1.3)), every endomorphism in $\mathrm{End}_{\bar{K}}(E)$ is rational over K, i.e., already defined over K,

$$\mathrm{End}_{\bar{K}}(E) = \mathrm{End}_K(E).$$

If $\mathrm{End}_K(E)$ is equal to the maximal order $\mathcal{O}_K$ and $p \in \mathbb{Z}$ is a prime that splits in $\mathcal{O}_K$ into two primes generated by π and $\bar{\pi}$, then we see that the π-adic Tate module $T_\pi E = \varprojlim_n E[\pi^n]$ carries an action of G_K since multiplication by π, by the above remark, is defined over K.

Let us recall a reduction criterion in terms of decomposition behaviour due to Deuring for primes of good reduction.

Proposition A.6.2. *Let E/K be an elliptic curve and let $\mathfrak{p}$ be a prime of K where E has good reduction. Write p in $\mathbb{Z}$ for the prime below $\mathfrak{p}$. Then, the reduction of E modulo $\mathfrak{p}$ is ordinary if and only if p splits in K.*

Proof. See [Lan87], chapter 13, theorem 12 and also Deuring's article [Deu41]. □

A.6.1 Fields generated by division points

Next we come to some properties of the extensions obtained by adjoining coordinates of division points of E to K that we will use repeatedly. Assume that E has complex multiplication by the maximal order $\mathcal{O}_K$. Let $\mathfrak{m}$ and $\mathfrak{n}$ be two integral ideals of $\mathcal{O}_K$. First note that for the ray class fields $K(\mathfrak{m})$ and $K(\mathfrak{n})$, in general, we have an equality

$$K(\mathfrak{m}) \cap K(\mathfrak{n}) = K(g.c.d.(\mathfrak{m}, \mathfrak{n})),$$

which is a simple exercise in class field theory. However, in general, we only have an inclusion

$$K(\mathfrak{m})K(\mathfrak{n}) \subset K(l.c.m.(\mathfrak{m}, \mathfrak{n})),$$

which need not be an equality. For extensions generated by division points of E the situation is nicer.

Proposition A.6.3. *Let $\mathfrak{m}$ and $\mathfrak{n}$ be two non-trivial integral ideals of $\mathcal{O}_K$. Then, we have identities*

$$K(E[\mathfrak{m}]) \cap K(E[\mathfrak{n}]) = K(E[g.c.d.(\mathfrak{m}, \mathfrak{n})]) \quad \text{and} \quad K(E[\mathfrak{m}])K(E[\mathfrak{n}]) = K(E[l.c.m.(\mathfrak{m}, \mathfrak{n})]).$$

Proof. Let us first prove the second identity. We clearly have

$$K(E[\mathfrak{m}])K(E[\mathfrak{m}]) \subset K(E[l.c.m.(\mathfrak{m}, \mathfrak{n})])$$

since $\mathfrak{m}$-, resp. $\mathfrak{n}$-division points are also $l.c.m.(\mathfrak{m}, \mathfrak{n})$-division points. On the other hand, let Q be a $l.c.m.(\mathfrak{m}, \mathfrak{n})$-division point of $E(\bar{K})$. We can find integral ideals $\mathfrak{m}'$ and $\mathfrak{n}'$ such that

$$\mathfrak{m}'\mathfrak{m} = l.c.m.(\mathfrak{m}, \mathfrak{n}) \quad \text{and} \quad \mathfrak{n}'\mathfrak{n} = l.c.m.(\mathfrak{m}, \mathfrak{n})$$

and $\mathfrak{m}'$ and $\mathfrak{n}'$ are easily seen to be coprime. Let $m', n' \in \mathcal{O}_K$ be generators (K has class number 1 by proposition A.6.1) of $\mathfrak{m}'$ and $\mathfrak{n}'$, respectively. Then we can find $a, b \in \mathcal{O}_K$, prime to each other, such that

$$am' + bn' = 1.$$

It follows that

$$Q = am'Q + bn'Q,$$

where $am'Q$ and $bn'Q$ are $\mathfrak{m}$- and $\mathfrak{n}$-division points, respectively. Since E is defined over K, addition on E is a K-rational operation and we see that the coordinates of Q already lie in the compositum $K(E[\mathfrak{m}])K(E[\mathfrak{n}])$.

Now, we come to the first identity. The inclusion

$$K(E[g.c.d.(\mathfrak{m},\mathfrak{n})]) \subset K(E[\mathfrak{m}]) \cap K(E[\mathfrak{n}])$$

is obvious. This time, we can find integral ideals $\mathfrak{m}'$ and $\mathfrak{n}'$ such that

$$\mathfrak{m} = \mathfrak{m}' \cdot g.c.d.(\mathfrak{m},\mathfrak{n}) \quad \text{and} \quad \mathfrak{n} = \mathfrak{n}' \cdot g.c.d.(\mathfrak{m},\mathfrak{n}).$$

Again, $\mathfrak{m}'$ and $\mathfrak{n}'$ are easily seen to be coprime. Assume we have $\mathfrak{m} = \prod_{\mathfrak{l}} \mathfrak{l}^{m_{\mathfrak{l}}}$ and $\mathfrak{n} = \prod_{\mathfrak{l}} \mathfrak{l}^{n_{\mathfrak{l}}}$, where $m_{\mathfrak{l}}$ and $n_{\mathfrak{l}}$ are the exact exponents of the prime $\mathfrak{l}$ in the product decomposition of $\mathfrak{m}$ and $\mathfrak{n}$, respectively. Let us define

$$\mathfrak{m}'' = \prod_{\mathfrak{l}\,|\mathfrak{m}'} \mathfrak{l}^{m_{\mathfrak{l}}} \quad \text{and} \quad \mathfrak{n}'' = \prod_{\mathfrak{l}\,|\mathfrak{n}'} \mathfrak{l}^{n_{\mathfrak{l}}}$$

where the products are taken precisely over those primes that divide $\mathfrak{m}'$ and $\mathfrak{n}'$, respectively. Since $\mathfrak{m}'$ and $\mathfrak{n}'$ are coprime, $\mathfrak{m}''$ and $\mathfrak{n}''$ are coprime, too. We claim that

$$\mathfrak{m} = l.c.m.\big(\mathfrak{m}'', g.c.d.(\mathfrak{m},\mathfrak{n})\big). \tag{A.6.1}$$

In order to show this write $\mathfrak{m}'' = \prod_{\mathfrak{l}} \mathfrak{l}^{m''_{\mathfrak{l}}}$ and $g.c.d.(\mathfrak{m},\mathfrak{n}) = \prod_{\mathfrak{l}} \mathfrak{l}^{d_{\mathfrak{l}}}$ for the product decompositions. Note that $d_{\mathfrak{l}} = \min(m_{\mathfrak{l}}, n_{\mathfrak{l}})$. By definition of the least common multiple, the exponent of a prime $\mathfrak{l}$ in the decomposition of $l.c.m.\big(\mathfrak{m}'', g.c.d.(\mathfrak{m},\mathfrak{n})\big)$ is given by

$$\max\{m''_{\mathfrak{l}}, d_{\mathfrak{l}}\}.$$

If the prime $\mathfrak{l}$ divides $\mathfrak{m}'$, then, by definition of $\mathfrak{m}''$, we have

$$m''_{\mathfrak{l}} = m_l \geq d_{\mathfrak{l}},$$

so the exponent of $\mathfrak{l}$ in $l.c.m.\big(\mathfrak{m}'', g.c.d.(\mathfrak{m},\mathfrak{n})\big)$ is given by m_l. Now assume that $\mathfrak{l} \nmid \mathfrak{m}'$. If $m_{\mathfrak{l}} = 0$, then $m''_{\mathfrak{l}} = 0$ and $d_{\mathfrak{l}} = 0$, so also in this case $m_{\mathfrak{l}}$ coincides with the exponent of $\mathfrak{l}$ in $l.c.m.\big(\mathfrak{m}'', g.c.d.(\mathfrak{m},\mathfrak{n})\big)$. The last case to consider is $\mathfrak{l} \nmid \mathfrak{m}'$ and $m_{\mathfrak{l}} \geq 1$. In this case $\mathfrak{l}^{m_{\mathfrak{l}}}$ must divide $g.c.d.(\mathfrak{m},\mathfrak{n})$, so that $m_{\mathfrak{l}} \leq d_{\mathfrak{l}}$. By definition of $d_{\mathfrak{l}}$ we then have $m_{\mathfrak{l}} = d_{\mathfrak{l}}$. Moreover, since $\mathfrak{l} \nmid \mathfrak{m}'$ we have $m''_{\mathfrak{l}} = 0$ and we conclude that also in this last case $m_{\mathfrak{l}}$ coincides with the exponent of $\mathfrak{l}$ in $l.c.m.\big(\mathfrak{m}'', g.c.d.(\mathfrak{m},\mathfrak{n})\big)$. This finishes the proof of (A.6.1). Similar to (A.6.1) we can show that

$$\mathfrak{n} = l.c.m.\big(\mathfrak{n}'', g.c.d.(\mathfrak{m},\mathfrak{n})\big).$$

Writing $\mathfrak{q} = g.c.d.(\mathfrak{m},\mathfrak{n})$ and using the second equality from the statement of the proposition proved above, we can now write

$$K(E[\mathfrak{m}]) = K\Big(E\big[l.c.m.\big(\mathfrak{m}'', \mathfrak{q}\big)\big]\Big) = K(E[\mathfrak{q}])(E[\mathfrak{m}''])$$

and, likewise,

$$K(E[\mathfrak{n}]) = K\Big(E\big[l.c.m.\big(\mathfrak{n}'', \mathfrak{q}\big)\big]\Big) = K(E[\mathfrak{q}])(E[\mathfrak{n}'']),$$

where the fields on the right are the ones obtained by adjoining coordinates of $\mathfrak{m}''$- and $\mathfrak{n}''$-division points, respectively, to $K(E[\mathfrak{q}])$. They coincide with $K(E[\mathfrak{q}])K(E[\mathfrak{m}''])$ and with $K(E[\mathfrak{q}])K(E[\mathfrak{n}''])$, respectively. Considering E as defined over $K(E[\mathfrak{q}])$ and recalling that $\mathfrak{m}''$ and $\mathfrak{n}''$ are coprime, ([dS87], corollary 1.7) yields

$$K(E[\mathfrak{m}]) \cap K(E[\mathfrak{n}]) = K(E[\mathfrak{q}])(E[\mathfrak{m}'']) \cap K(E[\mathfrak{q}])(E[\mathfrak{n}'']) = K(E[\mathfrak{q}]),$$

which finishes the proof. □

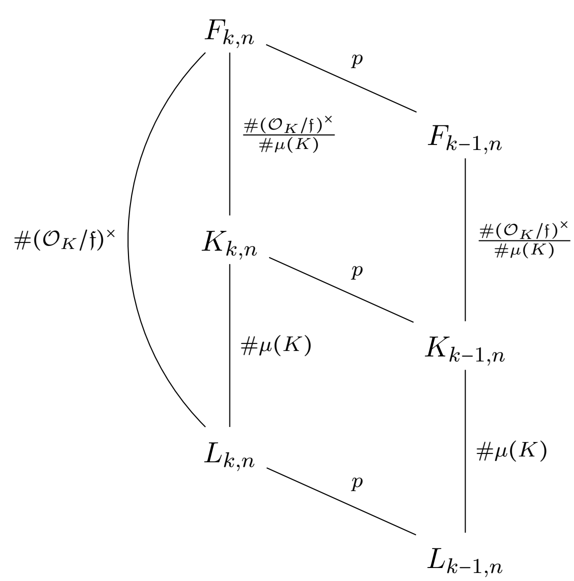
Now, assume that the prime number $p \in \mathbb{Z}$ splits in $\mathcal{O}_K$ into distinct primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. We define $K_{k,n} = K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$, $L_{k,n} = K(\bar{\mathfrak{p}}^k\mathfrak{p}^n)$ and $F_{k,n} = K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$. We write $\mu(K)$ for the roots of unity contained in K. For $k, n \geq 1$ such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\bar{\mathfrak{p}}^k\mathfrak{p}^n)^\times$ is injective, the cardinalities of the Galois groups over K are given by

$$\#\mathrm{Gal}(F_{k,n}/K) = \frac{\#(\mathcal{O}_K/\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)^\times}{\#\mu(K)} \tag{A.6.2}$$

$$\#\mathrm{Gal}(L_{k,n}/K) = \frac{\#(\mathcal{O}_K/\bar{\mathfrak{p}}^k\mathfrak{p}^n)^\times}{\#\mu(K)} \tag{A.6.3}$$

$$\#\mathrm{Gal}(K_{k,n}/K) = \#(\mathcal{O}_K/\bar{\mathfrak{p}}^k\mathfrak{p}^n)^\times, \tag{A.6.4}$$

where the first two equations follow from class field theory, see ([Neu07], VI, §1, Aufgabe 13), and the third from ([dS87], II, corollary 1.7). For $k \geq 2, n \geq 1$ such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\bar{\mathfrak{p}}^{k-1}\mathfrak{p}^n)^\times$ is injective, the fields build the following tower



(A.6.5)

where the numbers next to the edges are the degrees of the extensions. We define the following infinite extensions of K

$$F_\infty = \bigcup_{k,n} K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n), \quad K_\infty = \bigcup_{k,n} K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n]), \quad L_\infty = \bigcup_{k,n} K(\bar{\mathfrak{p}}^k\mathfrak{p}^n).$$

Lemma A.6.4. *Assume that $k, n \geq 1$ are big enough such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\bar{\mathfrak{p}}^{k-1}\mathfrak{p}^n)^\times$ is injective. Moreover, assume that $(p, \#\mu(K)) = 1$. Then, the restriction maps*

$$\mathrm{Gal}(K_{k,n}/L_{k,n}) \longrightarrow \mathrm{Gal}(K_{k-1,n}/L_{k-1,n})$$

are bijections. We have a similar statement for the roles of n and k interchanged. In particular, $G(K_\infty/L_\infty) = \varprojlim_{k,n} G(K_{k,n}/L_{k,n})$ has cardinality $\#\mu(K)$.

Proof. Since both groups have the same finite cardinality it is sufficient to show that the maps are injective. To show this, it clearly suffices to show that

$$L_{k,n}K_{k-1,n} = K_{k,n}.$$

But $L_{k,n}K_{k-1,n}$ is a subextension of the degree p extension $K_{k,n}/K_{k-1,n}$, so it suffices to show that $L_{k,n}K_{k-1,n}$ is strictly bigger than $K_{k-1,n}$. But the exponent of p in the cardinality of $\mathrm{Gal}(L_{k,n}K_{k-1,n}/K)$ is at least $(k-1)+(n-1)$ by our assumption $(p, \#\mu(K)) = 1$, while the exponent of p in the cardinality of $\mathrm{Gal}(K_{k-1,n}/K)$ is $(k-2)+(n-1)$. □

Lemma A.6.5. *Assume that $k, n \geq 1$ are big enough such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\bar{\mathfrak{p}}^{k-1}\mathfrak{p}^{n-1})^\times$ is injective. Moreover, assume that $(p, \#(\mathcal{O}_K/\mathfrak{f})^\times 6) = 1$. Then, in the following composite map, both of the restriction maps*

$$\mathrm{Gal}(F_{k,n}/F_{k-1,n}) \longrightarrow \mathrm{Gal}(K_{k,n}/K_{k-1,n}) \longrightarrow \mathrm{Gal}(L_{k,n}/L_{k-1,n})$$

are bijections. We have a similar statement for the roles of n and k interchanged.

Proof. Since all groups are of order p, it is sufficient to show that the composite is an injection. This, in turn, is equivalent to showing that $F_{k-1,n}L_{k,n} = F_{k,n}$. And since $[F_{k,n} : F_{k-1,n}] = p$ it suffices to show that $F_{k-1,n}L_{k,n}$ is strictly bigger than $F_{k-1,n}$. By the assumption $(p, \#(\mathcal{O}_K/\mathfrak{f})^\times 6) = 1$ the exponent of p in $[F_{k-1,n} : K]$ is $n-1+k-2$. However, the exponent of p in $[L_{k,n} : K]$ is $n-1+k-1$ which is less than or equal to the exponent of p in $[L_{k,n}F_{k-1,n} : K]$, showing that $L_{k,n}F_{k-1,n}$ is bigger than $F_{k-1,n}$. □

We then have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G(F_{k,n}/F_{k-1,n}) & \longrightarrow & G(F_{k,n}/F_{k-1,n-1}) & \longrightarrow & G(F_{k-1,n}/F_{k-1,n-1}) & \longrightarrow & 1 \\ & & \downarrow\cong & & \downarrow & & \downarrow\cong & & \\ 1 & \longrightarrow & G(K_{k,n}/K_{k-1,n}) & \longrightarrow & G(K_{k,n}/K_{k-1,n-1}) & \longrightarrow & G(K_{k-1,n}/K_{k-1,n-1}) & \longrightarrow & 1 \\ & & \downarrow\cong & & \downarrow & & \downarrow\cong & & \\ 1 & \longrightarrow & G(L_{k,n}/L_{k-1,n}) & \longrightarrow & G(L_{k,n}/L_{k-1,n-1}) & \longrightarrow & G(L_{k-1,n}/L_{k-1,n-1}) & \longrightarrow & 1 \end{array} \tag{A.6.6}$$

with exact rows. By the five lemma we get the following corollary.

Corollary A.6.6. *Let the setting be as in lemma A.6.5. Then, in the following composite map, both of the restriction maps*

$$\mathrm{Gal}(F_{k,n}/F_{k-1,n-1}) \longrightarrow \mathrm{Gal}(K_{k,n}/K_{k-1,n-1}) \longrightarrow \mathrm{Gal}(L_{k,n}/L_{k-1,n-1})$$

are bijections.

Lemma A.6.7. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and good ordinary reduction at p. Moreover, assume that $(p, \#(\mathcal{O}_K/\mathfrak{f})^\times) = 1$. Then, for any divisor $\mathfrak{f}'$ of $\mathfrak{f}$ and $k, n \geq 1$ such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)^\times$ is injective, the natural maps induced by restriction*

$$\mathrm{Gal}(K_{k+1,n}/K_{k,n}) \longrightarrow \mathrm{Gal}\Big(\big(K_{k+1,n} \cap K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^n)\big)/\big(K_{k,n} \cap K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)\big)\Big) \tag{A.6.7}$$

are injective.

