University of California
Santa Barbara

On the Galois Module Structure of the Square Root of the Inverse Different in Abelian Extensions

A dissertation submitted in partial satisfaction
of the requirements for the degree

Doctor of Philosophy
in
Mathematics

by

Cindy (Sin Yi) Tsang

Committee in charge:

Professor Adebisi Agboola, Chair
Professor Jon McCammond
Professor Mihai Putinar

June 2016

The Dissertation of Cindy (Sin Yi) Tsang is approved.

Professor Jon McCammond

Professor Mihai Putinar

Professor Adebisi Agboola, Committee Chair

March 2016

On the Galois Module Structure of the Square Root
of the Inverse Different in Abelian Extensions

by

Cindy (Sin Yi) Tsang

Dedicated to my beloved Grandmother.

Acknowledgements

I would like to thank my advisor Prof. Adebisi Agboola for his guidance and support. He has helped me become a more independent researcher in mathematics. I am indebted to him for his advice and help in my research and many other things during my life as a graduate student. I would also like to thank my best friend Tim Cooper for always being there for me.

Curriculum Vitæ

Cindy (Sin Yi) Tsang

Email: cindytsy@math.ucsb.edu
Website: https://sites.google.com/site/cindysinyitsang

Education

2016 PhD Mathematics (Advisor: Adebisi Agboola)
University of California, Santa Barbara

2013 MA Mathematics
University of California, Santa Barbara

2011 BS Mathematics (comprehensive option)
BA Japanese (with departmental honors)
University of Washington, Seattle

2010 Summer program in Japanese language and culture
Kobe University, Japan

Research Interests

Algebraic number theory, Galois module structure in number fields

Publications and Preprints

(4) Galois module structure of the square root of the inverse different over maximal orders, in preparation.

(3) Realizable classes and embedding problems, arXiv:1602.02342 [math.NT].

(2) On the realizable classes of the square root of the inverse different in the unitary class group, *To appear in Int. J. Number Theory.*

(1) On the Galois module structure of the square root of the inverse different in abelian extensions, *J. Number Theory 160 (2016), 759-804.*

Conference Presentations

2016 (11) Hermitian structure of the square root of the inverse different
Graduate Student Conference in Algebra, Geometry, and Topology

(10) Galois module structure of the square root of the inverse different over maximal orders
Underrepresented Students in Topology and Algebra Research Symposium

(9) Galois module structure of the square root of the inverse different in abelian extensions
SouthEast Regional Meeting on Numbers

(8) Harald Helfgott project group presentation
Arizona Winter School: Analytic Methods in Arithmetic Geometry

(7) Realizable classes and embedding problems
Joint Mathematics Meetings

2015 (6) Galois module structure of rings of integers and embedding problems
Symposium for Women in Mathematics in Southern California

(5) On the Galois module structure of the square root of the inverse different in abelian extensions
AMS Fall Western Sectional Meeting

(4) Galois modules and embedding problems (poster)
French-German Summer School in Galois Theory and Number Theory, U of Konstanz

(3) Normal integral basis and realizable classes
Women and Mathematics: Aspects in Algebraic Geometry, IAS Princeton

2014 (2) An overview in the study of Galois modules
Underrepresented Students in Topology and Algebra Research Symposium

2013 (1) Galois module structure of abelian extensions
Symposium for Women in Mathematics in Southern California

Conferences Attended

2016 Graduate Student Conference in Algebra, Geometry, and Topology
Underrepresented Students in Topology and Algebra Research Symposium
SouthEast Regional Meeting on Numbers
Arizona Winter School: Analytic Methods in Arithmetic Geometry
Automorphic Forms Workshop
Joint Mathematics Meetings

2015 Symposium for Women in Mathematics in Southern California
AMS Fall Western Section Meeting
French-German Summer School on Galois Theory and Number Theory
p-adic Methods in Number Theory, UC Berkeley
Women and Mathematics: Aspects of Algebraic Geometry, IAS Princeton
Underrepresented Students in Topology and Algebra Research Symposium
Arizona Winter School: Arithmetic and Higher-Dimensional Varieties
Nebraska Conference for Undergraduate Women in Mathematics

2014 Séminaire de Mathématiques Supérieures: Counting Arithmetic Objects
Underrepresented Students in Topology and Algebra Research Symposium
Arizona Winter School: Arithmetic Statistics
Joint Mathematics Meetings

2013 Symposium for Women in Mathematics in Southern California

2012 Symposium for Women in Mathematics in Southern California
MAA Inquiry-Based Learning Workshop, UC Santa Barbara

Seminar Talks at UC Santa Barbara

2016 Navigating in $\mathbb{F}_p$ and generalized Fibonacci numbers
Hermitian structure of the square root of the inverse different
Galois module structure of the square root of the inverse different
Introduction to abelian class field theory
Classical Iwasawa theory and $\mathbb{Z}_p$-extensions

2015 The inverse Galois problem over $\mathbb{Q}$
Diophantine equations and the Hasse principle
Galois modules and embedding problems

2014 Galois module structure of number fields
Primes of the form $x^2 + ny^2$
Introduction to supercharacters and superclasses

2014 Realizable classes of tame abelian extensions
Galois modules and realizable classes
Private-key, public-key, and quantum cryptography
Existence of a normal integral basis and ramification
A brief review on tensor product of modules

2012 An overview of valuation theory
Infinite Galois theory and profinite group topology

Other Seminar Talks

2015 Normal integral basis and embedding problems, *Keio U*

Grants, Fellowships, Awards, and Honors

2016 GSA Conference Travel Grant in January
UC Santa Barbara

Graduate Student Travel Grant to the Joint Mathematics Meetings
American Mathematical Society

2015	Academic Senate Doctoral Student Travel Grant *UC Santa Barbara*
	Department of Mathematics Graduate Merit Fellowship in Spring *UC Santa Barbara*
2014	Academic Senate Outstanding Teaching Assistant Award Nominee *UC Santa Barbara*
	GSA Event Co-Sponsorship funding for Hypatian Seminar in Winter *UC Santa Barbara*
2013	Department of Mathematics Graduate Merit Fellowship in Summer *UC Santa Barbara*
	Instructional Improvement Program Grant *UC Santa Barbara*
	Academic Senate Outstanding Teaching Assistant Award Nominee *UC Santa Barbara*
2012	NACURH, Inc. Institution Faculty/Staff of the Month in October *UC Santa Barbara*
2011	Graduated summa cum laude *UW Seattle*
2010	Tatsumi Scholarship for Excellence in the Study of Japanese *UW Seattle*

Service

2013-16	Co-organizer of the Graduate Algebra Seminar *UC Santa Barbara*
2012-16	Co-organizer of the Hypatian Seminar *UC Santa Barbara*
2015	Invited panelist on “Choosing a Mathematics Graduate Program” *Nebraska Conference for Undergraduate Women in Mathematics*
	Math Circle lesson on“Cool Math Magic Tricks” *UC Santa Barbara*

Teaching Experience at UC Santa Barbara

Instructional Development Projects

2013-2014	Calculus Study Resources on GauchoSpace

2012-2013	Online Math Lab

Teaching Assistant

Spring 2016	Linear Algebra with Applications
Winter 2016	Advanced Linear Algebra
Fall 2015	Linear Algebra with Applications
Summer 2015	Linear Algebra with Applications
Winter 2015	Transition to Higher Mathematics
Fall 2014	Advanced Linear Algebra
Spring 2014	Introduction to Topology
Winter 2014	Methods of Analysis
Fall 2013	Introduction to Abstract Algebra
Spring 2013	Calculus for Social Sciences I
Winter 2013	Calculus with Applications II
Fall 2012	Calculus with Applications I
Summer 2012	Differential Equations and Linear Algebra I
Spring 2012	Calculus for Social Sciences I Calculus for Social Sciences II
Winter 2012	Calculus for Social Sciences I
Fall 2011	Calculus for Social Sciences I

Grader

Winter 2015	Transition to Higher Mathematics
Winter 2014	Abstract Algebra
Fall 2012	Transition to Higher Mathematics
Spring 2012	Introduction to Complex Variables

Languages

Fluent in *Cantonese*, *English*, and *Japanese*.

Abstract

On the Galois Module Structure of the Square Root
of the Inverse Different in Abelian Extensions

by

Cindy (Sin Yi) Tsang

Let K be a number field with ring of integers $\mathcal{O}_K$ and let G be a finite group of odd order. Given a G-Galois K-algebra K_h, let A_h be the fractional ideal in K_h whose square is the inverse different of K_h/K, which exists by Hilbert's formula since G has odd order. By a theorem of B. Erez, we know that A_h is locally free over $\mathcal{O}_KG$ when K_h/K is *weakly ramified*, i.e. all of the second ramification groups in lower numbering attached to K_h/K are trivial. In this case, the module A_h determines a class $\mathrm{cl}(A_h)$ in the locally free class group $\mathrm{Cl}(\mathcal{O}_KG)$ of $\mathcal{O}_KG$. Such a class in $\mathrm{Cl}(\mathcal{O}_KG)$ will be called *A-realizable*, and *tame A-realizable* if K_h/K is in fact tame. We will write $\mathcal{A}(\mathcal{O}_KG)$ and $\mathcal{A}^t(\mathcal{O}_KG)$ for the sets of all A-realizable classes and tame A-realizable classes in $\mathrm{Cl}(\mathcal{O}_KG)$, respectively.

In this dissertation, we will consider the case when G is abelian. First of all, we will show that $\mathcal{A}^t(\mathcal{O}_KG)$ is in fact a subgroup of $\mathrm{Cl}(\mathcal{O}_KG)$ and that a class $\mathrm{cl}(A_h) \in \mathcal{A}(\mathcal{O}_KG)$ is tame A-realizable if the wildly ramified primes of K_h/K satisfy suitable assumptions. Our result will imply that $\mathcal{A}(\mathcal{O}_KG) = \mathcal{A}^t(\mathcal{O}_KG)$ holds if the primes dividing $|G|$ are totally split in $K/\mathbb{Q}$. Then, we will show that $\Psi(\mathcal{A}(\mathcal{O}_KG)) = \Psi(\mathcal{A}^t(\mathcal{O}_KG))$ holds without any extra assumptions. Here Ψ is the natural homomorphism $\mathrm{Cl}(\mathcal{O}_KG) \longrightarrow \mathrm{Cl}(\mathcal{M}(KG))$ afforded by extension of scalars and $\mathrm{Cl}(\mathcal{M}(KG))$ denotes the locally free class group of the maximal $\mathcal{O}_K$-order $\mathcal{M}(KG)$ in KG. Last but not least, we will show that the group structure of $\mathcal{A}^t(\mathcal{O}_KG)$ is connected to the study of embedding problems.

Contents

Curriculum Vitae **vi**

Abstract **xi**

1 Introduction **1**

1.1 Galois Module Structure of Rings of Integers . . . 1

1.2 The Square Root of the Inverse Different I . . . 3

1.3 The Square Root of the Inverse Different II . . . 6

1.4 Relation to the Study of Embedding Problems . . . 9

1.5 Previously Copyrighted Materials . . . 12

1.6 Notation and Conventions . . . 13

2 Prerequisites **16**

2.1 Locally Free Class Groups . . . 16

2.2 G-Forms and Unitary Class Groups . . . 18

2.3 Galois Algebras and Resolvends . . . 22

2.4 Cohomology and Reduced Resolvends . . . 28

2.5 The Modified Stickelberger Transpose . . . 32

3 The Class of the Square Root of the Inverse Different **38**

3.1 Computation using Resolvends . . . 38

3.2 Properties of Local Resolvends . . . 40

3.3 Proofs of Theorems 1.2.2 and 1.3.2 . . . 43

4 Characterization of the A-Realizable Classes in Cl($\mathcal{O}_K G$) and UCl($\mathcal{O}_K G$) **46**

4.1 Factorization of Local Homomorphisms . . . 47

4.2 Decomposition of Local Tame Resolvends . . . 49

4.3 Approximation Theorems . . . 54

4.4 Proofs of Theorems 1.2.3, 1.3.3, and 1.2.4 . . . 57

4.5 Decomposition of Local Wild Resolvends I . . . 61

4.6 Proofs of Theorem 1.2.6 and 1.3.4 . . . 70

5 Characterization of the A-Realizable Classes in Cl$(\mathcal{M}(KG))$ 72
5.1 Computation of Valuations 73
5.2 Decomposition of Local Wild Resolvends II 81
5.3 Proof of Theorem 1.2.8 89

6 Commutativity of the Basic Diagram 91
6.1 The Top Row: Hochschild-Serre Sequence 92
6.2 The Bottom Row: Fröhlich-Wall Sequence 95
6.3 Proof of Theorem 1.4.4 100

7 Characterization of the tame Σ-A-Realizable Classes in Cl$(\mathcal{O}_K G)$ 102
7.1 Choices of Embeddings and Uniformizers 103
7.2 Embeddings of Groups of Ideles 106
7.3 Preliminary Definitions 111
7.4 Proof of Theorem 1.4.5 (a) 113
7.5 The Quotient $\mathcal{A}^t_\Sigma(\mathcal{O}_K G)_V/\mathcal{A}^t_s(\mathcal{O}_K G)_V$ 116
7.6 Proof of Theorem 1.4.5 (b) 117

Bibliography 119

Chapter 1

Introduction

Let K be a number field with ring of integers $\mathcal{O}_K$ and let G be a finite group. The set of isomorphism classes of G-Galois K-algebras (see Section 2.3 for a brief review of Galois algebras) is in bijective correspondence with the pointed set $H^1(\Omega_K, G)$, where Ω_K is the absolute Galois group of K acting trivially on G. Given $h \in H^1(\Omega_K, G)$, we will write K_h for a Galois algebra representative of h and $\mathcal{O}_h$ for its ring of integers.

The Galois module structure of $\mathcal{O}_h$ has been a classical problem of interest in number theory (see Section 1.1 for a brief overview). In this dissertation, we will instead consider the Galois module structure of the fractional ideal A_h in K_h whose square is the inverse different of K_h/K (see Sections 1.2 to 1.4 for more details).

1.1 Galois Module Structure of Rings of Integers

Given $h \in H^1(\Omega_K, G)$, a classical theorem of E. Noether (see [11, Chapter I, Section 3], for example) implies that $\mathcal{O}_h$ is locally free over $\mathcal{O}_K G$ when K_h/K is tame. In view of this result, define

$$H_t^1(\Omega_K, G) := \{h \in H^1(\Omega_K, G) \mid K_h/K \text{ is tame}\}$$

and consider only the elements $h \in H_t^1(\Omega_K, G)$. In this case, the structure of $\mathcal{O}_h$ as a $\mathbb{Z}G$-module is completely understood due to a result of M. Taylor (see [22, Theorem 1]). For example, if G is abelian or if G has odd order, then $\mathcal{O}_h$ is free over $\mathbb{Z}G$. But very little is known about the structure of $\mathcal{O}_h$ as an $\mathcal{O}_KG$-module. We will recall some known results.

First of all, since $\mathcal{O}_h$ is locally free over $\mathcal{O}_KG$ (of rank one), it defines a class $\mathrm{cl}(\mathcal{O}_h)$ in the locally free class group $\mathrm{Cl}(\mathcal{O}_KG)$ of $\mathcal{O}_KG$. Such a class in $\mathrm{Cl}(\mathcal{O}_KG)$ is said to be *realizable*, and we will write $R(\mathcal{O}_KG)$ for the set of all realizable classes in $\mathrm{Cl}(\mathcal{O}_KG)$. In other words, the set $R(\mathcal{O}_KG)$ is the image of the natural map

$$\mathrm{gal} : H_t^1(\Omega_K, G) \longrightarrow \mathrm{Cl}(\mathcal{O}_KG); \quad \mathrm{gal}(h) := \mathrm{cl}(\mathcal{O}_h). \tag{1.1.1}$$

It is natural to ask for the properties of gal as well as the structure of the set $R(\mathcal{O}_KG)$.

For the moment, assume that G is abelian. Then, the pointed set $H^1(\Omega_K, G)$ is equal to $\mathrm{Hom}(\Omega_K, G)$ and thus has a group structure. It also contains $H_t^1(\Omega_K, G)$ as a subgroup (see Remark 2.3.5). However, the map gal is not a homomorphism in general, and so it is unclear whether $R(\mathcal{O}_KG)$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_KG)$. In [14, Theorem 6.17 and Corollary 6.20], L. McCulloh gave a complete characterization of the set $R(\mathcal{O}_KG)$ and showed that it is indeed a subgroup of $\mathrm{Cl}(\mathcal{O}_KG)$. His result in [14, Theorem 6.7] also implies that gal is *weakly multiplicative* in the following sense. For each $h \in H^1(\Omega_K, G)$, define

$$d(h) := \{\text{the primes in } \mathcal{O}_K \text{ which are ramified in } K_h/K\}. \tag{1.1.2}$$

Then, for all $h_1, h_2 \in H_t^1(\Omega_K, G)$ with $d(h_1) \cap d(h_2) = \emptyset$, we have

$$\mathrm{gal}(h_1h_2) = \mathrm{gal}(h_1)\mathrm{gal}(h_2). \tag{1.1.3}$$

This weak multiplicativity of gal was also proved in [3, Proposition 3.10] by J. Brinkhuis.

1.2 The Square Root of the Inverse Different I

In this section, assume that G has odd order. Given $h \in H^1(\Omega_K, G)$, we will write A_h for the fractional ideal in K_h whose square is the inverse different of K_h/K. Note that the inverse different of K_h/K indeed has a square root by Proposition 1.2.1 below because G has odd order.

Proposition 1.2.1 *Let p be a prime and let $F/\mathbb{Q}_p$ be a finite extension. Let N/F be a finite Galois extension with different ideal $\mathfrak{D}_{N/F}$ and let π_N be a uniformizer in N. Then, we have $\mathfrak{D}_{N/F} = (\pi_N)^{v_N(\mathfrak{D}_{N/F})}$ for*

$$v_N(\mathfrak{D}_{N/F}) = \sum_{n=0}^{\infty}(|\mathit{Gal}(N/F)_n| - 1), \tag{1.2.1}$$

where $\mathit{Gal}(N/F)_n$ denotes the n-th ramification group of N/F in lower numbering.

Proof. See [20, Chapter IV, Proposition 4], for example. We remark that (1.2.1) is also known as Hilbert's formula. ■

Given $h \in H^1(\Omega_K, G)$, a theorem of B. Erez (see [8, Theorem 1 in Section 2]) implies that A_h is locally free over $\mathcal{O}_K G$ when K_h/K is *weakly ramified* (see Definition 2.3.4). In view of this result, define

$$H^1_w(\Omega_K, G) := \{h \in H^1(\Omega_K, G) \mid K_h/K \text{ is weakly ramified}\}$$

and consider only the elements $h \in H^1_w(\Omega_K, G)$. In this case, the structure of A_h as a $\mathbb{Z}G$-module is reasonably understood. For example, we have that A_h is free over $\mathbb{Z}G$ if K_h/K is tame (see [8, Theorem 4]) or if the wild primes of K_h/K satisfy some suitable hypotheses (see [19, Theorem 1]). On the other hand, nothing is known about the structure of A_h as an $\mathcal{O}_K G$- module, and this is what we will study in this dissertation.

First of all, since A_h is locally free over $\mathcal{O}_K G$ (of rank one), it defines a class $\mathrm{cl}(A_h)$ in the locally free class group $\mathrm{Cl}(\mathcal{O}_K G)$ of $\mathcal{O}_K G$. Such a class in $\mathrm{Cl}(\mathcal{O}_K G)$ is said to be *A-realizable*, and *tame A-realizable* if K_h/K is tame. We will write $\mathcal{A}(\mathcal{O}_K G)$ and $\mathcal{A}^t(\mathcal{O}_K G)$ for the sets of all A-realizable and tame A-realizables classes in $\mathrm{Cl}(\mathcal{O}_K G)$, respectively. In other words, they are the images of $H^1_w(\Omega_K, G)$ and $H^1_t(\Omega_K, G)$, respectively, under the natural map

$$\mathrm{gal}_A : H^1_w(\Omega_K, G) \longrightarrow \mathrm{Cl}(\mathcal{O}_K G); \quad \mathrm{gal}_A(h) := \mathrm{cl}(A_h). \tag{1.2.2}$$

As in the case of rings of integers, we are interested in the properties of gal_A as well as the structures of the sets $\mathcal{A}(\mathcal{O}_K G)$ and $\mathcal{A}^t(\mathcal{O}_K G)$.

For the moment, assume that G is abelian. As pointed out in Section 1.1, the pointed set $H^1(\Omega_K, G)$ has a group structure and it contains $H^1_t(\Omega_K, G)$ as a subgroup. However, it only contains $H^1_w(\Omega_K, G)$ as a subset and gal_A restricted to the subgroup $H^1_t(\Omega_K, G)$ is not a homomorphism in general. Nevertheless, we will show that gal_A preserves inverses and is weakly multiplicative in the sense of (1.1.3). More precisely, we will prove (recall the notation introduced in (1.1.2)):

Theorem 1.2.2 *Let K be a number field and let G be a finite abelian group of odd order. For all $h, h_1, h_2 \in H^1_w(\Omega_K, G)$ with $d(h_1) \cap d(h_2) = \emptyset$, we have*

(a) $h^{-1} \in H^1_w(\Omega_K, G)$ and $gal_A(h^{-1}) = gal_A(h)^{-1}$; and

(b) $h_1h_2 \in H^1_w(\Omega_K, G)$ and $gal_A(h_1h_2) = gal_A(h_1)gal_A(h_2)$.

Because the map gal_A restricted to $H^1_t(\Omega_K, G)$ is not a homomorphism in general, it is unclear whether $\mathcal{A}^t(\mathcal{O}_K G)$ is subgroup of $\mathrm{Cl}(\mathcal{O}_K G)$. By using the techniques developed by McCulloh in [14], we will give a complete characterization of the set $\mathcal{A}^t(\mathcal{O}_K G)$ (see (4.4.6)) and show that it is indeed a subgroup of $\mathrm{Cl}(\mathcal{O}_K G)$. More precisely, we will prove:

Theorem 1.2.3 *Let K be a number field and let G be a finite abelian group of odd order. Then, the set $\mathcal{A}^t(\mathcal{O}_K G)$ is a subgroup of $Cl(\mathcal{O}_K G)$. Moreover, given $c \in \mathcal{A}^t(\mathcal{O}_K G)$ and a finite set T of primes in $\mathcal{O}_K$, there exists $h \in H^1_t(\Omega_K, G)$ such that*

(1) K_h/K is a field extension;

(2) K_h/K is unramified at all $v \in T$;

(3) $c = cl(A_h)$.

Observe that each $h \in H^1_t(\Omega_K, G)$ gives rise to two classes in $\mathrm{Cl}(\mathcal{O}_K G)$, namely $\mathrm{cl}(\mathcal{O}_h)$ and $\mathrm{cl}(A_h)$. It is then natural to ask how they are related. We will prove:

Theorem 1.2.4 *Let K be a number field and let G be a finite abelian group of odd order. We have $cl(A_h)cl(\mathcal{O}_h) = cl(\mathcal{O}_{h^2})$ for all $h \in H^1_t(\Omega_K, G)$, and hence $\mathcal{A}^t(\mathcal{O}_K G) \subset R(\mathcal{O}_K G)$.*

Remark 1.2.5 The equality in Theorem 1.2.4 is essentially a special case of a result of D. Burns (see [4, Theorem 1.4]).

Next, we consider the A-realizable classes $\mathrm{cl}(A_h)$ for the elements $h \in H^1_w(\Omega_K, G)$ that do not belong to $H^1_t(\Omega_K, G)$. Using the characterization of $\mathcal{A}^t(\mathcal{O}_K G)$ given in (4.4.6), we will prove that a class $\mathrm{cl}(A_h) \in \mathcal{A}(\mathcal{O}_K G)$ in fact belongs to $\mathcal{A}^t(\mathcal{O}_K G)$ if the wild primes of K_h/K satisfies suitable hypotheses. More precisely, we will prove:

Theorem 1.2.6 *Let K be a number field and let G be a finite abelian group of odd order. Let $h \in H^1_w(\Omega_K, G)$ and let V denote the set of primes in $\mathcal{O}_K$ which are wildly ramified in K_h/K. If*

(1) every $v \in V$ is unramified over $\mathbb{Q}$; and

(2) the ramification index of every $v \in V$ in K_h/K is prime,

then we have $cl(A_h) \in \mathcal{A}^t(\mathcal{O}_K G)$*.*

Remark 1.2.7 Assume further that every rational prime dividing $|G|$ is totally split in the extension $K/\mathbb{Q}$. Then, using [23, Theorem 1.1], it may be shown that conditions (1) and (2) in Theorem 1.2.6 are always satisfied. In this case, we have $\mathcal{A}(\mathcal{O}_K G) = \mathcal{A}^t(\mathcal{O}_K G)$.

In view of Remark 1.2.7, it is natural to ask whether the sets $\mathcal{A}(\mathcal{O}_K G)$ and $\mathcal{A}^t(\mathcal{O}_K G)$ are always equal. We will prove that this is so if we extend scalars to the maximal $\mathcal{O}_K$-order $\mathcal{M}(KG)$ in KG. More precisely, let $\mathrm{Cl}(\mathcal{M}(KG))$ denote the locally free class group of $\mathcal{M}(KG)$ and let

$$\Psi : \mathrm{Cl}(\mathcal{O}_K G) \longrightarrow \mathrm{Cl}(\mathcal{M}(KG))$$

be the natural homomorphism afforded by extension of scalars. We will prove:

Theorem 1.2.8 *Let K be a number field and let G be a finite abelian group of odd order. Then, we have $\Psi(\mathcal{A}(\mathcal{O}_K G)) = \Psi(\mathcal{A}^t(\mathcal{O}_K G))$.*

1.3 The Square Root of the Inverse Different II

In this section, we continue to assume that G has odd order. Given $h \in H^1(\Omega_K, G)$, let Tr_h denote the trace map of K_h/K. It is well-known that A_h is self-dual with respect to Tr_h (this follows from [12, Chapter 3, (2.14)], for example). In other words, we have

$$A_h = \{a \in K_h \mid Tr_h(aA_h) \subset \mathcal{O}_K\}.$$

The map Tr_h then induces a G-invariant symmetric $\mathcal{O}_K$-bilinear form $A_h \times A_h \longrightarrow \mathcal{O}_K$ on A_h. On the other hand, observe that there is a canonical G-invariant symmetric $\mathcal{O}_K$-bilinear from t_K on $\mathcal{O}_K G$ for which the elements of G form an orthonormal basis. That is, we have $t_K(s,t) = \delta_{st}$ for all $s, t \in G$.

As in Section 1.2, we consider only the elements $h \in H^1_w(\Omega_K, G)$, in which case A_h is locally free over $\mathcal{O}_K G$ (of rank one) by [8, Theorem 1 in Section 2]. In other words, for every prime v in $\mathcal{O}_K$, there is an isomorphism $\mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} A_h \simeq \mathcal{O}_{K_v} G$, where $\mathcal{O}_{K_v}$ denotes the ring of integers in the completion K_v of K at the prime v. It is natural to ask whether this isomorphism may be chosen such that the bilinear forms Tr_h and t_K are preserved, that is, whether (A_h, Tr_h) is *locally G-isometric* to $(\mathcal{O}_K G, t_K)$ (see Definition 2.2.6).

Remark 1.3.1 For $K = \mathbb{Q}$ and G abelian, Erez and J. Morales showed in [9, Theorem 4.1] that (A_h, Tr_h) is in fact *G-isometric* to $(\mathbb{Z}G, t_{\mathbb{Q}})$ (see Definition 2.2.1).

In what follows, assume in addition that G is abelian so that $\mathrm{UCl}(\mathcal{O}_K G)$, the *unitary class group of $\mathcal{O}_K G$*, is defined (see Subsection 2.2.2). As we will see in Section 3.1, the pair (A_h, Tr_h) is locally G-isometric to $(\mathcal{O}_K G, t_K)$ in this case, and hence determines a class $\mathrm{ucl}(A_h)$ in $\mathrm{UCl}(\mathcal{O}_K G)$. By abuse of terminology, such a class in $\mathrm{UCl}(\mathcal{O}_K G)$ will also be called *A-realizable*, and *tame A-realizable* if K_h/K is tame. We will write $\mathcal{A}_u(\mathcal{O}_K G)$ and $\mathcal{A}^t_u(\mathcal{O}_K G)$ for the sets of all A-realizable and tame A-realizable classes, that is, the images of $H^1_w(\Omega_K, G)$ and $H^1_t(\Omega_K, G)$, respectively, under the natural map

$$\mathrm{gal}_{A,u} : H^1_w(\Omega_K, G) \longrightarrow \mathrm{UCl}(\mathcal{O}_K G); \quad \mathrm{gal}_{A,u}(h) := \mathrm{ucl}(A_h).$$

We are interested in the properties of $\mathrm{gal}_{A,u}$ as well as the structures of both $\mathcal{A}_u(\mathcal{O}_K G)$ and $\mathcal{A}^t_u(\mathcal{O}_K G)$. Similar to Theorems 1.2.2, 1.2.3, and 1.2.6, we will prove (recall (1.1.2)):

Theorem 1.3.2 *Let K be a number field and let G be a finite abelian group of odd order. For all $h, h_1, h_2 \in H^1_w(\Omega_K, G)$ with $d(h_1) \cap d(h_2) = \emptyset$, we have*

(a) $h^{-1} \in H^1_w(\Omega_K, G)$ and $gal_{A,u}(h^{-1}) = gal_{A,u}(h)^{-1}$; and

(b) $h_1 h_2 \in H^1_w(\Omega_K, G)$ and $gal_{A,u}(h_1 h_2) = gal_{A,u}(h_1) gal_{A,u}(h_2)$.

Theorem 1.3.3 *Let K be a number field and let G be a finite abelian group of odd order. Then, the set $\mathcal{A}_u^t(\mathcal{O}_K G)$ is a subgroup of $UCl(\mathcal{O}_K G)$. Moreover, given $c \in \mathcal{A}_u^t(\mathcal{O}_K G)$ and a finite set T of primes in $\mathcal{O}_K$, there exists $h \in H_t^1(\Omega_K, G)$ such that*

(1) K_h/K is a field extension;

(2) K_h/K is unramified at all $v \in T$;

(3) $c = ucl(A_h)$.

Theorem 1.3.4 *Let K be a number field and let G be a finite abelian group of odd order. Let $h \in H_w^1(\Omega_K, G)$ and let V denote the set of primes in $\mathcal{O}_K$ which are wildly ramified in K_h/K. If*

(1) every $v \in V$ is unramified over $\mathbb{Q}$; and

(2) the ramification index of every $v \in V$ in K_h/K is prime,

then we have $ucl(A_h) \in \mathcal{A}_u^t(\mathcal{O}_K G)$.

Remark 1.3.5 In [15, Theorem 3.6], Morales proved that if G has prime order and the field K contains all $|G|$-th roots of unity, then $\mathcal{A}_u^t(\mathcal{O}_K G)$ is a subgroup of $\mathrm{UCl}(\mathcal{O}_K G)$. Thus, Theorem 1.3.3 is a generalization of his result.

Remark 1.3.6 There is a natural homomorphism (cf. Remark 2.2.11)

$$\Phi : \mathrm{UCl}(\mathcal{O}_K G) \longrightarrow \mathrm{Cl}(\mathcal{O}_K G); \quad \Phi([(X, T)]) = [X] \tag{1.3.1}$$

afforded by forgetting the given G-invariant symmetric $\mathcal{O}_K$-bilinear form T on any locally free $\mathcal{O}_K G$-module X. Theorems 1.3.2, 1.3.3 and 1.3.4 are therefore refinements of Theorems 1.2.2, 1.2.3 and 1.2.6, respectively. In fact, their proofs are essentially the same. To avoid repetition, we will only give the proofs of Theorems 1.3.2, 1.3.3 and 1.3.4.

1.4 Relation to the Study of Embedding Problems

In this section, assume that G is abelian and let K/k be a Galois subextension of K. Moreover, set $\Sigma := \mathrm{Gal}(K/k)$ and fix a left Σ-module structure on G.

Definition 1.4.1 Given a group extension

$$E_\Gamma : \quad 1 \longrightarrow G \longrightarrow \Gamma \longrightarrow \Sigma \longrightarrow 1$$

of Σ by G, a *solution* to the embedding problem $(K/k, G, E_\Gamma)$ is a Galois extension N/K for which N/k is Galois, and there exist isomorphisms $\mathrm{Gal}(N/K) \simeq G$ and $\mathrm{Gal}(N/k) \simeq \Gamma$ such that the diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(N/K) \arrow[r] \arrow[d, leftrightarrow, "\simeq"] & \mathrm{Gal}(N/k) \arrow[r] \arrow[d, leftrightarrow, "\simeq"] & \mathrm{Gal}(K/k) \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & G \arrow[r] & \Gamma \arrow[r] & \Sigma \arrow[r] & 1
\end{tikzcd}$$

commutes. If N/K is tame in addition, then we will call N/K a *tame solution*.

In [3], Brinkhuis connected the study of realizable classes to that of embedding problems (cf. Remark 1.4.3) by means of the following commutative diagram, called the *basic diagram* (see Chapter 6 below for the construction).

$$\begin{tikzcd}
H^1(\mathrm{Gal}(K^t/k), G) \arrow[r, "\mathrm{res}"] & \mathrm{Hom}(\Omega_K^t, G)^\Sigma \arrow[r, "tr"] \arrow[d, "\mathrm{gal}"'] & H^2(\Sigma, G) \arrow[d, "i^*"] \\
 & \mathrm{Cl}(\mathcal{O}_K G)^\Sigma \arrow[r, "\xi"] & H^2(\Sigma, (\mathcal{O}_K G)^\times)
\end{tikzcd} \quad (1.4.1)$$

Moreover, the top row is exact and all of the maps except possibly gal (recall (1.1.1)) are homomorphisms (cf. Remark 6.3.2). Here K^t is the maximal tamely ramified extension of K in some fixed algebraic closure of K and $\Omega_K^t := \mathrm{Gal}(K^t/K)$. Observe that we may identify $\mathrm{Hom}(\Omega_K^t, G)$ with $H_t^1(\Omega_K, G)$ since G is abelian (see Remark 2.3.5).

Remark 1.4.2 Diagram (1.4.1) is a modified and abridged version of the basic diagram constructed by Brinkhuis in [3, Theorem 5.1]. For example, the Picard group of $\mathcal{O}_K G$ was used in place of the locally free class group of $\mathcal{O}_K G$, but these two groups are canonically isomorphic for G abelian (see [7, Theorem 55.26], for example).

Remark 1.4.3 We will see in Proposition 6.1.2 below that a surjective $h \in \mathrm{Hom}(\Omega_K^t, G)^\Sigma$ gives rise to a tame solution to the embedding problem $(K/k, G, E_h)$, where E_h is determined by $tr(h)$. Now, suppose that i^* (see (6.0.2)) is injective (as is shown in [2, Theorem 4.1], this is so if K is a C.M. field and G or Σ has odd order). If $tr(h) \neq 1$ (which corresponds to E_h being non-split), then $\mathrm{cl}(\mathcal{O}_h) \neq 1$ as well since (1.4.1) commutes and ξ is a homomorphism.

In what follows, assume further that G has odd order. Essentially the same proof as that of [3, Theorem 5.1] will show that (1.4.1) is still commutative when gal is replaced by gal_A. More precisely, we will prove:

Theorem 1.4.4 *Let K/k be a Galois extension of number fields and set $\Sigma := Gal(K/k)$. Let G be a finite abelian group of odd order equipped with a fixed left Σ-module structure. Then, there is a commutative diagram*

$$\begin{tikzcd}
H^1(Gal(K^t/k), G) \arrow[r, "res"] & Hom(\Omega_K^t, G)^\Sigma \arrow[r, "tr"] \arrow[d, "gal_A"'] & H^2(\Sigma, G) \arrow[d, "i^*"] \\
& Cl(\mathcal{O}_K G)^\Sigma \arrow[r, "\xi"] & H^2(\Sigma, (\mathcal{O}_K G)^\times)
\end{tikzcd} \quad , \qquad (1.4.2)$$

where the top row is exact and all of the maps except possibly gal_A are homomorphisms.

A similar remark to Remark 1.4.3 shows that the commutativity of (1.4.2) relates the study of tame A-realizable classes to that of embedding problems.

Now, recall from Theorem 1.2.3 that $\mathcal{A}^t(\mathcal{O}_K G)$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_K G)$. In view of Theorem 1.4.4, it is then natural to ask whether the group structure of $\mathcal{A}^t(\mathcal{O}_K G)$ is also related to the study of embedding problems. For example, define

$$\begin{aligned}\mathcal{A}^t_\Sigma(\mathcal{O}_K G) &:= \{\mathrm{cl}(A_h) : h \in \mathrm{Hom}(\Omega^t_K, G)^\Sigma\};\\ \mathcal{A}^t_s(\mathcal{O}_K G) &:= \{\mathrm{cl}(A_h) : h \in \mathrm{Hom}(\Omega^t_K, G)^\Sigma \text{ and } tr(h) = 1\}.\end{aligned}$$

Classes in $\mathcal{A}^t_\Sigma(\mathcal{O}_K G)$ are said to be *tame* Σ*-*A*-realizable.* We want to determine whether the above subsets of $\mathcal{A}^t(\mathcal{O}_K G)$ are in fact subgroups, and if so, whether the group structure of their quotient $\mathcal{A}^t_\Sigma(\mathcal{O}_K G)/\mathcal{A}^t_s(\mathcal{O}_K G)$ is related to that of $H^2(\Sigma, G)$.

