Stark's Conjectures

Pieter Mostert

Thesis presented for the degree of Master of Science
in the Department of Mathematics and Applied Mathematics
University of Cape Town

February 2008

Acknowledgements

Firstly, I would like to thank my supervisor, Ken Hughes, for much advice given and many books lent. To all the other teachers and lecturers who've contributed to my mathematical education over the years, I thank you.

To my fellow masters students, thanks for keeping me company during the past two years. May the roads you travel be less bumpy than mine.

To everyone at IkamvaYouth, thank-you for the opportunity to do something practical with my mathematical knowledge. You will always be inspiring.

Finally, a big thank-you to my family – Ma, Da, Ingrid, Esther, and Karen – for all your support and love over the years.

Synopsis

We give a slightly more general version of the Rubin-Stark conjecture, but show that in most cases it follows from the standard version.

After covering the necessary background, we state the principal Stark conjecture and show that although the conjecture depends on a choice of a set of places and a certain isomorphism of $\mathbb{Q}[G]$-modules, it is independent of these choices. The conjecture is shown to satisfy certain 'functoriality' properties, and we give proofs of the conjecture in some simple cases.

The main body of this dissertation concerns a slightly more general version of the Rubin-Stark conjecture. A number of Galois modules connected with the conjecture are defined in chapter 4, and some results on exterior powers and Fitting ideals are stated.

In chapter 5 the Rubin-Stark conjecture is stated and we show how its truth is unaffected by lowering the top field, changing a set S of places appropriately, and enlarging moduli. We end by giving proofs of the conjecture in several cases.

A number of proofs, which would otherwise have interrupted the flow of the exposition, have been relegated to the appendix, resulting in this dissertation suffering from a bad case of appendicitis.

I know the meaning of plagiarism and declare that all of the work in this document, save for that which is properly acknowledged, is my own.

Contents

Chapter 1

Introduction

Many conjectures and results concern the interplay between algebraic objects (groups of units, class-groups, etc.) and analytic objects (special values of L-functions, etc.) The classic case of this is Dirichlet's class number formula ([BS66] theorem 2, p 313), which states that for any number field F, the leading coefficient of the Taylor expansion of the Dedekind zeta-function ζ_F at zero is given by

$$\frac{h_F R_F}{w_F},$$

where h_F, R_F and w_F are the class number, regulator and number of roots of unity of F respectively.

It is this relation that Stark tried to generalise to L-functions corresponding to arbitrary characters.

While we deal exclusively with number fields, Stark's conjectures have function-field analogues, and in fact the first-order Rubin-Stark conjecture has been proven for function-fields (see chapitre V of [Tat84]). There are also p-adic analogues (see [Sol02] for example), which we do not examine.

The first Stark-type conjectures appeared in a series of papers written by Harold Stark (as one might expect) between 1971 and 1980 ([Sta71], [Sta75],[Sta76], [Sta80]). The conjectures were reformulated by John Tate and given a more accessible treatment in the book [Tat84], based on a course given by Tate at the University of Orsay. No doubt this book also served to further general interest in the conjectures.

In [Sta80], Harold Stark gave a refined conjecture for abelian conjectures concerning the first derivatives of Artin L-functions at zero (conjecture 1, p 198), which was subsequently reformulated and slightly strengthened by Tate ([Tat84] conjecture St$(K/k, S)$, p 89). This was generalised by Karl Rubin in [Rub96], with the purpose of applying so-called 'Stark units' to Kolyvagin systems (see [Rub92]).

The most recent major advance is perhaps the work of David Burns ([Bur07], among others), who has shown that the Rubin-Stark conjecture follows from the equivariant Tamagawa number conjecture, and has formulated refined Stark-type conjectures generalising those of Gross in [Gro88] (conjecture 8.8).