Proof. We can write the map from (A.6.7) as the composite of the monomorphism

$$\mathrm{Gal}(K_{k+1,n}/K_{k,n}) \hookrightarrow \mathrm{Gal}(K_{k+1,n}/(K_{k,n} \cap K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n))) \tag{A.6.8}$$

and the epimorphism

$$\mathrm{Gal}\big(K_{k+1,n}/(K_{k,n} \cap K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n))\big) \twoheadrightarrow \mathrm{Gal}\Big(\big(K_{k+1,n} \cap K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^n)\big)/\big(K_{k,n} \cap K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)\big)\Big). \tag{A.6.9}$$

By ([dS87], II, corollary 1.7), $\mathrm{Gal}(K_{k+1,n}/K_{k,n})$ has order p. We next show that the kernel of the map (A.6.9) has order prime to p, which proves that (A.6.7) is injective. The kernel of the map (A.6.9) is given by

$$\mathrm{Gal}\big(K_{k+1,n}/(K_{k+1,n} \cap K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^n))\big) \cong \mathrm{Gal}\Big(\big(K_{k+1,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^n)\big)/K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^n)\Big),$$

which is a quotient of $\mathrm{Gal}\big(K(\mathfrak{f}\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^n))/K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+1}\mathfrak{p}^n)\big)$ by ([dS87], proposition 1.6). Due to our assumption on k, n and $\mathfrak{f}'$ and the fact that $(\mathfrak{f}, p) = 1$, class field theory, see ([Neu07], VI, §1, Aufgabe 13), shows that the latter Galois group has order

$$\frac{\#(\mathcal{O}_K/\mathfrak{f})^\times}{\#(\mathcal{O}_K/\mathfrak{f}')^\times},$$

which is prime to p by our assumption. ◻

A.6.2 Größencharacters and conductors

Let us write $\mathfrak{f}_\psi$ for the conductor of the Größencharacter ψ attached to E/K, which can be interpreted in several ways as we explain next, see also ([BV10], section 2) for a discussion. Writing Σ_{bad} for the primes of K where E has bad reduction, then ψ can be defined as a homomorphism from the free abelian group $I_{\Sigma_{bad}}$ on primes of K not belonging to Σ_{bad} to the multiplicative group $K^\times$. For a finite place ν where E has good reduction write $\tilde{E}_\nu/k_\nu$ for the reduction modulo ν, where k_ν denotes the residue field. By definition, $\psi(\nu) \in K^\times$ is the unique element that maps to the arithmetic Frobenius element in $\mathrm{End}_{k_\nu}(\tilde{E}_\nu)$ under the natural (injective) map

$$K = \mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathrm{End}_{k_\nu}(\tilde{E}_\nu) \otimes_{\mathbb{Z}} \mathbb{Q}$$

induced by reduction modulo ν, compare [Coaa] for the fact that one can lift the Frobenius elements to K. It is proved in [Coaa] that ψ is a Größencharacter of type A_0 in the sense of Weil [Wei55] with infinity type $(1,0)$, which means that there exists an ideal $\mathfrak{f}$ of K such that $\psi((x)) = x$ for all $x \in K^\times$ satisfying $\mathrm{ord}_{\nu_\mathfrak{q}}(x-1) \geq \mathrm{ord}_{\nu_\mathfrak{q}}(\mathfrak{f})$ for all $\mathfrak{q} \mid \mathfrak{f}$, where we write $\mathrm{ord}_{\nu_\mathfrak{q}}$ for the valuation function associated to $\mathfrak{q}$. $\mathfrak{f}_\psi$, by definition, is the smallest ideal $\mathfrak{f}$ with this propery as is also explained in [dS87]. Let p be a prime above which E has good reduction. Weil [Wei55] has shown that the character ψ_E can be extended to a character $G(K(p^\infty\mathfrak{f}_\psi)/K) \longrightarrow \mathbb{C}_p$ which we also denote by ψ, where we write $\mathbb{C}_p$ for the completion of an algebraic closure of $\mathbb{Q}_p$. The extension to $G(K(p^\infty\mathfrak{f}_\psi)/K)$ is defined in a way such that for the arithmetic Frobenius $(\nu, K(p^\infty\mathfrak{f}_\psi)/K)$ in $G(K(p^\infty\mathfrak{f}_\psi)/K)$ attached to a finite prime ν of K not above p where E has good reduction, we have $\psi((\nu, K(p^\infty\mathfrak{f}_\psi)/K)) = \psi(\nu)$, see also [dS87].

We also have the notion of conductor $\mathfrak{f}_{E/K}$ of E/K in terms representations of the inertia and higher ramification groups on Tate modules and certain torsion subgroups of E. We refer to Silverman ([Sil99], IV, §10) and the article [ST68] by Serre and Tate for a precise definition and the fact that $\mathfrak{f}_{E/K}$ is divisible precisely by the primes of K where E has bad reduction. The relation between $\mathfrak{f}_{E/K}$ and $\mathfrak{f}_\psi$ is given in the following

Theorem A.6.8. *For the conductors $\mathfrak{f}_\psi$ and $\mathfrak{f}_{E/K}$ we have have an equality*

$$\mathfrak{f}_\psi^2 = \mathfrak{f}_{E/K}$$

of ideals in $\mathcal{O}_K$. In particular, $\mathfrak{f}_\psi$ is divisible precisely by the primes where E/K has bad reduction.

Proof. See the article of Serre and Tate ([ST68], theorem 12, p.514). See also Deuring's work [Deu55] and [Deu56] or Shimura's book ([Shi71], theorem 7.42). □

A.6.3 Curves defined over $\mathbb{Q}$

Appendix A, §3 in Silverman's book [Sil99] contains a list of representatives with minimal discriminant and conductor of all $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over $\mathbb{Q}$ with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ of discriminant $-D$. The discriminant of any such quadratic imaginary field K belongs to the finite set

$$-D \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\},$$

which consists of numbers, all of which are divisible by one prime number only.

Moreover, if we restrict our attention to those $E/\mathbb{Q}$ that have complex multiplication by the maximal order $\mathcal{O}_K$, i.e., the full ring of integers of $K = \mathbb{Q}(\sqrt{-D})$, then the following holds. Let us write $\mathfrak{f}_{E/\mathbb{Q}}$ for the conductor of E over $\mathbb{Q}$. Then, each $\bar{\mathbb{Q}}$-isomorphism class of elliptic curves defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$ contains a representative $E/\mathbb{Q}$ such that

$\mathfrak{f}_{E/\mathbb{Q}}$ is divisible by only one prime number which is precisely the prime dividing $-D$.

In particular, if $l \in \mathbb{Z}$ is the prime dividing $\mathfrak{f}_{E/\mathbb{Q}}$, then l ramifies in K and we can write

$$\mathcal{O}_K l = \mathfrak{l}^2$$

for the prime $\mathfrak{l}$ in $\mathcal{O}_K$ that lies above the prime ideal generated by l. These considerations prove part of the following proposition. We can consider E also as defined over K and when we do, we write $\mathfrak{f}_{E/K}$ for the conductor of E/K.

Proposition A.6.9. *Let $E/\mathbb{Q}$ be a representative as above and $l \in \mathbb{Z}$ be the prime dividing $\mathfrak{f}_{E/\mathbb{Q}}$. Write $\mathfrak{l}$ for the prime of K above $\mathbb{Z}l$. Then, we have an equality of ideals*

$$\mathfrak{f}_{E/K} = \mathfrak{l}^r$$

for some $r \geq 2$ and r divisible by 2.

Proof. We have seen above that $\mathfrak{f}_{E/K}$ is divisible at most by one prime, namely $\mathfrak{l}$. But since the class number of K is 1, E has a global minimal equation over K and we can use a general result of Stroeker ([Str83], (1.7) Main Theorem) saying that E considered as an elliptic curve over K cannot have good reduction everywhere, so the exponent r must be greater or equal to 1. Theorem A.6.8 now concludes the proof. We note that we could have concluded that $r \geq 2$ independently of theorem A.6.8. In fact, since E has potential good reduction everywhere, the reduction type at $\mathfrak{l}$ must be additive and therefore $r \geq 2$. □

We also state a fact in this subsection concerning fields generated by division points, which we will use later when dealing with curves over $\mathbb{Q}$. If E is a curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$, K quadratic imaginary, then the following holds. Let us write $K_\infty = \cup_n K(E[p^n])$ and $\mathbb{Q}_\infty = \cup_n \mathbb{Q}(E[p^n])$.

Proposition A.6.10. *Assume that p splits in K. Then, we have an equality of fields $K_\infty = \mathbb{Q}_\infty$.*

The content of this proposition is that K is contained in $\mathbb{Q}_\infty$ for split primes p. Write π for a generator of one of the two primes of K above p. The proof of the proposition follows immediately from the following general lemma applied to

$$\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_\pi E),$$

the representation of the π-adic Tate module $T_\pi E$ of E and the two groups $G_K \triangleleft G_{\mathbb{Q}}$. In fact, we will see in (A.6.18) that we have $\mathrm{Ind}_{G_{\mathbb{Q}}}^{G_K} \rho \cong \rho_E$, where

$$\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p E),$$

and $\ker(\rho_E) = G_{\mathbb{Q}_\infty}$. The lemma now says that $G_{\mathbb{Q}_\infty} \subseteq \ker(\rho)$ and, in particular, $G_{\mathbb{Q}_\infty} \subset G_K$, which proves what we wanted.

Lemma A.6.11. *Let $H \triangleleft G$ be a normal subgroup of finite index n. Furthermore, let $\rho : H \longrightarrow \mathrm{Aut}_F(V)$ be a finite dimensional representation. Then, we have the inclusion*

$$\ker(\mathrm{Ind}_G^H \rho) \subseteq \ker(\rho),$$

where the kernels both are considered as subgroups of G.

Proof. Let g belong to $\ker(\mathrm{Ind}_G^H \rho)$. We fix both, a system of left coset representives $\sigma_1, \ldots, \sigma_n$ of H in G, with $\sigma_1 = 1$, and a F-basis $v_1, \ldots, v_m$ of V. $\mathrm{Ind}_G^H V = F[G] \otimes_{F[H]} V$ is a F-vector space with basis $(\sigma_i \otimes v_j)_{i,j}$. Now, for any i we can find a k and an element $h \in H$ such that $g\sigma_i = \sigma_k h$. By assumption on g we get

$$\sigma_i \otimes v_j = g(\sigma_i \otimes v_j) = (g\sigma_i) \otimes v_j = \sigma_k h \otimes v_j = \sigma_k \otimes \rho(h) v_j.$$

Since $(\sigma_i \otimes v_j)_{i,j}$ forms a basis, we must have $i = k$. Hence, $g = \sigma_i h \sigma_i^{-1}$, which belongs to H, since H is assumed to be normal in G. Moreover, by a similar reasoning, and since $g \in H$, we have

$$1 \otimes v = g(1 \otimes v) = 1 \otimes \rho(g) v,$$

for all $v \in V$, whence it follows that $v = \rho(g)v, \forall v \in V$ since $(\sigma_i \otimes v_j)_{i,j}$ is a basis. This implies that g belongs to $\ker(\rho)$, as was to be shown. □

We note that the Tate-module $T_p E$ for $E/\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$ is irreducible as a representation of $G_{\mathbb{Q}}$, see ([Ser98a], Chapter IV, 2.1) since E has no complex multiplication over $\mathbb{Q}$, by which we mean that $\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$, one has to allow a larger ground field to achieve complex multiplication, in fact, as we have remarked before $\mathrm{End}_K(E) = \mathcal{O}_K$.

A.6.4 The Tate modules $T_pE, T_\pi E$ and $T_{\bar\pi}E$

In this section we recall some facts about Tate module of elliptic curves with complex multiplication. Fix a prime number $p \in \mathbb{Z}_p$, $p \neq 2$, and embeddings $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ and $\overline{\mathbb{Q}} \subset \mathbb{C}$. Let E/K, K quadratic imaginary, be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and good reduction at p and set $K_\infty = \cup_n K_n$, where $K_n = K(E[p^n])$. We assume that p splits in K, i.e., $\mathcal{O}_K p = \mathfrak{p}\bar{\mathfrak{p}}$, $\bar{\mathfrak{p}} \neq \mathfrak{p}$, which implies that E has good ordinary reduction at $\mathfrak{p}$, see proposition A.6.2.

We write $\mathfrak{p}$ (resp. $\bar\nu$) for the prime of K (resp. K_∞) above p that is determined by the embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$. Moreover, we set $G = G(K_\infty/K)$ and $\mathcal{G}' = G(K_{\infty,\bar\nu}/K_\mathfrak{p})$. We identify $G(K_{\infty,\bar\nu}/K_\mathfrak{p})$ with the decomposition group of $\bar\nu$ in $\mathcal{G}$. Let us write $\psi = \psi_E$ for the Größencharacter attached to E. We define $\pi := \psi(\mathfrak{p})$ and write $\bar\pi = \overline{\psi(\mathfrak{p})}$ for the complex conjugate. Then, one has $\pi, \bar\pi \in \mathcal{O}_K$,

$$\pi \cdot \bar\pi = N_{K/\mathbb{Q}}(\pi) = N(\mathfrak{p}) = p,$$

where $N(\mathfrak{p}) = \#\mathcal{O}_K/\mathfrak{p}$, and

$$(\pi) = \mathfrak{p} \quad \text{and} \quad (\bar\pi) = \bar{\mathfrak{p}},$$

see ([Coaa], lecture 3, Lemma 8 and lecture 4, theorem 9). Moreover, if E is already defined over $\mathbb{Q}$ we also have

$$\psi(\bar{\mathfrak{p}}) = \overline{\psi(\mathfrak{p})} = \bar\pi$$

see ([Kat76], p. 559).

In any case, we have fixed $\mathcal{O}_K$-generators π of $\mathfrak{p}$ and $\bar\pi$ of $\bar{\mathfrak{p}}$. Note that π is a uniformizer for $\mathcal{O}_{K_\mathfrak{p}}$ and $\bar\pi$ is a unit in $\mathcal{O}_{K_\mathfrak{p}}$, i.e., belongs to $\mathcal{O}_{K_\mathfrak{p}}^\times$. Let us write $\mathfrak{m}$ for the valuation ideal of $\overline{\mathbb{Q}}_p$, i.e., $\mathfrak{m} = \bigcup_L \mathfrak{m}_L$ where the unions is taken over all finite subsextensions L of $\overline{\mathbb{Q}}_p/K_\mathfrak{p}$ and $\mathfrak{m}_L$ denotes the maximal ideal of $\mathcal{O}_L$. There is an exact sequence

$$0 \longrightarrow \widehat{E}(\mathfrak{m}) \xrightarrow{\iota_{\hat E}} E(\overline{\mathbb{Q}}_p) \xrightarrow{red_\mathfrak{p}} \tilde{E}(\overline{\mathbb{F}}_p) \longrightarrow 0, \tag{A.6.10}$$

and the element $\bar\pi$, as a unit in $\mathcal{O}_{K_\mathfrak{p}}^\times$, defines an isomorphism of the formal group $\widehat{E}/\mathcal{O}_{K_\mathfrak{p}}$ (and hence of $\widehat{E}(\mathfrak{m})$), see ([Ser10], section 3.3, proposition 3). In particular, $\widehat{E}(\mathfrak{m})$ does not contain any non-trivial $\bar\pi$-torsion. All non-trivial p-torsion of $\widehat{E}(\mathfrak{m})$ is π-torsion. Recall that due to our ordinary good reduction assumption $T_p\tilde{E} := \varprojlim_n \tilde{E}[p^n]$ and $T_p\widehat{E} := \varprojlim_n \hat{E}[p^n]$ are both free of rank 1 as $\mathbb{Z}_p$-modules. Let us make a remark about p-, π- and $\bar\pi$-primary Tate modules.

Remark A.6.12 (Conventions for Tate modules). One certainly defines the p-primary Tate module T_pE via the multpilication by p maps $E[p^{n+1}] \to E[p^n]$, $x \mapsto px$. For the π- and $\bar\pi$-primary Tate modules some authors adopt different conventions, one can either define $T_\pi E$ via the maps $E[\pi^{n+1}] \to E[\pi^n]$, $x \mapsto \pi x$, which will be our definition. Alternatively, recall that $p = \pi \cdot \bar\pi$, one could define a π-primary Tate module via the maps $E[\pi^{n+1}] \to E[\pi^n]$, $x \mapsto px$, which also gives a well-defined module which we will denote by $T_{\pi,\cdot p}E$ (similarly we define $T_{\bar\pi,\cdot p}E$). The modules $T_\pi E$ and $T_{\pi,\cdot p}E$ are isomorphic for which we recall that $E[\pi^n] \cong \mathcal{O}_K/(\mathfrak{p}^n)$ as $\mathcal{O}_K$-modules. π^n and

$\bar{\pi}^n$ are coprime and hence multiplication with $\bar{\pi}^n$ induces an isomorphism $\cdot\bar{\pi}^n : E[\pi^n] \xrightarrow{\sim} E[\pi^n]$. Passing to the projective limit we get an isomorphism

$$(\cdot\bar{\pi}^n)_n : T_{\pi,\cdot p}E \xrightarrow{\sim} T_\pi E, \quad (x_n)_n \longmapsto (\bar{\pi}^n x_n)_n.$$

Note that $T_{\pi,\cdot p}E$ naturally embedds into T_pE since the maps of the corresponding projective systems are compatible. $T_\pi E$ embedds into T_pE via the above isomorphism composed with $T_{\pi,\cdot p}E \hookrightarrow T_pE$. An analogous statement holds for the Tate modules $T_{\bar{\pi}}E$ and $T_{\bar{\pi},\cdot p}E$, where the latter is defined in an entirely similar fashion as $T_{\pi,\cdot p}E$.