We will prove the following partial result. Given a set V of primes in $\mathcal{O}_K$, define

$$\mathrm{Hom}(\Omega^t_K, G)^\Sigma_V := \{h \in \mathrm{Hom}(\Omega^t_K, G)^\Sigma \mid K_h/K \text{ is unramified at all } v \in V\} \qquad (1.4.3)$$

and

$$\begin{aligned}\mathcal{A}^t_\Sigma(\mathcal{O}_K G)_V &:= \{\mathrm{cl}(A_h) : h \in \mathrm{Hom}(\Omega^t_K, G)^\Sigma_V\};\\ \mathcal{A}^t_s(\mathcal{O}_K G)_V &:= \{\mathrm{cl}(A_h) : h \in \mathrm{Hom}(\Omega^t_K, G)^\Sigma_V \text{ with } tr(h) = 1\}.\end{aligned}$$

Write $\exp(G)$ for the exponent of the group G. We will prove:

Theorem 1.4.5 *Let K/k be a Galois extension of number fields and set $\Sigma := Gal(K/k)$. Let G be a finite abelian group of odd order on which Σ acts trivially on the left. Define $V = V_K$ to the set of primes in $\mathcal{O}_K$ which are ramified over k. Assume that k contains all* $\exp(G)$*-th roots of unity.*

(a) *The set* $\mathcal{A}^t_\Sigma(\mathcal{O}_KG)_V$ *is a subgroup of* $Cl(\mathcal{O}_KG)$*. Furthermore, given* $h \in Hom(\Omega^t_K, G)^\Sigma_V$ *and a finite set* T *of primes in* $\mathcal{O}_K$*, there exists* $h' \in Hom(\Omega^t_K, G)^\Sigma_V$ *such that*

(1) $K_{h'}/K$ *is a field extension;*

(2) $K_{h'}/K$ *is unramified at all* $v \in T$*;*

(3) $cl(A_{h'}) = cl(A_h)$*;*

(4) $tr(h') = tr(h)$*.*

In particular, the set $\mathcal{A}^t_s(\mathcal{O}_KG)_V$ *is also a subgroup of* $Cl(\mathcal{O}_KG)$*.*

(b) *The natural surjective map*

$$\phi_A : tr(Hom(\Omega^t_K, G)^\Sigma_V) \longrightarrow \frac{\mathcal{A}^t_\Sigma(\mathcal{O}_KG)_V}{\mathcal{A}^t_s(\mathcal{O}_KG)_V}; \quad \phi_A(tr(h)) := cl(A_h)\mathcal{A}^t_s(\mathcal{O}_KG)_V,$$

where $h \in Hom(\Omega^t_K, G)^\Sigma_V$*, is well-defined and is a homomorphism. Furthermore, if* i^* *is injective, then* ϕ_A *is an isomorphism.*

Remark 1.4.6 Theorem 1.4.5 still holds when A_h is replaced by $\mathcal{O}_h$, in which case the hypothesis that G has odd order is not required. The proofs of the analogous statements are verbatim. We simply have to use the characterization of $\mathrm{cl}(\mathcal{O}_h)$ given in [14, Theorem 6.7] rather than that of $\mathrm{cl}(A_h)$ given in Theorem 4.3.2 for $h \in \mathrm{Hom}(\Omega^t_K, G)$. Similarly, we have to use the commutativity of (1.4.1) rather than that of (1.4.2).

1.5 Previously Copyrighted Materials

Theorems 1.2.2, 1.2.3, 1.2.6, and a special case of Theorem 1.2.8 were first published in *On the Galois module structure of the square root of the inverse different in abelian extensions*, C. Tsang, J. Number Theory 160, Copyright @ 2016 Elsevier.

Theorems 1.3.2, 1.3.3, and 1.3.4 will soon appear in *On the realizable classes of the square root of the inverse different in the unitary class group*, C. Tsang, Int. J. Number Theory, Copyright @ 2016 World Scientific.

1.6 Notation and Conventions

Throughout this dissertation, we will fix a number field K and a finite group G. We will also fix a Galois subextension K/k of K and set $\Sigma := \mathrm{Gal}(K/k)$. Moreover, we will use the convention that all of the homomorphisms in the cohomology groups considered are continuous.

The symbol F will denote either a number field or a finite extension of $\mathbb{Q}_p$, where p is a prime number. Given such an F, we will define:

$$\begin{aligned}
\mathcal{O}_F &:= \text{the ring of integers in } F;\\
F^c &:= \text{a fixed algebraic closure of } F;\\
\mathcal{O}_{F^c} &:= \text{the integral closure of } \mathcal{O}_F \text{ in } F^c;\\
\Omega_F &:= \mathrm{Gal}(F^c/F);\\
F^t &:= \text{the maximal tamely ramified extension of } F \text{ in } F^c;\\
\Omega_F^t &:= \mathrm{Gal}(F^t/F);\\
M_F &:= \text{the set of all finite primes in } F;\\
[-1] &:= \text{the involution on } F^cG \text{ induced by the involution } s \mapsto s^{-1} \text{ on } G;\\
t_F &:= \text{the symmetric } G\text{-invariant } \mathcal{O}_F\text{-bilinear form } \mathcal{O}_FG \times \mathcal{O}_FG \longrightarrow \mathcal{O}_F\\
&\qquad \text{on } \mathcal{O}_FG \text{ for which } t_F(s,t) = \delta_{st} \text{ for all } s,t \in G.
\end{aligned}$$

We will let Ω_F and Ω_F^t act trivially on G on the left. We will further choose a compatible set $\{\zeta_n : n \in \mathbb{Z}^+\}$ of primitive roots of unity in F^c, that is to say, we have $(\zeta_{mn})^n = \zeta^n$ for all $m, n \in \mathbb{Z}^+$. For G abelian, we will write $\widehat{G}$ for the group of irreducible F^c-valued characters on G, and $\mathcal{M}(FG)$ for the unique maximal $\mathcal{O}_F$-order in FG.

Remark 1.6.1 Let $\mathbb{Q}^c$ denote a fixed algebraic closure of $\mathbb{Q}$ containing K. Naturally, we will choose $K^c = \mathbb{Q}^c$ and $k^c = \mathbb{Q}^c$. Moreover, we will choose the same compatible set of primitive roots of unity in $\mathbb{Q}^c$ for both k and K.

For F a number field and given $v \in M_F$, let F_v denote the completion of F at v and write $i_v : F^c \longrightarrow F_v^c$ for a fixed embedding extending the natural embedding $F \longrightarrow F_v$. By abuse of notation, we will also write i_v for the F-isomorphism $F^c \longrightarrow i_v(F^c)$ induced by i_v and i_v^{-1} for its inverse. Let $\widetilde{i_v}$ be the embedding $\Omega_{F_v} \longrightarrow \Omega_F$ induced by i_v. More specifically, we have

$$\widetilde{i_v}(\omega) := i_v^{-1} \circ \omega \circ i_v \qquad \text{for all } \omega \in \Omega_{F_v}. \tag{1.6.1}$$

Finally, if $\{\zeta_n : n \in \mathbb{Z}^+\}$ is the chosen compatible set of distinguished primitive roots of unity in F^c, then we will choose $\{i_v(\zeta_n) : n \in \mathbb{Z}^+\}$ to be that in F_v^c.

For F a finite extension of $\mathbb{Q}_p$ and given a finite extension N/F, let π_N denote a uniformizer in N and write q_N for the order of the residue field $\mathcal{O}_N/(\pi_N)$. Let v_N denote the additive valuation $N \longrightarrow \mathbb{Z} \cup \{\infty\}$ on N for which $v_N(\pi_N) = 1$. Given a fractional $\mathcal{O}_N$-ideal $\mathfrak{A}$ in N, we will also write $v_N(\mathfrak{A})$ for the unique integer for which $\mathfrak{A} = (\pi_N)^{v_N(\mathfrak{A})}$. Moreover, define:

$$\begin{aligned} e(N/F) &:= \text{the ramification index of } N/F; \\ F_{\pi_N,n} &:= \text{the } n\text{-th Lubin-Tate division field of } N \text{ corresponding to } \pi_N \end{aligned}$$

for each $n \in \mathbb{Z}_{\geq 0}$. Finally, if N/F is Galois, let $\mathrm{Gal}(N/F)_n$ denote the n-th ramification group of N/F in lower numbering for each $n \in \mathbb{Z}_{\geq 0}$, and write $A_{N/F}$ for the square root of the inverse of N/F if it exists.

Chapter 2

Prerequisites

2.1 Locally Free Class Groups

Let F be number field and let Λ be an $\mathcal{O}_F$-order in FG. We will recall the definition and an idelic description of the locally free class group $\mathrm{Cl}(\Lambda)$ of Λ (see [7, Chapter 6] for more details).

Definition 2.1.1 A Λ-*lattice* is a left Λ-module which is finitely generated and projective as an $\mathcal{O}_F$-module. Two Λ-lattices X and X' are *stably isomorphic* if there exists $k \in \mathbb{Z}^+$ such that $X \oplus \Lambda^k \simeq X' \oplus \Lambda^k$. The stable isomorphism class of X will be denoted by $[X]$.

Remark 2.1.2 If two Λ-lattices are isomorphic, then plainly they are stably isomorphic. The converse holds as well when G is abelian or when G has odd order (see [7, Theorems 51.2 and 51.24], for example).

Definition 2.1.3 Let X be a Λ-lattice. For each $v \in M_F$, define $X_v := \mathcal{O}_{F_v} \otimes_{\mathcal{O}_F} X$. We say that X is *locally isomorphic to* Λ or *locally free over* Λ *(of rank one)* if $X_v \simeq \Lambda_v$ as Λ_v-modules for all $v \in M_F$. The set of all such Λ-lattices will be denoted by $g(\Lambda)$.

Definition 2.1.4 The *locally free class group of $\mathcal{O}_F G$* is defined to be the set

$$\mathrm{Cl}(\mathcal{O}_F G) := \{[X] : X \in g(\Lambda)\}$$

equipped with the following group operation. Given $X, X' \in g(\Lambda)$, by [6, Corollary 31.7] there exists $X'' \in g(\Lambda)$ such that $X \oplus X' \simeq \mathcal{O}_F G \oplus X''$. It is simple to verify that $[X'']$ is uniquely determined by $[X]$ and $[X']$. We then define $[X][X'] := [X'']$.

Remark 2.1.5 The group operation of $\mathrm{Cl}(\Lambda)$ is usually written additively. Since we will use an idelic description of $\mathrm{Cl}(\Lambda)$, we will write it multiplicatively instead.

Definition 2.1.6 Let $J(FG)$ be the restricted direct product of the groups $(F_v G)^\times$ with respect to the subgroups $\Lambda_v^\times$ for $v \in M_F$. This definition does not depend on the choice of the $\mathcal{O}_F$-order Λ, since if Λ' is another $\mathcal{O}_F$-order in FG, then $\Lambda_v = \Lambda'_v$ for all but finitely many $v \in M_F$. Let

$$\partial = \partial_F : (FG)^\times \longrightarrow J(FG)$$

be the diagonal map and let

$$U(\Lambda) := \prod_{v \in M_F} \Lambda_v^\times$$

be the group of unit ideles.

The locally free Λ-lattices in FG are precisely those of the form

$$\Lambda \cdot c := \bigcap_{v \in M_F} (\Lambda_v \cdot c_v \cap FG), \tag{2.1.1}$$

where c ranges over all ideles in $J(FG)$. The map

$$j_\Lambda : J(FG) \longrightarrow \mathrm{Cl}(\Lambda); \quad j_\Lambda(c) := [\Lambda \cdot c] \tag{2.1.2}$$

is surjective because every $X \in g(\Lambda)$ may be embedded into FG, and is also a homomorphism by [6, Theorem 31.19]. If $\Lambda = \mathcal{O}_F G$, then we will write j for $j_{\mathcal{O}_F G}$ for simplicity.

Theorem 2.1.7 *If G is abelian, then the map j_Λ induces an isomorphism*

$$Cl(\Lambda) \simeq \frac{J(FG)}{\partial((FG)^\times)U(\Lambda)}.$$

Proof. See [7, Theorem 49.22 and Exercise 51.1], for example. ■

2.2 G-Forms and Unitary Class Groups

2.2.1 G-Forms

Let F be a number field or a finite extension of $\mathbb{Q}_p$. First, we will recall the definition of G-forms over $\mathcal{O}_F$ and give a brief review of their basic properties.

Definition 2.2.1 A *G-form over $\mathcal{O}_F$* is a pair (X, T) consisting of an $\mathcal{O}_F G$-lattice X and a G-invariant symmetric $\mathcal{O}_F$-bilinear form $T : X \times X \longrightarrow \mathcal{O}_F$ on X. Two G-forms (X, T) and (X', T') over $\mathcal{O}_F$ are said to be *G-isometric (over $\mathcal{O}_F$)* if there exists an isomorphism $\varphi : X \longrightarrow X'$ of $\mathcal{O}_F G$-modules such that

$$T'(\varphi(x), \varphi(y)) = T(x, y) \qquad \text{for all } x, y \in X.$$

Such an isomorphism φ is called a *G-isometry (over $\mathcal{O}_F$)*. The G-isometry class of (X, T) will be denoted by $[(X, T)]$.

Given a G-form (X, T) over $\mathcal{O}_F$, the form T extends uniquely to a G-invariant symmetric F-bilinear form on $F \otimes_{\mathcal{O}_F} X$ via linearity. By abuse of notation, we will use T to denote this F-bilinear form as well.

Definition 2.2.2 Let (X, T) be a G-form over $\mathcal{O}_F$. The *dual of X (with respect to T)* is defined to be the $\mathcal{O}_F$-module

$$X^* := \{x \in F \otimes_{\mathcal{O}_F} X \mid T(x, X) \subset \mathcal{O}_F\}.$$

We say that (X, T) is *self-dual (with respect to T)* if $X = X^*$. An element $x \in F \otimes_{\mathcal{O}_F} X$ is said to be *self dual (with respect to T)* if

$$T(s \cdot x, t \cdot x) = \delta_{st} \qquad \text{for all } s, t \in G.$$

Next, recall that t_F denotes the canonical symmetric $\mathcal{O}_F$-bilinear form on $\mathcal{O}_F G$ for which $t_F(s, t) = \delta_{st}$ for all $s, t \in G$. The G-forms (X, T) over $\mathcal{O}_F$ which are G-isometric to $(\mathcal{O}_F G, t_F)$ are precisely those which admit a free self-dual generator over $\mathcal{O}_F G$.

Proposition 2.2.3 *A G-form (X, T) over $\mathcal{O}_F$ is G-isometric to $(\mathcal{O}_F G, t_F)$ if and only if there exists $x \in X$ such that x is self-dual and $X = \mathcal{O}_F G \cdot x$.*

Proof. If $\varphi : \mathcal{O}_F G \longrightarrow X$ is a G-isometry, then $x := \varphi(1)$ is self-dual and $X = \mathcal{O}_F G \cdot x$. Conversely, if $x \in X$ is self-dual and $X = \mathcal{O}_F G \cdot x$, then the map $\mathcal{O}_F G \longrightarrow X$ defined by $\beta \mapsto \beta \cdot x$ is a G-isometry . ■

Now, recall also that $[-1]$ denotes the involution on $F^c G$ induced by the involution $s \mapsto s^{-1}$ on G. Given $c \in (FG)^\times$, whether the (full) $\mathcal{O}_F G$-lattice $\mathcal{O}_F G \cdot c$ in FG or the element c is self-dual (with respect to t_F) may be determined simply by considering the element $cc^{[-1]} \in (FG)^\times$ when G is abelian.

Proposition 2.2.4 *Assume that G is abelian and let $c \in (FG)^\times$.*

(a) The $\mathcal{O}_F G$-lattice $\mathcal{O}_F G \cdot c$ is self-dual if and only if $cc^{[-1]} \in (\mathcal{O}_F G)^\times$.

(b) The element c is self-dual if and only if $cc^{[-1]} = 1$.

Proof. Since t_F is $\mathcal{O}_F$-bilinear, an element $\beta \in FG$ lies in $\beta \in (\mathcal{O}_F G \cdot c)^*$ if and only if

$$t_F(\beta, sc) \in \mathcal{O}_F \qquad \text{for all } s \in G. \tag{2.2.1}$$

But G is abelian, and so $t_F(\beta, sc) = t_F(\beta c^{[-1]}, s)$, which is the coefficient of s in $\beta c^{[-1]}$, for any $s \in G$. Thus, (2.2.1) is equivalent to $\beta c^{[-1]} \in \mathcal{O}_F G$ and $(\mathcal{O}_F G \cdot c)^* = \mathcal{O}_F G \cdot (c^{[-1]})^{-1}$. It follows that $\mathcal{O}_F G \cdot c$ is self-dual if and only if $cc^{[-1]} \in (\mathcal{O}_F G)^\times$, which proves (a).

As for (b), simply observe that $t_F(sc, tc) = t_F(cc^{[-1]}, s^{-1}t)$ for all $s, t \in G$. It follows that c is self-dual if and only if $cc^{[-1]} = 1$. ■

Definition 2.2.5 In view of Proposition 2.2.4, define

$$\begin{aligned} FG_{(s)} &:= \{c \in (FG)^\times \mid cc^{[-1]} \in (\mathcal{O}_F G)^\times\}; \\ FG_{(1)} &:= \{c \in (FG)^\times \mid cc^{[-1]} = 1\}. \end{aligned}$$

Clearly both of the sets above are subgroups of $(FG)^\times$ when G is abelian.

2.2.2 Unitary Class Groups

Let F be a number field. We will also assume that G is abelian and of odd order. In this subsection, we will define the unitary class group of $\mathcal{O}_F G$, which was first introduced by Morales in [15, Section 2]. Our approach is slightly different, but the resulting group is canonically isomorphic to that defined in [15, Section 2].

Definition 2.2.6 Let (X, T) be a G-form over $\mathcal{O}_F$. For each $v \in M_F$, let T_v denote the G-invariant symmetric $\mathcal{O}_{F_v}$-bilinear on X_v obtained by extending T via linearity. We say that (X, T) is *locally G-isometric to* $(\mathcal{O}_F G, t_F)$ if (X_v, T_v) and $(\mathcal{O}_{F_v} G, t_{F_v})$ are G-isometric over $\mathcal{O}_{F_v}$ for all $v \in M_F$. The set of all such G-forms over $\mathcal{O}_F$ which are also G-isometric to (X', t_F) for some $\mathcal{O}_F G$-lattice X' in FG will be denoted by $g(\mathcal{O}_F G)_s$.

As a set, the unitary class group of $\mathcal{O}_F G$ is defined to be

$$\mathrm{UCl}(\mathcal{O}_F G) := \{[(X,T)] : (X,T) \in g(\mathcal{O}_F G)_s\}.$$

We will show that the set above has a group structure by giving it an idelic description. Note that by the definition of $g(\mathcal{O}_F G)_s$, it suffices to consider the G-forms (X, t_F), where X is an $\mathcal{O}_F G$-lattice contained in FG. The key lies in the following theorem.

Theorem 2.2.7 *Let X be an $\mathcal{O}_F G$-lattice contained in FG. We have $(X, t_F) \in g(\mathcal{O}_F G)_s$ if and only if X is locally free over $\mathcal{O}_F G$ and self-dual with respect to t_F.*

Proof. If $(X, t_F) \in g(\mathcal{O}_F G)_s$, then plainly X is locally free over $\mathcal{O}_F G$ and self-dual with respect to t_F by Propositions 2.2.3. As for the converse, see [9, Corollary 2.4]; we remark that its proof requires that G is abelian and of odd order. ■

Recall that the locally free $\mathcal{O}_F G$-lattices in FG are those of the form $\mathcal{O}_F G \cdot c$ (recall the notation in (2.1.1)), where c ranges over all ideles in $J(FG)$.

Definition 2.2.8 Let $J(FG_{(s)})$ be the restricted direct product of the groups $F_v G_{(s)}$ with respect to the subgroups $(\mathcal{O}_{F_v} G)^{\times}$ for $v \in M_F$.

Proposition 2.2.9 *Let $c, c' \in J(FG)$.*

(a) The G-form $(\mathcal{O}_F G \cdot c, t_F)$ belongs to $g(\mathcal{O}_F G)_s$ if and only if $c \in J(FG_{(s)})$.

(b) The G-forms $(\mathcal{O}_F G \cdot c, t_F)$ and $(\mathcal{O}_F G \cdot c', t_F)$ are G-isometric over $\mathcal{O}_F$ if and only if

$$c' c^{-1} \in \partial(FG_{(1)}) U(\mathcal{O}_F G).$$

Proof. For (a), it is a direct consequence of Proposition 2.2.4 (a) and Theorem 2.2.7. As for (b), observe that an isomorphism $\varphi : \mathcal{O}_F G \cdot c \longrightarrow \mathcal{O}_F G \cdot c'$ is of the form $x \mapsto \beta \cdot x$, where $\beta \in (FG)^\times$ is such that $c'c^{-1} \in \partial(\beta) \cdot U(\mathcal{O}_F G)$. Because t_F is $\mathcal{O}_F$-bilinear and G-invariant, this map φ is a G-isometry if and only if $t_F(\beta \cdot c, \beta \cdot sc) = t_F(c, sc)$ for all $s \in G$, which is equivalent to $t_F(\beta\beta^{[-1]}cc^{[-1]}, s) = t_F(cc^{[-1]}, s)$ for all $s \in G$. This latter condition holds precisely when $\beta\beta^{[-1]}cc^{[-1]} = cc^{[-1]}$, or equivalently when $\beta\beta^{[-1]} = 1$. It then follows that φ is a G-isometry if and only if $\beta \in FG_{(1)}$, and this proves the claim. ■

By Proposition 2.2.9 (a) and the definition of $g(\mathcal{O}_F G)_s$, the map

$$j_{(s)} : J(FG_{(s)}) \longrightarrow \mathrm{UCl}(\mathcal{O}_F G); \quad j_{(s)}(c) := [(\mathcal{O}_F G \cdot c, t_F)]$$

is a well-defined surjection. By Proposition 2.2.9 (b), the above induces a bijection

$$\frac{J(FG_{(s)})}{\partial(FG_{(1)})U(\mathcal{O}_F G)} \longrightarrow \mathrm{UCl}(\mathcal{O}_F G). \tag{2.2.2}$$

Since the quotient on the left is a group, this induces a group structure on $\mathrm{UCl}(\mathcal{O}_F G)$.

Definition 2.2.10 The *unitary class group of* $\mathcal{O}_F G$ is defined to be the set

$$\mathrm{UCl}(\mathcal{O}_F G) := \{[(X, T)] : (X, T) \in g(\mathcal{O}_F G)_s\}$$

equipped with the group structure induced by the bijection (2.2.2).

Remark 2.2.11 It is clear from Definition 2.2.10 and Theorem 2.1.7 that the map defined in Remark 1.3.6 is a homomorphism.

2.3 Galois Algebras and Resolvends

Let F be a number field or a finite extension of $\mathbb{Q}_p$. In this section, we will give a brief review of Galois algebras and resolvends (see [14, Section 1] for more details).

Definition 2.3.1 A *Galois algebra over F with group G* or *G-Galois F-algebra* is a commutative semi-simple F-algebra N on which G acts (on the left) as a group of automorphisms such that $N^G = F$ and $[N : F] = |G|$. Two G-Galois F-algebras are *isomorphic* if there is an F-algebra isomorphism between them which preserves the action of G.

The set of isomorphism classes of G-Galois F-algebras is in bijection with the pointed set (recall that Ω_F acts trivially on G)

$$H^1(\Omega_F, G) := \mathrm{Hom}(\Omega_F, G)/\mathrm{Inn}(G). \tag{2.3.1}$$

In particular, each $h \in \mathrm{Hom}(\Omega_F, G)$ is associated to the F-algebra

$$F_h := \mathrm{Map}_{\Omega_F}({}^hG, F^c),$$

where ${}^hG$ is the group G with Ω_F-action given by $(\omega \cdot s) := h(\omega)s$ for $s \in G$ and $\omega \in \Omega_F$. The G-action on F_h is defined by $(s \cdot a)(t) := a(ts)$ for $a \in F_h$ and $s, t \in G$.

Let $\{s_i\}$ be any set of coset representatives of $h(\Omega_F)\backslash G$. An element $a \in F_h$ is determined by the values $a(s_i)$, and each $a(s_i)$ may be arbitrarily chosen as long as it is fixed by all $\omega \in \ker(h)$. Letting $F^h := (F^c)^{\ker(h)}$, the choices of $\{s_i\}$ then induce an isomorphism

$$F_h \simeq \prod_{h(\Omega_F)\backslash G} F^h \tag{2.3.2}$$

of F-algebras. Since h induces an isomorphism $\mathrm{Gal}(F^h/F) \simeq h(\Omega_F)$, from (2.3.2) we see that $[F_h : F] = [G : h(\Omega_F)][F^h : F] = |G|$. Viewing F as embedded in F_h as the constant F-valued functions, we also have $F_h^G = F$. Hence, indeed F_h is a G-Galois F-algebra.

It is not difficult to verify that every G-Galois F-algebra is isomorphic to F_h for some homomorphism $h \in \mathrm{Hom}(\Omega_F, G)$, and that for $h, h' \in \mathrm{Hom}(\Omega_F, G)$ we have $F_h \simeq F_{h'}$ if and only if h and h' differ by an element in $\mathrm{Inn}(G)$. Hence, indeed the set of isomorphism classes of G-Galois F-algebras is in bijection with (2.3.1).

We make the remark that in the case that G is abelian, the pointed set $H^1(\Omega_F, G)$ is equal to $\mathrm{Hom}(\Omega_F, G)$ and in particular has a group structure.

Definition 2.3.2 Given $h \in \mathrm{Hom}(\Omega_F, G)$, let $F^h := (F^c)^{\ker(h)}$ as above. Let $\mathcal{O}^h := \mathcal{O}_{F^h}$ and define the *ring of integers of* F_h by

$$\mathcal{O}_h := \mathrm{Map}_{\Omega_F}({}^hG, \mathcal{O}^h).$$

If the inverse different of F^h/F has a square root, let $A^h := A_{F^h/F}$ and define the *square root of the inverse different of* F_h/F by

$$A_h := \mathrm{Map}_{\Omega_F}({}^hG, A^h).$$

In the sequel, whenever we write A_h for some $h \in \mathrm{Hom}(\Omega_F, G)$, we are implicitly assuming that $A_{F^h/F}$ exists (by Proposition 1.2.1, this is so when G has odd order).

Remark 2.3.3 For F a number field and $h \in \mathrm{Hom}(\Omega_F, G)$, for each $v \in M_F$ define

$$h_v \in \mathrm{Hom}(\Omega_{F_v}, G); \quad h_v := h \circ \widetilde{i_v}.$$

It is proved in [14, (1.4)] that $(F_v)_{h_v} \simeq F_v \otimes_F F_h$. We then have that $\mathcal{O}_{h_v} \simeq \mathcal{O}_{F_v} \otimes_{\mathcal{O}_F} \mathcal{O}_h$ and $A_{h_v} \simeq \mathcal{O}_{F_v} \otimes_{\mathcal{O}_F} A_h$ as well.

Definition 2.3.4 Given $h \in \mathrm{Hom}(\Omega_F, G)$, we say that F_h/F or h is *unramified* if F^h/F is unramified. Similarly for *tame*, *wild*, and *weakly ramified*. Recall that a finite Galois extension over F is said to be *weakly ramified* if all of the second ramification groups (in lower numbering) attached to it are trivial.

Remark 2.3.5 Clearly a homomorphism $h \in \mathrm{Hom}(\Omega_F, G)$ is tame if and only if it factors through the quotient map $\Omega_F \longrightarrow \Omega_F^t$. Hence, the subset of $\mathrm{Hom}(\Omega_F, G)$ consisting of the tame homomorphisms may be naturally identified with $\mathrm{Hom}(\Omega_F^t, G)$, and is in particular a subgroup of $\mathrm{Hom}(\Omega_F, G)$ in the case that G is abelian.

Now, consider the F^c-algebra $\mathrm{Map}(G, F^c)$ on which we let G act via $(s \cdot a)(t) := a(ts)$ for $a \in \mathrm{Map}(G, F^c)$ and $s, t \in G$. Note that F_h is then an FG-submodule of $\mathrm{Map}(G, F^c)$ for each $h \in \mathrm{Hom}(\Omega_F, G)$.

Definition 2.3.6 The *resolvend map* $\mathbf{r}_G : \mathrm{Map}(G, F^c) \longrightarrow F^cG$ is defined by

$$\mathbf{r}_G(a) := \sum_{s \in G} a(s)s^{-1}.$$

It is clear that $\mathbf{r}_G$ is an isomorphism of F^cG-modules, but not an isomorphism of F^cG-algebras because it does not preserve multiplication. Moreover, given $a \in \mathrm{Map}(G, F^c)$, we have that $a \in F_h$ if and only if

$$\omega \cdot \mathbf{r}_G(a) = \mathbf{r}_G(a)h(\omega) \qquad \text{for all } \omega \in \Omega_F. \tag{2.3.3}$$

In particular, if $\mathbf{r}_G(a)$ is invertible, then h is given by

$$h(\omega) = \mathbf{r}_G(a)^{-1}(\omega \cdot \mathbf{r}_G(a)) \qquad \text{for all } \omega \in \Omega_F.$$

The next proposition shows that resolvends may be used to identify elements $a \in F_h$ for which $F_h = FG \cdot a$ or $\mathcal{O}_h = \mathcal{O}_F G \cdot a$.

Proposition 2.3.7 *Assume that G is abelian and let $a \in F_h$.*

(a) We have $F_h = FG \cdot a$ if and only if $\mathbf{r}_G(a) \in (F^cG)^\times$.

(b) We have $\mathcal{O}_h = \mathcal{O}_F G \cdot a$ with h unramified if and only if $\mathbf{r}_G(a) \in (\mathcal{O}_{F^c} G)^\times$. Furthermore, if F is a finite extension of $\mathbb{Q}_p$ and h is unramified, then there exists $a \in \mathcal{O}_h$ such that $\mathcal{O}_h = \mathcal{O}_F G \cdot a$.

Proof. See [14, Proposition 1.8] for (a) and [14, (2.11)] for the first claim in (b). As for the second claim in (b), it follows from a classical theorem of Noether, or alternatively from [14, Proposition 5.5]. We note that only the first claim in (b) actually requires the assumption that G is abelian. ■

Next, we prove a similar criterion which uses resolvends to identify elements $a \in A_h$ for which $A_h = \mathcal{O}_F G \cdot a$. To that end, let $Tr : \mathrm{Map}(G, F^c) \longrightarrow F^c G$ denote the standard algebra trace map, which is defined by

$$Tr(a) := \sum_{s \in G} a(s),$$

which restricts to the trace map $Tr_h : F_h \longrightarrow F$ of F_h/F for each $h \in \mathrm{Hom}(\Omega_F, G)$. By abuse of notation, we will also write Tr_h for the G-invariant symmetric F-bilinear form $(a, b) \mapsto Tr_h(ab)$ on F_h induced by Tr_h.

Remark 2.3.8 It is well-known that A^h is self-dual with respect to the trace $Tr_{F^h/F}$ of F^h/F (this follows from [12, Chapter 3, (2.14)], for example). From this, we see that A_h is self-dual with respect to Tr_h. In particular, the trace map Tr_h induces a G-invariant symmetric $\mathcal{O}_F$-bilinear form $A_h \times A_h \longrightarrow \mathcal{O}_F$ on A_h and (A_h, Tr_h) is a G-form over $\mathcal{O}_F$.

Recall that $[-1]$ denotes the involution on $F^c G$ induced by the involution $s \mapsto s^{-1}$ on G. Moreover, a simple calculation shows that for all $a, b \in F_h$, we have

$$\mathbf{r}_G(a)\mathbf{r}_G(b)^{[-1]} = \sum_{s \in G} Tr((s \cdot a)b)s^{-1} \in FG. \tag{2.3.4}$$

Given $a \in F_h$, notice that $\mathcal{O}_F G \cdot a$ is a full lattice in F_h if and only if $\mathbf{r}_G(a) \in (F^c G)^\times$ by Proposition 2.3.7 (a). Given such an $a \in F_h$, analogous to Proposition 2.2.4, we may determine whether the $\mathcal{O}_F G$-lattice $\mathcal{O}_F G \cdot a$ or the element a is self-dual (with respect to Tr_h) by considering the element $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} \in (F^c G)^\times$ when G is abelian.

Proposition 2.3.9 *Assume that G is abelian and let $a \in F_h$ with $\mathbf{r}_G(a) \in (F^c G)^\times$.*

(a) The $\mathcal{O}_F G$-lattice $\mathcal{O}_F G \cdot a$ is self-dual if and only if $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} \in (\mathcal{O}_F G)^\times$.

(b) The element a is self-dual if and only if $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} = 1$.

Proof. Let $b \in F_h$ be such that $\{s \cdot b : s \in G\}$ is the dual basis of $\{s \cdot a : s \in G\}$ (with respect to Tr_h), so that $(\mathcal{O}_F G \cdot a)^* = \mathcal{O}_F G \cdot b$. It then follows that $\mathcal{O}_F G \cdot a$ is self-dual if and only if $\mathcal{O}_F G \cdot a = \mathcal{O}_F G \cdot b$, which in turn is equivalent to $\mathbf{r}_G(a)\mathbf{r}_G(b)^{-1} \in (\mathcal{O}_F G)^\times$. Since $\mathbf{r}_G(b)^{-1} = \mathbf{r}_G(a)^{[-1]}$ by (2.3.4), we see that (a) holds. As for (b), it follows directly from (2.3.4). ■

Proposition 2.3.10 *Assume that G is abelian and let $a \in A_h$. We have $A_h = \mathcal{O}_F G \cdot a$ if and only if*

$$\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} \in (\mathcal{O}_F G)^\times.$$

Proof. By Proposition 2.3.7 (a), both statements imply that $\mathbf{r}_G(a) \in (F^c G)^\times$, or equivalently that $\mathcal{O}_F G \cdot a$ is a full $\mathcal{O}_F G$-lattice in F_h. Assuming that this is the case, observe that because $a \in A_h$ and A_h is self-dual, we have

$$\mathcal{O}_F G \cdot a \subset A_h = A_h^* \subset (\mathcal{O}_F G \cdot a)^*.$$

Hence, we have $A_h = \mathcal{O}_F G \cdot a$ precisely when $\mathcal{O}_F G \cdot a$ is self-dual. The claim now follows from Proposition 2.3.9 (a). ■

Remark 2.3.11 Proposition 2.3.10 is an extremely useful tool and will be used repeatedly in the rest of this dissertation.

2.4 Cohomology and Reduced Resolvends

Let F be a number field or a finite extension of $\mathbb{Q}_p$. We will assume that G is abelian in this section. Following [14, Sections 1 and 2], we will use cohomology to define reduced resolvends and explain how they may be viewed as functions on characters of G. They will play a crucial role in the rest of this dissertation.

Recall that Ω_F acts trivially on G and define

$$\mathcal{H}(FG) := ((F^cG)^\times/G)^{\Omega_F}.$$

Taking Ω_F-cohomology of the short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & G \arrow[r] & (F^cG)^\times \arrow[r] & (F^cG)^\times/G \arrow[r] & 1 \end{tikzcd} \tag{2.4.1}$$

then yields the exact sequence

$$\begin{tikzcd} 1 \arrow[r] & G \arrow[r] & (FG)^\times \arrow[r, "rag"] & \mathcal{H}(FG) \arrow[r, "\delta"] & \mathrm{Hom}(\Omega_F, G) \arrow[r] & 1. \end{tikzcd} \tag{2.4.2}$$

Exactness on the right of (2.4.2) follows from the fact that $H^1(\Omega_F, (F^cG)^\times) = 1$, which is Hilbert's Theorem 90. Alternatively, a coset $\mathbf{r}_G(a)G \in \mathcal{H}(FG)$ belongs to the preimage of $h \in \mathrm{Hom}(\Omega_F, G)$ if and only if $h(\omega) = \mathbf{r}_G(a)^{-1}(\omega \cdot \mathbf{r}_G(a))$ for all $\omega \in \Omega_F$, which in turn is equivalent to $F_h = FG \cdot a$ by (2.3.3) and Proposition 2.3.7 (a). For any $h \in \mathrm{Hom}(\Omega_F, G)$, there always exists $a \in F_h$ with $F_h = FG \cdot a$ by the Normal Basis Theorem. This implies that δ is indeed surjective.

The exact same argument as above also shows that

$$\mathcal{H}(FG) = \{\mathbf{r}_G(a)G \mid F_h = FG \cdot a \text{ for some } h \in \mathrm{Hom}(\Omega_F, G)\}. \tag{2.4.3}$$

Similarly, we may define

$$\mathcal{H}(\mathcal{O}_F G) := ((\mathcal{O}_{F^c} G)^\times / G)^{\Omega_F}.$$

Then, the argument above together with Proposition 2.3.7 (b) imply that

$$\mathcal{H}(\mathcal{O}_F G) = \{r_G(a) \mid \mathcal{O}_h = \mathcal{O}_F G \cdot a \text{ for some unramified } h \in \mathrm{Hom}(\Omega_F, G)\}. \tag{2.4.4}$$

In view of Proposition 2.3.9, we will also define

$$\begin{aligned} \mathcal{H}(FG_{(s)}) &:= \{\mathbf{r}_G(a)G \in \mathcal{H}(FG) \mid \mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} \in (\mathcal{O}_F G)^\times\}; \\ \mathcal{H}(FG_{(1)}) &:= \{\mathbf{r}_G(a)G \in \mathcal{H}(FG) \mid \mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} = 1\}. \end{aligned} \tag{2.4.5}$$

It is obvious that both of the conditions $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} \in (\mathcal{O}_F G)^\times$ and $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} = 1$ are independent of the choice of the coset representative $\mathbf{r}_G(a)$. It is also clear that both of the sets above are subgroups of $\mathcal{H}(FG)$.