Let us consider the maps

$$E[p^n] \longrightarrow E[\pi^n] \times E[\bar{\pi}^n], \quad x \longmapsto (\bar{\pi}^n x, \pi^n x), \qquad n \geq 1, \tag{A.6.11}$$

for which we recall that $\pi \cdot \bar{\pi} = p$. It is a fact that $E[\pi^n] \cong \mathcal{O}_K/(\mathfrak{p}^n)$ as $\mathcal{O}_K$-modules and likewise for $\bar{\pi}$. Since 1 is a greatest common divisor of π^n and $\bar{\pi}^n$ in the principal ideal domain $\mathcal{O}_K$ (hence $\bar{\pi}^n$ acts bijectively on $\mathcal{O}_K/(\mathfrak{p}^n)$), we see that the map (A.6.11) is injective and therefore bijective as a map between two groups of order $(p^n)^2$. It is evident that the maps are $\mathbb{Z}_p[G]$-linear and are compatible with respect to the maps $E[p^n] \to E[p^{n-1}]$, $x \mapsto px$ and $E[\pi^n] \times E[\bar{\pi}^n] \to E[\pi^{n-1}] \times E[\bar{\pi}^{n-1}]$, $(y,z) \mapsto (\pi y, \bar{\pi} z)$. For the latter fact just note

$$(\bar{\pi}^{n-1}px, \pi^{n-1}px) = (\bar{\pi}^n \pi x, \pi^n \bar{\pi} x).$$

Hence, we get an isomorphism

$$T_pE \to T_\pi E \times T_{\bar{\pi}}E, \tag{A.6.12}$$

which fits into the commutative diagram of G_K-modules

$$\begin{array}{ccc} T_pE & \longrightarrow & T_\pi E \times T_{\bar{\pi}}E \\ \uparrow & \nearrow{\scriptstyle ((\cdot\bar{\pi}^n)_n, (\cdot\pi^n)_n)} & \\ T_{\pi,\cdot p}E \times T_{\bar{\pi},\cdot p}E & & \end{array} \tag{A.6.13}$$

where the vertical map is given by $(s,t) \longmapsto s+t$, the horizontal map is the map from (A.6.12) induced by (A.6.11) and the diagonal one is the product of the maps from remark A.6.12. Since the horizontal and the diagonal maps are isomorphisms, the vertical map is an isomorphism, too. In particular, we have a direct sum decomposition of G_K-modules

$$T_pE = T_{\pi,\cdot p}E \oplus T_{\bar{\pi},\cdot p}E. \tag{A.6.14}$$

The inverse of (A.6.11) is given by

$$E[\pi^n] \times E[\bar{\pi}^n] \ni (y,z) \longmapsto (\bar{\pi}^n)^{-1} y + (\pi^n)^{-1} z, \tag{A.6.15}$$

where, we recall, $\bar{\pi}^n$ acts bijectively on $E[\pi^n]$ and π^n acts bijectively on $E[\bar{\pi}^n]$ (Note: we do not claim that for $x \in E[p^n]$ we have $(\pi^n)^{-1}(\pi^n x) = x$, which is clearly false in general! Rather, we can always find $a_1, a_2 \in \mathcal{O}_K$ such that $a_1\pi^n + a_2\bar{\pi}^n = 1$ so that we can decompose $x = a_1\pi^n x + a_2\bar{\pi}^n x$ as the sum of a π^n-torsion element $a_2\bar{\pi}^n x$ and a $\bar{\pi}^n$-torsion element $a_1\pi^n x$).

Proposition A.6.13. *The exact sequence from (A.6.10) induces an exact sequence of $\mathcal{G}'$-modules*

$$0 \to T_p\hat{E} \xrightarrow{\iota_{\hat{E}}} T_pE \xrightarrow{red_{\mathfrak{p}}} T_p\tilde{E} \to 0, \tag{A.6.16}$$

which maps $T_p\hat{E}$ isomorphically to $T_{\pi,\cdot p}E$ and $T_{\bar{\pi},\cdot p}E$ isomorphically to $T_p\tilde{E}$.

Proof. The sequence is always left exact. Exactness on the right does not hold in general, but it holds under our assumption that E has CM by $\mathcal{O}_K$ and good ordinary reduction at $\mathfrak{p}$ above the split prime p. In fact, it follows from ([PR84], II, §1.2, Lemme 1, p.28) that

$$E(\overline{\mathbb{Q}}_p)(\bar{\pi}) \xrightarrow{red_{\mathfrak{p}}} \tilde{E}(\overline{\mathbb{F}}_p)(p)$$

is an isomorphism, where we write $N(\bar{\pi})$ and $N(p)$ for the $\bar{\pi}$- and p-primary torsion parts of an $\mathcal{O}_K$-module N, respectively. This induces an isomorphism of the Tate-modules

$$T_{\bar{\pi},\cdot p}E \cong T_p\tilde{E}.$$

Let us now show that $\iota_{\hat{E}}(T_p\hat{E}) = T_{\pi,\cdot p}E$. Recall that $\overline{\psi(\mathfrak{p})} = \bar{\pi}$ is a generator of $\bar{\mathfrak{p}}$. Since $\bar{\pi}$ acts as an isomorphism on the formal group, we have $\hat{E}(\mathfrak{m})(p) = \hat{E}(\mathfrak{m})(\pi)$, where $\mathfrak{m}$ denotes the valuation ideal of $\overline{\mathbb{Q}}_p$. Hence, the image of $T_p\hat{E}$ in T_pE under $\iota_{\hat{E}}$ is contained in $T_{\pi,\cdot p}E$, see remark A.6.12 for the definition of $T_{\pi,\cdot p}E$.

I thank Otmar Venjakob for pointing out that the image of $T_p\hat{E}$ in T_pE must then coincide with $T_{\pi,\cdot p}E$. In fact, $T_{\pi,\cdot p}E/T_p\hat{E}$ is of finite order (both modules are free of $\mathbb{Z}_p$-rank 1 and the one injects into the other) so for any $t \in T_{\pi,\cdot p}E$ the element $red_{\mathfrak{p}}(t)$ is of finite order. But $T_p\tilde{E}$ does not have any non-trivial torsion and therefore t must already belong to $T_p\hat{E}$. □

Assume now that E is already defined over $\mathbb{Q}$ and write $\mathcal{G} = G(K_\infty/\mathbb{Q})$. Write c for the complex conjugation isomorphism induced by $\overline{\mathbb{Q}} \subset \mathbb{C}$. We let c act on $(y,z) \in E[\pi^n] \times E[\bar{\pi}^n]$ by $c.(y,z) = (\bar{z}, \bar{y})$, and note that this is well-defined since

$$\pi^n \bar{z} = \overline{\bar{\pi}^n z} = 0 \tag{A.6.17}$$

and likewise for y. With this action (A.6.11) is $G_{\mathbb{Q}}$-linear. We extend this action to $T_\pi E \times T_{\bar{\pi}}E$ and get the $\mathcal{G}$-equivariant isomorphism

$$T_pE \ \cong\ T_\pi E \times T_{\bar{\pi}}E \ \cong\ \mathrm{Ind}_{\mathcal{G}}^{G} T_{\bar{\pi}}E \tag{A.6.18}$$

where the second map is the map induced by the G-equivariant injection $T_{\bar{\pi}}E \hookrightarrow T_\pi E \times T_{\bar{\pi}}E$ and the universal property of $\mathrm{Ind}_{\mathcal{G}}^{G} T_{\bar{\pi}}E$. Composing the inverse of (A.6.18) with the natural G-equivariant inclusion $T_{\bar{\pi}}E \hookrightarrow \mathrm{Ind}_{\mathcal{G}}^{G} T_{\bar{\pi}}E = \mathbb{Z}_p[\mathcal{G}] \otimes_{\mathbb{Z}_p[G]} T_{\bar{\pi}}E$, $(z_n)_n \mapsto 1 \otimes (z_n)_n$, we get

$$\iota_{\bar{\pi}} : T_{\bar{\pi}}E \hookrightarrow T_pE, \qquad (z_n)_n \longmapsto \big((\pi^n)^{-1} z_n\big)_n,$$

where $z_n \in E[\bar{\pi}^n]$, $n \geq 1$, compare (A.6.15). The elements $(\pi^n)^{-1} z_n \in E[\bar{\pi}^n]$ are $\bar{\pi}^n$-torsion points. Composing the last map with the natural projection $[-] : T_pE \twoheadrightarrow T_pE/T_p\widehat{E}$ we get

$$[\iota_{\bar{\pi}}] : T_{\bar{\pi}}E \to T_pE/T_p\widehat{E} \cong T/T^0 \tag{A.6.19}$$

which is an isomorphism by proposition A.6.13.

Remark A.6.14. Similar to $\iota_{\bar{\pi}}$, let us define $\iota_\pi : T_\pi E \hookrightarrow T_pE$, $(y_n)_n \longmapsto \big((\bar{\pi}^n)^{-1} y_n\big)_n$, the image of which is contained in $T_{\pi,\cdot p}E$. Then, the inverse of the G-equivariant map $T_pE \to T_\pi E \times T_{\bar{\pi}}E$, $t \mapsto (t_\pi, t_{\bar{\pi}})$ from (A.6.12) is given by

$$T_\pi E \times T_{\bar{\pi}}E \longrightarrow T_pE, \ (y,z) \longmapsto \iota_\pi(y) + \iota_{\bar{\pi}}(z).$$

For $t \in T_pE$ and for any $\sigma \in G = G(K_\infty/K)$, by G-equivariance, we have $\sigma t = \iota_\pi(\sigma(t_\pi)) + \iota_{\bar{\pi}}(\sigma(t_{\bar{\pi}}))$. In $T_pE/T_p\widehat{E}$, by proposition A.6.13, we therefore have

$$[\sigma t] = [\iota_\pi(\sigma(t_\pi)) + \iota_{\bar{\pi}}(\sigma(t_{\bar{\pi}}))] = [\iota_{\bar{\pi}}(\sigma(t_{\bar{\pi}}))] = [\iota_{\bar{\pi}}](\sigma(t_{\bar{\pi}})).$$

Similarly, for the complex conjugation isomorphism c and for any $\sigma \in G$, since in $T_\pi E \times T_{\bar{\pi}}E$

$$((\sigma c^{-1}t)_\pi, (\sigma c^{-1}t)_{\bar{\pi}}) = \sigma((c^{-1}t)_\pi, (c^{-1}t)_{\bar{\pi}}) = \sigma(c^{-1}(t_{\bar{\pi}}), c^{-1}(t_\pi)) = (\sigma c^{-1}(t_{\bar{\pi}}), \sigma c^{-1}(t_\pi)),$$

we get

$$[\sigma c^{-1} t] = [\iota_\pi(\sigma c^{-1}(t_{\bar{\pi}})) + \iota_{\bar{\pi}}(\sigma c^{-1}(t_\pi))] = [\iota_{\bar{\pi}}](\sigma c^{-1}(t_\pi)).$$

A.7 Modules over the completed group ring

Let $\mathcal{O}$ be a complete discrete valutation ring with uniformizer π and let G be a profinite group. For the notion of *pro-discrete* and *pseudo-compact* modules over a topological ring and the completed tensor product of such modules we refer to [Wit03]. We want to prove a fact about the topology of pseudo-compact modules over the completed group ring

$$\mathcal{O}[[G]] = \varprojlim_{n,U} (\mathcal{O}/\pi^n\mathcal{O})[G/U],$$

where U runs through the open normal subgroups of G. See ([NSW08], (5.2.17) Proposition) for the analogous statement for compact finitely generated $\mathbb{Z}_p[[G]]$-modules. For any open (or closed) subgroup U of G we write $I(U)$ for the kernel of the augmentation map $\mathcal{O}[[G]] \twoheadrightarrow \mathcal{O}$.

Remark A.7.1. (i) Underlying all of what follows in this section is the fact that the two-sided ideals of $\mathcal{O}[[G]]$ of the form

$$(\pi^n\mathcal{O}[[G]] + I(U)), \qquad n \geq 1, U \text{ open and normal in } G,$$

generate the topology of $\mathcal{O}[[G]]$ and that the modules

$$\mathcal{O}[[G]]/(\pi^n\mathcal{O}[[G]] + I(U)) \cong \mathcal{O}/\pi^n[G/U]$$

for open and normal U in G and $n \geq 1$, are discrete and of finite length as $\mathcal{O}$-modules, compare ([Sch11], Chapter IV, §19). Hence, the topological rings $\mathcal{O}$ and $\mathcal{O}[[G]]$ are pseudo-compact as right- and left-modules over themselves and $\mathcal{O}[[G]]$ is pseudo-compact as an $\mathcal{O}$-module.

(ii) Note that (as in the case of $\mathbb{Z}_p[[G]]$-modules) any $\mathcal{O}[[G]]$-linear map $M \to N$ between modules M, N equipped with the topologies induced by the submodules $\{\pi^n M + I(U)M\}_{n,U}$ and $\{\pi^n N + I(U)N\}_{n,U}$, respectively, where n ranges through $\mathbb{N}_{\geq 1}$ and U through the open normal subgroups of G, is continuous.

Proposition A.7.2. *Let G be a profinite group. The topology of any finitely generated pseudo-compact $\mathcal{O}[[G]]$-module M coincides with the topology induced by the submodules $\{\pi^n M + I(U)M\}_{n,U}$, where n ranges through $\mathbb{N}_{\geq 1}$ and U through the open normal subgroups of G.*

Proof. The author thanks Malte Witte for explanations regarding this proof. Consider a surjection

$$\varphi : \mathcal{O}[[G]]^k \twoheadrightarrow M, \qquad e_i \longmapsto m_i \tag{A.7.1}$$

where e_i denotes the element $(0, \dots, 1, \dots, 0)$ with a 1 at the i-th place. The map φ is continuous with respect to the given original topology of M, because M is a topological $\mathcal{O}[[G]]$-module. We can also endow M with the quotient topology. The proof proceeds in three steps. Whenever we consider a module we consider it as a $\mathcal{O}[[G]]$-module.

1. Step: We show that the quotient topology on M induced by φ coincides with the topology given by the submodules $\{\pi^n M + I(U)M\}_{n,U}$. We will show that the latter topology is at least as fine as the quotient topology, which implies that the two coincide, since φ is continuous with respect to the topology defined by $\{\pi^n M + I(U)M\}_{n,U}$ and the quotient topology is the finest topology on M such that φ is continuous.

Let M' be an open set of M with respect to the quotient topology, i.e., $\varphi^{-1}(M')$ is open, and take any $m \in M'$. Fix $x \in \mathcal{O}[[G]]^k$ such that $\varphi(x) = m$. Then $-m + M'$ is also open (with respect to the quotient topology), since $\varphi^{-1}(-m + M') = -x + \varphi^{-1}(M')$ is open. Now we can find an open submodule N of $\mathcal{O}[[G]]^k$ such that $N \subset \varphi^{-1}(-m + M')$. Since $\varphi^{-1}(\varphi(N)) = \cup_{x \in \ker(\varphi)}(x + N)$ is open, we see that $\varphi(N)$ is an open submodule of M (w.r.t. the quotient top.) and that $\varphi(N) \subset -m + M'$. We will show next that there is a set of the form $\pi^n M + I(U)M$ contained in $\varphi(N)$, which implies that

$$m + \pi^n M + I(U)M \subset m + \varphi(N) \subset M',$$

which shows that the topology generated by the $\pi^n M + I(U)M$ is at least as fine as the quotient topology.

So let V be any open submodule in M with respect to the quotient topology. By definition $\varphi^{-1}(V)$ is an open neighboorhood of 0 in $\mathcal{O}[[G]]^k$. For large enough n and small enough U we have

$$(\pi^n\mathcal{O}[[G]] + I(U))e_i \subset \varphi^{-1}(V), \qquad \forall i = 1, \dots k,$$

by continuity of the finitely many maps $\mathcal{O}[[G]] \to \mathcal{O}[[G]]^k$, $1 \longmapsto e_i$ and since the $\{\pi^m\mathcal{O}[[G]] + I(U')\}_{m,U'}$ generate the topology of $\mathcal{O}[[G]]$. Since V is a submodule, this implies that

$$\big(\pi^n\mathcal{O}[[G]] + I(U)\big)M = \big(\pi^n\mathcal{O}[[G]] + I(U)\big)\varphi(< e_1, \dots, e_k >_{\mathcal{O}[[G]]}) \subset V,$$

which is what we wanted to show.

2. Step: One has to show that M is pseudo-compact with respect to the quotient topology. Note that M is Hausdorff with respect to the original topology and φ is continuous with respect to the original topology, hence $\ker(\varphi) = \varphi^{-1}(\{0\})$ is closed in $\mathcal{O}[[G]]^k$. Then, one can show as in ([Gab62], Chapitre IV, §3, proof of Théorème 3) that $\mathcal{O}[[G]]^k/\ker(\varphi)$ equipped with the quotient topology is pseudo-compact, using ([Gab62], Chapitre IV, §3, Propositions 10, 11). Moreover, $\mathcal{O}[[G]]^k/\ker(\varphi) \to M$, where both modules are equipped with the quotient topology, is certainly a homeomorphism. Hence, M is pseudo-compact with respect to the quotient topology.

3. Step: Conclude that the original topology of M coincides with the topology generated by $\{\pi^n M + I(U)M\}_{n,U}$. We have shown that the latter topology coincides with the quotient topology in the first step. In the second step we have shown that M is pseudo-compact as a $\mathcal{O}[[G]]$-module with respect to the quotient topology. Hence the identity map

$$(M, \text{ quotient top.}) \longrightarrow (M, \text{ original top.})$$

is a continuous bijection of pseudo-compact $\mathcal{O}[[G]]$-modules. Now it follows as in (loc. cit., Chapitre IV, §3, proof of Théorème 3) that this must be a homeomorphism, which concludes the proof. The crucial fact used here is that for any open submodule U of $(M, \text{ quotient top.})$, the $\mathcal{O}[[G]]$-module M/U is Artinian. □

A.8 Ore sets over complete DVRs

Let $\mathcal{O}$ be a complete discrete valutation ring with uniformizer π, write $\mathbb{F} = \mathcal{O}/\mathcal{O}\pi$ and assume that $\mathrm{char}(\mathbb{F}) = p > 0$. Moreover, let $\mathcal{G}$ be a compact p-adic Lie group containing a closed normal subgroup $\mathcal{H}$ such that

$$\mathcal{G}/\mathcal{H} \cong \mathbb{Z}_p.$$

It follows that $\mathcal{G}$ is the semidirect product $\mathcal{G} = \mathcal{H} \rtimes \Gamma$ for some subgroup $\Gamma \cong \mathbb{Z}_p$. One can then show that $\Lambda(\mathcal{G}) = \mathcal{O}[[\mathcal{G}]]$ is a skew power series ring over $\mathcal{O}[[\mathcal{H}]]$, see ([Wit03], Proposition 3.2) and compare [SV04] and [SV10] for the study of such skew power series rings.