Definition 2.4.1 Let $\mathbf{r}_G(a)G \in \mathcal{H}(FG)$. We define $r_G(a) := \mathbf{r}_G(a)G$, called the *reduced resolvend of a*. Moreover, define $h_a \in \mathrm{Hom}(\Omega_F, G)$ by

$$h_a(\omega) := \mathbf{r}_G(a)^{-1}(\omega \cdot \mathbf{r}_G(a)) \qquad \text{for all } \omega \in \Omega_F.$$

called the *homomorphism associated to* $r_G(a)$. This definition is independent of the choice of the coset representative $\mathbf{r}_G(a)$, and we have $F_h = FG \cdot a$ by Proposition 2.3.7 (a) and (2.3.3). We say that $r_G(a)$ is *unramified* if h_a is unramified. Similarly for *tame* and *wild*.

Definition 2.4.2 For F a number field, let $J(\mathcal{H}(FG))$ be the restricted direct product of the groups $\mathcal{H}(F_vG)$ with respect to the subgroups $\mathcal{H}(\mathcal{O}_{F_v}G)$ for $v \in M_F$. Let

$$\eta = \eta_F : \mathcal{H}(FG) \longrightarrow J(\mathcal{H}(FG))$$

be the diagonal map and let

$$U(\mathcal{H}(\mathcal{O}_FG)) := \prod_{v \in M_F} \mathcal{H}(\mathcal{O}_{F_v}G)$$

be the group of unit ideles.

Next, we explain how reduced resolvends may be interpreted as functions on characters of G. Recall that $\widehat{G}$ denotes the group of irreducible F^c-valued characters on G.

First of all, let $\det : \mathbb{Z}\widehat{G} \longrightarrow \widehat{G}$ be the homomorphism given by

$$\det\left(\sum_{\chi} n_\chi \chi\right) := \prod_{\chi} \chi^{n_\chi} \tag{2.4.6}$$

and set $S_{\widehat{G}} := \ker(\det)$ (we remark that in [14], this set is denoted by $A_{\widehat{G}}$). Applying the functor $\mathrm{Hom}(-, (F^c)^\times)$ to the short exact sequence

$$0 \longrightarrow S_{\widehat{G}} \longrightarrow \mathbb{Z}\widehat{G} \xrightarrow{\det} \widehat{G} \longrightarrow 1$$

then yields the short exact sequence

$$1 \longrightarrow \mathrm{Hom}(\widehat{G}, (F^c)^\times) \longrightarrow \mathrm{Hom}(\mathbb{Z}\widehat{G}, (F^c)^\times) \longrightarrow \mathrm{Hom}(S_{\widehat{G}}, (F^c)^\times) \longrightarrow 1. \tag{2.4.7}$$

Exactness on the right of (2.4.7) follows from the fact that $(F^c)^\times$ is divisible and hence injective. We will identify the short exact sequences (2.4.1) and (2.4.7) as follows.

First, observe that we have canonical identifications

$$(F^cG)^\times = \mathrm{Map}(\widehat{G}, (F^c)^\times) = \mathrm{Hom}(\mathbb{Z}\widehat{G}, (F^c)^\times). \tag{2.4.8}$$

The second identification is given by extending the maps $\widehat{G} \longrightarrow (F^c)^\times$ via $\mathbb{Z}$-linearity, and the first is induced by characters as follows. On one hand, each resolvend $\mathbf{r}_G(a) \in (F^cG)^\times$ gives rise to a map $\varphi \in \mathrm{Map}(\widehat{G}, (F^c)^\times)$ defined by

$$\varphi(\chi) := \sum_{s\in G} a(s)\chi(s)^{-1}. \tag{2.4.9}$$

On the other hand, given $\varphi \in \mathrm{Map}(\widehat{G}, (F^c)^\times)$, one recovers $\mathbf{r}_G(a)$ by the formula

$$a(s) := \frac{1}{|G|}\sum_{\chi} \varphi(\chi)\chi(s) \qquad \text{for } s \in G. \tag{2.4.10}$$

Since $G = \mathrm{Hom}(\widehat{G}, (F^c)^\times)$ canonically, the third terms

$$(F^cG)^\times/G = \mathrm{Hom}(S_{\widehat{G}}, (F^c)^\times) \tag{2.4.11}$$

in (2.4.1) and (2.4.7), respectively, are naturally identified as well.

We have thus identified the exact sequences (2.4.1) and (2.4.7). Taking Ω_F-invariants then yields the commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\Omega_F}(\mathbb{Z}\widehat{G}, (F^c)^\times) \arrow[r] \arrow[d, equal] & \mathrm{Hom}_{\Omega_F}(S_{\widehat{G}}, (F^c)^\times) \arrow[d, equal] \\
(FG)^\times \arrow[r, "rag"'] & \mathcal{H}(FG)
\end{tikzcd}, \tag{2.4.12}$$

where rag is as in (2.4.2) and the corresponding map above is given by restriction to $S_{\widehat{G}}$.

Under the above identifications, clearly we have $\mathcal{H}(\mathcal{O}_F G) \subset \mathrm{Hom}_{\Omega_F}(S_{\widehat{G}}, \mathcal{O}_{F^c}^{\times})$.

Proposition 2.4.3 *If F a finite extension of $\mathbb{Q}_p$, where p does not divide $|G|$, then*

$$\mathcal{H}(\mathcal{O}_F G) = Hom_{\Omega_F}(S_{\widehat{G}}, \mathcal{O}_{F^c}^{\times}).$$

Proof. By (2.4.9) and (2.4.10), clearly $|G| \cdot \mathrm{Hom}(\mathbb{Z}\widehat{G}, \mathcal{O}_{F^c}^{\times}) \subset (\mathcal{O}_{F^c}G)^{\times} \subset \mathrm{Hom}(\mathbb{Z}\widehat{G}, \mathcal{O}_{F^c}^{\times})$. Since p does not divide $|G|$, we have $|G| \in \mathcal{O}_F^{\times}$ and thus $(\mathcal{O}_{F^c}G)^{\times} = \mathrm{Hom}(\mathbb{Z}\widehat{G}, \mathcal{O}_{F^c}^{\times})$. The desired equality now follows from the identification $\mathcal{H}(FG) = \mathrm{Hom}_{\Omega_F}(S_{\widehat{G}}, (F^c)^{\times})$. ■

Definition 2.4.4 For F a number field, observe that the homomorphism

$$\prod_{v \in M_F} rag_{F_v} : J(FG) \longrightarrow J(\mathcal{H}(FG)) \tag{2.4.13}$$

is clearly well-defined, and that the diagram

$$\begin{tikzcd}
(FG)^{\times} \arrow[r, "\partial"] \arrow[d, "rag_F"'] & J(FG) \arrow[d, "\prod_v rag_{F_v}"] \\
\mathcal{H}(FG) \arrow[r, "\eta"'] & J(\mathcal{H}(FG))
\end{tikzcd}$$

commutes. By abuse of notation, we will denote the map in (2.4.13) by $rag = rag_F$.

2.5 The Modified Stickelberger Transpose

Let F be a number field or a finite extension of $\mathbb{Q}_p$. We will assume that G is abelian and of odd order in this section. By modifying what has already been done in [14, Section 4] (see Remark 2.5.7), we define a modified Stickelberger map, whose transpose map will play an important role in the rest of this dissertation.

Recall from Section 1.6 that we have chosen a compatible set $\{\zeta_n : n \in \mathbb{Z}^+\}$ of primitive roots of unity in F^c and that $\widehat{G}$ denotes the group of irreducible F^c-valued characters on G.

Definition 2.5.1 For each $\chi \in \widehat{G}$ and $s \in G$, let $\upsilon(\chi, s) \in \{(1-|s|)/2, \ldots, (|s|-1)/2\}$ be the unique integer (note that $|s|$ is odd since G has odd order) such that $\chi(s) = (\zeta_{|s|})^{\upsilon(\chi,s)}$ and then define

$$\langle \chi, s \rangle_* := \upsilon(\chi, s)/|s|.$$

Extending this definition by $\mathbb{Q}$-linearity, we obtain a pairing $\langle\ ,\ \rangle_* : \mathbb{Q}\widehat{G} \times \mathbb{Q}G \longrightarrow \mathbb{Q}$, called the *modified Stickelberger pairing.* The map

$$\Theta_* : \mathbb{Q}\widehat{G} \longrightarrow \mathbb{Q}G; \quad \Theta_*(\psi) := \sum_{s\in G} \langle \psi, s \rangle_* s \tag{2.5.1}$$

is called the *modified Stickelberger map.*

Proposition 2.5.2 *Given $\psi \in \mathbb{Z}\widehat{G}$, we have $\Theta_*(\psi) \in \mathbb{Z}G$ if and only if $\psi \in S_{\widehat{G}}$.*

Proof. Write $\psi = \sum n_\chi \chi$ with $n_\chi \in \mathbb{Z}$. For any $s \in G$, we have

$$\begin{aligned}(\det \psi)(s) &= \prod_\chi \chi(s)^{n_\chi} \\ &= \prod_\chi (\zeta_{|s|})^{\upsilon(\chi,s)n_\chi} \\ &= (\zeta_{|s|})^{\sum_\chi |s|\langle \chi, s\rangle_* n_\chi} \\ &= (\zeta_{|s|})^{|s|\langle \psi, s\rangle_*}.\end{aligned}$$

Since $S_{\widehat{G}} = \ker(\det)$, this implies that $\psi \in S_{\widehat{G}}$ precisely when $\langle \psi, s\rangle_* \in \mathbb{Z}$ for all $s \in G$, or equivalently, when $\Theta_*(\psi) \in \mathbb{Z}G$. This proves the claim. ■

Up until now, we have let Ω_F act trivially on G. Below, we introduce other Ω_F-actions on G, one of which will make the $\mathbb{Q}$-linear map $\Theta_* : \mathbb{Q}\widehat{G} \longrightarrow \mathbb{Q}G$ preserve the Ω_F-action. Here, the Ω_F-action on $\widehat{G}$ is the canonical one induced by the Ω_F-action on the roots of unity in F^c.

Definition 2.5.3 Let $m = \exp(G)$ and let μ_m be the group of m-th roots of unity in F^c. The *m-th cyclotomic character of* Ω_F is the homomorphism $\kappa : \Omega_F \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ given by the equations

$$\omega(\zeta) = \zeta^{\kappa(\omega)} \qquad \text{for } \omega \in \Omega_F \text{ and } \zeta \in \mu_m.$$

For $n \in \mathbb{Z}$, let $G(n)$ be the group G equipped with the Ω_F-action given by

$$\omega \cdot s := s^{\kappa(\omega^n)} \qquad \text{for } s \in G \text{ and } \omega \in \Omega_F.$$

We will need $G(-1)$. But of course, if F contains all m-th roots of unity, then $\kappa = 1$ and $G(n) = G(0)$ is equipped with the trivial Ω_F-action for all $n \in \mathbb{Z}$.

Proposition 2.5.4 *The linear map $\Theta_* : \mathbb{Q}\widehat{G} \longrightarrow \mathbb{Q}G(-1)$ preserve the Ω_F-action.*

Proof. For any $\chi \in \widehat{G}$ and $s \in G(-1)$, we have $(\omega \cdot \chi)(s) = \chi(s^{\kappa(\omega)}) = \chi(\omega^{-1} \cdot s)$. Since s and $\omega^{-1} \cdot s$ have the same order, this implies that $\langle \omega \cdot \chi, s\rangle_* = \langle \chi, \omega^{-1} \cdot s\rangle_*$ and so

$$\begin{aligned}\Theta_*(\omega \cdot \chi) &= \sum_{s\in G} \langle \omega \cdot \chi, s\rangle_* s \\ &= \sum_{s\in G} \langle \chi, \omega^{-1} \cdot s\rangle_* s \\ &= \sum_{s\in G} \langle \chi, s\rangle_* (\omega \cdot s) \\ &= \omega \cdot \Theta_*(\chi).\end{aligned}$$

This shows that Θ_* preserves the Ω_F-action, as desired. ■

By Propositions 2.5.2 and 2.5.4, via restricting Θ_* we obtain an Ω_F-equivariant map $\Theta_* : S_{\widehat{G}} \longrightarrow \mathbb{Z}G(-1)$. Applying the functor $\mathrm{Hom}(-,(F^c)^\times)$ then yields an Ω_F-equivariant homomorphism

$$\Theta_*^t : \mathrm{Hom}(\mathbb{Z}G(-1),(F^c)^\times) \longrightarrow \mathrm{Hom}(S_{\widehat{G}},(F^c)^\times); \quad f \mapsto f \circ \Theta_*,$$

where Ω_F acts on homomorphisms as usual as follows. If X and X' are left Ω_F-modules and $\varphi : X \longrightarrow X'$ is a group homomorphism, then $(\varphi \cdot \omega)(x) := \omega^{-1} \cdot \varphi(\omega \cdot x)$ for $\omega \in \Omega_F$ and $x \in X$. Restricting to the Ω_F-invariant homomorphisms, we obtain a homomorphism

$$\Theta_*^t = \Theta_{*,F}^t : \mathrm{Hom}_{\Omega_F}(\mathbb{Z}G(-1),(F^c)^\times) \longrightarrow \mathrm{Hom}_{\Omega_F}(S_{\widehat{G}},(F^c)^\times),$$

called the *modified Stickelberger transpose*. Notice that we have a natural identification

$$\mathrm{Hom}_{\Omega_F}(\mathbb{Z}G(-1),(F^c)^\times) = \mathrm{Map}_{\Omega_F}(G(-1),(F^c)^\times).$$

To simplify notation, let

$$\Lambda(FG) := \mathrm{Map}_{\Omega_F}(G(-1),F^c); \tag{2.5.2}$$

$$\Lambda(\mathcal{O}_FG) := \mathrm{Map}_{\Omega_F}(G(-1),\mathcal{O}_{F^c}). \tag{2.5.3}$$

Then, we may view Θ_*^t as a homomorphism $\Theta_*^t : \Lambda(FG)^\times \longrightarrow \mathcal{H}(FG)$.

Proposition 2.5.5 *We have $\Theta_*^t(\Lambda(FG)^\times) \subset \mathcal{H}(FG_{(1)})$ (recall (2.4.5)).*

Proof. Let $g \in \Lambda(FG)^\times$ be given and let $r_G(a) \in \mathcal{H}(FG)$ be such that $\Theta_*^t(g) = r_G(a)$. Given $\psi \in S_{\widehat{G}}$, write $\psi = \sum_\chi n_\chi$ with $n_\chi \in \mathbb{Z}$ and define $\psi^{[-1]} := \sum_\chi n_\chi \chi^{-1}$. From (2.4.9), is it clear that $\mathbf{r}_G(a)^{[-1]}(\psi) = \mathbf{r}_G(a)(\psi^{[-1]})$. Observe further that $\Theta_*(\psi^{[-1]}) = -\Theta_*(\psi)$ by

Definition 2.5.1 and so $\Theta^t_*(g)(\psi^{[-1]}) = \Theta^t_*(g)(\psi)^{-1}$. Since $r_G(a) = \Theta^t_*(g)$ and $r_G(a)$ is the restriction of $\mathbf{r}_G(a)$ to $S_{\widehat{G}}$ via the identification in (2.4.11), we deduce that

$$\begin{aligned}(\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]})(\psi) &= \mathbf{r}_G(a)(\psi)\mathbf{r}_G(a)(\psi^{[-1]})\\ &= \Theta^t_*(g)(\psi)\Theta^t_*(g)(\psi^{[-1]})\\ &= 1.\end{aligned}$$

This shows that $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]}$ is the trivial map when restricted to $S_{\widehat{G}}$. By the identifications in (2.4.11), this means that $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} = t$ for some $t \in G$. Applying $[-1]$ to the above yields $\mathbf{r}_G(a)^{[-1]}\mathbf{r}_G(a) = t^{-1}$ and so $t = t^{-1}$. Since G has odd order, we must have $t = 1$. It follows that $r_G(a) \in \mathcal{H}(FG_{(1)})$, as desired. ■

Definition 2.5.6 For F a number field, let $J(\Lambda(FG))$ be the restricted direct product of the groups $\Lambda(F_vG)^\times$ with respect to the subgroups $\Lambda(\mathcal{O}_{F_v}G)^\times$ for $v \in M_F$. Let

$$\lambda = \lambda_F : \Lambda(FG)^\times \longrightarrow J(\Lambda(FG))$$

be the diagonal map and let

$$U(\Lambda(\mathcal{O}_FG)) := \prod_{v\in M_F} \Lambda(\mathcal{O}_{F_v}G)^\times$$

be the group of unit ideles.

Next, observe that the homomorphism

$$\prod_{v\in M_F} \Theta^t_{*,F_v} : J(\Lambda(FG)) \longrightarrow J(\mathcal{H}(FG)) \tag{2.5.4}$$

is well-defined by Proposition 2.4.3 and the fact that $\Theta^t_*(\Lambda(\mathcal{O}_{F_v}G)^\times) \subset \mathrm{Hom}_{\Omega_{F_v}}(S_{\widehat{G}}, \mathcal{O}^\times_{F^c_v})$

for all $v \in M_F$. Recall from Section 1.6 that we have chosen $\{i_v(\zeta_n) : n \in \mathbb{Z}^+\}$ to be the compatible set of primitive roots of unity in F_v^c. Hence, the diagram

$$\begin{tikzcd}
\Lambda(FG)^\times \arrow[r, "\lambda"] \arrow[d, "\Theta^t_{*,F}"'] & J(\Lambda(FG)) \arrow[d, "\prod_v \Theta^t_{*,F_v}"] \\
\mathcal{H}(FG) \arrow[r, "\eta"'] & J(\mathcal{H}(FG))
\end{tikzcd} \tag{2.5.5}$$

commutes. By abuse of notation, we will denote the map in (2.5.4) by $\Theta^t_* = \Theta^t_{*,F}$.

Remark 2.5.7 The *Stickelberger pairing* $\langle\ ,\ \rangle : \mathbb{Q}\widehat{G} \times \mathbb{Q}G \longrightarrow \mathbb{Q}$ in [14, Section 4] is defined to be the $\mathbb{Q}$-linear map such that for each $\chi \in \widehat{G}$ and $s \in G$, we have

$$\langle \chi, s\rangle = \upsilon'(\chi, s)/|s|,$$

where $\upsilon'(\chi, s) \in \{0, 1, \dots, |s| - 1\}$ is the unique integer such that $\chi(s) = (\zeta_{|s|})^{\upsilon'(\chi,s)}$. The *Stickelberger map* is defined analogously as in (2.5.1), but with $\langle\ ,\ \rangle_*$ replaced by $\langle\ ,\ \rangle$. Propositions 2.5.2 and 2.5.4 still hold when Θ_* is replaced by Θ (see [14, Propositions 4.3 and 4.5]). The same discussion following Proposition 2.5.4 then yields a homomorphism $\Theta^t = \Theta^t_F : \Lambda(FG)^\times \longrightarrow \mathcal{H}(FG)$, called the *Stickelberger tranpose*. However, notice that Proposition 2.5.5 does not hold when Θ^t_* is replaced by Θ^t.

For F a number field, the same discussion in Definition 2.5.6 yields a homomorphism

$$\Theta^t = \Theta^t_F : J(\Lambda(FG)) \longrightarrow J(\mathcal{H}(FG)).$$

This map was a key ingredient in [14], where McCulloh studied the Galois module structure of $\mathcal{O}_h$ for $h \in H^1_t(\Omega_F, G)$, or more precisely, the classes they determine in $\mathrm{Cl}(\mathcal{O}_FG)$.

Chapter 3

The Class of the Square Root of the Inverse Different

3.1 Computation using Resolvends

Let F be a number field. In what follows, assume that G is abelian and of odd order. Given a weakly ramified $h \in \mathrm{Hom}(\Omega_F, G)$, the classes $\mathrm{cl}(A_h)$ and $\mathrm{ucl}(A_h)$ in $\mathrm{Cl}(\mathcal{O}_F G)$ and $\mathrm{UCl}(\mathcal{O}_F G)$, respectively, defined by A_h may be computed using resolvends as follows.

First of all, recall that A_h is locally free over $\mathcal{O}_F G$ by [8, Theorem 1 in Section 2], in which case the $\mathcal{O}_F G$-rank of A_h is necessarily one. Moreover, we have $\mathcal{O}_{F_v} \otimes_{\mathcal{O}_F} A_h \simeq A_{h_v}$ from Remark 2.3.3. Hence, for each $v \in M_F$, there exists $a_v \in A_{h_v}$ such that

$$A_{h_v} = \mathcal{O}_{F_v} G \cdot a_v. \tag{3.1.1}$$

Moreover, by the Normal Basis Theorem, there exists $b \in F_h$ such that

$$F_h = FG \cdot b. \tag{3.1.2}$$

Since G has odd order, it follows from [1, Proposition 5.1] that $b \in F_h$ may be chosen to be self-dual. Note that $F_v G \cdot a_v = F_{h_v} = F_v G \cdot b$ for all $v \in M_F$ and that $\mathcal{O}_{F_v} G \cdot a_v = \mathcal{O}_{F_v} G \cdot b$ for all but finitely many $v \in M_F$. This implies that there exists $c \in J(FG)$ such that

$$a_v = c_v \cdot b \tag{3.1.3}$$

for all $v \in M_F$. Hence, the isomorphism $FG \longrightarrow F_h$ of FG-modules defined by $\beta \mapsto \beta \cdot b$ restricts to an isomorphism $\varphi : \mathcal{O}_F G \cdot c \longrightarrow A_h$ of $\mathcal{O}_F G$-modules. It follows that

$$\mathrm{cl}(A_h) = [\mathcal{O}_F G \cdot c] = j(c).$$

If $b \in F_h$ is self-dual, then $\mathbf{r}_G(b)\mathbf{r}_G(b)^{[-1]} = 1$ by Proposition 2.3.9 (b). From (2.3.4), it is easy to see that for all $s, t \in G$, we have $Tr_h(\varphi(s), \varphi(t)) = Tr_h(s \cdot b, t \cdot b) = \delta_{st} = t_F(s,t)$. This implies that φ is in fact a G-isometry. Because A_h is self-dual (recall Remark 2.3.8), the lattice $\mathcal{O}_F G \cdot c$ is self-dual with respect to t_F. It then follows from Proposition 2.2.4 (a) that $c \in J(FG_{(s)})$, and from Proposition 2.2.9 (a) that $(A_h, Tr_h) \in g(\mathcal{O}_F G)_s$ (recall Definition 2.2.6). Also, we have

$$\mathrm{ucl}(A_h) = [(\mathcal{O}_F G \cdot c, t_F)] = j_{(s)}(c).$$

Remark 3.1.1 For each $v \in M_F$, since the resolvend map $\mathbf{r}_G : \mathrm{Map}(G, F_v^c) \longrightarrow F_v^c G$ is an isomorphism of $F_v^c G$-modules, the equation $a_v = c_v \cdot b$ in (3.1.3) is equivalent to

$$\mathbf{r}_G(a_v) = c_v \cdot \mathbf{r}_G(b). \tag{3.1.4}$$

Using reduced resolvends, the equation above becomes

$$r_G(a_v) = rag(c_v) \cdot r_G(b). \tag{3.1.5}$$

Notice that the reduced resolvend $r_G(b)$ of an element $b \in F_h$ satisfying (3.1.2) is already characterized by (2.4.3), and by (2.4.5) if we require that $b \in F_h$ is self-dual in addition (recall Proposition 2.3.9 (b)). Thus, in order to characterize the classes $\mathrm{cl}(A_h)$ and $\mathrm{ucl}(A_h)$, it suffices to characterize the reduced resolvend $r_G(a_v)$ of an element $a_v \in A_{h_v}$ satisfying (3.1.1) for each $v \in M_F$.

3.2 Properties of Local Resolvends

Let F be a finite extension of $\mathbb{Q}_p$ and assume that G is abelian. In this section, whenever we write A_h for some $h \in \mathrm{Hom}(\Omega_F, G)$, we are implicitly assuming that $A_{F^h/F}$ exists (by Proposition 1.2.1, this is so when G has odd order).

We will prove two fundamental properties of the resolvends $\mathbf{r}_G(a)$ with $A_h = \mathcal{O}_F G \cdot a$ for a weakly ramified $h \in \mathrm{Hom}(\Omega_F, G)$. It will be helpful to recall the notation from Section 1.6 and the fact that the resolvend map $\mathbf{r}_G : \mathrm{Map}(G, F^c) \longrightarrow F^cG$ is an isomorphism of F^cG-modules.

Proposition 3.2.1 *Let $h \in Hom(\Omega_F, G)$ be weakly ramified.*

(a) The homomorphism h^{-1} is also weakly ramified.

(b) If $A_h = \mathcal{O}_F G \cdot a$, then there exists an element $a' \in A_{h^{-1}}$ with $\mathbf{r}_G(a') = \mathbf{r}_G(a)^{-1}$ such that $A_{h^{-1}} = \mathcal{O}_F G \cdot a'$.

Proof. Since $\ker(h) = \ker(h^{-1})$, we have $F^h = F^{h^{-1}}$ and so (a) clearly holds. As for (b), note that $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} \in (\mathcal{O}_F G)^\times$ by Proposition 2.3.10, so $\mathbf{r}_G(a)^{-1} = \beta \cdot \mathbf{r}_G(a)^{[-1]}$ for some $\beta \in (\mathcal{O}_F G)^\times$. We have $\mathbf{r}_G(a') = \mathbf{r}_G(a)^{-1}$ for some $a' \in \mathrm{Map}(G, F^c)$ since $\mathbf{r}_G$ is bijective. Notice that $a' \in F_{h^{-1}}$ by (2.3.3). Since $A^h = A^{h^{-1}}$ and $\mathbf{r}_G(a)^{-1} = \beta \cdot \mathbf{r}_G(a)^{[-1]}$, we see that in fact $a' \in A_{h^{-1}}$. Clearly $\mathbf{r}_G(a')\mathbf{r}_G(a')^{[-1]} \in (\mathcal{O}_F G)^\times$, so again by Proposition 2.3.10, we see that $A_{h^{-1}} = \mathcal{O}_F G \cdot a'$, as desired. ■

To prove the second fundamental property, we will need some facts concerning ramification groups (in lower numbering).

Lemma 3.2.2 *Let N^{nr}/F and N/F be finite Galois extensions with N^{nr}/F unramified.*

(a) If N/F is weakly ramified, then any Galois subextension L/F of N/F is also weakly ramified.

(b) The homomorphism $Gal(N^{nr}N/F) \longrightarrow Gal(N/F)$ defined by $\sigma \mapsto \sigma|_N$ induces an isomorphism $Gal(N^{nr}N/F)_n \simeq Gal(N/F)_n$ for all $n \in \mathbb{Z}_{\geq 0}$. In particular, if N/F is weakly ramified, then so is $N^{nr}N/F$.

(c) Let $e_0 := |Gal(N/F)_0/Gal(N/F)_1|$. If N/F is abelian, then for all $n \in \mathbb{Z}_{\geq 0}$ that are not divisible by e_0, we have $Gal(N/F)_n = Gal(N/F)_{n+1}$. In particular, if N/F is also wildly and weakly ramified, then $Gal(N/F)_0 = Gal(N/F)_1$.

Proof. See [23, Proposition 2.2] for (a) and (b); notice that the proof there is valid even when $F \neq \mathbb{Q}_p$. See [20, Chapter IV, Proposition 9, Corollary 2] for (c). ■

Proposition 3.2.3 *Let $h_1, h_2 \in Hom(\Omega_F, G)$ be such that h_1 is unramified.*

(a) We have $e(F^{h_1h_2}/F) = e(F^{h_2}/F)$.

Assume in addition that h_2 is weakly ramified.

(b) The homomorphism h_1h_2 is also weakly ramified and $v_{F^{h_1h_2}}(A^{h_1h_2}) = v_{F^{h_2}}(A^{h_2})$.

(c) If $\mathcal{O}_{h_1} = \mathcal{O}_F G \cdot a_1$ and $A_{h_2} = \mathcal{O}_F G \cdot a_2$, then there exists an element $a \in A_{h_1h_2}$ with $\mathbf{r}_G(a) = \mathbf{r}_G(a_1)\mathbf{r}_G(a_2)$ such that $A_{h_1h_2} = \mathcal{O}_F G \cdot a$.

Proof. Let $h := h_1h_2$. Note that $\ker(h_1) \cap \ker(h_2) = \ker(h_1) \cap \ker(h)$ so $F^{h_1}F^{h_2} = F^{h_1}F^h$. Since F^{h_1}/F is unramified, both $F^{h_1}F^{h_2}/F^{h_2}$ and $F^{h_1}F^h/F^h$ are unramified. Using the multiplicativity of ramification indices, we have $e(F^h/F) = e(F^{h_2}/F) = e(F^{h_1}F^{h_2}/F^{h_1})$, which proves (a). To summarize, we have the following the diagram, where the numbers indicate ramification indices and $e := e(F^{h_2}/F)$.

$$\begin{tikzcd}
& F^{h_1}F^{h_2} \arrow[dl, dash, "e"'] \arrow[d, dash, "1"'] \arrow[dr, dash, "1"] & \\
F^{h_1} \arrow[dr, dash, "1"'] & F^h \arrow[d, dash, "e"'] & F^{h_2} \arrow[dl, dash, "e"] \\
& F &
\end{tikzcd}$$

Now, assume in addition that F^{h_2}/F is weakly ramified. Since F^{h_1}/F is unramified, it follows from Lemma 3.2.2 (b) that $F^{h_1}F^{h_2}/F$ is also weakly ramified, and hence from Lemma 3.2.2 (a) that F^h/F is weakly ramified as well. Thus, indeed h is weakly ramified. Moreover, from Proposition 1.2.1, we know that

$$v_{F^h}(A^h) = -(|\mathrm{Gal}(F^h/F)_0| + |\mathrm{Gal}(F^h/F)_1| - 2)/2;$$
$$v_{F^{h_2}}(A^{h_2}) = -(|\mathrm{Gal}(F^{h_2}/F)_0| + |\mathrm{Gal}(F^{h_2}/F)_1| - 2)/2.$$

If $(e,p) = 1$, then F^h/F and F^{h_2}/F are both tame, and $\mathrm{Gal}(F^h/F)_1 = 1 = \mathrm{Gal}(F^{h_2}/F)_1$. If $(e,p) > 1$, then F^h/F and F^{h_2}/F are both wildly and weakly ramified. In this case, we have $\mathrm{Gal}(F^h/F)_0 = \mathrm{Gal}(F^h/F)_1$ and $\mathrm{Gal}(F^{h_2}/F)_0 = \mathrm{Gal}(F^{h_2}/F)_1$ by Lemma 3.2.2 (c). Since $|\mathrm{Gal}(F^h/F)_0| = e = |\mathrm{Gal}(F^{h_2}/F)_0|$, we have $v_{F^h}(A^h) = v_{F^{h_2}}(A^{h_2})$. This proves (b).

Finally, to prove (c), notice that $\mathbf{r}_G(a_i)\mathbf{r}_G(a_i)^{[-1]} \in (\mathcal{O}_F G)^\times$ for $i \in \{1,2\}$ by Propositions 2.3.7 (b) and 2.3.10. Let $a \in \mathrm{Map}(G, F^c)$ be such that $\mathbf{r}_G(a) = \mathbf{r}_G(a_1)\mathbf{r}_G(a_2)$, which exists as $\mathbf{r}_G$ is bijective. We have $a \in F_h$ by (2.3.3), and clearly $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} \in (\mathcal{O}_F G)^\times$. Hence, again by Proposition 2.3.10, we will have $A_h = \mathcal{O}_F G \cdot a$ as long as $a \in A_h$. But $A_h = \mathrm{Map}_{\Omega_F}({}^hG, A^h)$, so it remains to show that $a(s) \in A^h$ for all $s \in G$.

To that end, observe that $\mathbf{r}_G(a) = \mathbf{r}_G(a_1)\mathbf{r}_G(a_2)$ implies that for each $s \in G$, we have

$$a(s) = \sum_{rt=s} a_1(r)a_2(t).$$

On one hand, because $a_1 \in \mathcal{O}_{h_1}$, we have $v_{F^{h_1}F^{h_2}}(a_1(r)) \geq 0$ for all $r \in G$. On the other hand, since $a_2 \in A_{h_2}$ and $F^{h_1}F^{h_2}/F^{h_2}$ is unramified, we have $v_{F^{h_1}F^{h_2}}(a_2(t)) \geq v_{F^{h_2}}(A^{h_2})$ for all $t \in G$. We then see that $v_{F^{h_1}F^{h_2}}(a(s)) \geq v_{F^{h_2}}(A^{h_2})$. But $F^{h_1}F^{h_2}/F^h$ is unramified and $v_{F^{h_2}}(A^{h_2}) = v_{F^h}(A^h)$ from (b), so the above inequality becomes $v_{F^h}(a(s)) \geq v_{F^h}(A^h)$. This shows that $a(s) \in A^h$ for all $s \in G$, as desired. This proves (c). ■

Remark 3.2.4 Proposition 3.2.3 (c) turns out to be an extremely useful tool and will be used repeatedly in the rest of this dissertation.

3.3 Proofs of Theorems 1.2.2 and 1.3.2

Theorem 1.3.2 *Let K be a number field and let G be a finite abelian group of odd order. For all $h, h_1, h_2 \in H^1_w(\Omega_K, G)$ with $d(h_1) \cap d(h_2) = \emptyset$, we have*

(a) $h^{-1} \in H^1_w(\Omega_K, G)$ and $gal_{A,u}(h^{-1}) = gal_{A,u}(h)^{-1}$; and

(b) $h_1h_2 \in H^1_w(\Omega_K, G)$ and $gal_{A,u}(h_1h_2) = gal_{A,u}(h_1)gal_{A,u}(h_2)$.

Proof. To prove (a), let $h \in H^1_w(\Omega_K, G)$ be given. The fact that $h^{-1} \in H^1_w(\Omega_K, G)$ follows directly from Proposition 3.2.1 (a). Next, let $b \in K_h$ be as in (3.1.2), and we will take b to be self-dual. For each $v \in M_K$, let $a_v \in A_{h_v}$ and $c_v \in (K_vG)^\times$ be as in (3.1.1) and (3.1.3), respectively. As noted in Section 3.1, we have $c := (c_v) \in J(KG_{(s)})$ and $\mathrm{ucl}(A_h) = j_{(s)}(c)$.

Now, notice that $\mathbf{r}_G(b) \in (K^cG)^\times$ by Proposition 2.3.7 (a) and let $b' \in \mathrm{Map}(G, K^c)$ be such that $\mathbf{r}_G(b') = \mathbf{r}_G(b)^{-1}$; such an element b' exists because $\mathbf{r}_G$ is bijective. From (2.3.3) and Proposition 2.3.7 (a), we see that $b' \in K_{h^{-1}}$ and $K_{h^{-1}} = KG \cdot b'$. Clearly b' is also self-dual (with respect to $Tr_{h^{-1}}$) from Proposition 2.3.9 (b). For each $v \in M_K$, apply Proposition 3.2.1 (b) to obtain an element $a'_v \in A_{h_v^{-1}}$ with $\mathbf{r}_G(a'_v) = \mathbf{r}_G(a_v)^{-1}$ such that $A_{h_v^{-1}} = \mathcal{O}_{K_v}G\cdot a'_v$. Recall from (3.1.4) that $\mathbf{r}_G(a_v) = c_v\cdot\mathbf{r}_G(b)$, and so $\mathbf{r}_G(a'_v) = c_v^{-1}\cdot\mathbf{r}_G(b')$. It follows that $a'_v = c_v^{-1}\cdot b'$. As in Section 3.1, we then deduce that

$$\mathrm{ucl}(A_{h^{-1}}) = j_{(s)}(c^{-1}) = j_{(s)}(c)^{-1} = \mathrm{ucl}(A_h)^{-1}.$$

This completes the proof of (a).

To prove (b), let $h_1, h_2 \in H^1_w(\Omega_K, G)$ with $d(h_1)\cap d(h_2) = \emptyset$ be given. Set $h := h_1h_2$. The fact that $h \in H^1_w(\Omega_K, G)$ is a direct consequence of Proposition 3.2.3 (b). Next, for $i \in \{1, 2\}$, let $b_i \in K_{h_i}$ be as in (3.1.2), and we choose b_i to be self-dual. For each $v \in M_K$, let $a_{i,v} \in A_{(h_i)_v}$ and $c_{i,v} \in (K_vG)^\times$ be as in (3.1.1) and (3.1.3), respectively. As noted in Section 3.1, we have $c_i := (c_{i,v}) \in J(KG_{(s)})$ and $\mathrm{ucl}(A_{h_i}) = j_{(s)}(c_i)$.

Now, there exists $b \in \mathrm{Map}(G, K^c)$ such that $\mathbf{r}_G(b) = \mathbf{r}_G(b_1)\mathbf{r}_G(b_2)$, again because $\mathbf{r}_G$ is bijective. From (2.3.3) and Proposition 2.3.7 (a), we see that $b \in K_h$ and $K_h = KG\cdot b$. From Proposition 2.3.9 (b), it is clear that b is also self-dual (with respect to Tr_h). Note that for each $v \in M_K$, at least one of $(h_1)_v$ and $(h_2)_v$ is unramified as $d(h_1)\cap d(h_2) = \emptyset$. Then, by Proposition 3.2.3 (c), there exists $a_v \in A_{h_v}$ with $\mathbf{r}_G(a_v) = \mathbf{r}_G(a_{1,v})\mathbf{r}_G(a_{2,v})$ such that $A_{h_v} = \mathcal{O}_{K_v}G\cdot a_v$. Recall from (3.1.4) that $\mathbf{r}_G(a_{i,v}) = c_{i,v}\cdot\mathbf{r}_G(b_i)$ for $i \in \{1, 2\}$, and so $\mathbf{r}_G(a_v) = c_{1,v}c_{2,v}\cdot\mathbf{r}_G(b)$. It follows that $a_v = c_{1,v}c_{2,v}\cdot b$. As in Section 3.1, this gives

$$\mathrm{ucl}(A_h) = j_{(s)}(c_1c_2) = j_{(s)}(c_1)j_{(s)}(c_2) = \mathrm{ucl}(A_{h_1})\mathrm{ucl}(A_{h_2}).$$

This completes the proof of (b). ■

Theorem 1.2.2 *Let K be a number field and let G be a finite abelian group of odd order. For all $h, h_1, h_2 \in H^1_w(\Omega_K, G)$ with $d(h_1)\cap d(h_2) = \emptyset$, we have* *(a)* $h^{-1} \in H^1_w(\Omega_K, G)$ *and* $gal_A(h^{-1}) = gal_A(h)^{-1}$*; and*

(b) $h_1h_2 \in H^1_w(\Omega_K, G)$ *and* $gal_A(h_1h_2) = gal_A(h_1)gal_A(h_2)$*.*

Proof. This is a direct consequence of Thereom 1.3.2 because $\mathrm{gal}_A = \Phi \circ \mathrm{gal}_{A,u}$, where Φ is the homomorphism from (1.3.1) (cf. Remark 2.2.11). ■

Chapter 4

Characterization of the A-Realizable Classes in $\mathrm{Cl}(\mathcal{O}_K G)$ and $\mathrm{UCl}(\mathcal{O}_K G)$

Let F be a number field. In what follows, assume that G is abelian and of odd order. As discussed in Section 3.1, given a weakly ramified $h \in \mathrm{Hom}(\Omega_F, G)$, its square root of the inverse different A_h defines a class $\mathrm{cl}(A_h)$ in $\mathrm{Cl}(\mathcal{O}_F G)$, and a class $\mathrm{ucl}(A_h)$ in $\mathrm{UCl}(\mathcal{O}_F G)$. Recall also from Remark 3.1.1 that in order to characterize these two classes, it suffices to characterize the reduced resolvends $r_G(a_v)$ for which $A_{h_v} = \mathcal{O}_{F_v} G \cdot a_v$ for each $v \in M_F$. This is the goal of this chapter, and we will give a brief outline of our strategy below.

First, in Section 4.1, we will show that for each $v \in M_F$, we may factor $h_v = h_v^{nr} h_v^{tot}$ for some $h_v^{nr}, h_v^{tot} \in \mathrm{Hom}(\Omega_{F_v}, G)$ such that h_v^{nr} is unramified and that $F_v^{h_v^{tot}}/F_v$ is totally ramified. We then see from Proposition 3.2.3 (c) that it suffices to compute the reduced resolvends $r_G(a_{v,nr})$ and $r_G(a_{v,tot})$ for which $\mathcal{O}_{h_v^{nr}} = \mathcal{O}_{F_v} G \cdot a_{v,nr}$ and $A_{h_v^{tot}} = \mathcal{O}_{F_v} G \cdot a_{v,tot}$. The reduced resolvends $r_G(a_{v,nr})$ are already characterized by (2.4.4). Hence, it remains to compute the reduced resolvend $r_G(a_{v,tot})$. We will consider the case when h_v is tame in Section 4.2 and then the case when h_v is wild in Section 4.5. In the latter case, we will have to assume that v is unramified over $\mathbb{Q}$ and that $e(F_v^{h_v^{tot}}/F_v)$ is prime.

4.1 Factorization of Local Homomorphisms

Let F be a finite extension of $\mathbb{Q}_p$ and assume that G is abelian. In this section, we will write $\pi := \pi_F$ for a chosen uniformizer in F and $q := q_F$ for the order of $\mathcal{O}_F/(\pi)$. Let F^{nr} be the maximal unramified extension of F contained in F^c and define $\Omega_F^{nr} := \mathrm{Gal}(F^{nr}/F)$. It will also be helpful to recall the notation in Section 1.6.

Definition 4.1.1 Let $h \in \mathrm{Hom}(\Omega_F, G)$. We say that

$$h = h^{nr}h^{tot}, \qquad \text{where } h^{nr}, h^{tot} \in \mathrm{Hom}(\Omega_F, G)$$

is a *factorization of h with respect to π* if h^{nr} is unramified and $F^{h^{tot}} \subset F_{\pi,n}$ for some $n \in \mathbb{Z}_{\geq 0}$. The *level* of such a factorization is defined to be

$$\ell_\pi(h^{nr}h^{tot}) := \min\{n \in \mathbb{Z}_{\geq 0} \mid F^{h^{tot}} \subset F_{\pi,n}\}.$$

Proposition 4.1.2 *Every homomorphism $h \in Hom(\Omega_F, G)$ admits a factorization with respect to π. Moreover, for any such factorization $h = h^{nr}h^{tot}$, we have*

(a) $\ell_\pi(h^{nr}h^{tot}) = 0$ if and only if h is unramified;

(b) $\ell_\pi(h^{nr}h^{tot}) \leq 1$ if and only if h is tame;

(c) $\ell_\pi(h^{nr}h^{tot}) \leq 2$ if h is weakly ramified.

Proof. Let F^{ab} be the maximal abelian extension of F contained in F^c and let F_π be the union of $F_{\pi,n}$ for $n \in \mathbb{Z}_{\geq 0}$. We have $F^{ab} = F^{nr}F_\pi$ and $F^{nr} \cap F_\pi = F$ from Local Class Field Theory. Hence, there is a natural isomorphism $\mathrm{Gal}(F^{ab}/F) \simeq \mathrm{Gal}(F^{nr}/F) \times \mathrm{Gal}(F_\pi/F)$. We may then regard $\mathrm{Gal}(F^{nr}/F)$ and $\mathrm{Gal}(F_\pi/F)$ as subgroups of $\mathrm{Gal}(F^{ab}/F)$.

Now, since G is abelian, every $h \in \mathrm{Hom}(\Omega_F, G)$ factors through $\Omega_F \longrightarrow \mathrm{Gal}(F^{ab}/F)$.

Viewing h as a homomorphism $\mathrm{Gal}(F^{ab}/F) \longrightarrow G$, let h^{nr} and h^{tot} denote its restrictions to $\mathrm{Gal}(F^{nr}/F)$ and $\mathrm{Gal}(F_\pi/F)$, respectively. Then, clearly $h = h^{nr}h^{tot}$ is a factorization with respect to π. If $h = h^{nr}h^{tot}$ is any factorization of h with respect to π, then plainly (a) and (b) hold. As for (c), see the proofs of [5, Proposition 4.1 and Lemma 4.2]. ■

If $h \in \mathrm{Hom}(\Omega_F, G)$ is tame, then it factors through the quotient map $\Omega_F \longrightarrow \Omega_F^t$ and we may regard h as a homomorphism $\Omega_F^t \longrightarrow G$. In this case, a more explicit factorization of h may be given, which we will describe below.

First, we will recall the structures of the extensions F^{nr}/F and F^t/F and their Galois groups (see [10, Sections 7 and 8], for example). On one hand, the field F^{nr} is obtained by adjoining to F all n-th roots of unity for $(n,p) = 1$. Hence, the group Ω_F^{nr} is procyclic and is topologically generated by the Frobenius automorphism $\phi = \phi_F$ given by

$$\phi(\zeta_n) = \zeta_n^q \qquad \text{for all } (n,p) = 1. \tag{4.1.1}$$

As for the field F^t, it is obtained by adjoining to F^{nr} all n-th roots of π for $(n,p) = 1$. We will choose a coherent set of radicals $\{\pi^{1/n} : n \in \mathbb{Z}^+\}$ such that $(\pi^{1/mn})^n = \pi^{1/m}$ and then define $\pi^{m/n} := (\pi^{1/n})^m$ for $m, n \in \mathbb{Z}^+$. These choices of radicals then determine a distinguished topological generator $\sigma = \sigma_F$ of the procyclic group $\mathrm{Gal}(F^t/F^{nr})$ given by

$$\sigma(\pi^{1/n}) = \zeta_n\pi^{1/n} \qquad \text{for all } (n,p) = 1. \tag{4.1.2}$$

If we let ϕ also denote the unique lifting of ϕ from Ω_F^{nr} to Ω_F^t fixing the radicals $\pi^{1/n}$ for $(n,p) = 1$, then Ω_F^t is topologically generated by ϕ and σ. In particular, any homomorphism $h \in \mathrm{Hom}(\Omega_F^t, G)$ is uniquely determined by its values on ϕ and σ.

Remark 4.1.3 By abuse of notation, we will also write σ for some chosen lift of σ in Ω_F. If $h \in \mathrm{Hom}(\Omega_F, G)$ is tame, then the value $h(\sigma)$ is independent of the choice of the lift.

Next, notice that $\phi\sigma\phi^{-1}\sigma^{-1} = \sigma^{q-1}$ because both sides have the same effect on ζ_n and $\pi^{1/n}$ for $(n, p) = 1$. Let $(\Omega_F^t)^{ab}$ be the abelianization of Ω_F^t. Moreover, let $\overline{\phi}$ and $\overline{\sigma}$ be the images in $(\Omega_F^t)^{ab}$ of ϕ and σ, respectively. Then, the group $(\Omega_F^t)^{ab}$ is the direct product of the cyclic group $\langle\overline{\sigma}\rangle$ of order $q-1$ with the procyclic group topologically generated by $\overline{\phi}$. In view of this observation, define

$$G_{(q-1)} := \{s \in G \mid \text{the order of } s \text{ divides } q-1\}. \tag{4.1.3}$$

Because G is abelian, we see that any $h \in \mathrm{Hom}(\Omega_F^t, G)$ may be defined by specifying the values $h(\phi)$ and $h(\sigma)$, provided that $h(\sigma) \in G_{(q-1)}$.

Definition 4.1.4 Let $h \in \mathrm{Hom}(\Omega_F^t, G)$. Define

$$\begin{aligned} h^{nr} &\in \mathrm{Hom}(\Omega_F^t, G); \quad h^{nr}(\phi) := h(\phi) \text{ and } h^{nr}(\sigma) := 1; \\ h^{tot} &\in \mathrm{Hom}(\Omega_F^t, G); \quad h^{tot}(\phi) := 1 \text{ and } h^{tot}(\sigma) := h(\sigma). \end{aligned}$$

Clearly $h = h^{nr}h^{tot}$, which we will call the *factorization of h with respect to σ*.

Remark 4.1.5 Let $h \in \mathrm{Hom}(\Omega_F^t, G)$ and let $h = h^{nr}h^{tot}$ be the factorization of h with respect to σ. Clearly h^{nr} is unramified because $h^{nr}(\sigma) = 1$. We will also see in Proposition 4.2.2 that $F^{h^{tot}} = F(\pi^{1/|s|})$, where $s := h(\sigma) \in G_{(q-1)}$. This means that $h = h^{nr}h^{tot}$ is in fact a factorization of h with respect to $-\pi$ in the sense of Definition 4.1.1.

4.2 Decomposition of Local Tame Resolvends

Let F be a finite extension of $\mathbb{Q}_p$. We will assume that G is abelian and of odd order in this section. We will characterize the reduced resolvends $r_G(a)$ for which $A_h = \mathcal{O}_F G \cdot a$ for a tame $h \in \mathrm{Hom}(\Omega_F, G)$, or equivalently $h \in \mathrm{Hom}(\Omega_F^t, G)$ (recall Remark 2.3.5).

As in Section 4.1, we will write $\pi := \pi_F$ for a chosen uniformizer in F and $q := q_F$ for the order of $\mathcal{O}_F/(\pi)$. Let ϕ and σ be defined as in (4.1.1) and (4.1.2), respectively. Also, let $G_{(q-1)}$ be as in (4.1.3). We will also need a further definition.

Definition 4.2.1 For each $s \in G_{(q-1)}$, define $f_s = f_{F,s} \in \Lambda(FG)^\times$ by

$$f_s(t) := \begin{cases} \pi & \text{if } t = s \neq 1 \\ 1 & \text{otherwise} \end{cases}$$

(recall (2.5.2)). Notice that f_s indeed preserves Ω_F-action because all $(q-1)$-st roots of unity are contained in F, and so elements in $G_{(q-1)}$, as well as π, are fixed by Ω_F. Such a map in $\Lambda(FG)^\times$ is called a *prime $\mathfrak{F}$-element over F*. Also, define $\mathfrak{F}_F := \{f_s : s \in G_{(q-1)}\}$ to be the collection of all prime $\mathfrak{F}$-elements over F.

Proposition 4.2.2 *Given $s \in G_{(q-1)}$, define $h \in Hom(\Omega_F^t, G)$ by $h(\phi) = 1$ and $h(\sigma) = s$. Then, we have $F^h = F(\pi^{1/|s|})$, and there exists $a \in A_h$ such that $A_h = \mathcal{O}_F G \cdot a$ and*

$$r_G(a) = \Theta_*^t(f_s).$$

Proof. Let $e := |s|$ and $\Pi := \pi^{1/e}$. Notice that $F^h = F(\Pi)$ because $\ker(h)$ is topologically generated by ϕ and σ^e, which both fix Π, and $[\Omega_F^t : \ker(h)] = e = [F(\Pi) : F]$. Hence, the field F^h is totally ramified over F and has Π as a uniformizer. So, we have $\mathcal{O}^h = \mathcal{O}_F[\Pi]$ (see [20, Chapter I, Proposition 18], for example). Because $A^h = \Pi^{(1-e)/2}\mathcal{O}^h$ by Proposition 1.2.1, we see that $\{\Pi^{k+(1-e)/2} \mid k = 0, 1, \ldots, e-1\}$ is an $\mathcal{O}_F$-basis of A^h. We will show that their average

$$\alpha := \frac{1}{e}\sum_{k=0}^{e-1} \Pi^{k+\frac{1-e}{2}}$$

is a free generator of A^h over $\mathcal{O}_F\mathrm{Gal}(F^h/F)$. Note that $\alpha \in A^h$ because $(e, p) = 1$.

The group $\mathrm{Gal}(F^h/F)$ is cyclic of order e and is generated by the element $\Pi \mapsto \zeta_e \Pi$, which is the restriction of σ to F^h. For each $i = 0, 1, \ldots, e-1$, we have

$$\sigma^i(\alpha) = \frac{1}{e}\sum_{k=0}^{e-1} \zeta_e^{(k+\frac{1-e}{2})i}\Pi^{k+\frac{1-e}{2}}.$$

For $l = 0, 1, \ldots, e-1$, multiply the above equation by $\zeta_e^{-(l+(1-e)/2)i}$ to obtain

$$\sigma^i(\alpha)\zeta_e^{-(l+\frac{(1-e)}{2})i} = \frac{1}{e}\sum_{k=0}^{e-1} \zeta_e^{(k-l)i}\Pi^{k+\frac{1-e}{2}}.$$

Now, summing the above over all $i = 0, 1, \ldots, e-1$ then yields

$$\sum_{i=0}^{e-1}\sigma^i(\alpha)\zeta_e^{-(l+\frac{1-e}{2})i} = \frac{1}{e}\sum_{k=0}^{e-1}\Pi^{k+\frac{1-e}{2}}\sum_{i=0}^{e-1}\zeta_e^{(k-l)i} = \Pi^{l+\frac{1-e}{2}}. \tag{4.2.1}$$

Since $\{\Pi^{l+(1-e)/2} \mid l = 0, 1, \ldots, e-1\}$ is an $\mathcal{O}_F$-basis of A^h and $\zeta_e \in \mathcal{O}_F$, this shows that indeed $A^h = \mathcal{O}_F\mathrm{Gal}(F^h/F)\cdot\alpha$. Since $\alpha \in F^h$ and $A_h = \mathrm{Map}_{\Omega_F}({}^hG, A^h)$, it is not hard to see that the map $a \in \mathrm{Map}(G, F^c)$ given by

$$a(t) := \begin{cases} \omega(\alpha) & \text{if } t = h(\omega) \text{ for } \omega \in \Omega_F^t \\ 0 & \text{otherwise} \end{cases}$$

is well-defined and satisfies $A_h = \mathcal{O}_F G \cdot a$, as desired.

Finally, we will use the identification $\mathcal{H}(FG) = \mathrm{Hom}_{\Omega_F}(S_{\widehat{G}}, (F^c)^\times)$ in (2.4.12) to show that $r_G(a) = \Theta_*^t(f_s)$. To that end, let $\chi \in \widehat{G}$ and let $v := v(\chi, s)$ be as in Definition 2.5.1. Then, we have $\chi(s) = \zeta_e^v$ and $k := v - (1-e)/2 \in \{0, 1, \cdots, e-1\}$. On one hand, by the definition of a, we have

$$\mathbf{r}_G(a)(\chi) = \sum_{i=0}^{e-1}\sigma^i(\alpha)\chi(s)^{-i} = \sum_{i=0}^{e-1}\sigma^i(\alpha)\zeta_e^{-(k+\frac{1-e}{2})i}.$$

The same computation as in (4.2.2) then shows that $\mathbf{r}_G(a)(\chi) = \Pi^{k+\frac{1-e}{2}} = \pi^{\langle \chi, s\rangle_*}$. On the other hand, we have

$$\Theta_*^t(f_s)(\chi) = f_s\left(\sum_{t\in G}\langle \chi, t\rangle_* t\right) = \prod_{t\in G} f_s(t)^{\langle \chi, t\rangle_*} = \pi^{\langle \chi, s\rangle_*} \tag{4.2.2}$$

also. Hence, indeed $r_G(a) = \Theta_*^t(f_s)$, and this completes the proof. ■

Next, we will consider an arbitrary tame $h \in \mathrm{Hom}(\Omega_F, G)$.

Theorem 4.2.3 *Let $h \in Hom(\Omega_F^t, G)$. If $A_h = \mathcal{O}_F G \cdot a$, then we have*

$$r_G(a) = u\Theta_*^t(f_s)$$

for some $u \in \mathcal{H}(\mathcal{O}_F G)$ and for $s := h(\sigma)$.

Proof. Let $h = h^{nr}h^{tot}$ be the factorization of h with respect to σ. By Proposition 2.3.7 (b) and (2.4.4), there exists $a_{nr} \in \mathcal{O}_{h^{nr}}$ such that $\mathcal{O}_{h^{nr}} = \mathcal{O}_F G \cdot a_{nr}$ and $r_G(a_{nr}) = u'$ for some $u' \in \mathcal{H}(\mathcal{O}_F G)$. Similarly, by Proposition 4.2.2, we have $A_{h^{tot}} = \mathcal{O}_F G \cdot a_{tot}$ for some $a_{tot} \in A_{h_{tot}}$ with $r_G(a_{tot}) = \Theta_*^t(f_s)$, where $s := h(\sigma)$. Applying Proposition 3.2.3 (c), we then obtain an element $a' \in A_h$ with $\mathbf{r}_G(a') = \mathbf{r}_G(a_{nr})\mathbf{r}_G(a_{tot})$ such that $A_h = \mathcal{O}_F G \cdot a'$. Since $A_h = \mathcal{O}_F G \cdot a$ also, we have $a = \beta \cdot a'$ for some $\beta \in (\mathcal{O}_F G)^\times$. It follows that

$$r_G(a) = rag(\beta) r_G(a') = (rag(\beta)u')\Theta_*^t(f_s),$$

where $u := rag(\beta)u' \in \mathcal{H}(\mathcal{O}_F G)$. This proves the claim. ■

Theorem 4.2.4 *Let $s \in G_{(q-1)}$ and $u \in \mathcal{H}(\mathcal{O}_F G)$. If h is the homomorphism associated to $u\Theta_*^t(f_s)$, then h is tame and $h(\sigma) = s$. Moreover, there exists an element $a \in A_h$ such that $A_h = \mathcal{O}_F G \cdot a$ and*

$$r_G(a) = u\Theta_*^t(f_s).$$

Proof. Let h^{nr} and h^{tot} be the homomorphisms associated to u and $\Theta_*^t(f_s)$, respectively. Notice that h^{nr} is unramified by (2.4.4) and so $h^{nr}(\sigma) = 1$. We also know from Proposition 4.2.2 that h^{tot} is tame. Since $h = h^{nr}h^{tot}$ by definition, this implies that h is tame. In particular, we may view h as an element of $\mathrm{Hom}(\Omega_F^t, G)$ (recall Remark 2.3.5).

Now, Proposition 4.2.2 also implies that $h^{tot}(\phi) = 1$ and $h^{tot}(\sigma) = s$. We then deduce that $h(\sigma) = h^{tot}(\sigma) = s$, which proves the first claim. This also shows that $h = h^{nr}h^{tot}$ is the factorization of h with respect to σ. The same argument in the proof of Theorem 4.2.3 verbatim then shows that there exists $a \in A_h$ satisfying the desired properties. ∎

Remark 4.2.5 Theorems 4.2.3 and 4.2.4 are modifications of [14, Theorem 5.6], where McCulloh proved the analogous statements, but with A_h and Θ_*^t replaced by $\mathcal{O}_h$ and Θ^t, respectively (recall Remark 2.5.7).

The next proposition will be needed for the proof of Theorem 1.2.4. It will be helpful to recall the definitions of the pairing $\langle\ ,\ \rangle$ and the map Θ^t from Remark 2.5.7.

Proposition 4.2.6 *For all $s \in G_{(q-1)}$, we have $\Theta_*^t(f_s)\Theta^t(f_s) = \Theta^t(f_{s^2})$.*

Proof. Let $\chi \in \widehat{G}$ be given. As computed in (4.2.2) and the proof of [14, Proposition 5.4], we know that $(\Theta_*^t(f_s)\Theta^t(f_s))(\chi) = \pi^{\langle\chi,s\rangle + \langle\chi,s\rangle_*}$ and $\Theta^t(f_{s^2})(\chi) = \pi^{\langle\chi,s^2\rangle}$. So, it suffices to show that $\langle\chi,s\rangle_* + \langle\chi,s\rangle = \langle\chi,s^2\rangle$. To that end, let $e := |s|$ and let $k \in \{0,1,\dots,e-1\}$ be such that $\chi(s) = \zeta_e^k$, so $\chi(s^2) = \zeta_e^{2k}$. If $k \in \{0,1,\dots,(e-1)/2\}$, then $2k \in \{0,1,\dots,e-1\}$ and so

$$\langle\chi,s\rangle_* + \langle\chi,s\rangle = k/e + k/e = 2k/e = \langle\chi,s^2\rangle.$$

If $k \in \{(e+1)/2,\dots,e-1\}$, then $2k \in \{e+1,\dots,2e-2\}$ and so

$$\langle\chi,s\rangle_* + \langle\chi,s\rangle = (k-e)/e + k/e = (2k-e)/e = \langle\chi,s^2\rangle.$$

The completes the proof. ∎

4.3 Approximation Theorems

Let F be a number field. In what follows, assume that G is abelian and of odd order. We will give preliminary characterizations of the sets

$$\mathcal{A}^t(\mathcal{O}_FG) := \{\mathrm{cl}(A_h) : \text{tame } h \in \mathrm{Hom}(\Omega_F, G)\}$$

$$\mathcal{A}^t_u(\mathcal{O}_FG) := \{\mathrm{ucl}(A_h) : \text{tame } h \in \mathrm{Hom}(\Omega_F, G)\}$$

of tame A-realizable classes in $\mathrm{Cl}(\mathcal{O}_FG)$ and $\mathrm{UCl}(\mathcal{O}_FG)$, respectively.

Definition 4.3.1 Recall Definition 4.2.1 and define

$$\mathfrak{F} = \mathfrak{F}_F := \{f \in J(\Lambda(FG)) \mid f_v \in \mathfrak{F}_{F_v} \text{ for all } v \in M_F\}.$$

Theorem 4.3.2 *Let $h \in Hom(\Omega_F, G)$, say with $F_h = FG \cdot b$. Then, we have h is tame if and only if there exists $c \in J(FG)$ such that*

$$rag(c) = \eta(r_G(b))^{-1} u \Theta^t_*(f) \tag{4.3.1}$$

for some $u \in U(\mathcal{H}(\mathcal{O}_FG))$ and $f \in \mathfrak{F}$. Moreover, if (4.3.1) holds, then

(1) for all $v \in M_F$, we have $f_v = f_{F_v,s_v}$ for $s_v := h_v(\sigma_{F_v})$;

(2) for all $v \in M_F$, we have $f_v = 1$ if and only if h_v is unramified;

(3) $j(c) = cl(A_h)$;

(4) $c \in J(FG_{(s)})$ and $j_{(s)}(c) = ucl(A_h)$ if b is also self-dual.

Proof. First, assume that h is tame. For each $v \in M_F$, let $a_v \in A_{h_v}$ and $c_v \in (F_vG)^\times$ be as in (3.1.1) and (3.1.3), respectively. By Theorem 4.2.3, we have $r_G(a_v) = u_v\Theta^t_*(f_{F_v,s_v})$ for some $u_v \in \mathcal{H}(\mathcal{O}_{F_v}G)$ and for $s_v := h_v(\sigma_{F_v})$. This implies that $f_{F_v,s_v} = 1$ if and only if h_v is unramified, and so $f := (f_{F_v,s_v}) \in \mathfrak{F}$. Moreover, from equation (3.1.5), we obtain

$$rag(c_v) = r_G(b)^{-1} r_G(a_v) = r_G(b)^{-1} u_v \Theta_*^t(f_{F_v,s_v}).$$

Setting $c := (c_v) \in J(FG)$ and $u := (u_v) \in U(\mathcal{H}(\mathcal{O}_F G))$, we see that (4.3.1) indeed holds.

Conversely, suppose that there exists $c \in J(FG)$ such that the equality (4.3.1) holds for some $u \in U(\mathcal{H}(\mathcal{O}_F G))$ and $f \in \mathfrak{F}$. Then, for each $v \in M_F$, we have

$$rag(c_v) r_G(b) = u_v \Theta_*^t(f_v),$$

with $f_v = f_{F_v,s_v}$ say. Note that h is the homomorphism associated to $r_G(b)$, so clearly h_v is that associated to $u_v \Theta_*^t(f_{F_v,s_v})$ and thus is tame by Theorem 4.2.4. This shows that h is tame. Theorem 4.2.4 also gives $h_v(\sigma_{F_v}) = s_v$, which proves (1), and (2) follows directly from (1). Now, again by Theorem 4.2.4, there exists $a_v \in A_{h_v}$ such that $A_{h_v} = \mathcal{O}_{F_v} G \cdot a_v$ and $r_G(a_v) = u_v \Theta_*^t(f_{F_v,s_v})$. In particular, we obtain $r_G(a_v) = rag(c_v) r_G(b)$, meaning that there exists $t_v \in G$ such that

$$\mathbf{r}_G(a_v) = (c_v \cdot \mathbf{r}_G(b)) t_v = (c_v t_v) \cdot \mathbf{r}_G(b).$$

This implies that $a_v = (c_v t_v) \cdot b$. Set $t := (t_v) \in U(\mathcal{O}_F G)$. Then, as in Section 3.1, we see that $\mathrm{cl}(A_h) = j(ct) = j(c)$. If b is also self-dual, then $ct \in J(FG_{(s)})$ and so $c \in J(FG_{(s)})$. We have $\mathrm{ucl}(A_h) = j_{(s)}(ct) = j_{(s)}(c)$ as well. This proves (3) and (4). ■

Remark 4.3.3 Theorem 4.3.2 (without the statement in (4)) is analogous to [14, Theorem 6.7], where McCulloh proved the corresponding statements with A_h and Θ_*^t replaced by $\mathcal{O}_h$ and Θ^t, respectively (recall Remark 2.5.7). The proof is verbatim, except we have to use [14, Theorem 6.7] rather than Theorem 4.3.2 (cf. Remark 4.2.5).

Notice that Theorem 4.3.2 implies that for any $c \in J(FG)$, we have $j(c) \in \mathcal{A}^t(\mathcal{O}_FG)$ if and only if $rag(c)$ is an element of

$$\eta(\mathcal{H}(FG))U(\mathcal{H}(\mathcal{O}_FG))\Theta_*^t(\mathfrak{F}) \tag{4.3.2}$$

(recall (2.4.3)). Similarly, for any $c \in J(FG_{(s)})$, we have $j_{(s)}(c) \in \mathcal{A}_u^t(\mathcal{O}_FG)$ if and only if $rag(c)$ is an element of

$$\eta(\mathcal{H}(FG_{(1)}))U(\mathcal{H}(\mathcal{O}_FG))\Theta_*^t(\mathfrak{F}) \tag{4.3.3}$$

(recall (2.4.5) and Proposition 2.3.9 (b)). However, it is unclear whether the sets in (4.3.2) and (4.3.3) are subgroups of $J(\mathcal{H}(FG))$ because $\mathfrak{F}$ is only a subset of $J(\Lambda(FG))$. Below, we will state two approximation theorems which were proved by McCulloh in [14]. They will allow us to replace $\mathfrak{F}$ by $J(\Lambda(FG))$ in both (4.3.2) and (4.3.3).

First, we will need some further definitions (recall (2.5.2) and (2.5.3)).

Definition 4.3.4 Let $\mathfrak{m}$ be an ideal in $\mathcal{O}_F$. For each $v \in M_F$, define

$$U_{\mathfrak{m}}(\mathcal{O}_{F_v^c}) := (1 + \mathfrak{m}\mathcal{O}_{F_v^c}) \cap (\mathcal{O}_{F_v^c})^\times$$
$$U'_{\mathfrak{m}}(\Lambda(\mathcal{O}_{F_v}G)) := \{g_v \in \Lambda(\mathcal{O}_{F_v}G)^\times \mid g_v(s) \in U_{\mathfrak{m}}(\mathcal{O}_{F_v^c}) \text{ for all } s \in G \text{ with } s \neq 1\}$$

and set

$$U'_{\mathfrak{m}}(\Lambda(\mathcal{O}_FG)) := \left(\prod_{v \in M_F} U'_{\mathfrak{m}}(\Lambda(\mathcal{O}_{F_v}G))\right) \cap J(\Lambda(FG)).$$

Definition 4.3.5 For $g \in J(\Lambda(FG))$ and $s \in G$, define

$$g_s := \prod_{v \in M_F} g_v(s) \in \prod_{v \in M_F} (F_v^c)^\times.$$

Theorem 4.3.6 *Let $\mathfrak{m}$ be an ideal in $\mathcal{O}_F$ divisible by both $|G|$ and $\exp(G)^2$.*

(a) We have $Hom_{\Omega_{F_v}}(S_{\widehat{G}}, U_{\mathfrak{m}}(\mathcal{O}_{F_v^c})) \subset \mathcal{H}(\mathcal{O}_{F_v}G)$ for all $v \in M_F$.

(b) We have $\Theta_*^t(U'_{\mathfrak{m}}(\Lambda(\mathcal{O}_F G))) \subset U(\mathcal{H}(\mathcal{O}_F G))$.

Proof. See [14, Theorem 2.14] for (a). As for (b), observe that by (a), it suffices to show that for each $v \in M_F$, we have $\Theta_*^t(U'_{\mathfrak{m}}(\Lambda(\mathcal{O}_{F_v}G))) \subset \mathrm{Hom}_{\Omega_{F_v}}(S_{\widehat{G}}, U_{\mathfrak{m}}(\mathcal{O}_{F_v^c}))$. To that end, let $g_v \in U'_{\mathfrak{m}}(\Lambda(\mathcal{O}_{F_v}G))$ be given. For any $\psi \in S_{\widehat{G}}$, we have $\langle \psi, 1\rangle_* = 0$ and $\langle \psi, s\rangle_* \in \mathbb{Z}$ for all $s \in G$. Since $g_v(s) \in U_{\mathfrak{m}}(\mathcal{O}_{F_v^c})$ for $s \neq 1$, we see that

$$\Theta_*^t(g_v)(\psi) = g_v\left(\sum_{s\in G}\langle \psi, s\rangle_* s\right) = \prod_{s\neq 1} g_v(s)^{\langle \psi, s\rangle_*}$$

indeed lies in $U_{\mathfrak{m}}(\mathcal{O}_{F_v^c})$. This proves the claim. ■

Theorem 4.3.7 *Let $g \in J(\Lambda(FG))$ and let T be a finite subset of M_F. Then, there exists $f \in \mathfrak{F}$ such that $f_v = 1$ for all $v \in T$ and*

$$g \equiv f \qquad (mod\ \lambda(\Lambda(FG)^\times)U'_{\mathfrak{m}}(\Lambda(\mathcal{O}_F G))).$$

Moreover, we may choose f so that for each $s \in G(-1)$ with $s \neq 1$, there exists $\omega \in \Omega_F$ such that $f_{\omega\cdot s} \neq 1$ (recall Definition 2.5.3).

Proof. See [14, Proposition 6.14]. ■

4.4 Proofs of Theorems 1.2.3, 1.3.3, and 1.2.4

Theorem 1.2.4 *Let K be a number field and let G be a finite abelian group of odd order. We have $cl(A_h)cl(\mathcal{O}_h) = cl(\mathcal{O}_{h^2})$ for all $h \in H_t^1(\Omega_K, G)$, and hence $\mathcal{A}^t(\mathcal{O}_K G) \subset R(\mathcal{O}_K G)$.*

Proof. Let $h \in H^1_t(\Omega_K, G)$ be given, with $K_h = KG \cdot b$ say. On one hand, we know from Theorem 4.3.2 that $\mathrm{cl}(A_h) = j(c)$ for some $c \in J(KG)$ such that

$$rag(c) = \eta(r_G(b))^{-1}u\Theta^t_*(f), \tag{4.4.1}$$

where $u \in U(\mathcal{H}(\mathcal{O}_KG))$ and $f_v = f_{K_v,s_v}$ for $s_v := h_v(\sigma_{K_v})$. On the other hand, from [14, Theorem 6.7] (cf. Remark 4.3.3), we have $\mathrm{cl}(\mathcal{O}_h) = j(c')$ for some $c' \in J(KG)$ such that

$$rag(c') = \eta(r_G(b))^{-1}u\Theta^t(f),$$

where $u \in U(\mathcal{H}(\mathcal{O}_KG))$ and $f \in \mathfrak{F}$ may be assumed to be the same as those in (4.4.1). Then, we have

$$rag(cc') = \eta(r_G(b)^2)^{-1}u^2\Theta^t_*(f)\Theta^t(f).$$

Observe that h^2 is the homomorphism associated to $r_G(b)^2$. From Proposition 4.2.6, we also know that $\Theta^t_*(f)\Theta^t(f) = \Theta^t(f')$, where $f' \in \mathfrak{F}$ is given by $f'_v = f'_{K_v,s_v^2}$. It then follows from [14, Theorem 6.7] that $\mathrm{cl}(\mathcal{O}_{h^2}) = j(cc') = j(c)j(c') = \mathrm{cl}(A_h)\mathrm{cl}(\mathcal{O}_h)$, proving the first claim. Since $R(\mathcal{O}_KG)$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_KG)$ by [14, Corollary 6.21], we immediately deduce that $\mathcal{A}^t(\mathcal{O}_KG) \subset R(\mathcal{O}_KG)$, as desired. ■

Theorem 1.3.3 *Let K be a number field and let G be a finite abelian group of odd order. Then, the set $\mathcal{A}^t_u(\mathcal{O}_KG)$ is a subgroup of UCl$(\mathcal{O}_KG)$. Moreover, given $c \in \mathcal{A}^t_u(\mathcal{O}_KG)$ and a finite set T of primes in $\mathcal{O}_K$, there exists $h \in H^1_t(\Omega_K, G)$ such that*

(1) K_h/K is a field extension;

(2) K_h/K is unramified at all $v \in T$;

(3) $c = ucl(A_h)$.

Proof. Let ρ_u denote the composition of the homomorphism $J(KG_{(s)}) \longrightarrow J(\mathcal{H}(KG))$ obtained by restricting the map rag in Definition 2.4.4 followed by the quotient map

$$J(\mathcal{H}(KG)) \longrightarrow \frac{J(\mathcal{H}(KG))}{\eta(\mathcal{H}(KG_{(1)}))U(\mathcal{H}(\mathcal{O}_K G))\Theta_*^t(J(\Lambda(KG)))}.$$

We will show that $\mathcal{A}_u^t(\mathcal{O}_K G)$ is a subgroup of UCl($\mathcal{O}_K G$) by showing that

$$j_{(s)}^{-1}(\mathcal{A}_u^t(\mathcal{O}_K G)) = \ker(\rho_u), \tag{4.4.2}$$

or equivalently, that for any $c \in J(KG_{(s)})$, we have $j_{(s)}(c) \in \mathcal{A}_u^t(\mathcal{O}_K G)$ if and only if

$$rag(c) \in \eta(\mathcal{H}(KG_{(1)}))U(\mathcal{H}(\mathcal{O}_K G))\Theta_*^t(J(\Lambda(KG))). \tag{4.4.3}$$

To that end, let $c \in J(KG_{(s)})$ be given. First, suppose that $j_{(s)}(c) = \mathrm{ucl}(A_h)$ for some tame $h \in \mathrm{Hom}(\Omega_K, G)$, with $K_h = KG \cdot b$ say. Since G has odd order, we may take b to be self-dual by [1, Proposition 5.1], so $r_G(b) \in \mathcal{H}(KG_{(1)})$ by (2.4.3) and Proposition 2.3.9 (b). Also, by Theorem 4.3.2, there exists $c' \in J(KG_{(s)})$ such that $j_{(s)}(c') = \mathrm{ucl}(A_h)$ and

$$rag(c') \in \eta(\mathcal{H}(KG_{(1)}))U(\mathcal{H}(\mathcal{O}_K G))\Theta_*^t(J(\Lambda(KG))).$$

Since $j_{(s)}(c) = \mathrm{ucl}(A_h)$ also, from the bijection in (2.2.2), we see that

$$c \equiv c' \qquad (\mathrm{mod}\ \partial((KG_{(1)})U(\mathcal{O}_K G)).$$

It is then clear that (4.4.3) indeed holds.