In [CFK+05] a canonical Ore set $\mathcal{S}$ of $\mathbb{Z}_p[[\mathcal{G}]]$ was defined. The definition of the Ore set $\mathcal{S}$ from loc. cit. can be extended to Iwasawa algebras $\Lambda(\mathcal{G}) = \mathcal{O}[[\mathcal{G}]]$ with coefficients in $\mathcal{O}$ and is then given by

$$\mathcal{S} = \{f \in \Lambda(\mathcal{G}) \mid \Lambda(\mathcal{G})/\Lambda(\mathcal{G})f \text{ is finitely generated as a } \Lambda(\mathcal{H})-\text{module}\}. \tag{A.8.1}$$

Our first task is to show that $\mathcal{S}$, for general coefficient ring $\mathcal{O}$, is an Ore set and enjoys similar properties as in the $\mathbb{Z}_p$-coeffiecient case. We also define

$$\mathcal{S}^* = \bigcup_{n\geq 1} p^n \mathcal{S}. \tag{A.8.2}$$

A.8.1 Characterization

Let $\mathcal{O}$ be a complete discrete valutation ring as above. We will give different characterizations of the set $\mathcal{S}$ and prove that it is actually an Ore set in $\Lambda(\mathcal{G}) = \mathcal{O}[[\mathcal{G}]]$. We will proceed, with modifications whenever needed, as in [CFK+05] where the $\mathbb{Z}_p$-coefficient case was treated. First we recall the following proposition.

Proposition A.8.1. *If P is a pro-p group, then $\mathcal{O}[[P]]$ is a local ring with residue field $\mathbb{F} = \mathcal{O}/\mathcal{O}\pi$ and the unique maximal ideal $\mathfrak{m}(P)$ of $\mathcal{O}[[P]]$ (which coincides with the Jacobson radical) is equal to the kernel of the composite map $\mathcal{O}[[P]] \xrightarrow{\text{aug}} \mathcal{O} \xrightarrow{pr} \mathbb{F}$.*

Proof. See ([Sch11], Chapter IV, §19, Corollary 19.7). □

Now, fix a pro-p open subgroup $\mathcal{J}$ of $\mathcal{H}$, which is normal in $\mathcal{G}$. For example, since $\mathcal{G}$ is a p-adic Lie group, by Lazard's characterization, see [Laz65], we can find an open normal pro-p subgroup $\mathcal{J}'$ of $\mathcal{G}$. Then, $\mathcal{J} = \mathcal{J}' \cap \mathcal{H}$ is open in $\mathcal{H}$, pro-p and normal in $\mathcal{G}$. Similarly as in [CFK+05] we define maps

$$\varphi_{\mathcal{J}} : \Lambda(\mathcal{G}) \twoheadrightarrow \Lambda(\mathcal{G}/\mathcal{J}) \quad \text{and} \quad \psi_{\mathcal{J}} : \Lambda(\mathcal{G}) \twoheadrightarrow \Omega(\mathcal{G}/\mathcal{J}),$$

where we write $\Omega(G/J) = \mathbb{F}[[\mathcal{G}/\mathcal{J}]]$.

Lemma A.8.2. *Let $\mathcal{J}$ be a pro-p open subgroup of $\mathcal{H}$, which is normal in $\mathcal{G}$. Then,*

(i) $\mathcal{S}$ coincides with the set of those f in $\Lambda(\mathcal{G})$ such that $\Lambda(\mathcal{G}/\mathcal{J})/\Lambda(\mathcal{G}/\mathcal{J})\varphi_{\mathcal{J}}(f)$ is a finitely generated left $\mathcal{O}$-module,

(ii) $\mathcal{S}$ coincides with the set of those f in $\Lambda(\mathcal{G})$ such that $\Omega(\mathcal{G}/\mathcal{J})/\Omega(\mathcal{G}/\mathcal{J})\psi_{\mathcal{J}}(f)$ is a finitely generated left $\mathbb{F}$-module,

(iii) $\mathcal{S}$ coincides with the set of those f in $\Lambda(\mathcal{G})$ such that multiplication with $\psi_{\mathcal{J}}(f)$ from the right induces an injection $\Omega(\mathcal{G}/\mathcal{J}) \hookrightarrow \Omega(\mathcal{G}/\mathcal{J})$,

(iv) $\mathcal{S}$ coincides with the set of those f in $\Lambda(\mathcal{G})$ such that $\Lambda(\mathcal{G})/f\Lambda(\mathcal{G})$ is finitely generated as a right $\Lambda(\mathcal{H})$-module,

(v) *$\mathcal{S}$ coincides with the set of those f in $\Lambda(\mathcal{G})$ such that $\Lambda(\mathcal{G}/\mathcal{J})/\varphi_{\mathcal{J}}(f)\Lambda(\mathcal{G}/\mathcal{J})$ is a finitely generated right $\mathcal{O}$-module,*

(vi) *$\mathcal{S}$ coincides with the set of those f in $\Lambda(\mathcal{G})$ such that $\Omega(\mathcal{G}/\mathcal{J})/\psi_{\mathcal{J}}(f)\Omega(\mathcal{G}/\mathcal{J})$ is a finitely generated right $\mathbb{F}$-module,*

(vii) *$\mathcal{S}$ coincides with the set of those f in $\Lambda(\mathcal{G})$ such that multiplication with $\psi_{\mathcal{J}}(f)$ from the left induces an injection $\Omega(\mathcal{G}/\mathcal{J}) \hookrightarrow \Omega(\mathcal{G}/\mathcal{J})$.*

Proof. The proof is almost identical to ([CFK+05], Lemmata 2.1, 2.2). First note that a $\Lambda(\mathcal{H})$-module is finitely generated over $\Lambda(\mathcal{H})$ if and only if it is finitely generated over $\Lambda(\mathcal{J})$ since $\mathcal{J}$ is of finite index in $\mathcal{H}$, compare ([Sch11], Chapter IV, §19, Corollary 19.4 iv). Writing $N = \Lambda(\mathcal{G})/\Lambda(\mathcal{G})f$ for any element $f \in \Lambda(\mathcal{G})$ we have

$$N_{\mathcal{J}} \cong \Lambda(\mathcal{G}/\mathcal{J})/\Lambda(\mathcal{G}/\mathcal{J})\varphi_{\mathcal{J}}(f) \quad \text{and} \quad N/\mathfrak{m}(\mathcal{J})N \cong \Omega(\mathcal{G}/\mathcal{J})/\Omega(\mathcal{G}/\mathcal{J})\psi_{\mathcal{J}}(f),$$

where $N_{\mathcal{J}}$ denote the coinvariants and $\mathfrak{m}(\mathcal{J})$ is the maximal ideal of the local ring $\Lambda(\mathcal{J})$, compare proposition A.8.1. For the above isomorphisms note that for any ring R, any ideal I of R and for a R-module M passing to the quotient M/IM is right exact. The topological Nakayama lemma, see ([Bru66], Corollary 1.5), for the local pseudo-compact ring $\Lambda(\mathcal{J})$ now implies assertions (i) and (ii).

Now, as in the proof of ([CFK+05], Lemma 2.1), we choose a lifting Γ' of $\mathcal{G}/\mathcal{H}$ to $\mathcal{G}/\mathcal{J}$ so that $\mathcal{G}/\mathcal{J} = \mathcal{H}/\mathcal{J} \rtimes \Gamma'$. Γ' acts on $\mathcal{H}/\mathcal{J}$ by conjugation and we can find an open subgroup Π of Γ' that acts trivially on $\mathcal{H}/\mathcal{J}$ since the latter group is finite. Then, $\Pi \cong \mathbb{Z}_p$ and Π lies in the center of $\mathcal{G}/\mathcal{J}$. We note that for $\Omega(\Pi) = \mathbb{F}[[\Pi]]$ we have a topological isomorphism

$$\Omega(\Pi) \cong \mathbb{F}[[T]], \tag{A.8.3}$$

see ([Sch11], Chapter IV, §20, Proposition 20.1 and its proof). Hence, $\Omega(\Pi)$ is discrete valuation ring and, in particular, a principal ideal domain. Moreover, Π is of finite index in $\mathcal{G}/\mathcal{J}$ and therefore $\Omega(\mathcal{G}/\mathcal{J})$ is a free $\Omega(\Pi)$-module of finite rank, just reduce the coefficients modulo π in the proof of ([Sch11], Chapter IV, §19, Corollary 19.4 iv). For any $f \in \Lambda(\mathcal{G})$ consider the exact sequence

$$0 \to \ker(\cdot\psi_{\mathcal{J}}(f)) \to \Omega(\mathcal{G}/\mathcal{J}) \xrightarrow{\cdot\psi_{\mathcal{J}}(f)} \Omega(\mathcal{G}/\mathcal{J}) \to \operatorname{coker}(\cdot\psi_{\mathcal{J}}(f)) \to 0. \tag{A.8.4}$$

Now assume that f satisfies the condition of (iii). Then the above sequence reduces to a short exact sequence $0 \to \Omega(\mathcal{G}/\mathcal{J}) \to \Omega(\mathcal{G}/\mathcal{J}) \to \operatorname{coker}(\cdot\psi_{\mathcal{J}}(f)) \to 0$. Tensoring this exact sequence with the quotient field of $\Omega(\Pi)$, we conclude that $\operatorname{coker}(\cdot\psi_{\mathcal{J}}(f))$ must be a torsion $\Omega(\Pi)$-module. We consider $\operatorname{coker}(\cdot\psi_{\mathcal{J}}(f))$ as a finitely generated torsion $\mathbb{F}[[T]]$-module via (A.8.3) and choose $\mathbb{F}[[T]]$-generators $x_1, \ldots, x_k$. But then the annihilator of each x_i must be of the form $\mathbb{F}[[T]]T^{n_i}$ since $\mathbb{F}[[T]]$ is a DVR. It follows that $\operatorname{coker}(\cdot\psi_{\mathcal{J}}(f))$ is finitely generated over $\mathbb{F}$ and therefore f belongs to $\mathcal{S}$ by the characterization (ii).

On the other hand if f belongs to $\mathcal{S}$, then, by (ii), $\operatorname{coker}(\cdot\psi_{\mathcal{J}}(f))$ must be a torsion $\Omega(\Pi)$-module. If this were not true, then, by the structure theory of finitely generated modules over

PIDs, $\mathrm{coker}(\cdot\psi_{\mathcal{J}}(f))$ would contain a copy of $\Omega(\Pi) \cong \mathbb{F}[[T]]$ and then could not be finitely generated over $\mathbb{F}$, which would contradict (ii). But if $\mathrm{coker}(\cdot\psi_{\mathcal{J}}(f))$ is a torsion $\Omega(\Pi)$-module, then tensoring (A.8.4) with the quotient field of $\Omega(\Pi)$ shows that $\ker(\cdot\psi_{\mathcal{J}}(f))$ is $\Omega(\Pi)$-torsion. But this implies that $\ker(\cdot\psi_{\mathcal{J}}(f)) = 0$ since $\ker(\cdot\psi_{\mathcal{J}}(f))$ is contained in the finitely generated free $\Omega(\Pi)$-module $\Omega(\mathcal{G}/\mathcal{J})$. This completes the proof of (iii).

Now, since Π lies in the center of $\mathcal{G}/\mathcal{J}$, the ring $\Omega(\mathcal{G}/\mathcal{J})$ is an $\Omega(\Pi)$-algebra. In particular, for any $f \in \Lambda(\mathcal{G})$, multiplication with $\psi_{\mathcal{J}}(f)$ from the left on $\Omega(\mathcal{G}/\mathcal{J})$ is $\Omega(\Pi)$-left-linear. Recall that an endomorphism of finite dimensional vector spaces is injective if and only if it is surjective if and only if it is an isomorphism. Writing $Q(\Omega(\Pi))$ for the quotient ring of $\Omega(\Pi)$, we know by (iii) and since $\Omega(\mathcal{G}/\mathcal{J})$ does not contain non-trivial $\Omega(\Pi)$-torsion that f belongs to $\mathcal{S}$ if and only if multiplication by $\psi_{\mathcal{J}}(f)$ from the right induces a $Q(\Omega(\Pi))$-linear isomorphism

$$\cdot\psi_{\mathcal{J}}(f) : Q(\Omega(\Pi)) \otimes_{\Omega(\Pi)} \Omega(\mathcal{G}/\mathcal{J}) \longrightarrow Q(\Omega(\Pi)) \otimes_{\Omega(\Pi)} \Omega(\mathcal{G}/\mathcal{J}) \tag{A.8.5}$$

of finite dimensional $Q(\Omega(\Pi))$-vector spaces. So if f belongs to $\mathcal{S}$, then, in particular, there is an element $x \in Q(\Omega(\Pi)) \otimes_{\Omega(\Pi)} \Omega(\mathcal{G}/\mathcal{J})$ such that $x \cdot \psi_{\mathcal{J}}(f) = 1$. The element

$$1 - \psi_{\mathcal{J}}(f) \cdot x$$

then lies in the kernel of $\cdot\psi_{\mathcal{J}}(f)$, which is trivial, and hence $\psi_{\mathcal{J}}(f)\cdot x = 1$. Here, of course, we write $\psi_{\mathcal{J}}(f)$ also for its image $1 \otimes \psi_{\mathcal{J}}(f)$ in $Q(\Omega(\Pi)) \otimes_{\Omega(\Pi)} \Omega(\mathcal{G}/\mathcal{J})$. But $\psi_{\mathcal{J}}(f) \cdot x = 1$ implies that multiplication with $\psi_{\mathcal{J}}(f)$ from the left is surjective on $Q(\Omega(\Pi)) \otimes_{\Omega(\Pi)} \Omega(\mathcal{G}/\mathcal{J})$. In fact, for any y in $Q(\Omega(\Pi)) \otimes_{\Omega(\Pi)} \Omega(\mathcal{G}/\mathcal{J})$, xy maps to y under $\psi_{\mathcal{J}}(f)\cdot$, i.e., under mutliplication with $\psi_{\mathcal{J}}(f)$ from the left. Hence $\psi_{\mathcal{J}}(f)\cdot$ is an automorphism of the $Q(\Omega(\Pi))$-vector space $Q(\Omega(\Pi)) \otimes_{\Omega(\Pi)} \Omega(\mathcal{G}/\mathcal{J})$. In an entirely similar fashion one shows that if $\psi_{\mathcal{J}}(f)\cdot$ is an automorphism of the $Q(\Omega(\Pi))$-vector space $Q(\Omega(\Pi))\otimes_{\Omega(\Pi)}\Omega(\mathcal{G}/\mathcal{J})$, then $\cdot\psi_{\mathcal{J}}(f)$ is an automorphism of the $Q(\Omega(\Pi))$-vector space $Q(\Omega(\Pi)) \otimes_{\Omega(\Pi)} \Omega(\mathcal{G}/\mathcal{J})$.

But $\psi_{\mathcal{J}}(f)\cdot$ is an automorphism of the $Q(\Omega(\Pi))$-vector space $Q(\Omega(\Pi)) \otimes_{\Omega(\Pi)} \Omega(\mathcal{G}/\mathcal{J})$ if and only if multiplication with $\psi_{\mathcal{J}}(f)$ from the left induces an injection $\Omega(\mathcal{G}/\mathcal{J}) \hookrightarrow \Omega(\mathcal{G}/\mathcal{J})$, again since $\Omega(\mathcal{G}/\mathcal{J})$ does not contain non-trivial $\Omega(\Pi)$-torsion. We have shown that (vii) holds. (iv), (v), (vi) are now deduced from (vii) by reversing the arguments used for (i), (ii) and (iii), this time for right modules. □

We next state the analogue of the useful criterion ([CFK+05], Proposition 2.3) for finitely generated modules to be $\mathcal{S}$-torsion.

Proposition A.8.3. *For a finitely generated $\Lambda(\mathcal{G})$-module N the following are equivalent*

(i) N is finitely generated as a $\Lambda(\mathcal{H})$-module,

(ii) N is $\mathcal{S}$-torsion.

Proof. Using lemma A.8.2, one checks immediately that the proof of ([CFK+05], Proposition 2.3) also works for $\mathcal{O}$-coefficients. □

One can now deduce the important analogue of theorem ([CFK⁺05], Theorem 2.4).

Theorem A.8.4. *The set $\mathcal{S}$ is closed under mutliplication and it satisfies the left and right Ore conditions. Moreover, $\mathcal{S}$ contains no zero divisors.*

Proof. Using proposition A.8.3 and lemma A.8.2, one deduces the result just as one proves ([CFK⁺05], Theorem 2.4). □

Ore sets have been considered in a more general setting in [Wit03] and the Ore sets defined in loc. cit., in our setting and under the additional assumption that $\mathcal{G}$ contains no element of order p, coincide with our $\mathcal{S}$, which is proved in the following lemma. Let us first recall the following well-known facts.

Proposition A.8.5. *Let G be a profinite group. For the global dimension of $\mathcal{O}[[G]]$ we have*

$$\mathrm{gldim}(\mathcal{O}[[G]]) = \mathrm{gldim}(\mathcal{O}) + \mathrm{cd}_p G = 1 + \mathrm{cd}_p G.$$

If G is a compact p-adic Lie group with no elements of order p and dimension n as a p-adic Lie group, then $\mathrm{cd}_p G = n$. In particular, in this case $\mathcal{O}[[G]]$ has finite global dimension.

Proof. For the first fact see ([Bru66], Theorem 4.1) and recall that discrete valuation rings are regular local rings of Krull dimension 1 and that the Krull dimension coincides with the global dimension, see ([Ser56], Théorème 1) or ([Wei94], Main Theorem 4.4.16). For the second fact see ([Ser65], Corollaire (1)). □

Lemma A.8.6. *Assume that $\mathcal{G}$ contains no element of order p. Then, the set $\mathcal{S}$ coincides with those elements $f \in \Lambda(\mathcal{G})$ such that*

$$\Lambda(\mathcal{G}) \xrightarrow{\cdot f} \Lambda(\mathcal{G}),$$

considered as a complex, say, in degree 0 and 1, is a perfect complex of $\Lambda(\mathcal{H})$-modules, i.e., it is quasi-isomorphic to a bounded complex of finitely generated projective $\Lambda(\mathcal{H})$-modules.

Proof. Let f be an element of $\mathcal{S}$. Then, since $\Lambda(\mathcal{H})$ has finite global dimension by proposition A.8.5, there is a finite projective resolution

$$0 \to P_d \to \cdots \to P_1 \to \Lambda(\mathcal{G})/\Lambda(\mathcal{G})f \to 0,$$

where the P_i can be chosen to be finitely generated over $\Lambda(\mathcal{H})$ since $\Lambda(\mathcal{H})$ is Noetherian, compare ([Wei94], pd Lemma 4.1.6). But $\Lambda(\mathcal{G}) \xrightarrow{\cdot f} \Lambda(\mathcal{G})$, since f is a non-zero divisor, is quasi-isomorphic to $\Lambda(\mathcal{G})/\Lambda(\mathcal{G})f$ (concentrated in degree 1) and the latter is quasi-isomorphic to $0 \to P_d \to \cdots \to P_1 \to 0$, (where P_1 is placed in degree 1) which shows one inclusion of the claim.