Conversely, assume that (4.4.3) holds. Then, we have

$$rag(c) = \eta(r_G(b))^{-1}u\Theta_*^t(g) \tag{4.4.4}$$

for some $r_G(b) \in \mathcal{H}(KG_{(1)})$, $u \in U(\mathcal{H}(\mathcal{O}_K G))$, and $g \in J(\Lambda(KG))$. Now, let $\mathfrak{m}$ be an ideal in $\mathcal{O}_K$. By Theorem 4.3.7, there exists $f \in \mathfrak{F}$ such that

$$g \equiv f \qquad (\text{mod } \lambda(\Lambda(KG)^\times)U'_{\mathfrak{m}}(\Lambda(\mathcal{O}_K G))). \tag{4.4.5}$$

Choosing $\mathfrak{m}$ to be divisible by both $|G|$ and $\exp(G)^2$, from Proposition 2.5.5 and Theorem 4.3.6 (b), the above then implies that

$$\Theta^t_*(g) \equiv \Theta^t_*(f) \qquad (\text{mod } \eta(\mathcal{H}(KG_{(1)}))U(\mathcal{H}(\mathcal{O}_K G))).$$

Hence, changing b and u in (4.4.4) if necessary, we may assume that $g = f$. Note that b is self-dual by Proposition 2.3.9 (b) as $r_G(a) \in \mathcal{H}(KG_{(1)})$. If $h := h_b$ is the homomorphism associated to $r_G(b)$, then h is tame and $j_{(s)}(c) = \text{ucl}(A_h)$ by Theorem 4.3.2. This proves (7.4.1). It remains to show that h may be chosen such that (1) and (2) are satisfied.

Let T be a finite set of primes in $\mathcal{O}_K$. First of all, by Theorem 4.3.7, we may choose the $f \in \mathfrak{F}$ in (4.4.5) such that $f_v = 1$ for all $v \in T$. By Theorem 4.3.2, this implies that h_v is unramified for all $v \in T$, so (2) holds. We may also choose the $f \in \mathfrak{F}$ in (4.4.5) such that for each $s \in G(-1)$ with $s \neq 1$, there exists $\omega \in \Omega_K$ with $f_{\omega \cdot s} \neq 1$. In particular, we have $f_v = f_{K_v, \omega\cdot s}$ for some $v \in M_K$. But observe that $h_v(\sigma_{K_v}) = \omega \cdot s$ by Theorem 4.3.2 and that $\langle s \rangle = \langle \omega \cdot s \rangle$ by Definition 2.5.3. This shows that $s \in h(\Omega_K)$ for all $s \in G \setminus \{1\}$ and so h is surjective. It follows that K_h is a field, and so (1) holds as well. This completes the proof of the theorem. ■

Theorem 1.2.3 *Let K be a number field and let G be a finite abelian group of odd order. Then, the set $\mathcal{A}^t(\mathcal{O}_K G)$ is a subgroup of Cl($\mathcal{O}_K G$). Moreover, given $c \in \mathcal{A}^t(\mathcal{O}_K G)$ and a finite set T of primes in $\mathcal{O}_K$, there exists $h \in H^1_t(\Omega_K, G)$ such that*

(1) K_h/K is a field extension;

(2) K_h/K *is unramified at all* $v \in T$*;*

(3) $c = cl(A_h)$*.*

Proof. Since $\Phi(\mathrm{ucl}(A_h)) = \mathrm{cl}(A_h)$ for all $h \in H^1_w(\Omega_K, G)$, where Φ is the homomorphism in (1.3.1) (cf. Remark 2.2.11), this follows directly from Theorem 1.3.3.

Alternatively, let ρ be the composition of the homomorphism rag in Definition 2.4.4 followed by the quotient map

$$J(\mathcal{H}(KG)) \longrightarrow \frac{J(\mathcal{H}(KG))}{\eta(\mathcal{H}(KG))U(\mathcal{H}(\mathcal{O}_K G))\Theta^t_*(J(\Lambda(KG)))}.$$

Then, essentially the same argument as in the proof of Theorem 1.3.3 shows that

$$j^{-1}(\mathcal{A}^t(\mathcal{O}_K G)) = \ker(\rho),$$

or equivalently, that for any $c \in J(KG)$, we have $j(c) \in \mathcal{A}^t(\mathcal{O}_K G)$ if and only if

$$rag(c) \in \eta(\mathcal{H}(KG))U(\mathcal{H}(\mathcal{O}_K G))\Theta^t_*(J(\Lambda(KG))). \tag{4.4.6}$$

This shows that $\mathcal{A}^t(\mathcal{O}_K G)$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_K G)$. The second claim in the theorem may also be proved using a similar argument as that in the proof of Theorem 1.3.3. ■

4.5 Decomposition of Local Wild Resolvends I

Let F be a finite extension of $\mathbb{Q}_p$. We will assume that G is abelian and of odd order in this section. Under certain hypotheses, we will compute the reduced resolvends $r_G(a)$ for which $A_h = \mathcal{O}_F G \cdot a$ for a wildly and weakly ramified $h \in \mathrm{Hom}(\Omega_F, G)$. It will be helpful to recall the notation set up in Section 1.6.

First, we make the following observation.

Proposition 4.5.1 *Assume that $F/\mathbb{Q}_p$ is unramified and that p is odd. If N/F is a finite Galois extension with different ideal $\mathfrak{D}_{N/F}$ and $e(N/F) = p$, then N/F is weakly ramified and $v_N(\mathfrak{D}_{N/F}) = 2(p-1)$.*

Proof. Notice that $|\mathrm{Gal}(N/F)_0| = e(N/F) = p$. Moreover, since $\mathrm{Gal}(N/F)_0/\mathrm{Gal}(N/F)_1$ has order coprime to p (see [20, Chapter IV, Proposition 7, Corollary 1], for example), we must have $|\mathrm{Gal}(N/F)_1| = p$ as well. Now, suppose on the contrary that N/F is not weakly ramified. This means that $\mathrm{Gal}(N/F)_2 \neq 1$, and so we must have $|\mathrm{Gal}(N/F)_2| = p$. Then, Proposition 1.2.1 implies that

$$v_N(\mathfrak{D}_{N/F}) = \sum_{n=0}^{\infty}(|\mathrm{Gal}(N/F)_n| - 1) \geq 3(p-1).$$

From [16, Chapter III, Theorem 2.5], we also have that

$$v_N(\mathfrak{D}_{N/F}) \leq p - 1 + v_N(p).$$

But $v_N(p) = p$ since $e(N/\mathbb{Q}_p) = e(N/F)e(F/\mathbb{Q}_p) = p$. Hence, we have $2p - 1 \leq 3(p-1)$ and so $p = 2$, which is a contradiction. This proves that N/F must be weakly ramified, and the claim that $v_N(\mathfrak{D}_{N/F}) = 2(p-1)$ also follows. ■

The next proposition is analogous to Proposition 4.2.2 (also recall (2.5.2)).

Proposition 4.5.2 *Assume that $F/\mathbb{Q}_p$ is unramified and let $h \in Hom(\Omega_F, G)$ be so that $e(F^h/F) = p$ and $F^h \subset F_{p,2}$. Then, there exists $a \in A_h$ such that $A_h = \mathcal{O}_F G \cdot a$ and*

$$r_G(a) = \Theta_*^t(g)$$

for some $g \in \Lambda(FG)^\times$.

The proof of Proposition 4.5.2 will take up most of the rest of this section. In the sequel, assume that $F/\mathbb{Q}_p$ is unramified and let $h \in \mathrm{Hom}(\Omega_F, G)$ be as in Proposition 4.5.2. To simplify notation, set $L := F^h$ and let $\zeta := \zeta_p$ be the chosen primitive p-root of unity in F^c. Moreover, notice that since G has odd order, the hypothesis $e(F^h/F) = p$ implies that p is odd. Hence, by Proposition 4.5.1, the extension L/F is weakly ramified and we have $v_L(A_{L/F}) = 1 - p$. Finally, the hypothesis $L \subset F_{p,2}$ gives the following.

Lemma 4.5.3 *There exists $x \in F(\zeta)$ such that $L(\zeta) = F(\zeta, x^{1/p})$ and that $x^{1/p} - 1$ is a uniformizer in $L(\zeta)$.*

Proof. See [18, Section 3 and the discussion following Lemma 8]. This lemma requires the hypotheses that $F/\mathbb{Q}_p$ is unramified with p odd and that $L \subset F_{p,2}$. ■

Let $x \in F(\zeta)$ be given by the above lemma. The fact that $v_{L(\zeta)}(x^{1/p} - 1) \geq 1$ will be important, as we will see. We summarize the set-up in the following diagram, where the numbers indicate the ramification indices.

$$\begin{tikzcd}
 & L(\zeta) = F(\zeta, x^{1/p}) \arrow[dd, dash, "p"] \\
L \arrow[ur, dash, "p-1"] \arrow[dd, dash, "p"'] & \\
 & F(\zeta) \\
F \arrow[ur, dash, "p-1"'] \arrow[d, dash, "1"'] & \\
\mathbb{Q}_p \quad (p \text{ is odd}) &
\end{tikzcd}$$

$$L := F^h$$

$$v_L(A_{L/F}) = 1 - p$$

$$v_{L(\zeta)}(x^{1/p} - 1) = 1$$

Moreover, we will need some further notation.

Definition 4.5.4 Write $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. For each $i \in \mathbb{F}_p$, if z is an element of order 1 or p in a group, we will write z^i for z^{n_i}, where $n_i \in \mathbb{Z}$ is any integer representing i. We will also define $c(i) \in \{(1-p)/2, \ldots, (p-1)/2\}$ to be the unique integer representing i (cf. Definition 2.5.1). If $i \in \mathbb{F}_p^\times$, we will write i^{-1} for its multiplicative inverse in $\mathbb{F}_p^\times$.

Definition 4.5.5 For each $i \in \mathbb{F}_p^\times$, define

$$\omega_i \in \mathrm{Gal}(L(\zeta)/L); \quad \omega_i(\zeta) := \zeta^{i^{-1}}.$$

Moreover, define $x_i := \omega_i(x)$ and

$$x_i^{1/p} := \omega_i(x^{1/p}),$$

which is clearly a p-th root of x_i. We will also write y_i for $x_i^{1/p}$ to simplify notation.

Now, consider the element

$$\alpha := \frac{1}{p}\left(\sum_{k\in\mathbb{F}_p}\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}\right) = \frac{1}{p}\left(1 + \prod_{i\in\mathbb{F}_p^\times} y_i^{c(i)} + \cdots + \prod_{i\in\mathbb{F}_p^\times} y_i^{c(i(p-1))}\right). \tag{4.5.1}$$

We will show that the element $a \in \mathrm{Map}(G, F^c)$ defined by

$$a(s) := \begin{cases} \omega(\alpha) & \text{if } s = h(\omega) \text{ for } \omega \in \Omega_F \\ 0 & \text{otherwise} \end{cases} \tag{4.5.2}$$

is well-defined and that it satisfies the conclusion of Proposition 4.5.2.

Remark 4.5.6 The definition of the element α in (4.5.1) is motivated by the definition of $g \in \Lambda(FG)^\times$ in Lemma 4.5.11, the computation of $\Theta_*^t(g)(\chi)$ for $\chi \in \widehat{G}$ in (4.5.4), and the formula (2.4.10).

First, we will use a valuation argument to show that $\alpha \in A_{L/F}$.

Lemma 4.5.7 *We have $\alpha \in L$.*

Proof. By definition, we have $y_i \in L(\zeta)$ for all $i \in \mathbb{F}_p^\times$. So, clearly $\alpha \in L(\zeta)$ and we have $\alpha \in L$ if and only if α is fixed by the action of $\mathrm{Gal}(L(\zeta)/L)$. Now, notice that an element in $\mathrm{Gal}(L(\zeta)/L)$ is equal to ω_j for some $j \in \mathbb{F}_p^\times$. Moreover, observe that $\omega_j\omega_i = \omega_{ji}$ and so $\omega_j(y_i) = y_{ji}$ for all $i \in \mathbb{F}_p^\times$. Hence, for each $k \in \mathbb{F}_p$, we have

$$\omega_j\left(\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}\right) = \prod_{i\in\mathbb{F}_p^\times} y_{ji}^{c(ik)} = \prod_{i\in\mathbb{F}_p^\times} y_i^{c(j^{-1}ik)}.$$

This implies that ω_j permutes the summands

$$1, \prod_{i\in\mathbb{F}_p^\times} y_i^{c(i)}, \dots, \prod_{i\in\mathbb{F}_p^\times} y_i^{c(i(p-1))}$$

in the definition of α. This shows that $\omega_j(\alpha) = \alpha$ and so $\alpha \in L$. ■

Lemma 4.5.8 *For all $i \in \mathbb{F}_p^\times$ and $n \in \mathbb{Z}$, we have $v_{L(\zeta)}(y_i) = 0$ and $v_{L(\zeta)}(y_i^n - 1) \geq 1$.*

Proof. For each $i \in \mathbb{F}_p^\times$, we have $y_i - 1 = x_i^{1/p} - 1 = \omega_i(x^{1/p} - 1)$. Since $v_{L(\zeta)}(x^{1/p} - 1) = 1$, this implies that $v_{L(\zeta)}(y_i - 1) = 1$ and so $v_{L(\zeta)}(y_i) = 0$. Now, the second claim is obvious for $n = 0$. For $n \in \mathbb{Z}^+$, we have

$$v_{L(\zeta)}(y_i^n - 1) = v_{L(\zeta)}(y_i - 1) + v_{L(\zeta)}(y_i^{n-1} + \cdots + y_i + 1) \geq 1 + 0.$$

For $n \in \mathbb{Z}^-$, use the above to deduce that

$$v_{L(\zeta)}(y_i^n - 1) = v_{L(\zeta)}(y_i^n) + v_{L(\zeta)}(1 - y_i^{-n}) \geq 0 + 1.$$

This completes the proof of the lemma. ■

Proposition 4.5.9 *We have $\alpha \in A_{L/F}$.*

Proof. Recall that $v_L(A_{L/F}) = 1 - p$ and that $v_L(p) = p$. Hence, we have

$$\begin{aligned} v_L(\alpha) &= v_L\left(\sum_{k\in\mathbb{F}_p}\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}\right) - p \\ &= v_L\left(\sum_{k\in\mathbb{F}_p}\left(\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)} - 1\right) + p\right) - p \\ &\geq \min\left\{v_L\left(\sum_{k\in\mathbb{F}_p}\left(\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)} - 1\right)\right), p\right\} - p. \end{aligned}$$

By identifying $\mathbb{F}_p$ with $\{0, 1, \ldots, p-1\}$, for each $k \in \mathbb{F}_p$ we have

$$\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)} - 1 = \sum_{i=1}^{p-2}\left(\left(\prod_{l=i+1}^{p-1} y_l^{c(lk)}\right)(y_i^{c(ik)} - 1)\right) + (y_{p-1}^{c((p-1)k)} - 1).$$

It then follows from Lemma 4.5.8 the element above has positive valuation, and so

$$v_L\left(\sum_{k\in\mathbb{F}_p}\left(\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)} - 1\right)\right) \geq 1.$$

This shows that $v_L(\alpha) \geq 1 - p$, whence $\alpha \in A_{L/F}$, as claimed. ■

Next, we will compute the Galois conjugates of α in L/F. First, observe that because $[L : F]$ and $[F(\zeta) : F]$ are coprime, there is canonical isomorphism

$$\mathrm{Gal}(L(\zeta)/F) \simeq \mathrm{Gal}(L/F) \times \mathrm{Gal}(F(\zeta)/F).$$

Let $\tau \in \mathrm{Gal}(L/F)$ be the generator which is identified with

$$\widetilde{\tau} \in \mathrm{Gal}(L(\zeta)/F(\zeta)); \quad \widetilde{\tau}(x^{1/p}) := \zeta^{-1}x^{1/p} \tag{4.5.3}$$

via this isomorphism. We will also choose a lift ω_τ of τ in Ω_F.

Proposition 4.5.10 *For all $j, k \in \mathbb{F}_p$, we have*

$$\widetilde{\tau}^j\left(\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}\right) = \zeta^{jk}\cdot\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}.$$

In particular, this implies that for all $j \in \mathbb{F}_p$, we have

$$\tau^j(\alpha) = \frac{1}{p}\sum_{k\in\mathbb{F}_p}\left(\zeta^{jk}\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}\right).$$

Proof. Let $j, k \in \mathbb{F}_p$ be given. Since $\mathrm{Gal}(L(\zeta)/F)$ is abelian, for any $i \in \mathbb{F}_p^\times$ we have

$$\begin{aligned}
\widetilde{\tau}^j(y_i) &= (\widetilde{\tau}^j\circ\omega_i)(x^{1/p})\\
&= (\omega_i\circ\widetilde{\tau}^j)(x^{1/p})\\
&= \omega_i(\zeta^{-j}x^{1/p})\\
&= \zeta^{-i^{-1}j}y_i.
\end{aligned}$$

We then see that

$$\begin{aligned}
\widetilde{\tau}^j\left(\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}\right) &= \prod_{i\in\mathbb{F}_p^\times}\zeta^{-i^{-1}jik}y_i^{c(ik)}\\
&= \prod_{i\in\mathbb{F}_p^\times}\zeta^{-jk}y_i^{c(ik)}\\
&= (\zeta^{-jk})^{(p-1)}\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}\\
&= \zeta^{jk}\prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)},
\end{aligned}$$

which proves the proposition. ■

Finally, we will define the desired element $g \in \Lambda(FG)^\times$. Recall that ω_τ is a lift of τ in Ω_F and define $t := h(\omega_\tau)$. Notice that t has order p. It will also be helpful to recall Definition 2.5.3.

Lemma 4.5.11 *The map $g \in Map(G(-1), (F^c)^\times)$ given by*

$$g(s) := \begin{cases} x_i & \textit{if } s = t^i \textit{ for } i \in \mathbb{F}_p^\times \\ 1 & \textit{otherwise} \end{cases}$$

is well-defined and preserves Ω_F-actions. In particular, we have $g \in \Lambda(FG)^\times$.

Proof. Clearly g is well-defined since t has order p. To show that g preserves Ω_F-actions, let $\omega \in \Omega_F$ and $s \in G(-1)$ be given.

If $s = t^i$ for some $i \in \mathbb{F}_p^\times$, then s has order p and so $\omega \cdot s$ is determined by the action of ω on ζ. Let $j \in \mathbb{F}_p^\times$ be such that $\omega|_{F(\zeta)} = \omega_j|_{F(\zeta)}$. Then, we have $\omega^{-1}(\zeta) = \zeta^j$, which in turn gives $\omega \cdot s = s^j = t^{ij}$. It follows that

$$g(\omega \cdot s) = x_{ij} = \omega_j(x_i) = \omega(g(s)).$$

Now, if $\omega \cdot s = t^i$ for some $i \in \mathbb{F}_p^\times$, then the above shows that $s = \omega^{-1} \cdot (\omega \cdot s) = t^{ij}$ for some $j \in \mathbb{F}_p^\times$ as well. Hence, if $s \neq t^i$ for all $i \in \mathbb{F}_p^\times$, then the same holds for $\omega \cdot s$. In this case, we have

$$g(\omega \cdot s) = 1 = \omega(1) = \omega(g(s)).$$

Hence, indeed g preserves Ω_F-actions, and so $g \in \Lambda(FG)^\times$ by definition. ■

We are now ready to prove Proposition 4.5.2.

Proof. Let $a \in \mathrm{Map}(G, F^c)$ be as in (4.5.2) and let $g \in \Lambda(FG)^\times$ be as in Lemma 4.5.11. Since $\alpha \in A_{L/F}$ by Proposition 4.5.9 and $L = F^h$, it is clear that a is well-defined and that $a \in A_h$. We will show that $A_h = \mathcal{O}_F G \cdot a$ and $r_G(a) = \Theta_*^t(g)$.

First of all, we will use the identification $\mathcal{H}(FG) = \mathrm{Hom}_{\Omega_F}(S_{\widehat{G}}, (F^c)^\times)$ in (2.4.12) to show that $r_G(a) = \Theta^t_*(g)$. So, let $\chi \in \widehat{G}$ be given and let $k \in \mathbb{F}_p$ be such that $\chi(t) = \zeta^k$. By Definitions 2.5.1 and 4.5.4, we have $\langle \chi, t^i \rangle_* = c(ik)/p$ for all $i \in \mathbb{F}_p^\times$, and so

$$\Theta^t_*(g)(\chi) = g\left(\sum_{i\in\mathbb{F}_p^\times} \langle \chi, t^i\rangle_* t^i\right) = \prod_{i\in\mathbb{F}_p^\times} x_i^{\langle \chi, t^i\rangle_*} = \prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}. \tag{4.5.4}$$

On the other hand, by the definition of a, we have

$$\mathbf{r}_G(a)(\chi) = \sum_{j\in\mathbb{F}_p} \tau^j(\alpha)(\chi(t)^j)^{-1} = \sum_{j\in\mathbb{F}_p} \tau^j(\alpha)\zeta^{-jk}.$$

Then, using Proposition 4.5.10, we obtain

$$\begin{aligned}\mathbf{r}_G(a)(\chi) &= \frac{1}{p}\sum_{j\in\mathbb{F}_p}\sum_{l\in\mathbb{F}_p}\left(\zeta^{jl}\prod_{i\in\mathbb{F}_p^\times} y_i^{c(il)}\right)\zeta^{-jk}\\ &= \frac{1}{p}\sum_{l\in\mathbb{F}_p}\left(\prod_{i\in\mathbb{F}_p^\times} y_i^{c(il)}\sum_{j\in\mathbb{F}_p}\zeta^{j(l-k)}\right)\\ &= \prod_{i\in\mathbb{F}_p^\times} y_i^{c(ik)}.\end{aligned}$$

This shows that $r_G(a) = \Theta^t_*(g)$, and hence $\mathbf{r}_G(a)\mathbf{r}_G(a)^{[-1]} = 1$ by Proposition 2.5.5. We then deduce from Proposition 2.3.10 $A_h = \mathcal{O}_F G \cdot a$ as well. This completes the proof. ■

The next theorem is analogous to Theorem 4.2.3.

Theorem 4.5.12 *Assume that $F/\mathbb{Q}_p$ is unramified and let $h \in Hom(\Omega_F, G)$ be such that $e(F^h/F) = p$. If $A_h = \mathcal{O}_F G \cdot a$, then we have*

$$r_G(a) = u\Theta^t_*(g)$$

for some $u \in \mathcal{H}(\mathcal{O}_F G)$ and $g \in \Lambda(FG)^\times$.

Proof. Since $F/\mathbb{Q}_p$ is unramified and $e(F^h/F) = p$, we know from Proposition 4.5.1 that h is weakly ramified. Proposition 4.1.2 then implies that h has a factorization $h = h^{nr}h^{tot}$ with respect to p and we have $F^{h^{tot}} \subset F_{p,2}$. Notice also that $e(F^{h^{tot}}/F) = e(F^h/F) = p$ by Proposition 3.2.3 (a).

By Proposition 2.3.7 (b) and (2.4.4), there exists $a_{nr} \in \mathcal{O}_{h^{nr}}$ with $\mathcal{O}_{h^{nr}} = \mathcal{O}_F G \cdot a_{nr}$ and $r_G(a_{nr}) = u'$ for some $u' \in \mathcal{H}(\mathcal{O}_F G)$. Now, note that Proposition 4.5.2 applies to h^{tot}, and hence there exists $a_{tot} \in A_{h_{tot}}$ such that $A_{h^{tot}} = \mathcal{O}_F G \cdot a_{tot}$ and $r_G(a_{tot}) = \Theta^t_*(g)$ for some $g \in \Lambda(FG)^\times$. Using Proposition 3.2.3 (c), we then obtain an element $a' \in A_h$ such that $\mathbf{r}_G(a') = \mathbf{r}_G(a_{nr})\mathbf{r}_G(a_{tot})$ and $A_h = \mathcal{O}_F G \cdot a'$. But $A_h = \mathcal{O}_F G \cdot a$ also, and so $a = \beta \cdot a'$ for some $\beta \in (\mathcal{O}_F G)^\times$. It follows that

$$r_G(a) = rag(\beta) r_G(a') = (rag(\beta)u')\Theta^t_*(g),$$

where $u := rag(\beta)u' \in \mathcal{H}(\mathcal{O}_F G)$. This proves the claim. ■

4.6 Proofs of Theorem 1.2.6 and 1.3.4

Theorem 1.3.4 *Let K be a number field and let G be a finite abelian group of odd order. Let $h \in H^1_w(\Omega_K, G)$ and let V denote the set of primes in $\mathcal{O}_K$ which are wildly ramified in K_h/K. If*

(1) every $v \in V$ is unramified over $\mathbb{Q}$; and

(2) the ramification index of every $v \in V$ in K_h/K is prime,

then we have ucl$(A_h) \in \mathcal{A}^t_u(\mathcal{O}_K G)$.

Proof. Let $b \in K_h$ be as in (3.1.2), where we will take b to be self-dual. For each $v \in M_K$, let $a_v \in A_{h_v}$ and $c_v \in (K_v G)^\times$ be as in (3.1.1) and (3.1.3), respectively. Then, as noted in Section 3.1, we have $c := (c_v) \in J(KG_{(s)})$ and $\mathrm{ucl}(A_h) = j_{(s)}(c)$. Moreover, recall from (3.1.5) that we have $rag(c_v) = r_G(b)^{-1} r_G(a_v)$, where $r_G(b) \in \mathcal{H}(KG_{(1)})$ by (2.4.3) and Proposition 2.3.9 (b). From (4.4.3), we then see that $\mathrm{ucl}(A_h) \in \mathcal{A}^t_u(\mathcal{O}_K G)$ will hold as long as for all $v \in M_K$, we have

$$r_G(a_v) \in \mathcal{H}(\mathcal{O}_{K_v} G)\Theta^t_*(\Lambda(K_v G)^\times). \tag{4.6.1}$$

If $v \notin V$, then (4.6.1) follows from Theorem 4.2.3. If $v \in V$ and $p \in \mathbb{N}$ is the prime lying below v, then $K_v/\mathbb{Q}_p$ is unramified by hypothesis (1) and $e(K_v^{h_v}/K_v) = p$ by hypothesis (2). Hence, Theorem 4.5.12 applies and (4.6.1) holds. This proves the theorem. ■

Theorem 1.2.6 *Let K be a number field and let G be a finite abelian group of odd order. Let $h \in H^1_w(\Omega_K, G)$ and let V denote the set of primes in $\mathcal{O}_K$ which are wildly ramified in K_h/K. If*

(1) every $v \in V$ is unramified over $\mathbb{Q}$; and

(2) the ramification index of every $v \in V$ in K_h/K is prime,

then we have $cl(A_h) \in \mathcal{A}^t(\mathcal{O}_K G)$.

Proof. Since $\Phi(\mathrm{ucl}(A_h)) = \mathrm{cl}(A_h)$ for all $h \in H^1_w(\Omega_K, G)$, where Φ is the homomorphism in (1.3.1) (cf. Remark 2.2.11), this follows directly from Theorem 1.3.4. ■

Chapter 5

Characterization of the A-Realizable Classes in $\mathrm{Cl}(\mathcal{M}(KG))$

Let F be a number field. In what follows, assume that G is abelian and of odd order. As discussed in Section 3.1, given a weakly ramified $h \in \mathrm{Hom}(\Omega_F, G)$, its square root of the inverse different A_h defines a class $\mathrm{cl}(A_h)$ in $\mathrm{Cl}(\mathcal{O}_F G)$. Recall further from Remark 3.1.1 that in order to characterize this class, it suffices to study the reduced resolvends $r_G(a_v)$ for which $A_{h_v} = \mathcal{O}_{F_v} G \cdot a_v$ for each $v \in M_F$.

We have computed such reduced resolvends in Theorems 4.2.3 and 4.2.4 when h_v is tame, and in Theorem 4.5.12 when h_v is wild. In the latter case, we had to assume that v is unramified over $\mathbb{Q}$ and that $e(F_v^{h_v}/F_v)$ is prime. The goal of this chapter is to compute such reduced resolvends when h_v is wild and without these two additional assumptions. The crucial step is to prove that $\mathbf{r}_G(a_v)(\chi) \in \mathcal{O}_{F_v^c}^\times$ for all $\chi \in \widehat{G}$ (recall (2.4.9)). We will do so by first computing the valuations of certain Gauss sums over p-adic numbers. The description of $r_G(a_v)$ that we will obtain in Theorem 5.2.8, however, only characterizes the class $\Psi(\mathrm{cl}(A_h)) \in \mathrm{Cl}(\mathcal{M}(FG))$ and not the class $\mathrm{cl}(A_h) \in \mathrm{Cl}(\mathcal{O}_F G)$. Recall that $\mathcal{M}(FG)$ denotes the maximal $\mathcal{O}_F$-order in FG, and here $\Psi : \mathrm{Cl}(\mathcal{O}_F G) \longrightarrow \mathrm{Cl}(\mathcal{M}(FG))$ denotes the natural homomorphism afforded by extension of scalars.

Throughout this chapter, the symbol p will denote a prime number (not necessarily odd). We will also use the following notation (cf. Definition 4.5.4).

Definition 5.0.3 Write $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. For each $i \in \mathbb{F}_p$, if z is an element of order 1 or p in a group, we will write z^i for z^{n_i}, where $n_i \in \mathbb{Z}$ is any integer representing i. For p odd, we will also define $c(i) \in \{(1-p)/2, \ldots, (p-1)/2\}$ to be the unique integer representing i (cf. Definition 2.5.1). If $i \in \mathbb{F}_p^\times$, we will write i^{-1} for its multiplicative inverse in $\mathbb{F}_p^\times$.

Definition 5.0.4 Note that $\mathbb{Q}_p$ contains all $(p-1)$-st roots of unity. We will write $\widehat{\mathbb{F}_p^\times}$ for the group of $\mathbb{Q}_p$-valued characters on $\mathbb{F}_p^\times$. Given $\varphi \in \widehat{\mathbb{F}_p^\times}$, we will extend it to a map on $\mathbb{F}_p$ by setting $\varphi(0) = 0$. In addition, for each $n \in \mathbb{N}$ which divides $p-1$, let $R_n := (\mathbb{F}_p^\times)^n$ be the subgroup of $\mathbb{F}_p^\times$ consisting of the non-zero n-th powers in $\mathbb{F}_p$.

5.1 Computation of Valuations

5.1.1 Valuations of Gauss Sums over $\mathbb{Q}_p$

In this subsection, let ζ denote a primitive p-th root of unity in $\mathbb{Q}_p^c$. We will estimate the valuations of the following Gauss sums.

Definition 5.1.1 For each $\varphi \in \widehat{\mathbb{F}_p^\times}$ and $j \in \mathbb{F}_p$, define

$$G(\varphi, j) := \sum_{k \in \mathbb{F}_p} \varphi(k)\zeta^{jk}.$$

Lemma 5.1.2 *For all $\varphi \in \widehat{\mathbb{F}_p^\times}$ and $j \in \mathbb{F}_p^\times$, we have*

(a) $G(1,0) = p-1$ and $G(\varphi, 0) = 0$ if $\varphi \neq 1$;

(b) $G(\varphi, j) = \varphi(j)^{-1}G(\varphi, 1)$ and $G(1, j) = -1$.

Proof. The claims in (a) follow from the orthogonality of characters, and both equalities in (b) follow from a simple calculation. ■

In view of Lemma 5.1.2, it remains to consider the Gauss sums $G(\varphi, 1)$ for $\varphi \neq 1$.

Proposition 5.1.3 *Let $\varphi \in \widehat{\mathbb{F}_p^\times}$ be a character of order $n \neq 1$. For all $j \in \mathbb{F}_p^\times$, we have*

$$v_{\mathbb{Q}_p(\zeta)}(G(\varphi, j)) \geq (p-1)/n.$$

Proof. By the first claim in Lemma 5.1.2 (b), we have $v_{\mathbb{Q}_p(\zeta)}(G(\varphi, j)) = v_{\mathbb{Q}_p(\zeta)}(G(\varphi, 1))$ for all $j \in \mathbb{F}_p^\times$. Hence, it is enough to prove the above inequality for $j = 1$. We will do so by computing the valuation of the sum

$$S := \sum_{j \in \mathbb{F}_p} G(\varphi, j)^n$$

in two different ways. On one hand, using Definition 5.1.1, we have

$$\begin{aligned} S &= \sum_{j \in \mathbb{F}_p} \sum_{\substack{k_i \in \mathbb{F}_p \\ 1 \leq i \leq n}} \varphi(k_1 \cdots k_n) \zeta^{j(k_1 + \cdots + k_n)} \\ &= \sum_{\substack{k_i \in \mathbb{F}_p \\ 1 \leq i \leq n}} \varphi(k_1 \cdots k_n) \sum_{j \in \mathbb{F}_p} \zeta^{j(k_1 + \cdots + k_n)} \\ &= \sum_{\substack{k_i \in \mathbb{F}_p \\ 1 \leq i \leq n \\ k_1 + \cdots + k_n = 0}} \varphi(k_1 \cdots k_n) p. \end{aligned}$$

Since each $\varphi(k_1 \cdots k_n)$ is either 0 or a $(p-1)$-st root of unity, this shows that

$$v_{\mathbb{Q}_p(\zeta)}(S) \geq v_{\mathbb{Q}_p(\zeta)}(p) = p - 1. \tag{5.1.1}$$

On the other hand, recall from Lemma 5.1.2 (a) that $G(\varphi, 0) = 0$ since $\varphi \neq 1$, and from

Lemma 5.1.2 (b) that $G(\varphi, j) = \varphi(j)^{-1}G(\varphi, 1)$ for $j \in \mathbb{F}_p^\times$. Since φ has order n, we then deduce that

$$S = \sum_{j \in \mathbb{F}_p^\times} \varphi(j)^{-n} G(\varphi, 1)^n = (p-1)G(\varphi, 1)^n.$$

Since $p - 1 \in \mathbb{Z}_p^\times$ is a p-adic unit, this shows that

$$v_{\mathbb{Q}_p(\zeta)}(S) = n \cdot v_{\mathbb{Q}_p(\zeta)}(G(\varphi, 1)). \tag{5.1.2}$$

The desired inequality now follows from (5.1.1) and (5.1.2). ■

Proposition 5.1.4 *Let $\varphi \in \widehat{\mathbb{F}_p^\times}$ be a character of order $n \neq 1$. For all $j \in \mathbb{F}_p^\times$, we have*

$$\sum_{l=1}^{n-1} G(\varphi^l, j) = 1 + n \sum_{k \in R_n} \zeta^{jk}.$$

Proof. First of all, we have

$$\sum_{l=0}^{n-1} G(\varphi^l, j) = \sum_{l=0}^{n-1} \sum_{k \in \mathbb{F}_p} \varphi^l(k)\zeta^{jk} = \sum_{k \in \mathbb{F}_p} \zeta^{jk} \sum_{l=0}^{n-1} \varphi^l(k).$$

Note that $\ker(\varphi) = R_n$ because φ has order n. In particular, we may regard $1, \varphi, \cdots, \varphi^{n-1}$ as the distinct characters on $\mathbb{F}_p^\times / R_n$. By the orthogonality of characters, we see that

$$\sum_{l=0}^{n-1} \varphi^l(k) = \begin{cases} n & \text{if } k \in R_n \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\sum_{l=0}^{n-1} G(\varphi^l, j) = n \sum_{k \in R_n} \zeta^{jk}.$$

Since $G(1, j) = -1$ by Lemma 5.1.2 (b), the claim now follows. ■

5.1.2 Valuations of Local Wild Resolvents

Let F be a finite extension of $\mathbb{Q}_p$ and assume that G is abelian. First of all, we will recall the definition of resolvents (cf. (2.4.9)) and make a few important observations.

Definition 5.1.5 Let $a \in \mathrm{Map}(G, F^c)$ and $\chi \in \widehat{G}$. The *resolvent of a at χ* is defined by

$$(a \mid \chi) := \sum_{s \in G} a(s)\chi(s)^{-1}.$$

Lemma 5.1.6 *Let N/F be a finite abelian extension that is wildly and weakly ramified.*

(a) We have $Gal(N/F)_0 = Gal(N/F)_1$ and $Gal(N/F)_0$ is elementary p-abelian

(b) The inverse different of N/F has a square root, and $v_N(A_{N/F}) = 1 - |Gal(N/F)_0|$.