Next assume that $\Lambda(\mathcal{G}) \xrightarrow{\cdot f} \Lambda(\mathcal{G})$ is a perfect complex, quasi-isomorphic to the bounded complex $(Q_k, d_k)_k$ consisting of finitely generated projective $\Lambda(\mathcal{H})$-modules Q_i. Then, we have

$$\Lambda(\mathcal{G})/\Lambda(\mathcal{G})f \cong \ker(d_1)/\mathrm{im}(d_0).$$

But $\ker(d_1)$, as a submodule of Q_1, is finitely generated over $\Lambda(\mathcal{H})$ since $\Lambda(\mathcal{H})$ is Noetherian, which shows that f belongs to $\mathcal{S}$. □

A.8.2 Functorial properties

We will prove some functoriality results for the canonical Ore set $\mathcal{S}$. We will be interested in the functoriality with respect to the groups $\mathcal{H} \subset \mathcal{G}$ and with respect to the coefficient ring $\mathcal{O}$. Let us start with the groups.

Assume that G is an open subgroup of $\mathcal{G}$, not necessarily normal. Then G has finite index in $\mathcal{G}$ since $\mathcal{G}$ is compact. Define $H := G \cap \mathcal{H}$. Then, H is normal in G and we have an embedding $G/H \hookrightarrow \mathcal{G}/\mathcal{H} \cong \mathbb{Z}_p$. Hence, either $G/H = \{1\}$ or $G/H \cong \mathbb{Z}_p$. But G is of finite index in $\mathcal{G}$, so the image of G/H in $\mathcal{G}/\mathcal{H}$ is of finite index and therefore we must have

$$G/H \cong \mathbb{Z}_p.$$

For this setting we have two examples in mind.

Example A.8.7. (i) Let K be a perfect field, consider a p-adic Lie extension K_∞/K containing the cyclotomic $\mathbb{Z}_p$-extension K_{cyc} and write $\mathcal{G}$ for its Galois group $G(K_\infty/K)$. We define $\mathcal{H} = G(K_\infty/K_{cyc})$ so that $\mathcal{G}/\mathcal{H} \cong \mathbb{Z}_p$. Now let F/K be a finite Galois subextension of K_∞/K and write $G = G(K_\infty/F)$, which is open and normal in $\mathcal{G}$. We then have

$$H \overset{\text{def}}{=} G \cap \mathcal{H} = G\big(K_\infty/(K_{\text{cyc}}F)\big) = G(K_\infty/F_{\text{cyc}}),$$

where we write F_{cyc} for the cyclotomic $\mathbb{Z}_p$-extension of F.

(ii) The second example is one where G, in general, is not normal in $\mathcal{G}$. Let K be a number field, fix an algebraic closure $\bar{K}$, consider a p-adic Lie extension K_∞/K inside $\bar{K}$ containing the cyclotomic $\mathbb{Z}_p$-extension K_{cyc} and write $\mathcal{G}$ for its Galois group $G(K_\infty/K)$. We define $\mathcal{H} = G(K_\infty/K_{cyc})$ so that $\mathcal{G}/\mathcal{H} \cong \mathbb{Z}_p$. Now, let $\mathfrak{q}$ be a non-archimedean prime of K, fix an algebraic closure $\bar{K}_\mathfrak{q}$ and fix an embedding $\bar{K} \subset \bar{K}_\mathfrak{q}$. Write $\bar{\nu}$ for the prime of K_∞ above $\mathfrak{q}$ determined by the embedding $\bar{K} \subset \bar{K}_\mathfrak{q}$ and suppose that the decomposition group of $\bar{\nu}$ which we denote by $G := \mathcal{G}_{\bar{\nu}} \cong G(K_{\infty,\bar{\nu}}/K_\mathfrak{q})$ is of finite index in $\mathcal{G}$. Write $Z = K_\infty^{\mathcal{G}_{\bar{\nu}}}$ for the fixed field of the decomposition group $\mathcal{G}_{\bar{\nu}}$, which is a finite extension of K. Then, we have

$$H \overset{\text{def}}{=} G \cap \mathcal{H} = G\big(K_\infty/(K_{\text{cyc}}Z)\big) = G(K_\infty/Z_{\text{cyc}}),$$

and $G(K_\infty/Z_{\text{cyc}}) \cong G(K_{\infty,\bar{\nu}}/(K_\mathfrak{q})_{cyc})$.

We recall the following well-known result.

Lemma A.8.8. *$\Lambda(\mathcal{G})$ is free as a right (resp. left) $\Lambda(G)$-module of rank $n := [\mathcal{G} : G]$ generated by representatives $\sigma_1, \ldots, \sigma_n \in \mathcal{G}$ of the left (resp. right) cosets of G in $\mathcal{G}$. Moreover, $\Lambda(\mathcal{G}) \cong \operatorname{Ind}_{\mathcal{G}}^{G} \Lambda(G)$ as left (resp. right) $\mathcal{G}$-modules.*

Proof. For the first part see ([Sch11], Chapter IV, §19, Corollary 19.4 iv), which implies that for left coset representatives $\sigma_1, \ldots, \sigma_n \in \mathcal{G}$ (the case of right coset representatives works analogously) we have an isomorphism

$$\bigoplus_{i=1}^{n} \sigma_i \Lambda(G) \xrightarrow{\sim} \Lambda(\mathcal{G}).$$

But the module on the left carries a left $\mathcal{G}$-action (given by $g.(\sigma_i\lambda) = \sigma_{i(g)} g' \lambda$, where $i(g) \in \{1, \ldots, n\}$ and $g' \in G$ are such that $g\sigma_i = \sigma_{i(g)} g'$) such that the map is left $\mathcal{G}$-equivariant and such that $\bigoplus_{i=1}^{n} \sigma_i \Lambda(G) \cong \mathrm{Ind}_{\mathcal{G}}^{G} \Lambda(G)$, compare ([Lan05] XVIII, Theorem 7.3) for the last isomorphism. □

Recall that a finitely generated left $\Lambda(G)$-module M is also finitely presented since $\Lambda(G)$ is Noetherian ($\mathcal{G}$ and G are compact p-adic Lie groups). Moreover, $\Lambda(\mathcal{G})$ is pseudo-compact, both as a left $\Lambda(\mathcal{G})$-module and as a right $\Lambda(G)$-module. It follows by ([Wit03], Proposition 1.14) that

$$\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M \cong \Lambda(\mathcal{G}) \hat{\otimes}_{\Lambda(G)} M.$$

Corollary A.8.9. *For a finitely generated left $\Lambda(G)$-module M we have a natural isomorphism*

$$\mathrm{Ind}_{\mathcal{G}}^{G} M = \mathbb{Z}_p[\mathcal{G}] \otimes_{\mathbb{Z}_p[G]} M \xrightarrow{\sim} \Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M$$

of left $\Lambda(\mathcal{G})$-modules.

Proof. Using the previous lemma A.8.8 we have

$$\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M \cong \Big(\bigoplus_{i=1}^{n} \sigma_i \Lambda(G) \Big) \otimes_{\Lambda(G)} M \cong \bigoplus_{i=1}^{n} \sigma_i M \cong \mathrm{Ind}_{\mathcal{G}}^{G} M,$$

where $\bigoplus_{i=1}^{n} \sigma_i M$ is equipped with the left $\mathcal{G}$-action defined by $g.(\sigma_i m) = \sigma_{i(g)} g' m$, where $i(g) \in \{1, \ldots, n\}$ and $g' \in G$ are such that $g\sigma_i = \sigma_{i(g)} g'$. □

The Ore-set for G is defined by

$$S = \{ f \in \Lambda(G) \mid \Lambda(G)/\Lambda(G) f \text{ is finitely generated as a } \Lambda(H)\text{−module} \}.$$

We also consider the two Ore sets

$$S^* := \bigcup_{n=0}^{\infty} p^n S \qquad \text{and} \qquad \mathcal{S}^* := \bigcup_{n=0}^{\infty} p^n \mathcal{S}.$$

Let σ be any element in $\mathcal{G}$. We have a conjugation map $t_\sigma : \mathcal{G} \to \mathcal{G} \subset \Lambda(\mathcal{G})^\times, g \mapsto \sigma g \sigma^{-1}$ which induces an $\mathcal{O}$-algebra isomorphism

$$t_\sigma : \Lambda(\mathcal{G}) \to \Lambda(\mathcal{G}).$$

Remark A.8.10. (i) Note that the map t_σ coincides with the $\mathcal{O}$-algebra isomorphism $\Lambda(\mathcal{G}) \to \Lambda(\mathcal{G}), \lambda \mapsto \sigma\lambda\sigma^{-1}$.

(ii) Likewise, we get $\mathcal{O}$-algebra isomorphisms

$$t_\sigma : \Lambda(G) \to \Lambda(\sigma G\sigma^{-1}) \qquad \text{and} \qquad t_\sigma : \Lambda(H) \to \Lambda(\sigma H\sigma^{-1})$$

for any $\sigma \in \mathcal{G}$. If G is normal in $\mathcal{G}$, then H is normal in $\mathcal{G}$ and t_σ restricts to isomorphisms of $\Lambda(G)$ and $\Lambda(H)$, respectively.

(iii) For any $\sigma \in \mathcal{G}$ we have a commutative diagram

$$\begin{array}{ccccc} \Lambda(H) & \hookrightarrow & \Lambda(G) & \hookrightarrow & \Lambda(\mathcal{G}) \\ \downarrow t_\sigma & & \downarrow t_\sigma & & \downarrow t_\sigma \\ \Lambda(\sigma H\sigma^{-1}) & \hookrightarrow & \Lambda(\sigma G\sigma^{-1}) & \hookrightarrow & \Lambda(\mathcal{G}). \end{array} \tag{A.8.6}$$

For any $\sigma \in \mathcal{G}$ we also define

$$S_\sigma = \{f \in \Lambda(\sigma G\sigma^{-1}) \mid \Lambda(\sigma G\sigma^{-1})/\Lambda(\sigma G\sigma^{-1})f \text{ is finitely generated as a } \Lambda(\sigma H\sigma^{-1})\text{–module}\}$$

and $S^*_\sigma = \bigcup_n p^n S_\sigma$

Remark A.8.11. Note that $\sigma H\sigma^{-1} = \sigma G\sigma^{-1} \cap \mathcal{H}$, so had we started with the group $\sigma G\sigma^{-1}$ instead of G then S_σ would be the Ore set associated to $\sigma G\sigma^{-1}$ and $\sigma G\sigma^{-1} \cap \mathcal{H}$. Moreover, if G is normal in $\mathcal{G}$, then $S_\sigma = S$ for any $\sigma \in \mathcal{G}$.

We can now show how twisting through t_σ affects the Ore set S.

Lemma A.8.12. *We have $t_\sigma(S) = S_\sigma$ and $t_\sigma(S^*) = S^*_\sigma$ for every σ in $\mathcal{G}$. In particular, if G is normal in $\mathcal{G}$, then $t_\sigma(S) = S$ and $t_\sigma(S^*) = S^*$ for every σ in $\mathcal{G}$.*

Proof. The second statement follows from the first and the second equality of the first statement follows from the first equality. Let f be an element of S and choose $x_1, \ldots, x_k \in \Lambda(G)$ such that the images of the x_i in $\Lambda(G)/\Lambda(G)f$ generate $\Lambda(G)/\Lambda(G)f$ as a $\Lambda(H)$-module. We claim that (the images of) $t_\sigma(x_1), \ldots, t_\sigma(x_k)$ generate $\Lambda(\sigma G\sigma^{-1})/\Lambda(\sigma G\sigma^{-1})t_\sigma(f)$ as a $\Lambda(\sigma H\sigma^{-1})$-module, which would imply that $t_\sigma(f)$ belongs to S_σ. Indeed, for any λ in $\Lambda(\sigma G\sigma^{-1})$ consider $t_{\sigma^{-1}}(\lambda) \in \Lambda(G)$. We can find $\lambda_1, \ldots, \lambda_k \in \Lambda(H)$ and $\lambda' \in \Lambda(G)$ such that

$$t_{\sigma^{-1}}(\lambda) = \sum_{i=1}^k \lambda_i x_i + \lambda' f.$$

Applying t_σ to both sides yields

$$\lambda = \sum_{i=1}^{k} t_\sigma(\lambda_i) t_\sigma(x_i) + t_\sigma(\lambda') t_\sigma(f),$$

where $t_\sigma(\lambda_i) \in \Lambda(\sigma H \sigma^{-1})$ and $t_\sigma(\lambda') \in \Lambda(\sigma G \sigma^{-1})$. This shows that the $t_\sigma(x_1), \dots, t_\sigma(x_k)$ indeed generate $\Lambda(\sigma G \sigma^{-1})/\Lambda(\sigma G \sigma^{-1}) t_\sigma(f)$ over $\Lambda(\sigma H \sigma^{-1})$. It follows that $t_\sigma(S) \subseteq S_\sigma$ for all $\sigma \in \mathcal{G}$. In the same way one shows that $t_{\sigma^{-1}}(S_\sigma) \subseteq S$, i.e., $S_\sigma \subseteq t_\sigma(S)$. □

Remark A.8.13. (i) The previous lemma applied to $G = \mathcal{G}$ shows that for $\sigma \in \mathcal{G}$ we always have $t_\sigma(\mathcal{S}) = \mathcal{S}$, i.e., any Ore set of the form $\mathcal{S} \subset \Lambda(\mathcal{G})$ is invariant under twists for $\sigma \in \mathcal{G}$.

(ii) The proof also works for any ring isomorphism $\iota : \Lambda(G) \to \Lambda(G)$ that restricts to an isomorphism of $\Lambda(H)$, implying that $\iota(S) \subset S$ and hence also $\iota(S) = S$.

Lemma A.8.14. *Let M be a $\Lambda(G)$-module which is finitely generated as a $\Lambda(H)$-module. Then, $\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M$ is finitely generated as a $\Lambda(\mathcal{H})$-module.*

Proof. Let $\sigma_1, \dots, \sigma_n \in \mathcal{G}$ be representatives of the (left-) cosets of G in $\mathcal{G}$. Then, by corollary A.8.9, we have an isomorphism

$$\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M \cong \mathbb{Z}_p[\mathcal{G}] \otimes_{\mathbb{Z}_p[G]} M \cong \bigoplus_{i=1}^{n} \sigma_i M$$

where each $\sigma_i M$ can be considered as a $\sigma_i \Lambda(G) \sigma_i^{-1}$-module. An element $\lambda \in \sigma_i \Lambda(G) \sigma_i^{-1}$ acts on an element $\sigma_i x$ of $\sigma_i M$ by $\lambda \sigma_i x = \sigma_i t_{\sigma_i^{-1}}(\lambda) x$, where we note that $t_{\sigma_i^{-1}}(\lambda)$ belongs to $\Lambda(G)$ and therefore acts on M.

Now, let $x_1, \dots, x_k$ be a set of $\Lambda(H)$-generators of M, then $\sigma_i x_1, \dots, \sigma_i x_k$ generate $\sigma_i M$ over $\sigma_i \Lambda(H) \sigma_i^{-1}$. Since $\sigma_i \Lambda(H) \sigma_i^{-1} \subset \Lambda(\mathcal{H})$ for all $i = 1, \dots, n$, we see that $\sigma_i M$ is contained in the $\Lambda(\mathcal{H})$-submodule of $\bigoplus_{j=1}^{n} \sigma_j M$ generated by $\sigma_i x_1, \dots, \sigma_i x_k$. Hence, $\sigma_1 x_1, \dots, \sigma_1 x_k, \sigma_2 x_1, \dots, \sigma_n x_k$ generate $\bigoplus_{j=1}^{n} \sigma_j M$ over $\Lambda(\mathcal{H})$. In particular, $\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M$ is finitely generated over $\Lambda(\mathcal{H})$. □

Corollary A.8.15. *We have $S \subseteq \mathcal{S}$ and $S^* \subseteq \mathcal{S}^*$.*

Proof. The second equality follows from the first. Let f be an element of S. Then, we have an isomorphism

$$\Lambda(\mathcal{G})/\Lambda(\mathcal{G}) f \cong \Lambda(\mathcal{G}) \otimes_{\Lambda(G)} (\Lambda(G)/\Lambda(G) f)$$

and the corollary follows from the previous lemma A.8.14. □

Corollary A.8.16. *Let M be a finitely generated $\Lambda(G)$-module which is S^*-torsion. Then, the module $\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M$ is finitely generated over $\Lambda(\mathcal{G})$ and it is $\mathcal{S}^*$-torsion.*

Proof. For any module N denote by $N(p)$ the p-primary torsion part of N. Then $M/(M(p))$ is S-torsion and, by proposition A.8.3, $M/(M(p))$ is finitely generated over $\Lambda(H)$. By lemma A.8.14, $\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} \big(M/(M(p))\big)$ is finitely generated as a $\Lambda(\mathcal{H})$-module. The surjection

$$\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} \big(M/(M(p))\big) \twoheadrightarrow \big(\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M\big)\Big/\Big(\big(\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M\big)(p)\Big)$$

implies that $\big(\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M\big)\Big/\Big(\big(\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M\big)(p)\Big)$ is finitely generated over $\Lambda(\mathcal{H})$ and hence that it is $\mathcal{S}$-torsion by proposition A.8.3. Hence, $\Lambda(\mathcal{G}) \otimes_{\Lambda(G)} M$ is $\mathcal{S}^*$-torsion. □

Let us now study the functoriality with respect to the coefficient ring. Let $\mathcal{O}'$ be a complete discrete valuation ring with uniformizer π' containing the complete DVR $\mathcal{O}$ with uniformizer π. We do not assume that the residue fields are finite. The topology of $\mathcal{O}$, resp. $\mathcal{O}'$, is the π- resp π'-adic one, i.e., the topology induced by the ideals $\pi^n\mathcal{O}$, $n \geq 1$, and $(\pi')^n\mathcal{O}'$, respectively. For any topological ring A, we will write

$$\mathcal{PC}(A)$$

for the category of pseudo-compact A-modules with continuous homomorphisms as morphisms, which is an abelian category, see ([Gab62], Chapitre IV, §3, Théorème 3) - as remarked in [Wit03], the proof in [Gab62] of this fact does not require A to be pseudo-compact.

The rings $\mathcal{O}/\pi^n\mathcal{O}$ have finite length n as $\mathcal{O}$-modules which follows immediately from the fact that $\mathcal{O}/\pi\mathcal{O}$ has length 1 and by induction using the obvious exact sequences. Therefore, $\mathcal{O}$ is pseudo-compact as a module over itself. The same applies to $\mathcal{O}'$. Important for our purposes is the following

Proposition A.8.17. *Assume that $\mathcal{O}'/\mathcal{O}$ has finite ramification index, i.e., we can write $\pi = u \cdot (\pi')^e$ for some unit $u \in (\mathcal{O}')^\times$ and some $e \in \mathbb{N}$. Then, the functor*

$$\mathcal{PC}(\mathcal{O}) \longrightarrow \mathcal{PC}(\mathcal{O}'), \quad N \longrightarrow \mathcal{O}'\hat{\otimes}_{\mathcal{O}}N$$

is exact.

Proof. For the right exactness see the general result ([Wit03], Proposition 1.10) which uses only that $\mathcal{O}'$ is pseudo-compact as a module over itself (and the fact that the ideals $(\pi')^n\mathcal{O}'$ are also $\mathcal{O}$-modules). For the left exactness let

$$\varphi : N \hookrightarrow M$$

be a continuous injection of pseudo-compact $\mathcal{O}$-modules. For any open $\mathcal{O}$-submodule U of M, M/U is discrete, see (loc. cit., Proposition 1.2). Therefore $\varphi^{-1}(U)$ is both, open and closed in N. $\mathcal{O}'$ is torsion-free over the principal ideal domain $\mathcal{O}$ and therefore flat over $\mathcal{O}$, see ([Rot09], §3.3, Corollary 3.50). Hence for any open submodule U of M we get an injection

$$\mathcal{O}' \otimes_{\mathcal{O}} \big(N/\varphi^{-1}(U)\big) \hookrightarrow \mathcal{O}' \otimes_{\mathcal{O}} \big(M/U\big). \tag{A.8.7}$$

Since N and M are pseudo-compact $N/\varphi^{-1}(U)$ and M/U are of finite length as $\mathcal{O}$-modules, see ([Wit03], Proposition 1.2). In particular, $N/\varphi^{-1}(U)$ and M/U are both finitely generated over $\mathcal{O}$. But for finitely generated $\mathcal{O}$-modules T one has $\mathcal{O}'\hat{\otimes}_{\mathcal{O}}T = \mathcal{O}' \otimes_{\mathcal{O}} T$. Indeed, all finitely generated $\mathcal{O}$-modules are finitely presented and by the five-lemma it is sufficient to prove the equality for finitely generated free $\mathcal{O}$-modules. Since the completed tensor product commutes with finite products it is sufficient to show the identity for $T = \mathcal{O}$, but in this case we have

$$\mathcal{O}'\hat{\otimes}_{\mathcal{O}}\mathcal{O} \stackrel{\text{def}}{=} \varprojlim_{m,n} \big(\mathcal{O}'/(\pi')^m \otimes_{\mathcal{O}} \mathcal{O}/\pi^n\big) = \varprojlim_{n} \big(\mathcal{O}'/(\pi')^{n\cdot e} \otimes_{\mathcal{O}} \mathcal{O}/\pi^n\big) \cong \varprojlim_{n} \mathcal{O}'/(\pi')^{n\cdot e} = \mathcal{O}',$$

where we used the isomorphism $\mathcal{O}'/(\pi')^{n\cdot e} \otimes_{\mathcal{O}} \mathcal{O}/\pi^n \cong \mathcal{O}'/(\pi')^{n\cdot e}$, which holds by the finite ramification assumption.

Hence we can rewrite (A.8.7) as

$$\mathcal{O}'\hat{\otimes}_{\mathcal{O}}\big(N/\varphi^{-1}(U)\big) \hookrightarrow \mathcal{O}'\hat{\otimes}_{\mathcal{O}}\big(M/U\big).$$

Passing to the projective limit (which is left exact) over all open submodules U of M and using ([Wit03], Proposition 1.7), which states that the completed tensor product commutes with projective limits $N = \varprojlim_i N_i$ of filtered systems $(N_i)_i$ such that the structure maps $N \to N_i$ are surjective, we get

$$\mathcal{O}'\hat{\otimes}_{\mathcal{O}}\big(\varprojlim_{U} N/\varphi^{-1}(U)\big) \hookrightarrow \mathcal{O}'\hat{\otimes}_{\mathcal{O}}\big(\varprojlim_{U} M/U\big), \tag{A.8.9}$$

note that filtered means directed and that the systems $(M/U)_U$ and $(N/\varphi^{-1}(U))_U$ are directed. We certainly have a homeomorphism $M \cong \varprojlim_U M/U$. Moreover, we have $\bigcap_U \varphi^{-1}(U) = \{0\}$, where U ranges through all open submodules of M. Indeed, if x belongs to $\bigcap_U \varphi^{-1}(U)$, then $\varphi(x) \in \bigcap_U U = \{0\}$ (M is Hausdorff), hence x belongs to the kernel of φ which is trivial. We have noted above that all submodules of the form $\varphi^{-1}(U)$, where U is an open submodule of M, are closed in N. It follows from ([Gab62], Chapitre IV, §3, Proposition 10) that $N \cong \varprojlim_U N/\varphi^{-1}(U)$ (and this is a homeomorphism since it is a continuous bijection of pseudo-compact modules, compare (loc. cit, Chapitre IV, §3, proof of Théorème 3)). Hence, the map from (A.8.9) implies that $\mathcal{O}'\hat{\otimes}_{\mathcal{O}}N \hookrightarrow \mathcal{O}'\hat{\otimes}_{\mathcal{O}}M$ is injective. □

Let us continue to assume that $\mathcal{O}'/\mathcal{O}$ has finite ramification index, i.e., we can write $\pi = u\cdot(\pi')^e$ for some unit $u \in (\mathcal{O}')^\times$ and some $e \in \mathbb{N}$. We write

$$\mathcal{S}_{\mathcal{O}} \quad \text{and} \quad \mathcal{S}_{\mathcal{O}'}$$

for the Ore sets in $\mathcal{O}[[\mathcal{G}]]$ and $\mathcal{O}'[[\mathcal{G}]]$, respectively, which are both pseudo-compact rings, see ([Sch11], Chapter IV, §19). We have

$$\mathcal{O}[[\mathcal{G}]] = \varprojlim_{n,U}(\mathcal{O}/\pi^n\mathcal{O})[\mathcal{G}/U],$$

where U runs through the open normal subgroups of $\mathcal{G}$. Since the modules $(\mathcal{O}/\pi^n\mathcal{O})[\mathcal{G}/U]$ are finite products of $\mathcal{O}/\pi^n\mathcal{O}$ they are of finite length over $\mathcal{O}$, which means that $\mathcal{O}[[\mathcal{G}]]$ and likewise $\mathcal{O}[[\mathcal{H}]]$ are also pseudo-compact as $\mathcal{O}$-modules. The same applies to the $\mathcal{O}'$-modules $\mathcal{O}'[[\mathcal{G}]]$ and $\mathcal{O}'[[\mathcal{H}]]$. We have an isomorphism

$$\mathcal{O}'\hat{\otimes}_{\mathcal{O}}\mathcal{O}[[\mathcal{G}]] = \varprojlim_{n,U}\Big((\mathcal{O}'/(\pi')^{n\cdot e}) \otimes_{\mathcal{O}} (\mathcal{O}/\pi^n)[\mathcal{G}/U]\Big) \cong \varprojlim_{n,U}(\mathcal{O}'/(\pi')^{n\cdot e})[\mathcal{G}/U] = \mathcal{O}'[[\mathcal{G}]], \quad (A.8.10)$$

where we use that, by the finite ramification assumption, we have $(\mathcal{O}'/(\pi')^{n\cdot e})\otimes_{\mathcal{O}}(\mathcal{O}/\pi^n)[\mathcal{G}/U] \cong (\mathcal{O}'/(\pi')^{n\cdot e})[\mathcal{G}/U]$.

Remark A.8.18. The author wants to thank Malte Witte for pointing out the following facts. Let M be a finitely generated $\mathcal{O}[[\mathcal{G}]]$-module, which is then finitely presented since $\mathcal{O}[[\mathcal{G}]]$ is Noetherian. Let

$$\mathcal{O}[[\mathcal{G}]]^r \to \mathcal{O}[[\mathcal{G}]]^k \to M \to 0 \quad (A.8.11)$$

be a finite presentation. Equipped with the quotient topology, M becomes a pseudo-compact $\mathcal{O}[[\mathcal{G}]]$-module, in fact, it also becomes a pseudo-compact $\mathcal{O}$-module, since $\mathcal{O}[[\mathcal{G}]]^r$ and $\mathcal{O}[[\mathcal{G}]]^k$ are pseudo-compact over $\mathcal{O}[[\mathcal{G}]]$ and $\mathcal{O}$, see ([Gab62], Chapitre IV, §3, proof of Théorème 3). Alternatively, if M already is a pseudo-compact $\mathcal{O}[[\mathcal{G}]]$-module, then its topology must coincide with the quotient topology, see loc. cit. In any case, the exact sequence in (A.8.11) is an exact sequence of pseudo-compact $\mathcal{O}$-modules.

One can now deduce that for the finitely generated $\mathcal{O}[[\mathcal{G}]]$-module there is an isomorphism of $\mathcal{O}'[[\mathcal{G}]]$-modules

$$\mathcal{O}'[[\mathcal{G}]] \otimes_{\mathcal{O}[[\mathcal{G}]]} M \cong \mathcal{O}'\hat{\otimes}_{\mathcal{O}} M \quad (A.8.12)$$

induced by the universal property of $- \otimes_{\mathcal{O}[[\mathcal{G}]]} -$. In fact, using the right-exactness of $\mathcal{O}'\hat{\otimes}_{\mathcal{O}}-$, the finite presentation (A.8.11), the five lemma and the fact that the completed tensor product commutes with finite products, one reduces to the case where $M = \mathcal{O}[[\mathcal{G}]]$, which was treated in (A.8.10). For further information on completed tensor products see also Brumer's article [Bru66].

As before, we write $\mathcal{S}^*_{\mathcal{O}} = \bigcup_{n\geq 1} p^n\mathcal{S}_{\mathcal{O}}$ and $\mathcal{S}^*_{\mathcal{O}'} = \bigcup_{n\geq 1} p^n\mathcal{S}_{\mathcal{O}'}$.

Lemma A.8.19. *We have inclusions* $\mathcal{S}_{\mathcal{O}} \subset \mathcal{S}_{\mathcal{O}'}$ *and* $\mathcal{S}^*_{\mathcal{O}} \subset \mathcal{S}^*_{\mathcal{O}'}$.

Proof. The second inclusion follows from the first. Let f be an element of $\mathcal{S}_{\mathcal{O}}$ and $\mathcal{O}[[\mathcal{H}]]^k \twoheadrightarrow \mathcal{O}[[\mathcal{G}]]/\mathcal{O}[[\mathcal{G}]]f$ be a surjection, then by right exactness of $\mathcal{O}'\hat{\otimes}_{\mathcal{O}}-$ we have

$$\mathcal{O}'[[\mathcal{H}]]^k \cong \mathcal{O}'\hat{\otimes}_{\mathcal{O}}(\mathcal{O}[[\mathcal{H}]]^k) \twoheadrightarrow \mathcal{O}'\hat{\otimes}_{\mathcal{O}}\big(\mathcal{O}[[\mathcal{G}]]/\mathcal{O}[[\mathcal{G}]]f\big) \cong \mathcal{O}'[[\mathcal{G}]]/\mathcal{O}'[[\mathcal{G}]]f,$$

hence f belongs to $\mathcal{S}_{\mathcal{O}'}$. □

Lemma A.8.20. *If M is a finitely generated $\mathcal{O}[[\mathcal{G}]]$-module, which is $\mathcal{S}^*_{\mathcal{O}}$-torsion, then the module $\mathcal{O}'[[\mathcal{G}]] \otimes_{\mathcal{O}[[\mathcal{G}]]} M$ is $\mathcal{S}^*_{\mathcal{O}'}$-torsion.*

Proof. First consider an element of the form $\lambda \otimes m$ of $\mathcal{O}'[[\mathcal{G}]] \otimes_{\mathcal{O}[[\mathcal{G}]]} M$. Let s be an element of $\mathcal{S}^*_{\mathcal{O}}$ such that $sm = 0$. Since s also belongs to $\mathcal{S}^*_{\mathcal{O}'}$ by lemma A.8.19, the left Ore condition implies that there exist $\lambda' \in \mathcal{O}'[[\mathcal{G}]]$ and $s' \in \mathcal{S}^*_{\mathcal{O}'}$ such that

$$\lambda' s = s' \lambda.$$

We get $s' \cdot (\lambda \otimes m) = \lambda' s \otimes m = \lambda' \otimes sm = 0$. For a general element $\sum_{i=1}^n \lambda_i \otimes m_i$ we can now proceed by induction on n. For $\lambda_n \otimes m_n$ let s_n be an element of $\mathcal{S}^*_{\mathcal{O}} \subset \mathcal{S}^*_{\mathcal{O}'}$ that annihilates m_n. By the Ore condition we can then find $\lambda'_n \in \mathcal{O}'[[\mathcal{G}]]$ and $s'_n \in \mathcal{S}^*_{\mathcal{O}'}$ such that $\lambda'_n s_n = s'_n \lambda_n$. Then we get

$$s'_n \cdot \sum_{i=1}^n \lambda_i \otimes m_i = \sum_{i=1}^n s'_n \lambda_i \otimes m_i = \sum_{i=1}^{n-1} s'_n \lambda_i \otimes m_i.$$

For the sum on the right, by the induction hypothesis, we can find an element $t \in \mathcal{S}^*_{\mathcal{O}'}$ that annihilates it. Hence, $ts'_n \in \mathcal{S}^*_{\mathcal{O}'}$ annihilates $\sum_{i=1}^n \lambda_i \otimes m_i$. □

A.9 The Iwasawa algebra $\Lambda(\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times)$ and its modules

Our study of the Iwasawa algebra $\Lambda(\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times)$ is motivated by the following example from arithmetic geometry. Let E/K be an elliptic curve with complex multiplication by $\mathcal{O}_K$, the ring of integers of the quadratic imaginary field K. Assume that E has good reduction above the prime p and that p splits in K into two distinct primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ with generators π and $\overline{\pi}$, respectively. We write $K_n = K(E[p^{n+1}])$ for $0 \leq n \leq \infty$ and define $G = \mathrm{Gal}(K_\infty/K)$. Moreover, we write $\kappa_1 : G \longrightarrow \mathbb{Z}_p^\times$ (respectively $\kappa_2 : G \longrightarrow \mathbb{Z}_p^\times$) for the character giving the action of G on $T_\pi E$ (respectively on $T_{\overline{\pi}} E$). The two characters induce an isomorphism

$$(\kappa_1, \kappa_2) : G \xrightarrow{\sim} \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times. \tag{A.9.1}$$

We write $\Gamma = \mathrm{Gal}(K_\infty/K_0)$ and $\Delta = \mathrm{Gal}(K_0/K)$. Under the isomorphism (A.9.1) Γ maps isomorphically onto $(1 + p\mathbb{Z}_p) \times (1 + p\mathbb{Z}_p) \cong \mathbb{Z}_p^2$ and Δ maps to $\mu_{p-1} \times \mu_{p-1}$. We now want to study the Iwasawa algebra of $G = \Delta \times \Gamma$.

We write χ_i, $i = 1, 2$, for the restriction of κ_i to Δ. So, χ_1 and χ_2 are $\mathbb{Z}_p^\times$-valued characters of the finite group Δ. Products of the form $\chi_1^{i_1} \chi_2^{i_2}$ give all characters in $\mathrm{Hom}(\Delta, \mathbb{Z}_p^\times)$ for i_1 and i_2 running through sets of representatives of $\mathbb{Z}/(p-1)$. Given such a pair (i_1, i_2) we write

$$e_{i_1,i_2} = \frac{1}{(p-1)^2} \sum_{\delta \in \Delta} \chi_1^{i_1}(\delta^{-1}) \chi_2^{i_2}(\delta^{-1}) \delta$$

for the idempotent in $\mathbb{Z}_p[\Delta]$ associated to $\chi_1^{i_1} \chi_2^{i_2}$. For any $\mathbb{Z}_p[\Delta]$-module M we write $M^{(i_1,i_2)}$ for the submodule $e_{i_1,i_2} M$ of M on which Δ acts through $\chi_1^{i_1} \chi_2^{i_2}$, yielding a decomposition

$$M = \prod_{(i_1,i_2)} M^{(i_1,i_2)}.$$

In particular, we can apply this to $M = \mathbb{Z}_p[\Delta]$ and, since $\mathbb{Z}_p$ contains the $(p-1)$-th roots of unity, we immediately see that $\mathbb{Z}_p[\Delta]^{(i_1,i_2)}$ is just a copy of $\mathbb{Z}_p$ on which Δ acts through $\chi_1^{i_1}\chi_2^{i_2}$.

Coming back to the Iwasawa algebra $\Lambda(G) \cong \mathbb{Z}_p[[\Delta \times \Gamma]] \cong \mathbb{Z}_p[\Delta][[\Gamma]]$ the above decomposition induces

$$\Lambda(G) = \prod_{(i_1,i_2)} \Lambda(G)^{(i_1,i_2)} \cong \prod_{(i_1,i_2)} \mathbb{Z}_p[\Delta]^{(i_1,i_2)}[[\Gamma]].$$

Next, we fix a topological generator u of $1 + p\mathbb{Z}_p$ and let γ_1, γ_2 be the elements of Γ such that $\kappa_1(\gamma_1) = u = \kappa_2(\gamma_2)$ and $\kappa_1(\gamma_2) = 1 = \kappa_2(\gamma_1)$. Using these generators we can define an isomorphism

$$\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T_1, T_2]], \qquad \gamma_i \longmapsto 1 + T_i, \quad i = 1, 2.$$

We see that $\Lambda(G)$ is given by $(p-1)^2$ copies of the local integral ring $\mathbb{Z}_p[[T_1, T_2]]$.

A.9.1 The Ore Set S and some of its elements

We define a subset S of $\Lambda(G)$ by

$$S = \{f \in \Lambda(G) \mid \Lambda(G)/\Lambda(G)f \text{ is finitely generated over } \Lambda(H)\},$$

which is an Ore set as we have seen in subsection A.8.1. Next we fix a prime ideal $\mathfrak{q}$ of K, $\mathfrak{q} \neq \mathcal{O}_K$, subject to the following conditions:

(i) $(\mathfrak{q}, 6p\mathfrak{f}) = 1$,

(ii) $N(\mathfrak{q})$ is congruent to 1 modulo p, in symbols

$$N(\mathfrak{q}) \equiv 1 \bmod p.$$

Note that by Dirichlet's theorem on arithmetic progressions infinitely many such prime ideals exist, compare ([Neu07], VII, (5.14) p. 490). Henceforth, we will write q for the prime of $\mathbb{Q}$ below $\mathfrak{q}$.