(c) There exists $\alpha \in A_{N/F}$ such that $A_{N/F} = \mathcal{O}_F Gal(N/F) \cdot \alpha$.

Proof. The equality $\mathrm{Gal}(N/F)_0 = \mathrm{Gal}(N/F)_1$ was proved in Lemma 3.2.2 (c). It follows that $\mathrm{Gal}(N/F)_0$ is elementary p-abelian because the quotients $\mathrm{Gal}(N/F)_n/\mathrm{Gal}(N/F)_{n+1}$ are p-abelian for all $n \in \mathbb{Z}^+$ by [20, Chapter IV, Proposition 7, Corollary 3]. The claims in (b) then follow immediately from Proposition 1.2.1 since $\mathrm{Gal}(N/F)_2 = 1$. From (a) and (b), we obtain $v_N(A_{N/F}) \equiv 1 \pmod{|\mathrm{Gal}(N/F)_1|}$. The existence of $\alpha \in A_{N/F}$ in (c) then follows from [13, Theorem 1.1]. ■

Next, we compute the resolvents $(a \mid \chi)$ of an element a for which $A_h = \mathcal{O}_F G \cdot a$ for a wildly and weakly ramified $h \in \mathrm{Hom}(\Omega_F, G)$. We note that for any such $h \in \mathrm{Hom}(\Omega_F, G)$, the inverse different of F^h/F has a square root by Lemma 5.1.6 (b) and so A_h exists.

Proposition 5.1.7 *Let $h \in Hom(\Omega_F, G)$ be wildly and weakly ramified such that F^h/F is totally ramified. Then, there exists $a \in A_h$ such that $A_h = \mathcal{O}_F G \cdot a$ and*

$$(a \mid \chi) \in \mathcal{O}_{F^c}^{\times} \qquad \textit{for all } \chi \in \widehat{G}. \tag{5.1.3}$$

The proof of Proposition 5.1.7 will take up most of the rest of this subsection. In the following, let $h \in \mathrm{Hom}(\Omega_F, G)$ be as in Proposition 5.1.7 and set $L := F^h$. We will also write ζ for a primitive p-th root of unity in F^c. Moreover, let $\alpha \in A_{L/F}$ be any element such that $A_{L/F} = \mathcal{O}_F\mathrm{Gal}(L/F) \cdot \alpha$; such an element α exists by Lemma 5.1.6 (c). It is clear that the map $a \in \mathrm{Map}(G, F^c)$ given by

$$a(s) := \begin{cases} \omega(\alpha) & \text{if } s = h(\omega) \text{ for } \omega \in \Omega_F \\ 0 & \text{otherwise} \end{cases} \tag{5.1.4}$$

is well-defined and it satisfies $A_h = \mathcal{O}_F G \cdot a$. It remains to show that $(a \mid \chi) \in \mathcal{O}_{F^c}^\times$ holds for all $\chi \in \widehat{G}$. To that end, notice that for any $\chi \in \widehat{G}$, we have

$$(a \mid \chi) = \sum_{s \in h(\Omega_F)} a(s)\chi(s)^{-1}. \tag{5.1.5}$$

Observe that $h(\Omega_F) \simeq \mathrm{Gal}(L/F)$, which is equal to $\mathrm{Gal}(L/F)_0$ because L/F is totally ramified. It then follows from Lemma 5.1.6 (a) that $h(\Omega_F)$ has exponent p. In particular, this implies that $(a \mid \chi)$ is an element of $L(\zeta)$.

Lemma 5.1.8 *For all $\chi \in \widehat{G}$, we have $v_{L(\zeta)}((a \mid \chi^{-1})) = -v_{L(\zeta)}((a \mid \chi))$. In particular, we have $v_F(Tr(a)) = 0$.*

Proof. We know from Proposition 2.3.10 that $\mathbf{r}_G(a)(\chi)\mathbf{r}_G(a)^{[-1]}(\chi) \in \mathcal{O}_{F(\zeta)}^\times$ for all $\chi \in \widehat{G}$. Since $\mathbf{r}_G(a)^{[-1]}(\chi) = (a \mid \chi^{-1})$, the first claim clearly holds. Observe that $Tr(a) = (a \mid 1)$, so clearly $v_F(Tr(a)) = 0$ holds as well. ■

Next, notice that we have a canonical isomorphism

$$\mathrm{Gal}(L(\zeta)/F) \simeq \mathrm{Gal}(L/F) \times \mathrm{Gal}(F(\zeta)/F)$$

because $[L : F]$ and $[F(\zeta) : F]$ are coprime. We will consider two different cases.

Proposition 5.1.9 *If $[F(\zeta):F]$ is even, then $(a \mid \chi) \in \mathcal{O}_{F^c}^{\times}$ for all $\chi \in \widehat{G}$.*

Proof. If $[F(\zeta):F]$ is even, then the group $\mathrm{Gal}(F(\zeta)/F)$ contains the element ω_{-1} such that $\omega_{-1}(\zeta) = \zeta^{-1}$. Set $\omega := \mathrm{id}_L \times \omega_{-1}$. Then, for any $\chi \in \widehat{G}$, we see from (5.1.5) that

$$(a \mid \chi^{-1}) = \sum_{s \in h(\Omega_F)} a(s)\chi(s) = \omega\left(\sum_{s \in h(\Omega_F)} a(s)\chi(s)^{-1}\right) = \omega((a \mid \chi)).$$

This shows that $(a \mid \chi)$ and $(a \mid \chi^{-1})$ are Galois conjugates in $L(\zeta)/F$, and hence have the same valuation in $L(\zeta)$. It then follows from Lemma 5.1.8 that $(a \mid \chi) \in \mathcal{O}_{F^c}^{\times}$. ∎

Proposition 5.1.10 *If $[F(\zeta):F] < p-1$, then $(a \mid \chi) \in \mathcal{O}_{F^c}^{\times}$ for all $\chi \in \widehat{G}$.*

Proof. If $[F(\zeta):F] < p-1$, then $\mathrm{Gal}(F(\zeta)/F) \simeq R_n$ for some $n \in \mathbb{N} \setminus \{1\}$ dividing $p-1$. Suppose on the contrary that there exists $\chi \in \widehat{G}$ such that $v_{L(\zeta)}((a \mid \chi)) \neq 0$. In view of Lemma 5.1.8, replacing χ by χ^{-1} if necessary, we may assume that $v_{L(\zeta)}((a \mid \chi)) > 0$. We also know that $\chi \neq 1$. For each $k \in R_n$, let ω_k denote the element such that $\omega_k(\zeta) = \zeta^k$ and set $\widetilde{\omega_k} := \mathrm{id}_L \times \omega_k$. Observe that from (5.1.5), we have

$$(a \mid \chi^k) = \sum_{s \in h(\Omega_F)} a(s)\chi(s)^{-k} = \widetilde{\omega_k}\left(\sum_{s \in h(\Omega_F)} a(s)\chi(s)^{-1}\right) = \widetilde{\omega_k}((a \mid \chi)).$$

This implies that $(a \mid \chi)$ and $(a \mid \chi^k)$ are Galois conjugates in $L(\zeta)/F$, and hence have the same valuation in $L(\zeta)$. In particular, we have $v_{L(\zeta)}((a \mid \chi^k)) > 0$ for all $k \in R_n$.

Next, let $\varphi \in \widehat{\mathbb{F}_p^{\times}}$ be any character of order n. For each $s \in h(\Omega_F)$, let $j_s \in \mathbb{F}_p$ denote the element such that $\chi^{-1}(s) = \zeta^{j_s}$ and consider the sum

$$S := \sum_{s \in h(\Omega_F)} a(s) \sum_{l=1}^{n-1} G(\varphi^l, j_s).$$

Below, we will compute the valuation of S to obtain a contradiction.

Notice that by Lemma 5.1.6, there exists $r \in \mathbb{Z}^+$ such that $\mathrm{Gal}(L/F)_0 \simeq (\mathbb{Z}/p\mathbb{Z})^r$. Moreover, set $e := e(F/\mathbb{Q}_p)$ and $d := e(F(\zeta)/F)$. We summarize the set-up in the diagram below, where the numbers indicate ramification indices.

$$\begin{tikzcd}
 & L(\zeta) \arrow[d, dash, "p^r"] \\
L \arrow[ur, dash, "d"] \arrow[dd, dash, "p^r"'] & \\
 & F(\zeta) \arrow[dd, dash, "\frac{ed}{p-1}"] \\
F \arrow[ur, dash, "d"'] \arrow[ur, dash, bend left, "R_n"] \arrow[dd, dash, "e"'] & \\
 & \mathbb{Q}_p(\zeta) \\
\mathbb{Q}_p \arrow[ur, dash, "p-1"'] &
\end{tikzcd}$$

$$L := F^h$$

$$v_L(A_{L/F}) = 1 - p^r$$

First of all, for each $l = 1, 2, \ldots, n-1$, we have $\varphi^l \neq 1$ because φ has order $n \neq 1$. If $j_s = 0$, then $G(\varphi^l, j_s) = 0$ by Lemma 5.1.2 (a). If $j_s \neq 0$, then using Proposition 5.1.3 and the fact that $v_L(A_{L/F}) = 1 - p^r$, we deduce that

$$\begin{aligned} v_{L(\zeta)}(a(s)G(\varphi^l, j_s)) &\geq d(1-p^r) + \frac{ed}{p-1} \cdot p^r \cdot \frac{p-1}{n} \\ &= dp^r\left(\frac{e}{n} - 1\right) + d. \end{aligned} \tag{5.1.6}$$

Since $d \leq |R_n| = (p-1)/n$ and $ed \geq p-1$ by the multiplicativity of ramification indices, we see that $e \geq n$ and so (5.1.6) is positive. We then deduce that $v_{L(\zeta)}(S) > 0$.

Next, let H be the subgroup of $h(\Omega_F)$ consisting of the elements s for which $j_s = 0$. Since $G(\varphi^l, 0) = 0$ for $l = 1, 2, \ldots, n-1$, using Proposition 5.1.4, we may rewrite

$$S = \sum_{s \in h(\Omega_F)} a(s)\left(1 + n \sum_{k \in R_n} \zeta^{j_s k}\right) - \sum_{s \in H} a(s)\left(1 + n \sum_{k \in R_n} \zeta^{(0)k}\right).$$

Using (5.1.5) and the fact that $\chi^{-1}(s) = \zeta^{j_s}$ for each $s \in h(\Omega_F)$, the above simplifies to

$$S = Tr(a) + n \sum_{k \in R_n} (a \mid \chi^k) - p \sum_{s \in H} a(s).$$

Recall that $v_F(Tr(a)) = 0$ from Lemma 5.1.8. Since $v_{L(\zeta)}(S) > 0$ and $v_{L(\zeta)}((a \mid \chi^k)) > 0$ for all $k \in R_n$, we deduce that

$$v_L\left(p \sum_{s \in H} a(s)\right) = 0.$$

But this in turn implies that

$$0 \geq v_L(p) + v_L(A_{L/F}) = ep^r + (1 - p^r) = p^r(e-1) + 1,$$

which is impossible because $e \geq 1$. Hence, we must have $(a \mid \chi) \in \mathcal{O}_{F^c}^\times$ for all $\chi \in \widehat{G}$. ∎

We are now ready to prove Proposition 5.1.7.

Proof. Let $a \in \text{Map}(G, F^c)$ be as in (5.1.4). We already know that $A_h = \mathcal{O}_F G \cdot a$, and so it remains to show that (5.1.3) also holds. If $p = 2$, then $(a \mid \chi) = (a \mid \chi^{-1})$ for all $\chi \in \widehat{G}$ because of (5.1.5). We then see from Lemma 5.1.8 that (5.1.3) indeed holds. If p is odd, then either $[F(\zeta) : F] = p - 1$, which is even, or $[F(\zeta) : F] < p - 1$. We then see from Propositions 5.1.9 and 5.1.10 that (5.1.3) holds in this case as well. ∎

The next theorem is the key to the proof of Theorem 5.2.8.

Theorem 5.1.11 *Let $h \in Hom(\Omega_F, G)$ be wildly and weakly ramified. If $A_h = \mathcal{O}_F G \cdot a$, then*

$$(a \mid \chi) \in \mathcal{O}_{F^c}^\times \qquad \textit{for all } \chi \in \widehat{G}.$$

Proof. By Proposition 4.1.2, there exists a factorization $h = h^{nr}h^{tot}$ of h, with respect to some chosen uniformizer in F say. Moreover, the extension $F^{h^{tot}}/F$ is also wildly and weakly ramified by Proposition 3.2.3 (a) and (b).

Now, there exists $a_{nr} \in \mathcal{O}_{h^{nr}}$ such that $\mathcal{O}_{h^{nr}} = \mathcal{O}_F G \cdot a_{nr}$ and $\mathbf{r}_G(a_{nr}) \in (\mathcal{O}_{F^c} G)^\times$ by Proposition 2.3.7 (b). In particular, we have

$$(a_{nr} \mid \chi) \in \mathcal{O}_{F^c}^\times \qquad \text{for all } \chi \in \widehat{G}. \tag{5.1.7}$$

On the other hand, there exists $a_{tot} \in A_{h^{tot}}$ such that $A_{h^{tot}} = \mathcal{O}_F G \cdot a_{tot}$ and

$$(a_{tot} \mid \chi) \in \mathcal{O}_{F^c}^\times \qquad \text{for all } \chi \in \widehat{G} \tag{5.1.8}$$

by Proposition 5.1.7. Applying Proposition 3.2.3 (c), we then obtain an element $a' \in A_h$ such that $A_h = \mathcal{O}_F G \cdot a'$ and $\mathbf{r}_G(a') = \mathbf{r}_G(a_{nr})\mathbf{r}_G(a_{tot})$. Since $A_h = \mathcal{O}_F G \cdot a$ also, we have $a = \beta \cdot a'$ for some $\beta \in (\mathcal{O}_F G)^\times$. In particular, we have

$$(a \mid \chi) = \beta(\chi)(a_{nr} \mid \chi)(a_{tot} \mid \chi) \qquad \text{for all } \chi \in \widehat{G}.$$

Clearly $\beta(\chi) \in \mathcal{O}_{F^c}^\times$ for all $\widehat{G}$. It then follows from (5.1.7) and (5.1.8) that $(a \mid \chi) \in \mathcal{O}_{F^c}^\times$ for all $\chi \in \widehat{G}$ as well. This proves the theorem. ■

5.2 Decomposition of Local Wild Resolvends II

Let F be a finite extension of $\mathbb{Q}_p$. We will assume that G is abelian and of odd order in this section. We will compute the reduced resolvends $r_G(a)$ for which $A_h = \mathcal{O}_F G \cdot a$, where $h \in \mathrm{Hom}(\Omega_F, G)$ is any wildly and weakly ramified homomorphism. It will be helpful to recall the notation set up in Definitions 5.0.3 and 5.0.4.

First of all, by modifying the proof of Proposition 4.5.2, we will prove the following analogous result (recall (2.5.2)).

Proposition 5.2.1 *Let $h \in Hom(\Omega_F, G)$ be wildly and weakly ramified such that F^h/F has degree p. Then, there exists $a \in F_h$ such that $F_h = FG \cdot a$ and*

(1) $r_G(a) = \Theta_*^t(g)$ for some $g \in \Lambda(FG)^\times$;

(2) $(a \mid \chi) \in \mathcal{O}_{F^c}^\times$ for all $\chi \in \widehat{G}$.

The proof of Proposition 5.2.1 will take up most of the rest of this section. In what follows, let $h \in \mathrm{Hom}(\Omega_F, G)$ be as in Proposition 5.2.1. To simplify notation, set $L := F^h$ and let $\zeta := \zeta_p$ be the chosen primitive p-root of unity in F^c. Since G has odd order, the hypothesis that F^h/F has degree p implies that p is odd. In addition, let $\alpha' \in A_{L/F}$ be such that $A_{L/F} = \mathcal{O}_F\mathrm{Gal}(L/F) \cdot \alpha'$; such an element α' exists by Lemma 5.1.6 (c).

Next, notice that $\mathrm{Gal}(F(\zeta)/F) \simeq R_n$ for some $n \in \mathbb{N}$ dividing $p-1$ and let d denote the image of $(p-1)/n$ in $\mathbb{F}_p$. Moreover, there is a canonical isomorphism

$$\mathrm{Gal}(L(\zeta)/F) \simeq \mathrm{Gal}(L/F) \times \mathrm{Gal}(F(\zeta)/F)$$

because $[L : F]$ and $[F(\zeta) : F]$ are coprime. We will fix a generator τ of $\mathrm{Gal}(L/F)$ and let $\widetilde{\tau} \in \mathrm{Gal}(L(\zeta)/F(\zeta))$ be the element which is identified with τ. We summarize the set-up in the following diagram, where the numbers indicate the degrees of the extensions.

$$\begin{tikzcd}
 & L(\zeta) \arrow[d, dash, "p"'] \arrow[d, dash, bend left=60, "\langle\widetilde{\tau}\rangle"] \\
L \arrow[ur, dash, "\frac{p-1}{n}"] \arrow[dd, dash, "p"] \arrow[dd, dash, bend right=60, "\langle\tau\rangle"'] & \\
 & F(\zeta) \\
F \arrow[ur, dash, "\frac{p-1}{n}"'] \arrow[ur, dash, bend left=40, "R_n"] \arrow[d, dash] & \\
\mathbb{Q}_p \quad (p \text{ is odd}) &
\end{tikzcd}$$

$L := F^h$

$A_{L/F} = \mathcal{O}_F\mathrm{Gal}(L/F) \cdot \alpha'$

$d := (p-1)/n \pmod p$

Definition 5.2.2 For each $i \in \mathbb{F}_p$, define

$$y_i := \sum_{k \in \mathbb{F}_p} \tau^k(\alpha')\zeta^{-ik}.$$

First, we will give some basic properties of these elements $y_i \in L(\zeta)$.

Lemma 5.2.3 *For all $i \in \mathbb{F}_p$, we have*

(1) $y_i \in \mathcal{O}_{L(\zeta)}^{\times}$; and

(2) $\widetilde{\tau}(y_i) = \zeta^i y_i$; and

(3) $y_i^p \in F(\zeta)$.

Proof. The map $a' \in \mathrm{Map}(G, F^c)$ defined by

$$a'(s) := \begin{cases} \omega(\alpha') & \text{if } s = h(\omega) \text{ for } \omega \in \Omega_F \\ 0 & \text{otherwise} \end{cases}$$

is clearly well-defined and it satisfies $A_h = \mathcal{O}_F G \cdot a'$ (cf. (5.1.4)). Let ω_τ be a lift of τ in Ω_F and set $t := h(\omega_\tau)$. Note that t has order p. If $\chi \in \widehat{G}$ is such that $\chi(t) = \zeta^i$, then

$$(a' \mid \chi) = \sum_{s \in h(\Omega_F)} a'(s)\chi(s)^{-1} = \sum_{k \in \mathbb{F}_p} \tau^k(\alpha')\chi(t)^{-k}$$

(cf. (5.1.5)), which is equal to y_i. We then deduce from Theorem 5.1.11 that (a) holds. As for (b), it follows from a simple calculation. Using (b), we further deduce that

$$N_{L(\zeta)/F(\zeta)}(y_i) = \prod_{k \in \mathbb{F}_p} \widetilde{\tau}^k(y_i) = \prod_{k \in \mathbb{F}_p} \zeta^{ik} y_i = y_i^p.$$

Thus, indeed $y_i^p \in F(\zeta)^\times$, and this proves the lemma. ■

Next, consider the element (cf. (4.5.1))

$$\alpha := \frac{1}{p}\left(\sum_{k\in\mathbb{F}_p}\prod_{i\in R_n} y_i^{c(i^{-1}k)}\right) = \frac{1}{p}\left(1+\prod_{i\in R_n} y_i^{c(i^{-1})}+\cdots+\prod_{i\in R_n} y_i^{c(i^{-1}(p-1))}\right).$$

We will show that the element $a \in \mathrm{Map}(G, F^c)$ defined by

$$a(s) := \begin{cases} \omega(\alpha) & \text{if } s = h(\omega) \text{ for } \omega \in \Omega_F \\ 0 & \text{otherwise} \end{cases} \tag{5.2.1}$$

is well-defined and that it satisfies the conclusion of Proposition 5.2.1.

Definition 5.2.4 For each $i \in R_n$, define

$$\omega_i \in \mathrm{Gal}(L(\zeta)/L); \quad \omega_i(\zeta) := \zeta^i$$

(cf. Definition 4.5.5 and note that our notation here is different). Clearly, we have

$$\omega_i(y_j) = y_{ij} \qquad \text{for all } j \in \mathbb{F}_p. \tag{5.2.2}$$

First of all, we will show that $\alpha \in L$ (cf. Lemma 4.5.7) and then compute the Galois conjugates of α in L/F (cf. Proposition 4.5.10).

Lemma 5.2.5 *We have $\alpha \in L$.*

Proof. By definition, we have $y_i \in L(\zeta)$ for all $i \in \mathbb{F}_p$. So, clearly $\alpha \in L(\zeta)$ and we have $\alpha \in L$ if and only if α is fixed by the action of $\mathrm{Gal}(L(\zeta)/L)$. Now, notice that an element in $\mathrm{Gal}(L(\zeta)/L)$ is equal to ω_j for some $j \in R_n$. For each $k \in \mathbb{F}_p$, we have

$$\omega_j\left(\prod_{i\in R_n} y_i^{c(i^{-1}k)}\right) = \prod_{i\in R_n} y_{ij}^{c(i^{-1}k)} = \prod_{i\in R_n} y_i^{c(i^{-1}jk)}$$

by (5.2.2). This implies that ω_j permutes the summands

$$1, \prod_{i\in R_n} y_i^{c(i^{-1})}, \ldots, \prod_{i\in R_n} y_i^{c(i^{-1}(p-1))}$$

in the definition of α and hence fixes α. Thus, indeed $\alpha \in L$. ■

Proposition 5.2.6 *For all $j, k \in \mathbb{F}_p$, we have*

$$\widetilde{\tau}^j \left(\prod_{i\in R_n} y_i^{c(i^{-1}k)} \right) = \zeta^{jkd} \cdot \prod_{i\in R_n} y_i^{c(i^{-1}k)}.$$

In particular, this implies that for all $j \in \mathbb{F}_p$, we have

$$\tau^j(\alpha) = \frac{1}{p} \sum_{k\in\mathbb{F}_p} \left(\zeta^{jkd} \prod_{i\in R_n} y_i^{c(i^{-1}k)} \right).$$

Proof. Let $j, k \in \mathbb{F}_p$ be given. Since $\mathrm{Gal}(L(\zeta)/F)$ is abelian, for any $i \in R_n$, we have

$$\begin{aligned} \widetilde{\tau}^j(y_i) &= (\widetilde{\tau}^j \circ \omega_i)(y_1) \\ &= (\omega_i \circ \widetilde{\tau}^j)(y_1) \\ &= \omega_i(\zeta^j y_1) \\ &= \zeta^{ij} y_i. \end{aligned}$$

by (5.2.2) and Lemma 5.2.3 (2). We then see that

$$\begin{aligned} \widetilde{\tau}^j \left(\prod_{i\in R_n} y_i^{c(i^{-1}k)} \right) &= \prod_{i\in R_n} \zeta^{ijc(i^{-1}k)} y_i^{c(i^{-1}k)} \\ &= \prod_{i\in R_n} \zeta^{jk} y_i^{c(i^{-1}k)} \\ &= \zeta^{jk(p-1)/n} \cdot \prod_{i\in R_n} y_i^{c(i^{-1}k)}. \end{aligned}$$

Since $d := (p-1)/n \pmod{p}$, the proposition now follows. ■

Next, we will define the desired element $g \in \Lambda(FG)^\times$ (cf. Lemma 4.5.11). Below, we will fix a lift ω_τ of τ in Ω_F and set $t := h(\omega_\tau)$. Notice that t has order p. It will also be helpful to recall Definition 2.5.3.

Lemma 5.2.7 *The map $g \in Map(G(-1), (F^c)^\times)$ given by*

$$g(s) := \begin{cases} y_i^p & \text{if } s = t^{d^{-1}i^{-1}} \text{ for } i \in R_n \\ 1 & \text{otherwise} \end{cases}$$

is well-defined and preserves Ω_F-actions. In particular, we have $g \in \Lambda(FG)^\times$.

Proof. Clearly g is well-defined since t has order p. To show that g preserves Ω_F-actions, let $\omega \in \Omega_F$ and $s \in G(-1)$ be given.

If $s = t^{d^{-1}i^{-1}}$ for some $i \in R_n$, then s has order p and $\omega \cdot s$ is determined by the action of ω on ζ. Let $j \in R_n$ be such that $\omega|_{F(\zeta)} = \omega_j|_{F(\zeta)}$. Then, we have $\omega^{-1}(\zeta) = \zeta^{j^{-1}}$, which in turn gives $\omega \cdot s = s^{j^{-1}} = t^{d^{-1}(ij)^{-1}}$. Recall further that $y_i^p \in F(\zeta)$ by Lemma 5.2.3 (3) and that $y_{ij} = \omega_j(y_i)$ by (5.2.2). It follows that

$$g(\omega \cdot s) = y_{ij}^p = \omega_j(y_i^p) = \omega(g(s)).$$

Now, if $\omega \cdot s = t^{d^{-1}i^{-1}}$ for some $i \in R_n$, then the above implies $s = \omega^{-1} \cdot (\omega \cdot s) = t^{d^{-1}(ij)^{-1}}$ for some $j \in R_n$ as well. Hence, if $s \neq t^{d^{-1}i^{-1}}$ for all $i \in R_n$, then the same holds for $\omega \cdot s$. In this case, we have

$$g(\omega \cdot s) = 1 = \omega(1) = \omega(g(s)).$$

Hence, indeed g preserves Ω_F-actions, and so $g \in \Lambda(FG)^\times$ by definition. ■

We are now ready to prove Proposition 5.2.1.

Proof. Let $a \in \mathrm{Map}(G, F^c)$ be as in (5.2.1) and let $g \in \Lambda(FG)^\times$ be as in Lemma 5.2.7. Since $\alpha \in L$ by Lemma 5.2.5 and $L = F^h$, clearly a is well-defined and $a \in F_h$.

First of all, we will use the identification $\mathcal{H}(FG) = \mathrm{Hom}_{\Omega_F}(S_{\widehat{G}}, (F^c)^\times)$ in (2.4.12) to show that $r_G(a) = \Theta_*^t(g)$. So, let $\chi \in \widehat{G}$ be given and let $k \in \mathbb{F}_p$ be such that $\chi(t) = \zeta^k$. By Definitions 2.5.1 and 4.5.4, we have $\langle \chi, t^{d^{-1}i^{-1}} \rangle_* = c(d^{-1}i^{-1}k)/p$ for all $i \in R_n$, and so

$$\Theta_*^t(g)(\chi) = g\left(\sum_{i \in R_n} \langle \chi, t^{d^{-1}i^{-1}} \rangle_* t^{d^{-1}i^{-1}}\right) = \prod_{i \in R_n} y_i^{c(d^{-1}i^{-1}k)}.$$

On the other hand, by the definition of a, we have

$$\mathbf{r}_G(a)(\chi) = \sum_{j \in \mathbb{F}_p} \tau^j(\alpha)(\chi(t)^j)^{-1} = \sum_{j \in \mathbb{F}_p} \tau^j(\alpha)\zeta^{-jk}.$$

Then, using Proposition 5.2.6, we obtain

$$\begin{aligned}\mathbf{r}_G(a)(\chi) &= \frac{1}{p}\sum_{j \in \mathbb{F}_p}\sum_{l \in \mathbb{F}_p}\left(\zeta^{jld}\prod_{i \in R_n} y_i^{c(i^{-1}l)}\right)\zeta^{-jk} \\ &= \frac{1}{p}\sum_{l \in \mathbb{F}_p}\left(\prod_{i \in R_n} y_i^{c(i^{-1}l)}\sum_{j \in \mathbb{F}_p}\zeta^{j(dl-k)}\right) \\ &= \prod_{i \in R_n} y_i^{c(i^{-1}d^{-1}k)}.\end{aligned}$$

So, indeed $r_G(a) = \Theta_*^t(g)$. Since $y_i \in \mathcal{O}_{L(\zeta)}^\times$ for all $i \in \mathbb{F}_p$ by Lemma 5.2.3 (1), the above computation also shows that $(a \mid \chi) \in \mathcal{O}_{L(\zeta)}^\times$ for all $\chi \in \widehat{G}$ and that $F_h = FG \cdot a$ by Proposition 2.3.7 (a). Hence, the map a in (5.2.1) satisfies all of the desired properties. ■

The next theorem is analogous to Theorem 4.5.12.

Theorem 5.2.8 *Let $h \in$ Hom(Ω_F, G) be wildly and weakly ramified. If $A_h = \mathcal{O}_F G \cdot a$, then there exists $\beta \in \mathcal{M}(FG)^\times$ such that*

$$r_G(a) = rag(\beta)u\Theta_*^t(g)$$

for some $u \in \mathcal{H}(\mathcal{O}_F G)$ and $g \in \Lambda(FG)^\times$.

Proof. By Proposition 4.1.2, there exists a factorization $h = h^{nr}h^{tot}$ of h, with respect to some chosen uniformizer of F say. From Proposition 3.2.3 (a) and (b), we know that h^{tot} is also wildly and weakly ramified. Because $F^{h^{tot}}/F$ is totally ramified, Lemma 5.1.6 (a) implies that $\mathrm{Gal}(F^{h^{tot}}/F)$ is elementary p-abelian.

Since $h^{tot}(\Omega_F) \simeq \mathrm{Gal}(F^{h^{tot}}/F)$, we have

$$h^{tot}(\Omega_F) = H_1 \times H_2 \times \cdots \times H_r \tag{5.2.3}$$

for subgroups $H_1, H_2, \ldots, H_r$ each of order p. For each $i = 1, 2, \ldots, r$, define

$$h_i \in \mathrm{Hom}(\Omega_F, G); \quad h_i(\omega) := \pi_i(h^{tot}(\omega)),$$

where $\pi_i : h^{tot}(\Omega_F) \longrightarrow H_i$ is the projection map given by (5.2.3). By definition, we have $h^{tot} = h_1h_2\cdots h_r$. For each $i = 1, 2, \ldots, r$, it is clear that $F^{h_i} \subset F^{h^{tot}}$ and $[F^{h_i} : F] = p$. Hence, Proposition 5.2.1 applies and there exists $a_i \in F_{h_i}$ with $F_{h_i} = FG \cdot a_i$ such that

$$r_G(a_i) = \Theta^t_*(g_i) \qquad \text{for some } g_i \in \Lambda(FG)^\times$$

and $(a_i \mid \chi) \in \mathcal{O}^\times_{F^c}$ for all $\chi \in \widehat{G}$. On the other hand, by Proposition 2.3.7 (b) and (2.4.4), there exists $a_{nr} \in \mathcal{O}_{h^{nr}}$ such that $\mathcal{O}_{h^{nr}} = \mathcal{O}_F G \cdot a_{nr}$ and

$$r_G(a_{nr}) = u \qquad \text{for some } u \in \mathcal{H}(\mathcal{O}_F G).$$

Let $a' \in \mathrm{Map}(G, F^c)$ be such that $\mathbf{r}_G(a') = \mathbf{r}_G(a_{nr})\mathbf{r}_G(a_1)\cdots\mathbf{r}_G(a_r)$; such an element a' exists because $\mathbf{r}_G$ is bijective. We have that $a' \in F_h$ by (2.3.3) and that $F_h = FG \cdot a'$ by Proposition 2.3.7 (a). But $F_h = FG \cdot a$ also, so $a = \beta \cdot a'$ for some $\beta \in (FG)^\times$. It follows that

$$r_G(a) = rag(\beta)r_G(a') = rag(\beta)u\Theta^t_*(g),$$

where $g := g_1 g_2 \cdots g_r \in \Lambda(FG)^\times$. It remains to show that $\beta \in \mathcal{M}(FG)^\times$.

To that end, notice that $\mathcal{M}(FG)^\times = \mathrm{Map}_{\Omega_F}(\widehat{G}, \mathcal{O}_{F^c}^\times)$ via the identification in (2.4.8). Moreover, for any $\chi \in \widehat{G}$, we have

$$(a \mid \chi) = \beta(\chi)(a_{nr} \mid \chi)(a_1 \mid \chi) \cdots (a_r \mid \chi).$$

It is clear that $(a_{nr} \mid \chi) \in \mathcal{O}_{F^c}^\times$ because $\mathbf{r}_G(a_{nr}) \in (\mathcal{O}_{F^c}G)^\times$. We also have $(a \mid \chi) \in \mathcal{O}_{F^c}^\times$ by Theorem 5.1.11 and $(a_1 \mid \chi), \ldots, (a_r \mid \chi) \in \mathcal{O}_{F^c}^\times$ by choice. It follows that $\beta(\chi) \in \mathcal{O}_{F^c}^\times$ and so indeed $\beta \in \mathcal{M}(FG)^\times$. ■

5.3 Proof of Theorem 1.2.8

Theorem 1.2.8 *Let K be a number field and let G be a finite abelian group of odd order. Then, we have $\Psi(\mathcal{A}(\mathcal{O}_K G)) = \Psi(\mathcal{A}^t(\mathcal{O}_K G))$.*

Proof. Let $h \in H_w^1(\Omega_K, G)$ be given, with $K_h = KG{\cdot}b$ say. For each $v \in M_K$, let $a_v \in A_{h_v}$ and $c_v \in (K_v G)^\times$ be as in (3.1.1) and (3.1.3), respectively. As explained in Section 3.1, we have $c := (c_v) \in J(KG)$ and $\mathrm{cl}(A_h) = j(c)$. We want to show that $\Psi(j(c)) = \Psi(j(c'))$ for some $c' \in J(KG)$ with $j(c') \in \mathcal{A}^t(\mathcal{O}_K G)$.

Notice that for each $v \in M_K$, there exists $\beta_v \in \mathcal{M}(K_v G)^\times$ such that

$$rag(\beta_v) r_G(a_v) \in \mathcal{H}(\mathcal{O}_{K_v} G)\Theta_*^t(\Lambda(K_v G)^\times). \tag{5.3.1}$$

Indeed, if h_v is tame, then we may take $\beta_v = 1$ by Theorem 4.2.3. If h_v is wild, then such a β_v exists by Theorem 5.2.8. Let $\beta := (\beta_v) \in U(\mathcal{M}(KG))$ and define $c' := \beta c \in J(KG)$. Observe that

$$\ker(\Psi) = j(\partial((KG)^\times)U(\mathcal{M}(KG)))$$

by Theorem 2.1.7 and so $\Psi(j(c)) = \Psi(j(c'))$. Moreover, for each $v \in M_K$, we have

$$rag(c'_v) = rag(\beta_v)rag(c) = r_G(b)^{-1}(rag(\beta_v)r_G(a_v))$$

from equation (3.1.5). Since $r_G(b) \in \mathcal{H}(KG)$ by (2.4.3), we deduce from (5.3.1) that

$$rag(c') \in \eta(\mathcal{H}(KG))U(\mathcal{H}(\mathcal{O}_K G))\Theta^t_*(J(\Lambda(KG))).$$

It then follows from (4.4.6) that $j(c') \in \mathcal{A}^t(\mathcal{O}_K G)$, and this proves the theorem. ■

Chapter 6

Commutativity of the Basic Diagram

Recall from Section 1.6 that K/k is a fixed Galois subextension of K and $\Sigma := \mathrm{Gal}(K/k)$. Throughout this chapter, we will assume that G is abelian and fix a left Σ-module structure on G. Via the quotient map $\mathrm{Gal}(K^t/k) \longrightarrow \Sigma$, this induces a natural left $\mathrm{Gal}(K^t/k)$-action on G. Via the natural action of $\mathrm{Gal}(K^t/k)$ on K^t, this extends to a left $\mathrm{Gal}(K^t/k)$-action on K^tG. In view of Remark 2.3.5, we will identify $\mathrm{Hom}(\Omega_K^t, G)$ with the subgroup of $\mathrm{Hom}(\Omega_K, G)$ consisting of the tame homomorphisms.

The goal of this chapter is to explain the construction of the basic diagram

$$\begin{tikzcd}
H^1(\mathrm{Gal}(K^t/k), G) \arrow[r, "\mathrm{res}"] & \mathrm{Hom}(\Omega_K^t, G)^\Sigma \arrow[r, "tr"] \arrow[d, "\mathrm{gal}"'] & H^2(\Sigma, G) \arrow[d, "i^*"] \\
& \mathrm{Cl}(\mathcal{O}_K G)^\Sigma \arrow[r, "\xi"] & H^2(\Sigma, (\mathcal{O}_K G)^\times)
\end{tikzcd} \tag{6.0.1}$$

that we had in (1.4.1) (cf. Remark 1.4.2), where the top row is exact and all of the maps except possibly gal (recall (1.1.1)) are homomorphisms. Here

$$i^* : H^2(\Sigma, G) \longrightarrow H^2(\Sigma, (\mathcal{O}_K G)^\times) \tag{6.0.2}$$

denotes the homomorphism induced by the natural inclusion map $G \longrightarrow (\mathcal{O}_K G)^\times$. Then, assuming that G has odd order, we will show that (6.0.1) still makes sense and commutes when gal is replaced by gal_A (recall (1.2.2)). Essentially the same proof will also recover the already known fact that (6.0.1) commutes, in which case the assumption that G has odd order is not required.