Definition A.9.1. *For $k, n \geq 1$ we write*

$$(\mathfrak{q}, K_{k,n}/K) \in G(K_{k,n}/K)$$

for the arithmetic Frobenius at $\mathfrak{q}$ in $G(K_{k,n}/K)$. The elements $(\mathfrak{q}, K_{k,n}/K)$ are compatible with respect to restriction maps. We therefore get an element $(\mathfrak{q}, K_\infty/K) \in G(K_\infty/K)$. Any prime (valuation) $\mathfrak{q}'$ of K_∞ above $\mathfrak{q}$ must be fixed by $(\mathfrak{q}, K_\infty/K) \in G(K_\infty/K)$ because all the restrictions of $\mathfrak{q}'$ to subfields $K_{k,n}$ are fixed by $(\mathfrak{q}, K_\infty/K)_{|K_{k,n}} = (\mathfrak{q}, K_{k,n}/K)$. This implies that $(\mathfrak{q}, K_\infty/K)$ lies in the decomposition group $D_{\mathfrak{q}'/\mathfrak{q}} \subset G(K_\infty/K)$. And since $(\mathfrak{q}, K_\infty/K)_{|K_{k,n}}$ is the Frobenius for all $k, n \geq 1$, $(\mathfrak{q}, K_\infty/K)$ must also be the Frobenius in $D_{\mathfrak{q}'/\mathfrak{q}}$.

We defined $\Delta = \mathrm{Gal}(K_0/K)$ where $K_0 = K(E[p])$. The restriction map induces an isomorphism

$$G(K_\infty/K^{cyc}K^{acyc}) \cong \Delta$$

and from now on, by abuse of notation, we shall write Δ for $G(K_\infty/K^{cyc}K^{acyc})$.

Lemma A.9.2. *Let $\mathfrak{q}$ satisfy the above two conditions (i) and (ii). Then, the element $x_\mathfrak{q} := N(\mathfrak{q}) - (\mathfrak{q}, K_\infty/K)$ belongs to the Ore set S of $\Lambda(G)$.*

Proof. We recall that $G \cong G(K^{cyc}/K) \times G(K^{acyc}/K) \times \Delta$, where Δ is finite and of order prime to p. Under this decomposition H corresponds to $G(K^{acyc}/K) \times \Delta$ and we write $J \subset H$ for the pro-p open subgroup of H corresponding to $G(K^{acyc}/K)$. We note that J is normal in G and $G/J \cong G(K^{cyc}/K) \times \Delta$. Considering $G(K^{cyc}/K) \times G(K^{acyc}/K)$ as a subgroup of G, we write F for the fixed field of $G(K^{cyc}/K) \times G(K^{acyc}/K)$, implying that $\Delta \cong \mathrm{Gal}(F/K)$ and $G/J \cong \mathrm{Gal}(FK^{cyc}/K)$.

We write ψ_J for canonical map $\Lambda(G) \longrightarrow \Omega(G/J)$ and recall from ([CFK$^+$05], Lemma 2.1, p. 166) that an element f in $\Lambda(G)$ belongs to S if and only if

$$\Omega(G/J)\big/\Omega(G/J)\psi_J(f)$$

is finite. Since $(\mathfrak{q}, 6p\mathfrak{f}) = 1$, $\mathfrak{q}$ is unramified in K_∞. We recall that, by definition, $\sigma_\mathfrak{q} = (\mathfrak{q}, K_\infty/K)$ is the arithmetic Frobenius element in the decomposition group $G(K_{\infty,\bar{\mathfrak{q}}}/K_\mathfrak{q}) \subseteq G$ for some fixed prime $\bar{\mathfrak{q}}$ of K_∞ above $\mathfrak{q}$. The image $\overline{\sigma_\mathfrak{q}}$ of $\sigma_\mathfrak{q}$ in G/J is then the Frobenius in $G((FK^{cyc})_{\bar{\mathfrak{q}}}/K_\mathfrak{q}) \subset G/J$, where we also write $\bar{\mathfrak{q}}$ for the restriction of $\bar{\mathfrak{q}}$ to FK^{cyc}. In particular, $\overline{\sigma_\mathfrak{q}}$ is a topological generator of $G(F^{cyc})_\mathfrak{q} := G((FK^{cyc})_{\bar{\mathfrak{q}}}/K_\mathfrak{q})$. Moreover, $G(F^{cyc})_\mathfrak{q}$ is of finite index in G/J, because both groups contain precisely one copy of $\mathbb{Z}_p$. This implies that $\Omega(G/J)$ is finitely generated as a $\Omega(G(F^{cyc})_\mathfrak{q}/K_\mathfrak{q}))$-module. It is therefore sufficient to show that

$$\Omega(G(F^{cyc})_\mathfrak{q})\big/\Omega(G(F^{cyc})_\mathfrak{q})\psi_J(x_\mathfrak{q})$$

is finite. But this can be shown. Indeed, by condition (ii) for $\mathfrak{q}$ we have

$$\psi_J(x_\mathfrak{q}) = \overline{N(\mathfrak{q})} - \overline{\sigma_\mathfrak{q}} = 1 - \overline{\sigma_\mathfrak{q}}.$$

Let us consider the augmentation map,

$$\mathrm{aug}:\ \Omega(G(F^{cyc})_\mathfrak{q}) \longrightarrow \mathbb{F}_p,$$

the kernel of which, we will now show, is precisely $\Omega(G(F^{cyc})_\mathfrak{q})\psi_J(x_\mathfrak{q})$, which then concludes the proof.

It is a fact that each finite quotient of $G(F^{cyc})_\mathfrak{q}$ is cyclic, generated by the image of $\overline{\sigma_\mathfrak{q}}$, and that for finite cyclic groups $< \tau >$, generated by τ, the kernel of the augmentation map

$$\mathbb{F}_p[< \tau >] \longrightarrow \mathbb{F}_p,$$

is generated by $1 - \tau$. Now we can use a compactness argument to conclude the proof, which, for the sake of completeness, we recall. First note that $\Omega(G(F^{cyc})_\mathfrak{q})\psi_J(x_\mathfrak{q})$, as the image of the compact algebra $\Omega(G(F^{cyc})_\mathfrak{q})$ under the continuous multiplication with $\psi_J(x_\mathfrak{q})$, is compact. Let $\lambda \in \Omega(G(F^{cyc})_\mathfrak{q})$ belong to $\ker(\mathrm{aug})$. Then, for each open, normal subgroup $U \subset G(F^{cyc})_\mathfrak{q}$ the projection λ_U of λ to $\mathbb{F}_p[G(F^{cyc})_\mathfrak{q}/U]$ belongs to the kernel of $\mathrm{aug}_U : \mathbb{F}_p[G(F^{cyc})_\mathfrak{q}/U] \longrightarrow \mathbb{F}_p$ and we see by the above fact for finite cyclic groups that the pre-image of $\{\lambda_U\}$ under the canonical continuous projection map

$$\varphi_U : \Omega(G(F^{cyc})_\mathfrak{q})\psi_J(x_\mathfrak{q}) \longrightarrow \mathbb{F}_p[G(F^{cyc})_\mathfrak{q}/U]$$

is non-empty (we use here, that the maps defining the projective limit $\Omega(G(F^{cyc})_\mathfrak{q})$ are surjective). We now claim that

$$\bigcap_U \varphi_U^{-1}(\lambda_U) \neq \varnothing,$$

where the intersection is taken over all open, normal U in $G(F^{cyc})_\mathfrak{q}$. Assume the contrary. Since each $\varphi_U^{-1}(\lambda_U)$ is closed ($\mathbb{F}_p[G(F^{cyc})_\mathfrak{q}/U]$ has the discrete topology), $\bigcup_U \varphi_U^{-1}(\lambda_U)^c$ is an open covering of $\Omega(G(F^{cyc})_\mathfrak{q})\psi_J(x_\mathfrak{q})$. By compactness, we can find a finite subcovering such that

$$\bigcup_{i=1}^n \varphi_{U_i}^{-1}(\lambda_{U_i})^c = \Omega(G(F^{cyc})_\mathfrak{q})\psi_J(x_\mathfrak{q}),$$

for which we then have $\bigcap_{i=1}^n \varphi_{U_i}^{-1}(\lambda_{U_i}) = \varnothing$. But this contradicts the fact that for $V = \bigcap_{i=1}^n U_i$, $\varphi_V^{-1}(\lambda_V) \neq \varnothing$. Therefore, $\bigcap_U \varphi_U^{-1}(\lambda_U) \neq \varnothing$, showing that λ indeed belongs to $\Omega(G(F^{cyc})_\mathfrak{q})\psi_J(x_\mathfrak{q})$. □

The proof of the previous lemma also shows that the following lemma holds.

Lemma A.9.3. *Let $\mathfrak{q}$ be a prime ideal that satisfies the above condition (i), i.e., $(\mathfrak{q}, 6p\mathfrak{f}) = 1$. Then, the element $y_\mathfrak{q} = 1 - (\mathfrak{q}, K_\infty/K)$ belongs to the Ore set S of $\Lambda(G)$.*

Now, let us consider a prime $\mathfrak{l}$ dividing the conductor $\mathfrak{f}$ of E/K and let $r = n_\mathfrak{l}$ be its exact exponent in the prime decomposition of $\mathfrak{f}$. Recall the facts about $L_\infty \subset K_\infty \subset F_\infty$ from subsection A.6.1. Since $\mathfrak{l}$ is unramified in $K(\frac{\mathfrak{f}}{\mathfrak{l}^r}p^\infty) = \bigcup_{k,n} K(\frac{\mathfrak{f}}{\mathfrak{l}^r}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$ we can consider

$$(\mathfrak{l}, K(\frac{\mathfrak{f}}{\mathfrak{l}^r}p^\infty)/K)$$

which is the Frobenius for $\mathfrak{l}$ in $G(K(\frac{\mathfrak{f}}{\mathfrak{l}^r}p^\infty)/K)$, compare remark A.9.1. Certainly, $(\mathfrak{l}, K(\frac{\mathfrak{f}}{\mathfrak{l}^r}p^\infty)/K)$ restricts to $(\mathfrak{l}, L_\infty/K)$. We define $\sigma_\mathfrak{l}$ to be a lift of $(\mathfrak{l}, K(\frac{\mathfrak{f}}{\mathfrak{l}^r}p^\infty)/K)$ to $G(F_\infty/K)$ and also write $\sigma_\mathfrak{l}$ for its restriction to K_∞. With this notation, $\sigma_\mathfrak{l}$ restricted to L_∞ also gives $(\mathfrak{l}, L_\infty/K)$.

Remark A.9.4. We remark that the field $L_\infty = \bigcup_{k,n} K(\bar{\mathfrak{p}}^k\mathfrak{p}^n)$ contains all p-power roots of unity $\mu_{p^\infty}(\bar{K})$. This is because for a primitive p^m-th root of unity ζ_{p^m}, the field $K(\zeta_{p^m})$ is unramified outside p. In particular, its conductor over K is only divisible by the primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ and therefore we must have $K(\zeta_{p^m}) \subset L_{k,n}$ for some $k, n \geq 1$.

Lemma A.9.5. *The element $1-\sigma_{\mathfrak{l}}^{-1}$ belongs to S.*

Proof. For this we have to be more careful than previously for the element $N(\mathfrak{q})-(\mathfrak{q},K_\infty/K)$, $\mathfrak{q}$ prime to $\mathfrak{f}$. In this proof, let us write σ for $\sigma_{\mathfrak{l}}^{-1}$.

Again, we consider the decomposition $G \cong G(K^{cyc}/K)\times G(K^{acyc}/K)\times\Delta$, where Δ is finite of order d prime to p and write

$$\sigma = (\sigma_c, \sigma_a, \sigma_f),$$

where σ_c is the projection of σ to $G(K^{cyc}/K)$, σ_a is the projection of σ to $G(K^{acyc}/K)$ and σ_f is the projection of σ to Δ. We then have

$$\sigma^d = (\sigma_c^d, \sigma_a^d, 1)$$

which belongs to the subgroup $G(K^{cyc}/K)\times G(K^{acyc}/K)$ of G. Moreover, for general $a,b\in\Lambda(G)$, we have a surjection

$$\Lambda(G)/\Lambda(G)ab \twoheadrightarrow \Lambda(G)/\Lambda(G)b,$$

showing that if $a\cdot b$ belongs to S, then so does b. Therefore, since we can write

$$1-\sigma^d = \left(1+\sigma+\cdots+\sigma^{d-1}\right)\cdot\left(1-\sigma\right),$$

it is sufficient to show that $1-\sigma^d$ belongs to S. As above, we write ψ_J for canonical map $\Lambda(G)\longrightarrow\Omega(G/J)$ where we write J for the pro-p open subgroup of $H = G(K^{acyc}/K)\times\Delta$ corresponding to $G(K^{acyc}/K)$. Now, one of the equivalent conditions for $1-\sigma^d$ to belong to S is that

$$\Omega(G/J)\big/\Omega(G/J)\psi_J(1-\sigma^d)$$

is finite. Since $\mathrm{Gal}(K^{cyc}/K)$ is of finite index in $G/J\cong\mathrm{Gal}(K^{cyc}/K)\times\Delta$, $\Omega(G/J)$ is finitely generated as a $\Omega(G(K^{cyc}/K))$-module. Since, $\psi_J(\sigma^d)$ belongs to $\Omega(G(K^{cyc}/K))$ (this would not have been true for σ, which is why we had to take the d-th power!), we see that it is sufficient to show that

$$\Omega(G(K^{cyc}/K))\big/\Omega(G(K^{cyc}/K))\psi_J(1-\sigma^d)$$

is finite. But σ^{-1} restricts to a Frobenius element for the prime $\mathfrak{l}$ in the outside p unramified extension K^{cyc}/K. In particular, since d is a unit in $\mathbb{Z}_p$, σ^d restricts to a topological generator of the decomposition group $D_{\mathfrak{l}}\subset G(K^{cyc}/K)$. However, $D_{\mathfrak{l}}\cong\mathbb{Z}_p$ is of finite index in $G(K^{cyc}/K)$ and we can conclude the proof, as above, by noting that $\psi_J(1-\sigma^d)$ generates the augmentation ideal of $\Omega(D_{\mathfrak{l}})$. □

Bibliography

[AB06] K. Ardakov and K. A. Brown. Ring-theoretic properties of Iwasawa algebras: a survey. In *Extra Volume: John Coates' Sixtieth Birthday*, pages 7–33. Documenta Math., 2006.

[AW06] K. Ardakov and S. Wadsley. Characteristic elements for p-torsion Iwasawa modules. *J. Algebraic Geometry*, 15:339–377, 2006.

[AW08] K. Ardakov and S. Wadsley. K_0 and the dimension filtration for p-torsion Iwasawa modules. *Proc. London Math.*, 97(no. 3):31–59, 2008.

[BH03] P. Balister and S. Howson. Note on Nakayama's Lemma for compact Λ-modules. *Asian Math. J.*, Vol. 1:224–229, 2003.

[BH06] C.J. Bushnell and G. Henniart. *The Local Langlands Conjecture for* $GL(2)$. Springer-Verlag, Berlin Heidelberg, 2006.

[BIV98] R. Brüske, F. Ischebeck, and F. Vogel. *Kommutative Algebra*. Bibliographisches Institut & F.A. Brockhaus AG, Mannheim, 1998.

[BK90] S. Bloch and K. Kato. Tamagawa numbers of motives and L-functions. In *Grothendieck Festschrift 1*, volume 86 of *Progress in Math.*, pages 333–400. Birkhäuser, 1990.

[Ble04] W. Bley. Wild Euler systems of elliptic units and the Equivariant Tamagawa Number Conjecture. *Journal für die reine und angewandte Mathematik*, 577:117–146, 2004.

[Ble06] W. Bley. On the Equivariant Tamagawa Numer Conjecture for Abelian Extensions of a Quadratic Imaginary Field. *Documenta Mathematica*, 11:73–118, 2006.

[Bou04] N. Bourbaki. *Integration II, Chapters 7 - 9*. Springer-Verlag, Berlin Heidelberg, 2004.

[Bre93] G. Bredon. *Topology and Geometry*. Springer-Verlag, New York, 1993.

[Bru66] A. Brumer. Pseudocompact Algebras, Profinite Groups and Class Formations. *Journal of Algebra*, 4:442–470, 1966.

[BV10] T. Bouganis and O. Venjakob. On the Non-commutative Main Conjecture for Elliptic Curves with Complex Multiplication. *Asian J. Math.*, 14(no. 3):385–416, 2010.

[Cas03] J. Cassels. *Local Fields*. Cambridge University Press, Cambridge, 2003.

[CFK+05] J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob. On the GL_2 main conjecture for elliptic curves without complex multiplication. *Publ. Math. IHES*, 101(no. 1), 2005.

[Coaa] J. Coates. Iwasawa Theory of Elliptic Curves with Complex Multiplication. `http://math.arizona.edu/~taolapkei/pdf/Iwasawa-Coates.pdf`. lecture notes.

[Coab] J. Coates. Lectures on the Birch-Swinnerton-Dyer Conjecture. Preprint.

[Col79] R. F. Coleman. Division values in local fields. *Inventiones Math.*, 53:91–116, 1979.

[Col83] R. F. Coleman. Local Units Modulo Circular Units. *Proc. of the Amer. Math. Soc.*, 89(1):1–7, 1983.

[Cona] B. Conrad. Étale Cohomology. `http://math.unice.fr/~dehon/CohEtale-09/Elencj_Etale/CONRAD%20Etale%20Cohomology.pdf`. notes.

[Conb] B. Conrad. The Lattice of S-Integers. `http://math.stanford.edu/~conrad/248APage/handouts/Sintlattice.pdf`. Handout Math 248A.

[CS06] J. Coates and R. Sujatha. *Cyclotomic Fields and Zeta Values*. Springer-Verlag, Berlin Heidelberg, 2006.

[CS10] J. Coates and R. Sujatha. The Main Conjecture. *To appear*, 2010. Article for the Guwahati Workshop.

[CW77] J. Coates and A. Wiles. On the Conjecture of Birch and Swinnerton-Dyer. *Inventiones Mathematicae*, 39:223–251, 1977.

[CW78] J. Coates and A. Wiles. On p-adic l-Functions and Elliptic Units. *J. Austral. Math. Soc.*, (Series A) 26:1–25, 1978.

[Dam70] R. M. Damerell. L-Functions of elliptic curves with complex multiplication, I. *Acta. Arith.*, 17(number 3):287–301, 1970.