Definition 6.0.2 For each $\gamma \in \Sigma$, we choose once and for all a lift $\overline{\gamma}$ of γ in $\mathrm{Gal}(K^t/k)$ with $\overline{1} = 1$

6.1 The Top Row: Hochschild-Serre Sequence

Recall that Ω_K^t acts trivially on G on the left. From the Hochschild-Serre spectral sequence (see [21, Chapter I Section 2.6], for example) associated to the group extension

$$1 \longrightarrow \Omega_K^t \longrightarrow \mathrm{Gal}(K^t/k) \longrightarrow \Sigma \longrightarrow 1,$$

we then obtain an exact sequence

$$H^1(\mathrm{Gal}(K^t/k), G) \xrightarrow{\mathrm{res}} \mathrm{Hom}(\Omega_K^t, G)^\Sigma \xrightarrow{tr} H^2(\Sigma, G). \tag{6.1.1}$$

Here res is given by restriction and tr is the *transgression map*. We remark that (6.1.1) is also part of the five-term inflation-restriction exact sequence in group cohomology (see [17, Proposition 1.6.7], for example). Below, we will recall the definitions of the Σ-action on $\mathrm{Hom}(\Omega_K^t, G)$ and the map tr in this particular setting.

Definition 6.1.1 The Σ-action on $\mathrm{Hom}(\Omega_K^t, G)$ is defined by

$$(h \cdot \gamma)(\omega) := \gamma^{-1} \cdot h(\overline{\gamma}\omega\overline{\gamma}^{-1}) \qquad \text{for all } \omega \in \Omega_K^t$$

for $h \in \mathrm{Hom}(\Omega_K^t, G)$ and $\gamma \in \Sigma$. This definition is independent of the choice of the lift $\overline{\gamma}$ because G is abelian. Next, define $\overline{c} : \Sigma \times \Sigma \longrightarrow \Omega_K^t$ by setting $\overline{c}(\gamma, \delta) := (\overline{\gamma})(\overline{\delta})(\overline{\gamma\delta})^{-1}$. The *transgression map* $tr : \mathrm{Hom}(\Omega_K^t, G)^\Sigma \longrightarrow H^2(\Sigma, G)$ (see [17, Proposition 1.6.6], for example) is defined by

$$tr(h) := [h \circ \overline{c}],$$

where $[-]$ denotes the cohomology class. This definition is also independent of the choice of the lifts $\overline{\gamma}$ for $\gamma \in \Sigma$.

Next, we explain how the exact sequence (6.1.1) is related to the study of embedding problems. To that end, first observe that each group extension

$$E_\Gamma : \quad 1 \longrightarrow G \xrightarrow{\iota} \Gamma \longrightarrow \Sigma \longrightarrow 1$$

of Σ by G induces a left Σ-module structure on G via conjugation in Γ as follows. For each $\gamma \in \Sigma$, choose a lift $\sigma(\gamma)$ of γ in Γ. Then, for $s \in G$, we have

$$\gamma * s = \iota^{-1}(\sigma(\gamma)\iota(s)\sigma(\gamma)^{-1}). \tag{6.1.2}$$

This definition does not depend upon the choice of the lift $\sigma(\gamma)$ because G is abelian. In addition, define a map $c_{E_\Gamma} : \Sigma \times \Sigma \longrightarrow G$ by

$$c_{E_\Gamma}(\gamma, \delta) := \iota^{-1}(\sigma(\gamma)\sigma(\delta)\sigma(\gamma\delta)^{-1}). \tag{6.1.3}$$

Let $E(K/k, G)$ denote the set of all equivalence classes of the group extensions of Σ by G for which the induced left Σ-module structure on G coincides with the one that we have fixed. It is well-known (see [17, Theorem 1.2.4] or [24, Theorem 6.6.3], for example) that the map $E_\Gamma \mapsto c_{E_\Gamma}$ induces a bijection between $E(K/k, G)$ and the group $H^2(\Sigma, G)$, and the map c_{E_Γ} represents the trivial cohomology class if and only if E_Γ splits.

Proposition 6.1.2 *Let $h \in Hom(\Omega_K^t, G)^\Sigma$ be surjective. Then, the field $L := (K^t)^{\ker(h)}$ is a tame solution to the embedding problem $(K/k, G, E_h)$ for some group extension E_h of Σ by G whose equivalence class corresponds to $tr(h)$.*

Proof. First, we will show that L/k is Galois by showing that $\mathrm{Gal}(K^t/L)$, which is equal to $\ker(h)$, is normal in $\mathrm{Gal}(K^t/k)$. So, let $\omega_k \in \mathrm{Gal}(K^t/k)$ be given and write $\omega_k = \overline{\gamma}\omega_0$ for some $\gamma \in \Sigma$ and $\omega_0 \in \Omega_K^t$. For any $\omega \in \ker(h)$, we have

$$\begin{aligned} h(\omega_k\omega\omega_k^{-1}) &= h(\overline{\gamma}\omega_0\omega\omega_0^{-1}\overline{\gamma}^{-1}) \\ &= \gamma \cdot (h \cdot \gamma)(\omega_0\omega\omega_0^{-1}) \\ &= \gamma \cdot (h(\omega_0)h(\omega)h(\omega_0)^{-1}), \end{aligned}$$

where the last equality follows because h is Σ-invariant and is a homomorphism on Ω_K^t. Since $\omega \in \ker(h)$, we then deduce that $h(\omega_k\omega\omega_k^{-1}) = 1$ and hence $\omega_k\omega\omega_k^{-1} \in \ker(h)$. This shows that $\ker(h)$ is normal in $\mathrm{Gal}(K^t/k)$ and so L/k is Galois.

Next, note that since h is surjective, it induces an isomorphism $\overline{h} : \mathrm{Gal}(L/K) \longrightarrow G$. Let $\Gamma_h := \mathrm{Gal}(L/k)$ and let $\iota : G \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \Gamma_h$ denote the homomorphism $\overline{h}^{-1}$ followed by the natural inclusion $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/k)$. Then, the diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(L/K) \arrow[r] \arrow[d, "\overline{h}"] & \mathrm{Gal}(L/k) \arrow[r] \arrow[d, equal] & \mathrm{Gal}(K/k) \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & G \arrow[r, "\iota"] & \Gamma_h \arrow[r] & \Sigma \arrow[r] & 1
\end{tikzcd}$$

clearly commutes. Notice that L/K is clearly tame since L is contained in K^t. It follows that L/K is a tame solution to the embedding problem $(K/k, G, E_h)$, where E_h denotes the group extension of Σ by G in the bottom row in the above diagram.

Finally, for each $\gamma \in \Sigma$, choose $\sigma(\gamma) := \overline{\gamma}|_L$ to be a lift of γ in Γ_h. The left Σ-module structure on G via conjugation in Γ_h is then given as follows. Given any $s \in G$, since h is surjective, we have $h(\omega) = s$ for some $\omega \in \Omega_K^t$. Then, we have

$$\begin{aligned} \gamma * s &= \iota^{-1}(\sigma(\gamma)\iota(s)\sigma(\gamma)^{-1}), \\ &= \overline{h}((\overline{\gamma}|_L)(\omega|_L)(\overline{\gamma}|_L)^{-1}) \\ &= h(\overline{\gamma}\omega\overline{\gamma}^{-1}) \\ &= \gamma \cdot s, \end{aligned}$$

where the last equality follows because h is Σ-invariant. This shows that the equivalence class of E_h lies in $E(K/k, G)$. Also, the map $c_{E_h} : \Sigma \times \Sigma \longrightarrow G$ in (6.1.3) is given by

$$\begin{aligned} c_{E_h}(\gamma, \delta) &= \iota^{-1}(\sigma(\gamma)\sigma(\delta)\sigma(\gamma\delta)^{-1}) \\ &= \overline{h}((\overline{\gamma}|_L)(\overline{\delta}|_L)(\overline{\gamma\delta}|_L)^{-1}) \\ &= (h \circ \overline{c})(\gamma, \delta), \end{aligned}$$

and so the equivalence class of E_h corresponds to $tr(h)$. This proves the proposition. ■

6.2 The Bottom Row: Fröhlich-Wall Sequence

Notice that $\mathcal{O}_K G$ equipped with the natural left Σ-action, namely that induced by the given left Σ-action on G and $\mathcal{O}_K$ (recall that $\Sigma := \mathrm{Gal}(K/k)$), is a Σ-ring. That is, for all $\gamma \in \Sigma$ and $\beta, \beta' \in \mathcal{O}_K G$, we have $\gamma \cdot (\beta + \beta') = \gamma \cdot \beta + \gamma \cdot \beta'$ and $\gamma \cdot (\beta\beta') = (\gamma \cdot \beta)(\gamma \cdot \beta')$. We obtain a homomorphism

$$\xi : \mathrm{Cl}(\mathcal{O}_K G)^{\Sigma} \longrightarrow H^2(\Sigma, (\mathcal{O}_K G)^{\times})$$

from the Fröhlich-Wall sequence associated to $\mathcal{O}_K G$ (see [3, Section 1], for example). We will recall the definitions of the Σ-action on $\mathrm{Cl}(\mathcal{O}_K G)$ and the map ξ in the subsequent subsections.

6.2.1 The Left Σ-Action on $\mathrm{Cl}(\mathcal{O}_K G)$

Definition 6.2.1 Let X and X' be $\mathcal{O}_K G$-modules. A group isomorphism $\varphi : X \longrightarrow X'$ is called a *semilinear isomorphism* if there exists a $\gamma \in \Sigma$ such that

$$\varphi(\beta \cdot x) = (\gamma \cdot \beta) \cdot \varphi(x) \qquad \text{for all } \beta \in \mathcal{O}_K G \text{ and } x \in X.$$

Moreover, any such $\gamma \in \Sigma$ is called a *grading of* φ.

Definition 6.2.2 Let $[X] \in \mathrm{Cl}(\mathcal{O}_K G)$. Given $\gamma \in \Sigma$, define $\gamma \cdot [X] := [Y]$ if there exists a semilinear isomorphism $\varphi : X \longrightarrow Y$ having γ as a grading. Clearly the isomorphism class $[Y]$ of Y (recall Remark 2.1.2) is uniquely determined by that of X. Moreover, note that such a Y always exists, as we may take $Y := X_\gamma$ to be the abelian group X equipped with the structure

$$\beta * x := (\gamma^{-1} \cdot \beta) \cdot x \qquad \text{for all } \beta \in (\mathcal{O}_K G)^\times \text{ and } x \in X_\gamma \tag{6.2.1}$$

as an $\mathcal{O}_K G$-module and take $\varphi = \mathrm{id}_X$ to be the identity on X.

It is clear that Definition 6.2.2 defines a left Σ-action on the group $\mathrm{Cl}(\mathcal{O}_K G)$. Below, we will verify that $\mathrm{Cl}(\mathcal{O}_K G)$ is in fact a left Σ-module under this action and so $\mathrm{Cl}(\mathcal{O}_K G)^\Sigma$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_K G)$.

Proposition 6.2.3 *Let $[X], [X'] \in Cl(\mathcal{O}_K G)$. For all $\gamma \in \Sigma$, we have*

$$\gamma \cdot ([X][X']) = (\gamma \cdot [X])(\gamma \cdot [X']).$$

Proof. Let $[X''] \in \mathrm{Cl}(\mathcal{O}_K G)$ be such that $[X''] = [X][X']$. By Definition 2.1.4, this means that there exists an isomorphism

$$\varphi : X \oplus X' \longrightarrow \mathcal{O}_K G \oplus X''$$

of $\mathcal{O}_K G$-modules. Let X_γ denote the abelian group X equipped with the $\mathcal{O}_K G$-structure defined as in (6.2.1), and similarly for X'_γ and X''_γ. Let $\varphi_\gamma : \mathcal{O}_K G \longrightarrow \mathcal{O}_K G$ denote the bijective map given by $\beta \mapsto \gamma \cdot \beta$. Then, the map

$$(\varphi_\gamma \oplus \mathrm{id}_{X''}) \circ \varphi : X_\gamma \oplus X'_\gamma \longrightarrow \mathcal{O}_K G \oplus X''_\gamma$$

is an isomorphism of $\mathcal{O}_K G$-modules and so $[X''_\gamma] = [X_\gamma][X'_\gamma]$, as desired. ■

The next proposition ensures that diagram (1.4.2) is well-defined.

Proposition 6.2.4 *Let $h \in Hom(\Omega_K^t, G)^\Sigma$ be such that A_h exists. For all $\gamma \in \Sigma$, the map*

$$\varphi_\gamma : \mathbf{r}_G(A_h) \longrightarrow \mathbf{r}_G(A_h); \quad \varphi_\gamma(\mathbf{r}_G(a)) := \overline{\gamma} \cdot \mathbf{r}_G(a) \tag{6.2.2}$$

is well-defined and is a semilinear isomorphism having γ as a grading. In particular, we have $\gamma \cdot [A_h] = [A_h]$ and so $gal_A(Hom(\Omega_K^t, G)^\Sigma) \subset Cl(\mathcal{O}_K G)^\Sigma$ when G has odd order.

Proof. First, we will check that $\varphi_\gamma(\mathbf{r}_G(A_h)) \subset \mathbf{r}_G(A_h)$ so that φ_γ is well-defined. To that end, let $a \in A_h$ be given and let $a' \in \mathrm{Map}(G, K^c)$ be such that $\overline{\gamma} \cdot \mathbf{r}_G(a) = \mathbf{r}_G(a')$, which exists since $\mathbf{r}_G$ is bijective. We will use (2.3.3) to check that $a' \in K_h$. So let $\omega \in \Omega_K^t$ be given. Since $a \in K_h$, we have $\overline{\gamma}^{-1}\omega\overline{\gamma} \cdot \mathbf{r}_G(a) = \mathbf{r}_G(a)h(\overline{\gamma}^{-1}\omega\overline{\gamma})$ and so

$$\omega \cdot \mathbf{r}_G(a') = \overline{\gamma} \cdot (\overline{\gamma}^{-1}\omega\overline{\gamma} \cdot \mathbf{r}_G(a)) = \mathbf{r}_G(a')(h \cdot \gamma^{-1})(\omega).$$

Since h is Σ-invariant, we then see that $\omega \cdot \mathbf{r}_G(a') = \mathbf{r}_G(a')h(\omega)$ and so $a' \in K_h$. To show that in fact $a' \in A_h$, observe that K^h/k is Galois because h is Σ-invariant (cf. the proof of Proposition 6.1.2). Let $\mathfrak{D}_{K^h/k}$ denote the different ideal of K^h/k. Similarly for $\mathfrak{D}_{K^h/K}$ and $\mathfrak{D}_{K/k}$. Then, we have $\mathfrak{D}_{K^h/k} = \mathfrak{D}_{K^h/K}\mathfrak{D}_{K/k}$. But notice that $\overline{\gamma}(\mathfrak{D}_{K^h/k}) = \mathfrak{D}_{K^h/k}$ and $\overline{\gamma}(\mathfrak{D}_{K/k}) = \mathfrak{D}_{K/k}$. It follows that $\overline{\gamma}(\mathfrak{D}_{K^h/K}) = \mathfrak{D}_{K^h/K}$ and so $\overline{\gamma}(A_{K^h/K}) = A_{K^h/K}$ as well. Since $a \in A_h$, we deduce that $a' \in A_h$ and so $\varphi_\gamma(\mathbf{r}_G(a)) \in \mathbf{r}_G(A_h)$. This shows that φ_γ is well-defined.

Once we see that φ_γ is well-defined, it is now clear that φ_γ is a semilinear isomorphism having γ as a grading. Since the resolvend map restricts to an isomorphism $A_h \simeq \mathbf{r}_G(A_h)$ of $\mathcal{O}_K G$-modules, we have $[A_h] = [\mathbf{r}_G(A_h)]$ and the above shows that $\gamma \cdot [A_h] = [A_h]$. ■

Remark 6.2.5 Let $h \in \mathrm{Hom}(\Omega_K^t, G)^\Sigma$. Essentially the same argument as in the proof of Proposition 6.2.4 shows that for all $\gamma \in \Sigma$, the map

$$\varphi_\gamma : \mathbf{r}_G(\mathcal{O}_h) \longrightarrow \mathbf{r}_G(\mathcal{O}_h); \quad \varphi_\gamma(\mathbf{r}_G(a)) := \overline{\gamma} \cdot \mathbf{r}_G(a)$$

is well-defined and is a semilinear isomorphism having γ as a grading. In particular, we have $\gamma \cdot [\mathcal{O}_h] = [\mathcal{O}_h]$ and so $\mathrm{gal}(\mathrm{Hom}(\Omega_K^t, G)^\Sigma) \subset \mathrm{Cl}(\mathcal{O}_K G)^\Sigma$.

6.2.2 The Homomorphism ξ

Definition 6.2.6 Given an $\mathcal{O}_K G$-module X, define $\mathrm{Sem}(X)$ to be the group consisting of all pairs of the form (φ, γ), where $\varphi : X \longrightarrow X$ is a semilinear isomorphism having γ as a grading, and the group operation is defined by $(\varphi, \gamma)(\varphi', \gamma') := (\varphi\varphi', \gamma\gamma')$. Moreover, let $\mathrm{Aut}(X)$ denote the group of $\mathcal{O}_K G$-automorphisms on X. The map

$$\mathfrak{g}_X : \mathrm{Sem}(X) \longrightarrow \Sigma; \quad \mathfrak{g}_X(\varphi, \gamma) := \gamma$$

is then a homomorphism with $\ker(\mathfrak{g}_X) = \mathrm{Aut}(X)$.

Now, consider an element $[X] \in \mathrm{Cl}(\mathcal{O}_K G)^{\Sigma}$. The fact that $[X]$ is Σ-invariant means that $\mathfrak{g}_X$ is surjective. Moreover, since X is locally free over $\mathcal{O}_K G$ (of rank one), an $\mathcal{O}_K G$-automorphism of X is of the form $\psi_\beta : x \mapsto \beta \cdot x$ for some $\beta \in (\mathcal{O}_K G)^{\times}$. Hence, we may identify $\mathrm{Aut}(X)$ with $(\mathcal{O}_K G)^{\times}$. We then obtain a group extension

$$\begin{tikzcd} E_X : \quad 1 \arrow[r] & (\mathcal{O}_K G)^{\times} \arrow[r, "\mathfrak{i}_X"] & \mathrm{Sem}(X) \arrow[r, "\mathfrak{g}_X"] & \Sigma \arrow[r] & 1 \end{tikzcd}$$

of Σ by $(\mathcal{O}_K G)^{\times}$, where $\mathfrak{i}_X(\beta) := (\psi_\beta, 1)$. Notice that this group extension induces a left Σ-module structure on $(\mathcal{O}_K G)^{\times}$ via conjugation in $\mathrm{Sem}(X)$ as follows (cf. (6.1.2)). For each $\gamma \in \Sigma$, choose a lift (φ_γ, γ) of γ in $\mathrm{Sem}(\Sigma)$. Then, for $\beta \in (\mathcal{O}_K G)^{\times}$, we have

$$\gamma * \beta = \mathfrak{i}_X^{-1}((\varphi_\gamma, \gamma)(\psi_\beta, 1)(\varphi_\gamma^{-1}, \gamma^{-1})) = \mathfrak{i}_X^{-1}((\varphi_\gamma \psi_\beta \varphi_\gamma^{-1}, 1)). \tag{6.2.3}$$

But for any $x \in (\mathcal{O}_K G)^{\times}$, we have $(\varphi_\gamma \psi_\beta \varphi_\gamma^{-1})(x) = \varphi_\gamma(\beta \cdot \varphi_\gamma^{-1}(x)) = (\gamma \cdot \beta) \cdot x$. It follows that $\varphi_\gamma \psi_\beta \varphi_\gamma^{-1} = \psi_{\gamma \cdot \beta}$ and so $\gamma * \beta = \gamma \cdot \beta$. In other words, the left Σ-module structure on $(\mathcal{O}_K G)^{\times}$ given by (6.2.3) coincides with the existing one.

Hence, analogously to the bijective correspondence between $E(K/k, G)$ and $H^2(\Sigma, G)$ described in Section 6.1, the group extension E_X also defines a class in $H^2(\Sigma, (\mathcal{O}_K G)^{\times})$. In particular, it is represented by the 2-cocycle $d_X : \Sigma \times \Sigma \longrightarrow (\mathcal{O}_K G)^{\times}$ determined by the equations (cf. (6.1.3))

$$d_X(\gamma, \delta) \cdot x = (\varphi_\gamma \varphi_\delta \varphi_{\gamma\delta}^{-1})(x) \qquad \text{for all } x \in X. \tag{6.2.4}$$

Definition 6.2.7 Define $\xi : \mathrm{Cl}(\mathcal{O}_K G)^{\Sigma} \longrightarrow H^2(\Sigma, (\mathcal{O}_K G)^{\times})$ by setting $\xi([X]) := [d_X]$, where $[-]$ denotes the cohomology class. It is not hard to see that this definition depends only on the isomorphism class $[X]$ of X (recall Remark 2.1.2).

Proposition 6.2.8 *The map ξ is a homomorphism.*

Proof. Let $[X], [X'] \in \mathrm{Cl}(\mathcal{O}_K G)^\Sigma$ be given and let $X'' := X \otimes_{\mathcal{O}_K G} X'$. Since G is abelian, [7, Theorem 55.16] implies that X'' is locally free over $\mathcal{O}_K G$ (of rank one). Moreover, we have $[X][X'] = [X'']$ (cf. the proof of [7, Theorem 55.26]).

For each $\gamma \in \Sigma$, let φ_γ and φ'_γ be semilinear automorphisms on X and X', respectively, having γ as a grading. Then, clearly $\varphi''_\gamma := \varphi_\gamma \otimes \varphi'_\gamma$ is a semilinear automorphism on X'' having γ as a grading. Let d_X be defined as in (6.2.4). Similarly for $d_{X'}$ and $d_{X''}$. Then, for all $\gamma, \delta \in \Sigma$, $x \in X$, and $x' \in X'$, we have

$$\begin{aligned} d_{X''}(\gamma,\delta) \cdot (x \otimes x') &= (\varphi''_\gamma \varphi''_\delta \varphi''^{-1}_{\gamma\delta})(x \otimes x') \\ &= (\varphi_\gamma \varphi_\delta \varphi^{-1}_{\gamma\delta})(x) \otimes (\varphi'_\gamma \varphi'_\delta \varphi'^{-1}_{\gamma\delta})(x') \\ &= (d_X(\gamma,\delta) \cdot x) \otimes (d_{X'}(\gamma,\delta) \cdot x') \\ &= (d_X(\gamma,\delta) d_{X'}(\gamma,\delta)) \cdot (x \otimes x'). \end{aligned}$$

This shows that $d_{X''} = d_X d_{X'}$ and so $\xi([X'']) = \xi([X])\xi([X'])$, as desired. ■

6.3 Proof of Theorem 1.4.4

Theorem 1.4.4 *Let K/k be a Galois extension of number fields and set $\Sigma := Gal(K/k)$. Let G be a finite abelian group of odd order equipped with a fixed left Σ-module structure. Then, there is a commutative diagram*

$$\begin{tikzcd} H^1(Gal(K^t/k), G) \arrow[r, "res"] & Hom(\Omega_K^t, G)^\Sigma \arrow[r, "tr"] \arrow[d, "gal_A"'] & H^2(\Sigma, G) \arrow[d, "i^*"] \\ & Cl(\mathcal{O}_K G)^\Sigma \arrow[r, "\xi"] & H^2(\Sigma, (\mathcal{O}_K G)^\times) \end{tikzcd} ,$$

where the top row is exact and all of the maps except possibly gal_A are homomorphisms.

Proof. Notice that the diagram makes sense because $\mathrm{gal}_A(\mathrm{Hom}(\Omega_K^t, G)^\Sigma) \subset \mathrm{Cl}(\mathcal{O}_K G)^\Sigma$ by Proposition 6.2.4. We already know that the top row is exact. The maps res, tr, and i^* are also clearly homomorphisms, and ξ is a homomorphism by Proposition 6.2.8. Thus, it remains to verify the equality $i^* \circ tr = \xi \circ \mathrm{gal}_A$.

To that end, let $h \in \mathrm{Hom}(\Omega_K^t, G)^\Sigma$ be given. By Definition 6.1.1, the class $(i^* \circ tr)(h)$ is represented by the 2-cocycle $d : \Sigma \times \Sigma \longrightarrow (\mathcal{O}_K G)^\times$ defined by

$$d(\gamma, \delta) := h((\overline{\gamma})(\overline{\delta})(\overline{\gamma\delta})^{-1}).$$

Next, let $X := \mathbf{r}_G(A_h)$. Note that $X \simeq A_h$ as $\mathcal{O}_K G$-modules and so $\mathrm{gal}_A(h) = [X]$. For each $\gamma \in \Sigma$, let $\varphi_\gamma : X \longrightarrow X$ be defined as in (6.2.2), which is a semilinear isomorphism having γ as a grading by Proposition 6.2.4. By Definition 6.2.7, the class $(\xi \circ \mathrm{gal}_A)(h)$ is then represented by the 2-cocycle $d_X : \Sigma \times \Sigma \longrightarrow (\mathcal{O}_K G)^\times$ defined by the equations

$$d_X(\gamma, \delta) \cdot x = ((\overline{\gamma})(\overline{\delta})(\overline{\gamma\delta})^{-1}) \cdot x \qquad \text{for all } x \in X.$$

But $(\overline{\gamma})(\overline{\delta})(\overline{\gamma\delta})^{-1} \in \Omega_K^t$. It then follows from (2.3.3) that

$$((\overline{\gamma})(\overline{\delta})(\overline{\gamma\delta})^{-1}) \cdot x = h((\overline{\gamma})(\overline{\delta})(\overline{\gamma\delta})^{-1})) \cdot x \qquad \text{for all } x \in X.$$

This shows that $d_X = d$, whence $(i^* \circ tr)(h) = (\xi \circ \mathrm{gal}_A)(h)$, as desired. ■

Remark 6.3.2 Essentially the same proof as that of Theorem 1.4.4 (cf. Remark 6.2.5) shows that (1.4.1) also makes sense, where the top row is exact and all of the maps except possibly gal are homomorphims, and that (1.4.1) commutes (cf. Remark 1.4.2).

Chapter 7

Characterization of the tame Σ-A-Realizable Classes in $\mathrm{Cl}(\mathcal{O}_K G)$

As in Chapter 6, recall that K/k is a fixed Galois subextension of K and $\Sigma := \mathrm{Gal}(K/k)$. Throughout this chapter, we will assume that G is abelian and fix a left Σ-module structure of G. It will be helpful to recall from Remark 1.6.1 that we have chosen $K^c = \mathbb{Q}^c = k^c$ as well as the same compatible set $\{\zeta_n : n \in \mathbb{Z}\}$ of primitive roots of unity in $\mathbb{Q}^c$ for both k and K. We will also identify $\mathrm{Hom}(\Omega_K^t, G)$ with the subgroup of $\mathrm{Hom}(\Omega_K, G)$ consisting of the tame homomorphisms (cf. Remark 2.3.5) as follows.

Definition 7.0.3 Let $h \in \mathrm{Hom}(\Omega_K^t, G)$. For $\omega \in \Omega_K$, we will write $h(\omega)$ for $h(\omega|_{K^t})$. In particular, we will sometimes regard h as a homomorphism $\Omega_K \longrightarrow G$.

Definition 7.0.4 Define V_k to be the set of primes in M_k which are ramified in K/k, and define V_K to be the set of primes in M_K lying above the primes in V_k.

The goal of this chapter is to characterize, under the hypotheses of Theorem 1.4.5, the tame Σ-A-realizable classes coming from the homomorphisms $h \in \mathrm{Hom}(\Omega_K^t, G)_V^\Sigma$ (recall (1.4.3)). We will do so by refining the characterization of $\mathcal{A}^t(\mathcal{O}_K G)$ given in (4.4.6). The crucial step is to make suitable choices for the embeddings $i_v : \mathbb{Q}^c \longrightarrow K_v^c$ and the uniformizers π_v in K_v for $v \in M_K$. We will need the following notation (cf. Definition 6.0.2).

Definition 7.0.5 For each $w \in M_k$, let $i_w : \mathbb{Q}^c \longrightarrow k_w^c$ be the chosen embedding extending the natural embedding $k \longrightarrow k_w$. The prime $v_w \in M_K$ for which the v_w-adic absolute value on K is induced by i_w is called the *distinguished prime (in K) above w*. Moreover, for each $v \in M_K$ lying above w, choose an element $\gamma_v \in \Sigma$ such that $v = v_w \circ \gamma_v^{-1}$, and choose $\gamma_{v_w} = 1$. We choose once and for all a lift $\overline{\gamma_v}$ of γ_v in Ω_k with $\overline{\gamma_{v_w}} = 1$.

7.1 Choices of Embeddings and Uniformizers

7.1.1 Choices of Embeddings

Definition 7.1.1 Given $v \in M_K$, let $w \in M_k$ be the prime lying below v and note that the v-adic absolute value on K is induced by $i_w \circ \overline{\gamma_v}^{-1}$. Via restricting $i_w \circ \overline{\gamma_v}^{-1}$, we then obtain an embedding $K \longrightarrow k_w^c$ which extends to a continuous embedding $K_v \longrightarrow k_w^c$. We will lift this to an isomorphism $\varepsilon_v^{-1} : K_v^c \longrightarrow k_w^c$. We will then define $i_v : \mathbb{Q}^c \longrightarrow K_v^c$ by setting $i_v := \varepsilon_v \circ i_w \circ \overline{\gamma_v}^{-1}$, which clearly extends the natural embedding $K \longrightarrow K_v$.

To summarize, for all $v \in M_K$ and $w \in M_k$ such that w lies below v, the following diagram commutes.

$$\begin{tikzcd}
K_{v_w}^c \arrow[rr, bend left, "\widetilde{\gamma_v}"] & k_w^c \arrow[l, "\varepsilon_{v_w}"'] \arrow[r, "\varepsilon_v"] & K_v^c \\
\mathbb{Q}^c \arrow[u, hook, "i_{v_w}"] \arrow[r, equal] & \mathbb{Q}^c \arrow[u, hook, "i_w"] \arrow[r, "\overline{\gamma_v}"] & \mathbb{Q}^c \arrow[u, hook, "i_v"]
\end{tikzcd}$$

Here, we define $\widetilde{\gamma_v} := \varepsilon_v \circ \varepsilon_{v_w}^{-1}$ and notice that we have $\widetilde{\gamma_v} = 1$. Observe also that we have the relation

$$i_v = \widetilde{\gamma_v} \circ i_{v_w} \circ \overline{\gamma_v}^{-1}. \tag{7.1.1}$$

Proposition 7.1.2 *Let $h \in Hom(\Omega_K^t, G)^\Sigma$. Then, for all $v \in M_K$ and $w \in M_k$ such that w lies below v, we have (recall Definition 7.0.3)*

$$h_v(\widetilde{\gamma_v} \circ \omega \circ \widetilde{\gamma_v}^{-1}) = \gamma_v \cdot h_{v_w}(\omega) \qquad \textit{for all } \omega \in \Omega_{K_{v_w}}.$$

Proof. Let $v \in M_K$ and $w \in M_k$ be such that w lies below v. We have $h_v = h \circ \widetilde{i_v}$ (recall (1.6.1)) by definition. Using (7.1.1), we then deduce that

$$\begin{aligned} h_v(\widetilde{\gamma_v} \circ \omega \circ \widetilde{\gamma_v}^{-1}) &= h(i_v^{-1} \circ \widetilde{\gamma_v} \circ \omega \circ \widetilde{\gamma_v}^{-1} \circ i_v) \\ &= h(\overline{\gamma_v} \circ i_{v_w}^{-1} \circ \omega \circ i_{v_w} \circ \overline{\gamma_v}^{-1}) \\ &= \gamma_v \cdot (h \cdot \gamma_v)(i_{v_w}^{-1} \circ \omega \circ i_{v_w}) \\ &= \gamma_v \cdot h_{v_w}(\omega), \end{aligned}$$

where the last equality follows because h is Σ-invariant. This proves the claim. ■

7.1.2 Choices of Uniformizers and their Radicals

For each $w \in M_k$, let π_w be a chosen uniformizer in k_w and let $\{\pi_w^{1/n} : n \in \mathbb{Z}^+\}$ denote the chosen coherent set of radicals of π_w in k_w^c (recall Section 4.1).

Definition 7.1.3 Given $v \in M_K$, let $w \in M_k$ be the prime lying below v. If $v \notin V_K$, we will choose $\pi_v := \varepsilon_v(\pi_w)$ to be the uniformizer in K_v, and $\pi_v^{1/n} := \varepsilon_v(\pi_w^{1/n})$ for $n \in \mathbb{Z}^+$ to the coherent radicals of π_v in K_v^c. If $v \in V_K$, then we will choose the uniformizer in K_v and its radicals arbitrarily.

Lemma 7.1.4 *For all $v \in M_K$ and $w \in M_k$ such that w lies below v, we have $v \notin V_K$ if and only if $v_w \notin V_K$. In particular, we have $\pi_v^{1/n} = \widetilde{\gamma}_v(\pi_{v_w}^{1/n})$ for all $n \in \mathbb{Z}^+$ in this case.*

Proof. Since K/k is Galois, clearly $v \notin V_K$ if and only if $v_w \notin V_K$. Since $\widetilde{\gamma}_v = \varepsilon_v \circ \varepsilon_{v_w}^{-1}$, it is also clear that $\pi_v^{1/n} = \varepsilon_v(\pi_w^{1/n}) = \widetilde{\gamma}_v(\varepsilon_{v_w}(\pi_w^{1/n})) = \widetilde{\gamma}_v(\pi_{v_w}^{1/n}))$ for all $n \in \mathbb{Z}^+$ in this case. ■

Next, observe that the choices made in Definitions 7.1.1 and 7.1.3 in turn determine a distinguished topological generator $\sigma_v = \sigma_{K_v}$ of $\mathrm{Gal}(K_v^t/K_v^{nr})$ (recall (4.1.2)). In particular, because we chose $\{i_v(\zeta_n) : n \in \mathbb{Z}^+\}$ to be the compatible set of primitive roots of unity in K_v^c, we have

$$\sigma_v(\pi_v^{1/n}) = i_v(\zeta_n)\pi_v^{1/n} \qquad \text{for } (n,p) = 1, \tag{7.1.2}$$

where p denotes the rational prime lying below v. As noted in Remark 4.1.3, by abuse of notation, we will also use σ_v to denote some chosen lift of σ_v in Ω_{K_v}.

Proposition 7.1.5 *Let $h \in Hom(\Omega_K^t, G)^\Sigma$. Then, for all $v \in M_K$ and $w \in M_k$ such that w lies below v and $v \notin V_K$, we have*

$$h_v(\sigma_v) = \gamma_v \cdot h_{v_w}(\sigma_{v_w})$$

provided that ζ_{e_v} is contained in k, where $e_v := |h_v(\sigma_v)|$.

Proof. Let $v \in M_K$ and $w \in M_k$ be such that w lies below v and $v \notin V_K$. We already know from Proposition 7.1.2 that $h_v(\widetilde{\gamma}_v \circ \sigma_{v_w} \circ \widetilde{\gamma}_v^{-1}) = \gamma_v \cdot h_{v_w}(\sigma_{v_w})$ (cf. Definition 7.0.3). Thus, it suffices to show that $h_v(\widetilde{\gamma}_v \circ \sigma_{v_w} \circ \widetilde{\gamma}_v^{-1}) = h_v(\sigma_v)$, or equivalently, that $\widetilde{\gamma}_v \circ \sigma_{v_w} \circ \widetilde{\gamma}_v^{-1}$ and σ_v have the same action on the fixed field $L := K_v^{h_v}$ of $\ker(h_v)$.

Let $h_v = h_v^{nr} h_v^{tot}$ be the factorization of h_v with respect to σ_v (recall Definition 4.1.4). Set $L^{nr} := K_v^{h_v^{nr}}$ and $L^{tot} := K_v^{h_v^{tot}}$. Clearly $L \subset L^{nr}L^{tot}$, and both $\widetilde{\gamma}_v \circ \sigma_{v_w} \circ \widetilde{\gamma}_v^{-1}$ and σ_v

act as the identity on L^{nr} because L^{nr}/K_v is unramified. We also have $L^{tot} = K_v(\pi_v^{1/e_v})$ by Proposition 4.2.2. Hence, it remains to show that

$$(\widetilde{\gamma_v} \circ \sigma_{v_w} \circ \widetilde{\gamma_v}^{-1})(\pi_v^{1/e_v}) = \sigma_v(\pi_v^{1/e_v}).$$

But $\pi_v^{1/e_v} = \widetilde{\gamma_v}(\pi_{v_w}^{1/e_v})$ by Lemma 7.1.4 since $v \notin V_K$. Using (7.1.2), we then obtain

$$\begin{aligned}
(\widetilde{\gamma_v} \circ \sigma_{v_w} \circ \widetilde{\gamma_v}^{-1})(\pi_v^{1/e_v}) &= \widetilde{\gamma_v}(i_{v_w}(\zeta_{e_v})\pi_{v_w}^{1/e_v}) \\
&= (\widetilde{\gamma_v} \circ i_{v_w})(\zeta_{e_v})\pi_v^{1/e_v} \\
&= (\widetilde{\gamma_v} \circ i_{v_w} \circ \overline{\gamma_v}^{-1})(\zeta_{e_v})\pi_v^{1/e_v} \\
&= i_v(\zeta_{e_v})\pi_v^{1/e_v} \\
&= \sigma_v(\pi_v^{1/e_v}),
\end{aligned}$$

where $\overline{\gamma_v}^{-1}(\zeta_{e_v}) = \zeta_{e_v}$ because $\zeta_{e_v} \in k$ by hypothesis and $i_v = \widetilde{\gamma_v} \circ i_{v_w} \circ \overline{\gamma_v}^{-1}$ by (7.1.1). So, indeed $\widetilde{\gamma_v} \circ \sigma_{v_w} \circ \widetilde{\gamma_v}^{-1}$ and σ_v have the same action on L. This proves the claim. ■

7.2 Embeddings of Groups of Ideles

In this section, assume that k contains all $\exp(G)$-th roots of unity. In this case, we have $\Lambda(FG) = \mathrm{Map}(G, F)$ for $F \in \{k, K, k_w, K_v\}$, where $w \in M_k$ and $v \in M_K$ (recall Definition 2.5.3 and (2.5.2); notice that their definitions do not require that G has odd order). The isomorphisms ε_v for $v \in M_K$ then induce the following embeddings of groups of ideles. It will be helpful to recall Definitions 2.4.2 and 2.5.6.