[Dam71] R. M. Damerell. L-Functions of elliptic curves with complex multiplication, II. *Acta. Arith.*, 19(number 3):311–317, 1971.

[DdSMS03] J. Dixon, M. du Sautoy, A. Mann, and D. Segal. *Analytic Pro-p Groups*. Cambridge University Press, Cambridge, 2003.

[Del73] P. Deligne. Les constantes des équations fonctionnelles des fonctions L. In *Modular functions of one variable II*, volume 349 of *Lecture Notes in Mathematics*, pages 501–597. Springer, 1973.

[Deu41] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[Deu55] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlecht Eins, II. *Nachr. Akad. Wiss. Göttingen*, 2:13–42, 1955.

[Deu56] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlecht Eins, III. *Nachr. Akad. Wiss. Göttingen*, 4:37–67, 1956.

[DG11] S. Dasgupta and M. Greenberg. The Rank One Abelian Stark Conjecture. `http://swc.math.arizona.edu/aws/2011/2011DasguptaGreenbergNotes.pdf`, 2011. Course Notes.

[dS87] E. de Shalit. *Iwasawa theory of elliptic curves with complex multiplication*, volume 3 of *Perspectives in Mathematics*. Academic Press, 1987.

[FK06] T. Fukaya and K. Kato. A formulation of conjectures on p-adic zeta functions in non-commutative Iwasawa theory. In N. N. Uraltseva, editor, *Proceedings of the St. Petersburg Mathematical Society Volume XII*, volume 219 of *AMS Translations, Series 2*. American Mathematical Society, 2006.

[Fla04] M. Flach. The equivariant Tamagawa number conjecture: a survey. In *Stark's conjectures: recent work and new directions*, volume 358 of *Contemporary Mathematics*, pages 79–125. American Mathematical Society, 2004.

[Fla09] M. Flach. Iwasawa theory and motivic L-functions and Galois module structures. *Pure Appl. Math. Q.*, 5(no. 1):255–294, 2009.

[FM87] J.-M. Fontaine and W. Messing. p-adic periods and p-adic étale cohomology. In *Current Trends in Arithmetical Algebraic Geometry*, volume 67 of *Contemporary Mathematics*, pages 179–207. American Mathematical Society, 1987.

[FO] J.-M. Fontaine and Y. Ouyang. Theory of p-adic Galois Representations. `http://www.math.u-psud.fr/~fontaine/galoisrep.pdf`. Yet unpublished.

[Fon82] J.-M. Fontaine. Sur certains types de representations p-adiques du groupe de galois d'un corps local; construction d'un anneau de barsotti-tate. *Annals of Mathematics*, 115(3):529–577, 1982.

[Fon94] J.-M. Fontaine. Le corps des périodes p-adiques. *Astérisque*, 223:59–111, 1994.

[FPR91] J.-M. Fontaine and B. Perrin-Riou. Autour des conjectures de Bloch and Kato: cohomologie galoisienne et valeurs de fonctions L. In *Motives*, volume 55 Part 1 of *Proceedings of Symposia in Pure Mathematics*. American Mathematical Society, 1991.

[FV02] I. B. Fesenko and S. V. Vostokov. *Local Fields and Their Extensions*, volume 121 of *Translations of Mathematical Monographs*. American Mathematical Society, 2002.

[Gab62] P. Gabriel. Des catégories abéliennes. *Bulletin de la S.M.F.*, 90:323–448, 1962.

[Gre85] R. Greenberg. On the critical values of Hecke L-functions for imaginary quadratic fields. *Inventiones Mathematicae*, 79:79–94, 1985.

[Gre89] R. Greenberg. Iwasawa theory for p-adic representations. In *Algebraic Number Theory - in honor of K. Iwasawa*, volume 17 of *Advanced Studies in Pure Mathematics*. Acadamic Press, 1989.

[Gre94] R. Greenberg. Iwasawa Theory and p-adic Deformations of Motives. In *Motives*, volume 55 Part 2 of *Proceedings of Symposia in Pure Mathematics*. American Mathematical Society, 1994.

[Gre01a] R. Greenberg. Introduction to Iwasawa theory for elliptic curves. In *Arithmetic Algebraic Geometry*, volume 9 of *IAS/PArk City MAth. Ser.*, pages 407–464. Amer. Math. Soc., 2001.

[Gre01b] R. Greenberg. Iwasawa Theory - Past and Present. In *Class Field Theory - Its Centenary and Prospect*, volume 30 of *Advanced Studies in Pure Mathematics*, pages 335–385. Mathematical Society of Japan, 2001.

[Hid93] H. Hida. *Elementary theory of L-functions and Eisenstein series*, volume 26 of *London Mathemacial Society Student Texts*. Cambridge University Press, Cambridge, 1993.

[Iwa64] K. Iwasawa. On some modules in the theory of cyclotomic fields. *J. Math. Soc. Japan*, Vol. 16(No. 1), 1964.

[Iwa69] K. Iwasawa. On p-adic L-functions. *Annals of Mathematics*, 89(1):198–205, 1969.

[Iwa73] K. Iwasawa. On $\mathbb{Z}_l$-extensions of algebraic number fields. *Ann. of Math.*, 98(2):246–326, 1973.

[Jan88] U. Jannsen. Continuous Étale Cohomology. *Math. Ann.*, 280:207–245, 1988.

[Jan89] U. Jannsen. Iwasawa modules up to isomorphism. In *Algebraic Number Theory - in honor of K. Iwasawa*, volume 17 of *Advanced Studies in Pure Mathematics*. Acadamic Press, 1989.

[Kak11] M. Kakde. Proof of the main conjecture of noncommutative Iwasawa theory for totally real number fields in certain cases. *J. Algebraic Geometry*, 20, 2011.

[Kak13] M. Kakde. The main conjecture of Iwasawa theory for totally real fields. *Inventiones Math.*, 193:539–626, 2013.

[Kat] K. Kato. Lectures on the approach to Iwasawa theory of Hasse-Weil L-functions via B_{dR} II. preprint.

[Kat76] M. Katz. p-adic Interpolation of real analytic Eisenstein series. *Annals of Mathematics*, 104:459–571, 1976.

[Kat04] K. Kato. p-adic Hodge Theory and Values of Zeta Functions of Modular Forms. *Astérisque*, 295, 2004.

[Kat06] K. Kato. Universal norms of p-units in some non-commutative Galois extensions. In *Extra Volume: John Coates' Sixtieth Birthday*, pages 551–566. Documenta Math., 2006.

[Kat07] K. Kato. Iwasawa theory and generalizations. In *Proceedings of the International Congress of Mathematicians, Madrid 2006*, volume I, pages 335–357. European Mathematical Society, 2007.

[KL64] T. Kubota and H.-W. Leopoldt. Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen dirichletschen L-Funktionen. *Crelle J.*, 214/215:328–339, 1964.

[Kol90] V. Kolyvagin. Euler Systems. In *The Grothendieck Festschrift*, volume II. Birkh 1990.

[Kum75] E. E. Kummer. Collected papers. In *Contributions to number theory*, volume I, pages viii + 957. Springer-Verlag, 1975.

[Lam99] T. Y. Lam. *Lectures on Modules and Rings*. Springer-Verlag, New York, 1999.

[Lan70] S. Lang. *Algebraic Number Theory*. Addison-Wesley, Reading, MA, 1970.

[Lan83] S. Lang. *Abelian varieties*. Springer-Verlag, New York, 1983.

[Lan87] S. Lang. *Elliptic Functions*. Springer-Verlag, New York, 1987.

[Lan90] S. Lang. *Cyclotomic Fields I and II, Combined Second Edition, With an Appendix by Karl Rubin*. Springer-Science+Business Media, LLC, New York, 1990.

[Lan05] S. Lang. *Algebra*. Springer Science+Business Media, LLC, New York, 2005.

[Laz65] M. Lazard. Groupes analytiques p-adiques. *Publ. Math. IHES*, 26, 1965.

[Mah58] K. Mahler. An interpolation series for a continuous function of a p-adic variable. *J. für reine und angew. Math.*, 199:23–34, 1958.

[Mat55] A. Mattuck. Abelian varieties over p-adic ground fields. *Annals of Mathematics*, 62(1):92–119, 1955.

[Maz72] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Inventiones Math.*, 18:183–266, 1972.

[Maz77] B. Mazur. Review: Ernst edward kummer, collected papers. *Bull. Amer. Math. Soc.*, 83(5):976–988, 1977.

[Mil80] J.S. Milne. *Étale Cohomology*. Princeton University Press, Princeton, New Jersey, 1980.

[Mil86a] J.S. Milne. Abelian Varieties (Storrs, Conn., 1984. In *Arithmetic Geometry*. Springer, New York, 1986.

[Mil86b] J.S. Milne. *Arithmetic Duality Theorems*. Academic Press, Orlando, Florida, 1986.

[Mil08] J. Milne. Abelian Varieties. `/http://www.jmilne.org/math/CourseNotes/AV.pdf`, 2008. Course Notes Version 2.0.

[Mil13a] J. Milne. Class Field Theory. `http://www.jmilne.org/math/CourseNotes/CFT.pdf`, 2013. Course Notes Version 4.02.

[Mil13b] J. Milne. Lectures on étale Cohomology. `http://www.jmilne.org/math/CourseNotes/LEC.pdf`, 2013. Version 2.21.

[MR87] J. C. McConnell and J. C. Robson. *Noncommutative Noetherian Rings*. American Mathematical Society, Providence, Rhode Island, 1987.

[MSD74] B. Mazur and P. Swinnerton-Dyer. Arithmetic of weil curves. *Inventiones Math.*, 25:1–61, 1974.

[Mum85] D. Mumford. *Abelian Varieties*. Published for the Tata Institute of Fundamental Research, Bombay, by Oxford University Press, 1985.

[MW84] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbb{Q}$. *Inventiones Math.*, 76:179–330, 1984.

[Nek93] J. Nekovář. On p-adic height pairings. In *Séminaire de Théorie des Nombres de Paris 1990/91*, volume 108 of *Progress in Math.*, pages 127–202. Birkhäuser, 1993.

[Nek06] J. Nekovář. Selmer complexes. *Astérisque*, 310:viii+559, 2006.

[Neu69] J. Neukirch. *Klassenkörpertheorie*. Bibliographisches Institut, Mannheim, 1969.

[Neu07] J. Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin Heidelberg, 2007.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Springer-Verlag, Berlin Heidelberg, 2008.

[OV02] Y. Ochi and O. Venjakob. On The Structure of Selmer Groups over p-adic Lie Extensions. *J. Algebraic Geometry*, 11:547–580, 2002.

[Poi67] G. Poitou. *Cohomologie galoisienne des modules finis*, volume 13 of *Travaux et recherches mathématiques*. Dunod, 1967.

[PR84] B. Perrin-Riou. *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, volume 17. Mémoires de la société mathématique de France, 1984.

[PR92] B. Perrin-Riou. Théorie d'Iwasawa et hauteurs p-adiques. *Inventiones Mathematicae*, 109, 1992.

[PR94] B. Perrin-Riou. Représentation p-adiques ordinaires. *Inventiones Mathematicae*, 223, 1994.

[PR00] B. Perrin-Riou. *p-adic L-functions and p-adic representations*, volume 3 of *SMF/AMS Texts and Monographs*. American Mathematical Society, 2000.

[Rob73] G. Robert. Unités elliptiques. *Bull. Soc. Math. France*, 36, 1973.

[Rob90] G. Robert. Concernant la relation de distribution satisfaite par la fonction φ associée à un réseau complexe. *Inventiones Mathematicae*, 100:231–257, 1990.

[Rob90] G. Robert. La racine 12-ième canonique de $\Delta(L)^{[\underline{L}:L]}/\Delta(\underline{L})$. *Séminaire de Théorie des Nombres Paris*, pages 209–232, 1989-90.

[Ros94] J. Rosenberg. *Algebraic K-theory and its Applications*. Springer-Verlag, New York, 1994.

[Rot09] J. Rotman. *An Introduction to Homological Algebra*. Springer, New York, 2009.

[Rub87] K. Rubin. Tate-shafarevich groups and l-functions of elliptic curves with complex multiplication. *Inventiones Mathematicae*, 89:527–560, 1987.

[Rub91] K. Rubin. The "main conjectures" of Iwasawa theory for quadratic imaginary fields. *Inventiones Mathematicae*, 103:25–68, 1991.

[Rub99] K. Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. In C. Viola, editor, *Arithmetic theory of elliptic curves*, volume 1716 of *Lecture Notes in Math.*, pages 167–234. Springer-Verlag, New York, 1999.

[Rub00] K. Rubin. *Euler Systems.* Number 147 in Annals of Mathematics Studies. Princeton University Press, Princeton, 2000.

[Sch85] P. Schneider. p-adic height pairings. II. *Inventiones Mathematicae*, 79:329–374, 1985.

[Sch89] P. Schneider. Motivic Iwasawa Theory. In *Algebraic Number Theory*, Adv. Stud. Pure Math. 1989.

[Sch11] P. Schneider. *p-Adic Lie Groups.* Springer-Verlag, Berlin Heidelberg, 2011.

[Ser56] J.-P. Serre. Sur la dimension homologique des anneaux et des modules noethériens. In *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko*, pages 175–189. Science Council of Japan, 1956.

[Ser65] J.-P. Serre. Sur la Dimension Cohomologique des Groupes Profinis. *Topology*, 3:413–420, 1965.

[Ser95] J.-P. Serre. *Local Fields.* Springer-Verlag, New York, 1995.

[Ser97] J.-P. Serre. *Galois Cohomology.* Springer-Verlag, Berlin Heidelberg, 1997.

[Ser98a] J.-P. Serre. *Abelian l-adic Representations and Elliptic Curves*, volume 7 of *Research Notes in Mathematics.* A K Peters, Wellesley, Massachusetts, 1998.

[Ser98b] J.-P. Serre. La distribution d'Euler Poincaré d'un groupe profini. In A. J. Scholl and R. L. Taylor, editors, *Galois representations in arithmetic algebraic geometry*, volume 254 of *Lecture Note Series*, pages 461–493. London Mathematical Society, 1998.

[Ser10] J.-P. Serre. Local class field theory. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory.* London Mathematical Society, 2010. 2nd edition.

[Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic forms.* Princeton University Press, Princeton, 1971.

[Sil86] J. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.

[Sil99] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1999.

[Sri08] V. Srinivas. *Algebraic K-Theory.* Birkhäuser, Boston, 2008.

[ST68] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. Math.*, 88:492–517, 1968.

[Sta80] H. M. Stark. L-functions at $s = 1$. IV. First Derivatives at $s = 0$. *Advances in Math.*, 35:197–235, 1980.

[Str83] R. J. Stroeker. Reduction of elliptic curves over imaginary quadratic number fields. *Pacific J. Math.*, 108(2):451–463, 1983.

[SU] C. Skinner and E. Urban. The Iwasawa main conjectures for gl_2. Preprint.

[SV04] P. Schneider and O. Venjakob. On the dimension theory of skew power series rings. *eprint arXiv:math/0406342*, 132, 2004.

[SV10] P. Schneider and O. Venjakob. Localizations and completions of skew power series. *American J. Math.*, 132(1):1–36, 2010.

[Tat63] J. Tate. Duality Theorems in Galois cohomology over number fields. In *Proceedings of the International Congress of Mathematicians (Stockholm, 1962)*, pages 288–295. Inst. Mittag-Leffler, 1963.

[Tat76] J. Tate. Relations between K_2 and Galois Cohomology. *Inventiones Mathematicae*, 36:257–274, 1976.

[Tat79] J. Tate. Number theoretic background. In A. Borel and W. Casselman, editors, *Automorphic Forms, representations and L-functions*, volume 33(2) of *Proc. Symposia Pure Math.*, pages 3–26. American Mathematical Society, 1979.

[Tat84] J. Tate. *Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$*. Birkhäuser, Boston, 1984.

[Tha88] F. Thaine. On the ideal class group of real abelian number fields. *Ann. of Math.*, 128:1–18, 1988.

[Ven00] O. Venjakob. Iwasawa Theory of p-adic Lie Extensions. `http://archiv.ub.uni-heidelberg.de/volltextserver/1451/1/THESIS.pdf`, 2000. Heidelberg University, Doktorarbeit.

[Ven03] O. Venjakob. Characteristic Elements in Noncommutative Iwasawa Theory. `http://www.mathi.uni-heidelberg.de/~otmar/papervenjakob/habil.pdf`, 2003. Heidelberg University, Habilitationsschrift.

[Ven05] O. Venjakob. From the Birch and Swinnerton-Dyer conjecture over the equivariant Tamagawa number conjecture to non-commutative Iwasawa theory. In *L-functions and Galois representations*, volume 320 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, 2005.

[Ven13] O. Venjakob. On Kato's local ϵ-isomorphism conjecture for rank one Iwasawa modules. *To appear in ANT*, 2013.

[Vig12] S. Viguié. Global Units Modulo Elliptic Units And Ideal Class Groups. *International Journal of Number Theory*, 8(3):569–588, 2012.

[Was97] L. Washington. *Introduction to Cyclotomic Fields.* Springer-Verlag, New York, 1997.

[Wei55] A. Weil. On certain type of characters of the idèle class group of an algebraic number field. In *Proc. Int. Symp. on Alg. Number Theory at Tokyo-Nikko*, pages 1–7. 1955.

[Wei94] C. A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge studies in advanced mathematics.* Cambridge University Press, Cambridge, 1994.

[Wei13] C. A. Weibel. *The K-book: an introduction to algebraic K-theory*, volume 145 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, Rhode Island, 2013.

[Wil90] A. Wiles. The Iwasawa main conjecture for totally real fields. *Ann. of Math.*, 131:493–540, 1990.

[Win80] J.-P. Wintenberger. Structure galoisienne de limites projectives d'unités locales. *Compositio Mathematica*, 42(1):89–103, 1980.

[Wit03] M. Witte. On a localisation sequence for the K-theory of skew power series rings. *Journal of K-Theory*, 11(1):125–154, 103.

[Wit04] M. Witte. Die äquivariante Hauptvermutung der Iwasawa-Theorie für die zyklotomische $\mathbb{Z}_p$-Erweiterung abelscher Zahlkörper. `http://www.mathi.uni-heidelberg.de/~witte/docs/diplom.pdf`, 2004. Universität Leipzig, Diplomarbeit.

[Yag82] R. I. Yager. On two variable p-adic L-functions. *The Annals of Mathematics*, 115(2):411–449, 1982.

[Z1́0] G. Zábrádi. Pairings and functional equations over the GL_2-extension. *Proc. London Math. Soc.*, 101(3):893–930, 2010.