Definition 7.2.1 Define $\nu : J(\Lambda(kG)) \longrightarrow J(\Lambda(KG))$ by setting

$$\nu(g)_v := \varepsilon_v \circ g_w$$

for each $v \in M_K$, where $w \in M_k$ is the prime lying below v.

Similarly, define $\mu : J(\mathcal{H}(kG)) \longrightarrow J(\mathcal{H}(KG))$ by setting

$$\mu((r_G(a))_v := r_G(\varepsilon_v \circ a_w)$$

for each $v \in M_K$, where $w \in M_k$ is the prime lying below v and $r_G(a)_w = r_G(a_w)$. Notice that the definition of μ does not require that k contains all $\exp(G)$-th roots of unity.

First, we will prove some basic properties concerning the map ν. To that end, recall that the choices of uniformizers π_w in k_w for $w \in M_k$ determine a subset $\mathfrak{F}_k$ of $J(\Lambda(kG))$ (recall Definitions 4.2.1 and 4.3.1; again their definitions do not require that G has odd order). Similarly, the choices of uniformizers π_v in K_v for $v \in M_K$ made in Definition 7.1.3 determine a subset $\mathfrak{F}_K$ of $J(\Lambda(KG))$.

Proposition 7.2.2 *Let $f \in \mathfrak{F}_k$ and write $f_w = f_{k_w,s_w}$ for each $w \in M_k$. For all $v \in M_K$ and $w \in M_k$ such that w lies below v and $v \notin V_K$, we have $\nu(f)_v = f_{K_v,s_w}$. In particular, if $f_w = 1$ for all $w \in V_k$, then $\nu(f) \in \mathfrak{F}_K$.*

Proof. Let $v \in M_K$ and $w \in M_k$ be such that w lies below v and $v \notin V_K$. Also, let q_v and q_w denote the orders of the residue fields of K_v and k_w, respectively. The order of s_w divides $q_w - 1$ by definition and hence divides $q_v - 1$. Because $v \notin V_K$, we have $\pi_v = \varepsilon_v(\pi_w)$ by definition and it is clear that $\nu(f)_v = f_{K_v,s_w}$. We then see that $\nu(f)_v \in \mathfrak{F}_{K_v}$. If $f_w = 1$ for all $w \in V_k$, then clearly $\nu(f)_v = 1$ lies in $\mathfrak{F}_{K_v}$ for all $v \in V_K$ as well. We then deduce that $\nu(f) \in \mathfrak{F}_K$ in this case. ■

Proposition 7.2.3 *Let $f \in \mathfrak{F}_K$ and write $f_v = f_{K_v,s_v}$ for each $v \in M_K$. If*

(1) $s_v = 1$ for all $v \in V_K$; and

(2) $s_v = s_{v_w}$ for all $v \in M_K$ and $w \in M_k$ such that w lies below v,

then we have $f = \nu(g)$ for some $g \in J(\Lambda(kG))$.

Proof. For each $w \in M_k$, recall that $\Lambda(k_w G) = \mathrm{Map}(G, k_w)$ and define $g_w \in \Lambda(k_w G)^\times$ by

$$g_w(s) := \begin{cases} \pi_w & \text{if } s = s_{v_w} \neq 1 \\ 1 & \text{otherwise.} \end{cases}$$

Note that $g := (g_w)_w \in J(\Lambda(kG))$ because $f \in J(\Lambda(KG))$ implies that $s_v = 1$ for all but finitely many $v \in M_K$. To prove that $f = \nu(g)$, let $v \in M_K$ be given and let $w \in M_k$ be the prime lying below v. If $s_{v_w} \neq 1$, then $s_v \neq 1$ also by (2) and so $v \notin V_K$ by (1). In this case, we have $\pi_v = \varepsilon_v(\pi_w)$ by definition. Because $s_v = s_{v_w}$ by (2), we then deduce that $\nu(g)_v = f_{K_v, s_v}$. If $s_{v_w} = 1$, then $s_v = 1$ by (2) and clearly $\nu(g)_v = 1 = f_{K_v, s_v}$. This shows that $f = \nu(g)$ and so $f \in \nu(J(\Lambda(kG)))$, as claimed. ■

Next, we will show that certain diagrams involving ν and μ are commutative.

Proposition 7.2.4 *The diagram*

$$\begin{tikzcd}
\Lambda(kG)^\times \arrow[r, "\lambda_k"] \arrow[d, "\iota_\Lambda"'] & J(\Lambda(kG)) \arrow[d, "\nu"] \\
\Lambda(KG)^\times \arrow[r, "\lambda_K"'] & J(\Lambda(KG))
\end{tikzcd}$$

commutes, where ι_Λ denotes the map induced by the natural inclusion $k \longrightarrow K$.

Proof. Recall that λ_k and λ_K denote the diagonal maps. Now, let $g \in \Lambda(kG)^\times$ be given. Also, let $v \in M_K$ and let $w \in M_k$ be the prime lying below v. Then, we have

$$(\nu \circ \lambda_k)(g)_v = \varepsilon_v \circ i_w \circ g = i_v \circ \overline{\gamma_v} \circ g$$

since $\varepsilon_v \circ i_w = i_v \circ \overline{\gamma_v}$ by Definition 7.1.1. Since g takes values in k, we have $\overline{\gamma_v} \circ g = g$ and so

$$(\nu \circ \lambda_k)(g)_v = i_v \circ g = (\lambda_K \circ \iota_\Lambda)(g)_v.$$

Hence, we have $\nu \circ \lambda_k = \lambda_K \circ \iota_\Lambda$ and the diagram commutes. ■

Proposition 7.2.5 *The diagram*

$$\begin{tikzcd}
J(\Lambda(kG)) \arrow[r, "\nu"] \arrow[d, "\Theta^t_{*,k}"'] & J(\Lambda(KG)) \arrow[d, "\Theta^t_{*,K}"] \\
J(\mathcal{H}(kG)) \arrow[r, "\mu"'] & J(\mathcal{H}(KG))
\end{tikzcd}$$

commutes, provided that G has odd order so that $\Theta^t_{*,k}$ and $\Theta^t_{*,K}$ are defined.

Proof. Let $g \in J(\Lambda(kG))$ be given. Also, let $v \in M_K$ and let $w \in M_k$ be the prime lying below v. On one hand, we have

$$(\Theta^t_{*,K} \circ \nu)(g)_v = \Theta^t_{*,K}(\varepsilon_v \circ g_w). \tag{7.2.1}$$

On the other hand, let $r_G(a_w) \in \mathcal{H}(k_w G)$ be such that $\Theta^t_{*,k}(g_w) = r_G(a_w)$ so that

$$(\mu \circ \Theta^t_{*,k})(g)_v = r_G(\varepsilon_v \circ a_w). \tag{7.2.2}$$

Moreover, recall from the identification $\mathcal{H}(k_w G) = \mathrm{Hom}_{\Omega_{k_w}}(S_{\widehat{G}_w}, (k_w^c)^\times)$ in (2.4.12) that we have $r_G(a_w)(\psi) = \Theta^t_{*,k}(g)(\psi)$ for all $\psi \in S_{\widehat{G}_w}$. Here $\widehat{G}_w$ denotes the group of irreducible k_w^c-valued characters on G and recall that $S_{\widehat{G}_w} \subset \mathbb{Z}\widehat{G}_w$. Below, we will show that (7.2.1) and (7.2.2) are equal using the identification $\mathcal{H}(K_v G) = \mathrm{Hom}_{\Omega_{K_v}}(S_{\widehat{G}_v}, (K_v^c)^\times)$ in (2.4.12). Here $\widehat{G}_v$ denotes the groups of irreducible K_v^c-valued characters on G and $S_{\widehat{G}_v} \subset \mathbb{Z}\widehat{G}_v$.

To that end, let $\psi \in S_{\widehat{G}_v}$ and write $\psi = \sum_\chi n_\chi \chi$. Define $\varepsilon_v^{-1} \circ \psi := \sum_\chi n_\chi (\varepsilon_v^{-1} \circ \chi)$, which clearly lies in $S_{\widehat{G}_w}$ (recall (2.4.6)). Since $r_G(a_w) = \Theta^t_{*,k}(g_w)$, we then deduce that

$$\begin{aligned} r_G(\varepsilon_v \circ a_w)(\psi) &= \varepsilon_v(r_G(a_w)(\varepsilon_v^{-1} \circ \psi)) \\ &= \varepsilon_v\left(\prod_{s\in G} g_w(s)^{\langle \varepsilon_v^{-1}\circ\psi, s\rangle_*}\right) \\ &= \prod_{s\in G} (\varepsilon_v \circ g_w)(s)^{\langle \psi, s\rangle_*} \\ &= \Theta^t_{*,K}(\varepsilon_v \circ g_w)(\psi). \end{aligned} \tag{7.2.3}$$

The third equality above holds because $\langle \varepsilon_v^{-1} \circ \psi, s\rangle_* = \langle \psi, s\rangle_*$ for all $s \in G$, which we will prove below. Observe that clearly it suffices to show that $\langle \varepsilon_v^{-1} \circ \chi, s\rangle_* = \langle \chi, s\rangle_*$ holds for all $\chi \in \widehat{G}_v$ and $s \in G$. Recall that we chose the same compatible set $\{\zeta_n : n \in \mathbb{Z}^+\}$ of roots of unity in $\mathbb{Q}^c$ for both k and K. We also chose $\{i_v(\zeta_n) : n \in \mathbb{Z}^+\}$ and $\{i_w(\zeta_n) : n \in \mathbb{Z}^+\}$ to be the compatible sets of roots of unity in K_v^c and k_w^c, respectively.

Now, let $\chi \in \widehat{G}_v$ and $s \in G$ be given. Let $\upsilon = \upsilon(\chi, s)$ be as in Definition 2.5.1. Then, we have $\chi(s) = i_v(\zeta_{|s|})^\upsilon$ and $\langle \chi, s\rangle_* = \upsilon/|s|$. Observe that

$$\begin{aligned} (\varepsilon_v^{-1} \circ \chi)(s) &= (\varepsilon_v^{-1} \circ i_v)(\zeta_{|s|})^\upsilon \\ &= (i_w \circ \overline{\gamma_v}^{-1})(\zeta_{|s|})^\upsilon \\ &= i_w(\zeta_{|s|})^\upsilon, \end{aligned}$$

where $\varepsilon_v^{-1} \circ i_v = i_w \circ \overline{\gamma_v}^{-1}$ by Definition 7.1.1 and $\overline{\gamma_v}^{-1}(\zeta_{|s|}) = \zeta_{|s|}$ because k contains all $\exp(G)$-th roots of unity. Again by Definition 2.5.1, this shows that $\langle \varepsilon_v^{-1} \circ \chi, s\rangle_* = \upsilon/|s|$ as well. Hence, we have $\langle \chi, s\rangle_* = \langle \varepsilon_v^{-1} \circ \chi, s\rangle_*$ and so the third equality in (7.2.3) indeed holds. It follows that (7.2.1) and (7.2.2) are equal and so $\Theta^t_{*,K} \circ \nu = \mu \circ \Theta^t_{*,k}$. This shows that the diagram commutes. ■

7.3 Preliminary Definitions

In this section, we will assume that the left Σ-action on G is trivial. Then, the Ω_k-action on G induced by the natural quotient map $\Omega_k \longrightarrow \Sigma$ and the given Σ-action on G is trivial, which agrees with the convention set up in Section 1.6. From the Hochschild-Serre spectral sequence associated to the group extension

$$1 \longrightarrow \Omega_K \longrightarrow \Omega_k \longrightarrow \Sigma \longrightarrow 1,$$

we then obtain an exact sequence

$$\mathrm{Hom}(\Omega_k, G) \xrightarrow{\mathrm{res}} \mathrm{Hom}(\Omega_K, G)^{\Sigma} \xrightarrow{tr} H^2(\Sigma, G) \tag{7.3.1}$$

which is analogous to (6.1.1). Here res denotes restriction. The Σ-action on $\mathrm{Hom}(\Omega_K, G)$ and the *transgression map tr* are defined in the exact same manner as in Definition 6.1.1. More precisely, for each $\gamma \in \Sigma$, choose and fix a lift $\overline{\gamma}$ of γ in Ω_k.

Definition 7.3.1 The Σ-action on $\mathrm{Hom}(\Omega_K, G)$ is defined by

$$(h \cdot \gamma)(\omega) := \gamma^{-1} \cdot h(\overline{\gamma}\omega\overline{\gamma}^{-1}) \qquad \text{for all } \omega \in \Omega_K$$

for $h \in \mathrm{Hom}(\Omega_K, G)$ and $\gamma \in \Sigma$. This definition is independent of the choice of the lift $\overline{\gamma}$ because G is abelian. Next, define $\overline{c} : \Sigma \times \Sigma \longrightarrow \Omega_K$ by setting $\overline{c}(\gamma, \delta) := (\overline{\gamma})(\overline{\delta})(\overline{\gamma\delta})^{-1}$. The *transgression map tr* : $\mathrm{Hom}(\Omega_K, G)^{\Sigma} \longrightarrow H^2(\Sigma, G)$ is defined by

$$tr(h) := [h \circ \overline{c}],$$

where $[-]$ denotes the cohomology class. This definition is also independent of the choice of the lifts $\overline{\gamma}$ for $\gamma \in \Sigma$.

Remark 7.3.2 If we regard $\mathrm{Hom}(\Omega_K^t, G)$ as a subset of $\mathrm{Hom}(\Omega_K, G)$ via Remark 7.0.3, then the Σ-action $\mathrm{Hom}(\Omega_K^t, G)$ and the transgression map on $\mathrm{Hom}(\Omega_K^t, G)^\Sigma$ induced by Definition 7.3.1 agree with those in Definition 6.1.1. In particular, the identical notation does not cause any confusion.

Definition 7.3.3 Define (recall Definition 2.4.1)

$$\begin{aligned} \mathcal{H}_\Sigma(KG) &:= \{r_G(a) \in \mathcal{H}(KG) \mid h_a \in \mathrm{Hom}(\Omega_K, G)^\Sigma\}; \\ \mathcal{H}_s(KG) &:= \{r_G(a) \in \mathcal{H}(KG) \mid h_a \in \mathrm{Hom}(\Omega_K, G)^\Sigma) \text{ and } tr(h_a) = 1\}. \end{aligned}$$

It is clear that both of the sets above are subgroups of $\mathcal{H}(KG)$.

Proposition 7.3.4 *Assume that k contains all* $\exp(G)$*-th roots of unity. Then, we have*

$$(\Theta^t_{*,K} \circ \nu)(\lambda_k(\Lambda(kG)^\times)) \subset \eta(\mathcal{H}_s(KG)),$$

provided that G has odd order so that $\Theta^t_{*,K}$ is defined.

Proof. Because k contains all $\exp(G)$-th roots of unity, the map ν is defined and results from Section 7.2 apply. Now, let $g \in \Lambda(kG)^\times$ be given. We have

$$(\Theta^t_{*,K} \circ \nu)(\lambda_k(g)) = (\Theta^t_{*,K} \circ \lambda_K)(\iota_\Lambda(g)) = (\eta \circ \Theta^t_{*,K})(\iota_\Lambda(g)),$$

where $\nu \circ \lambda_k = \lambda_K \circ \iota_\Lambda$ by Proposition 7.2.4 and $\Theta^t_{*,K} \circ \lambda_K = \eta \circ \Theta^t_{*,K}$ because diagram (2.5.5) commutes. Recall that $\iota_\Lambda : \Lambda(kG)^\times \longrightarrow \lambda(KG)^\times$ denotes the map induced by the natural inclusion $k \longrightarrow K$. Thus, it suffices to show that $\Theta^t_{*,K}(\iota_\Lambda(g)) \in \mathcal{H}_s(KG)$.

To that end, first recall that $\mathcal{H}(kG) = ((\mathbb{Q}^c G)^\times / G)^{\Omega_k}$ and $\mathcal{H}(KG) = ((\mathbb{Q}^c G)^\times / G)^{\Omega_K}$ by definition. Let $\iota_\mathcal{H} : \mathcal{H}(kG) \longrightarrow \mathcal{H}(KG)$ denote the natural inclusion induced by the inclusion $\Omega_K \subset \Omega_k$. From the identification (2.4.11), we see that there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\Omega_k}(S_{\widehat{G}}, (\mathbb{Q}^c)^\times) \arrow[r] \arrow[d, equal] & \mathrm{Hom}_{\Omega_K}(S_{\widehat{G}}, (\mathbb{Q}^c)^\times) \arrow[d, equal] \\
\mathcal{H}(kG) \arrow[r, "\iota_{\mathcal{H}}"'] & \mathcal{H}(KG)
\end{tikzcd}.$$

From this, it is clear that if $\Theta^t_{*,k}(g) = r_G(a)$, then $\Theta^t_{*,K}(\iota_\Lambda(g)) = \iota_{\mathcal{H}}(r_G(a))$. In particular, the homomorphism h associated to $\Theta^t_{*,K}(\iota_\Lambda(g))$ is equal to $res(h_a)$. Since (7.3.1) is exact, we then see that $h \in \mathrm{Hom}(\Omega_K, G)^\Sigma$ and $tr(h) = 1$. Thus, indeed $\Theta^t_{*,K}(\iota_\Lambda(g)) \in \mathcal{H}_s(KG)$, and this proves the claim. ■

7.4 Proof of Theorem 1.4.5 (a)

Theorem 1.4.5 *Let K/k be a Galois extension of number fields and set $\Sigma := Gal(K/k)$. Let G be a finite abelian group of odd order on which Σ acts trivially on the left. Define $V = V_K$ to the set of primes in $\mathcal{O}_K$ which are ramified over k. Assume that k contains all $\exp(G)$-th roots of unity.*

(a) The set $\mathcal{A}^t_\Sigma(\mathcal{O}_K G)_V$ is a subgroup of $Cl(\mathcal{O}_K G)$. Furthermore, given $h \in Hom(\Omega^t_K, G)^\Sigma_V$ and a finite set T of primes in $\mathcal{O}_K$, there exists $h' \in Hom(\Omega^t_K, G)^\Sigma_V$ such that

(1) $K_{h'}/K$ is a field extension;

(2) $K_{h'}/K$ is unramified at all $v \in T$;

(3) $cl(A_{h'}) = cl(A_h)$;

(4) $tr(h') = tr(h)$.

In particular, the set $\mathcal{A}^t_s(\mathcal{O}_K G)_V$ is also a subgroup of $Cl(\mathcal{O}_K G)$.

Proof. Let ρ_Σ denote the composition of the homomorphism rag given in Definition 2.4.4 followed by the natural quotient map

$$J(\mathcal{H}(KG)) \longrightarrow \frac{J(\mathcal{H}(KG))}{\eta(\mathcal{H}_\Sigma(KG))U(\mathcal{H}(\mathcal{O}_K G))(\Theta^t_{*,K} \circ \nu)(J(\Lambda(kG)))}.$$

We will show that $\mathcal{A}^t_\Sigma(\mathcal{O}_K G)_V$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_K G)$ by showing that

$$j^{-1}(\mathcal{A}^t_\Sigma(\mathcal{O}_K G)_V) = \ker(\rho_\Sigma), \tag{7.4.1}$$

or equivalently, that for any $c \in J(KG)$, we have $j(c) \in \mathcal{A}^t_\Sigma(\mathcal{O}_K G)_V$ if and only if

$$rag(c) \in \eta(\mathcal{H}_\Sigma(KG))U(\mathcal{H}(\mathcal{O}_K G))(\Theta^t_{*,K} \circ \nu)(J(\Lambda(kG))). \tag{7.4.2}$$

To that end, let $c \in J(KG)$ be given. First, assume that (7.4.2) holds, so

$$rag(c) = \eta(r_G(b))^{-1}u(\Theta^t_{*,K} \circ \nu)(g) \tag{7.4.3}$$

for some $r_G(b) \in \mathcal{H}_\Sigma(KG)$, $u \in U(\mathcal{H}(\mathcal{O}_K G))$, and $g \in J(\Lambda(kG))$. Let $\mathfrak{m}$ be an ideal in $\mathcal{O}_k$. Then, by Theorem 4.3.7, there exists $f \in \mathfrak{F}_k$ such that $f_w = 1$ for all primes $w \in M_k$ which are ramified in K/k and

$$g \equiv f \qquad (\mathrm{mod}\ \lambda_k(\Lambda(kG)^\times)U'_\mathfrak{m}(\Lambda(\mathcal{O}_k G))).$$

Choosing $\mathfrak{m}$ to be divisible by $|G|$ and $\exp(G)^2$, by Theorem 4.3.6 (b), the above yields

$$\Theta^t_{*,k}(g) \equiv \Theta^t_{*,k}(f) \qquad (\mathrm{mod}\ \Theta^t_{*,k}(\lambda_k(\Lambda(kG)^\times))U(\mathcal{H}(\mathcal{O}_k G))).$$

Since $\mu \circ \Theta^t_{*,k} = \Theta^t_{*,K} \circ \nu$ by Proposition 7.2.5, by Proposition 7.3.4, applying μ to the above equation then yields

$$(\Theta^t_{*,K}\circ\nu)(g)\equiv(\Theta^t_{*,K}\circ\nu)(f)\qquad(\mathrm{mod}\ \eta(\mathcal{H}_s(KG))U(\mathcal{H}(\mathcal{O}_KG))).\tag{7.4.4}$$

Thus, by changing b and u in (7.4.3) if necessary, we may assume that $g=f$. Note that $\nu(f)_v=1$ for all $v\in V$ and that $\nu(f)\in\mathfrak{F}_K$ by Proposition 7.2.2. Hence, if $h:=h_b$ is the homomorphism associated to $r_G(b)$, then h is tame with h_v unramified for all $v\in V$ and $j(c)=\mathrm{cl}(A_h)$ by Theorem 4.3.2. Since $r_G(b)\in\mathcal{H}_\Sigma(KG)$, we know that h is Σ-invariant, and the above then shows that $j(c)\in\mathcal{A}^t_\Sigma(\mathcal{O}_KG)_V$.

Conversely, assume that $j(c)=\mathrm{cl}(A_h)$ for some $h\in\mathrm{Hom}(\Omega^t_K,G)^\Sigma_V$, with $K_h=KG\cdot b$ say. Then, by Theorem 4.3.2, there exists $c'\in J(KG)$ such that $j(c')=\mathrm{cl}(A_h)$ and

$$rag(c')=\eta(r_G(b))^{-1}u\Theta^t_{*,K}(f')\tag{7.4.5}$$

for some $u\in U(\mathcal{H}(\mathcal{O}_KG))$ and $f'\in\mathfrak{F}_K$. Moreover, for each $v\in M_K$, we have $f'_v=f'_{K_v,s_v}$ for $s_v=h_v(\sigma_{K_v})$, and $s_v=1$ if $v\in V$. Since Σ acts trivially on G, by Proposition 7.1.5, we have $s_v=s_{v_w}$ for all $v\in M_K$ and $w\in M_k$ with w lying below v (recall Definition 7.0.5). Proposition 7.2.3 then implies that $f'=\nu(g)$ for some $g\in J(\Lambda(kG))$. Since $j(c)=\mathrm{cl}(A_h)$ also, by Theorem 2.1.7, we have

$$c\equiv c'\qquad(\mathrm{mod}\ \partial((KG)^\times)U(\mathcal{O}_KG)).$$

Clearly $rag((KG)^\times)\subset\mathcal{H}_s(KG)$. We may then write (7.4.5) as

$$rag(c)=\eta(r_G(b)r_G(b'))^{-1}uu'(\Theta^t_{*,K}\circ\nu)(g)\tag{7.4.6}$$

for some $r_G(b')\in\mathcal{H}_s(KG)$ and $u'\in\mathcal{H}(\mathcal{O}_KG)$. Note that $r_G(b)\in\mathcal{H}_\Sigma(KG)$ because h is Σ-

invariant. It follows that (7.4.2) indeed holds. This proves (7.4.1), and it remains to show the existence of $h' \in \mathrm{Hom}(\Omega_K^t, G)_V^{\Sigma}$ such that (1) to (4) are satisfied.

Let T be a finite set of primes in $\mathcal{O}_K$. First, notice that the same discussion following (7.4.3) shows that there exists $f \in \mathfrak{F}_k$ such that (7.4.4) holds. In particular, by changing b' and u' in (7.4.6) if necessary, we may assume that $g = f$. By Theorem 4.3.7, we may also assume that $f_w = 1$ for all $w \in M_k$ lying below the primes in $V \cup T$, and that $f_s \neq 1$ for all $s \in G$ with $s \neq 1$ (notice that Ω_k acts trivially on $G(-1)$ because k contains all $\exp(G)$-th roots of unity). In particular, by Proposition 7.2.2, we have that $\nu(f)_v = 1$ for all $v \in V \cup T$ and $\nu(f) \in \mathfrak{F}_K$.

Now, let h' be the homomorphism associated to $r_G(b)r_G(b')$. From (7.4.6) and Theorem 4.3.2, we then deduce that h' is tame with h'_v unramified for all $v \in V \cup T$ and that $j(c) = \mathrm{cl}(A_h)$, whence (2) and (3) hold. Because $r_G(b') \in \mathcal{H}_s(KG)$ and $h = h_b$ is Σ-invariant, it is clear that $h' \in \mathrm{Hom}(\Omega_K^t, G)_V^{\Sigma}$ and we have $tr(h') = tr(h)$, and so (4) holds as well. Finally, for each $s \in G$ with $s \neq 1$, we have $f_s \neq 1$ by choice so $f_w = f_{k_w,s}$ for some $w \in M_k$. Then, we have $\nu(f)_v = f_{K_v,s}$ by Proposition 7.2.2 and hence $h'_v(\sigma_{K_v}) = s$ by Theorem 4.3.2. This means that h' is surjective so $K_{h'}$ is a field, as claimed in (1).

Because gal_A is weakly multiplicative (recall Theorem 1.2.2 (b)), what we have proved above implies that $\mathcal{A}_s^t(\mathcal{O}_K G)_V$ is closed under multiplication. Since $\mathrm{Cl}(\mathcal{O}_K G)$ is finite, it follows that $\mathcal{A}_s^t(\mathcal{O}_K G)_V$ is also a subgroup of $\mathrm{Cl}(\mathcal{O}_K G)$. This proves the theorem. ■

7.5 The Quotient $\mathcal{A}_\Sigma^t(\mathcal{O}_K G)_V/\mathcal{A}_s^t(\mathcal{O}_K G)_V$

In what follows, we will assume all of the hypotheses stated in Theorem 1.4.5. Then, the sets $\mathcal{A}_\Sigma^t(\mathcal{O}_K G)_V$ and $\mathcal{A}_s^t(\mathcal{O}_K G)_V$ are both subgroups of $\mathrm{Cl}(\mathcal{O}_K G)$ by Theorem 1.4.5 (a). We are interested in the group structure of the quotient $\mathcal{A}_\Sigma^t(\mathcal{O}_K G)_V/\mathcal{A}_s^t(\mathcal{O}_K G)_V$ and its relation to that of $tr(\mathrm{Hom}(\Omega_K^t, G)_V^{\Sigma})$.

Proposition 7.5.1 *Let $h, h_1, h_2 \in Hom(\Omega_K^t, G)_V^\Sigma$.*

(a) $cl(A_{h_1})cl(A_{h_2}) = cl(A_{h_1 h_2 h_s})$ for some $h_s \in Hom(\Omega_K^t, G)_V^\Sigma$ with $tr(h_s) = 1$.

(b) $cl(A_h)cl(A_{h^{-1}}) \equiv 1 \ (mod\ \mathcal{A}_s^t(\mathcal{O}_K G)_V)$.

(c) If $tr(h_1) = tr(h_2)$, then $cl(A_{h_1}) \equiv cl(A_{h_2}) \ (mod\ \mathcal{A}_s^t(\mathcal{O}_K G)_V)$.

Proof. By Theorem 1.4.5 (a), there exists $h_2' \in \mathrm{Hom}(\Omega_K^t, G)_V^\Sigma$ such that $\mathrm{cl}(A_{h_2'}) = \mathrm{cl}(A_{h_2})$, $tr(h_2') = tr(h_2)$, and $d(h_2') \cap d(h_1) = \emptyset$ (recall the notation introduced in (1.1.2)). From Theorem 1.2.2 (b), we then deduce that

$$\mathrm{cl}(A_{h_1})\mathrm{cl}(A_{h_2}) = \mathrm{cl}(A_{h_1 h_2'}) = \mathrm{cl}(A_{h_1 h_2 h_s}),$$

where $h_s := h_2^{-1} h_2'$. It is clear that $tr(h_s) = 1$, and so (a) holds. As for (b), simply note that $\mathrm{cl}(A_h)\mathrm{cl}(A_{h^{-1}}) = 1$ by Theorem 1.2.2 (a). Alternatively, notice that (b) follows from (a) applied to $h_1 = h$ and $h_2 = h^{-1}$; this alternative argument is important because the equality $\mathrm{cl}(\mathcal{O}_h)\mathrm{cl}(\mathcal{O}_{h^{-1}}) = 1$ does not hold in general (cf. Remark 1.4.6).

Now, to prove (c), first observe that (a) and (b) together imply that

$$\mathrm{cl}(A_{h_1})\mathrm{cl}(A_{h_2})^{-1} \equiv \mathrm{cl}(A_{h_1})\mathrm{cl}(A_{h_2^{-1}}) \equiv \mathrm{cl}(A_{h_1 h_2^{-1} h_s}) \qquad (\mathrm{mod}\ \mathcal{A}_s^t(\mathcal{O}_K G)_V)$$

for some $h_s \in \mathrm{Hom}(\Omega_K^t, G)_V^\Sigma$ with $tr(h_s) = 1$. If $tr(h_1) = tr(h_2)$, then $tr(h_1 h_2^{-1} h_s) = 1$ and we deduce that $\mathrm{cl}(A_{h_1}) \equiv \mathrm{cl}(A_{h_2})$ (mod $\mathcal{A}_s^t(\mathcal{O}_K G)_V$), as desired. ■

7.6 Proof of Theorem 1.4.5 (b)

Theorem 1.4.5 *Let K/k be a Galois extension of number fields and set $\Sigma := Gal(K/k)$. Let G be a finite abelian group of odd order on which Σ acts trivially on the left. Define*

$V = V_K$ to the set of primes in $\mathcal{O}_K$ which are ramified over k. Assume that k contains all $\exp(G)$-th roots of unity.

(b) The natural surjective map

$$\phi_A : tr(Hom(\Omega_K^t, G)_V^{\Sigma}) \longrightarrow \frac{\mathcal{A}_{\Sigma}^t(\mathcal{O}_K G)_V}{\mathcal{A}_s^t(\mathcal{O}_K G)_V}; \quad \phi_A(tr(h)) := cl(A_h)\mathcal{A}_s^t(\mathcal{O}_K G)_V,$$

where $h \in Hom(\Omega_K^t, G)_V^{\Sigma}$, is well-defined and is a homomorphism. Furthermore, if i^* is injective, then ϕ_A is an isomorphism.

Proof. The map ϕ_A is well-defined by Proposition 7.5.1 (c). To show that it is a homomorphism, let $h_1, h_2 \in \mathrm{Hom}(\Omega_K^t, G)_V^{\Sigma}$ be given. Note that by Proposition 7.5.1 (a), there exists $h_s \in \mathrm{Hom}(\Omega_K^t, G)_V^{\Sigma}$ such that $tr(h_s) = 1$ and $\mathrm{cl}(A_{h_1})\mathrm{cl}(A_{h_2}) = \mathrm{cl}(A_{h_1 h_2 h_s})$. Then, we see that

$$\phi_A(tr(h_1))\phi_A(tr(h_2)) = \phi_A(tr(h_1 h_2 h_s)) = \phi_A(tr(h_1 h_2))$$

and so ϕ_A is indeed a homomorphism. This proves the first claim.

To prove the second claim, let $h \in \mathrm{Hom}(\Omega_K^t, G)_V^{\Sigma}$ be such that $\phi_A(tr(h)) = 1$. This means that $\mathrm{cl}(A_h) \in \mathcal{A}_s^t(\mathcal{O}_K G)_V$. Because $\mathcal{A}_s^t(\mathcal{O}_K G)$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_K G)$ by Theorem 1.4.5 (a), we have $\mathrm{cl}(A_h)^{-1} = \mathrm{cl}(A_{h_s})$ for some $h_s \in \mathrm{Hom}(\Omega_K^t, G)_V^{\Sigma}$ with $tr(h_s) = 1$. In particular, we may assume that $d(h_s) \cap d(h) = \emptyset$ (recall (1.1.2)). Since gal_A is weakly multiplicative by Theorem 1.2.2 (b), we deduce that

$$1 = \mathrm{cl}(A_h)\mathrm{cl}(A_{h_s}) = \mathrm{cl}(A_{hh_s}).$$

Now, recall Theorem 1.4.4. Since ξ is a homomorphism, we obtain $(\xi \circ \mathrm{gal}_A)(hh_s^{-1}h_s') = 1$ and hence $(i^* \circ tr)(hh_s) = 1$. If i^* is injective, then this implies that $tr(hh_s) = 1$ and so $tr(h) = 1$. Hence, in this case the map ϕ_A is injective and so is an isomorphism. ■

Bibliography

[1] E. Bayer-Fluckiger and H. W. Lenstra, *Forms in odd degree extensions and self-dual normal bases*, *Amer. J. Math.* **112(3)** (1990) 359–373.

[2] J. Brinkhuis, *Embedding problems and normal integral bases*, *Math. Ann.* **264** (1983) 537–543.

[3] J. Brinkhuis, *Galois modules and embedding problems*, *J. Reine Angew. Math.* **346** (1984) 141–165.

[4] D. Burns, *Adams operations and wild Galois structure invariants*, *Proc. London Math. Soc. (3)* **71** (1995) 241–262.

[5] N. P. Byott, *Integral Galois module structure of some Lubin-Tate extensions*, *J. Number Theory* **77** (1999) 252–273.

[6] C. W. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders Vol. I.* John Wiley & Sons Inc., New York, 1987.

[7] C. W. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders Vol. II.* John Wiley & Sons Inc., New York, 1987.

[8] B. Erez, *The Galois structure of the square root of the inverse different*, *Math. Z.* **208(2)** (1991) 239–255.

[9] B. Erez and J. Morales, *The Hermitian structure of rings of integers in odd degree abelian extensions*, *J. Number Theory* **41** (1992) 92–104.

[10] A. Fröhlich, *Local fields*, in *Algebraic number theory* (J. W. S. Cassels and A. Fröhlich, eds.). Academic Press Inc., London, 1967.

[11] A. Fröhlich, *Galois module structure of algebraic integers.* Ergebnisse der Mathematik und ihrer Grenzgebiete 1, Springer-Verlag, Berlin Heidelberg, 1983.

[12] A. Fröhlich and M. J. Taylor, *Algebraic number theory.* Cambridge University Press, 1991.

[13] H. Johnston, *Explicit integral Galois module structure of weakly ramified extensions of local fields*, *Proc. Amer. Math. Soc.* **143** (2015) 5059–5071.

[14] L. R. McCulloh, *Galois module structure of abelian extensions*, *J. Reine Angew. Math.* **375/376** (1987) 259–306.

[15] J. Morales, *Trace forms and Stickelberger relations*, *J. Number Theory* **51** (1995) 118–129.

[16] J. Neukirch, *Algebraic number theory.* Grundlehren der mathematischen Wissenschaften 322, Springer-Verlag, Berlin Heidelberg, 1999.

[17] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields 2nd Ed.,*. Grundlehren der mathematischen Wissenschaften 323, Springer-Verlag, Berlin Heidelberg, 2008.

[18] E. J. Pickett, *Explicit construction of self-dual integral normal bases for the square-root of the inverse different*, *J. Number Theory* **129** (2009) 1773–1785.

[19] E. J. Pickett and S. Vinatier, *Self-dual Integral Normal Bases and Galois Module Structure*, *Compos. Math.* **149** (2013) 1175–1202.

[20] J. P. Serre, *Local fields, english ed.* Graduate text in mathematics 67, Springer-Verlag, New York, 1979.

[21] J. P. Serre, *Galois cohomology, english ed.* Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[22] M. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, *Invent. math* **63** (1981) 41–79.

[23] S. Vinatier, *Structure galoisienne dans les extensions faiblement ramifiées de $\mathbb{Q}$*, *J. Number Theory* **91** (2001) 126–152.

[24] C. A. Weibel, *An introduction to homological algebra.* Cambridge studies in advanced Mathematics 38, Cambridge University Press, 1994.