1.1 Background, notation and conventions

We will assume results from basic algebraic number theory, representation theory, homological algebra etc. However, we give a brief summary, without proofs, of some results from algebraic number theory which will be used in this thesis, and use this to fix notation and terminology. We also state some facts and make some conventions regarding group representations. Other results can be found in the appendices.

1.1.1 Algebraic Number Theory

Proofs of most of the results in this subsection can be found in [Cas67] or [Nar90], although the terminology may not agree. If F is a field, a *valuation* on F is a map

$$\phi : F \to \mathbb{R}_{\geq 0}$$

satisfying

i) $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in F$,

ii) $\phi(x) = 0 \Leftrightarrow x = 0$,

iii) $\exists C \geq 1$ s.t. $\phi(x+y) \leq C \max\{\phi(x), \phi(y)\}$ for all $x, y \in F$.

Every field has at least one valuation, the trivial one which takes on the value 0 at 0 and is 1 everywhere else.

Each valuation determines a topology on F which turns it into a topological field, and we define two valuations on F to be equivalent if they determine the same topology. This gives an equivalence relation on the set of valuations of F, and one can show that ϕ_1 and ϕ_2 are in the same equivalence class iff there is a $\lambda > 0$ such that $\phi_1(x) = \phi_2(x)^\lambda$ for all $x \in F$. A valuation is said to be *non-archimedean* if we can take $C = 1$ in condition *iii)* above, and *archimedean* otherwise. Clearly this terminology can be extended to equivalence classes of valuations.

From now on we suppose F is a number field (a finite field extension of the rationals). The ring of integers, discriminant and group of roots of unity of a number field F will be denoted by $\mathcal{O}_F$, d_F and μ_F respectively. We define a *place* of F to be an equivalence class of non-trivial valuations of F. By Ostrowski's theorem ([Nar90],p90), the archimedean places are in one-to-one correspondence with embeddings of F in $\mathbb{C}$ modulo complex conjugation, while the non-archimedean places are in one-to-one correspondence with non-trivial prime ideals of $\mathcal{O}_F$. We say that an archimedean place is *real* if the corresponding embedding maps F into $\mathbb{R}$, and *complex* if it does not. For every place v we single out a normalised valuation, written $x \mapsto |x|_v$ and defined as follows:

If v is non-archimedean, corresponding to the prime ideal $\mathfrak{p}$, $|x|_v = (N\mathfrak{p})^{-\mathrm{ord}_\mathfrak{p}(x)}$, where $\mathrm{ord}_\mathfrak{p}(x) := \mathrm{ord}_\mathfrak{p}(x\mathcal{O}_F)$ is the exponent of $\mathfrak{p}$ in the prime ideal decomposition of $x\mathcal{O}_F$, and where $N\mathfrak{p} = \#(\mathcal{O}_F/\mathfrak{p})^*$. We will also write $\mathrm{ord}_v = \mathrm{ord}_\mathfrak{p}$ and $Nv = N\mathfrak{p}$.

If v is archimedean, corresponding to an embedding $\varphi : F \to \mathbb{C}$, then $|x|_v = |\varphi(x)|^\delta$, where δ is 1 or 2 depending on whether v is real or complex respectively.

If v is a non-archimedean place of F, corresponding to the prime ideal $\mathfrak{p}$, $\mathbb{F}(v) = \mathcal{O}_F/\mathfrak{p}$ will denote the residue field of v.

The set of archimedean places of F will be written as $S_{\infty,F}$.

A *modulus* of F is an element of the free abelian group on the non-archimedean and real archimedean places of F, where all coefficients are non-negative, and all coefficients corresponding to the real archimedean places are at most 1. Thus we may also think of a modulus as being a pair consisting of an integral $\mathcal{O}_F$-ideal and a set of real places of F. We write this free abelian group multiplicatively, and say that the modulus $\mathfrak{m}$ divides $\mathfrak{m}'$ iff $\mathfrak{m}'\mathfrak{m}^{-1}$ is a modulus. In this case we write $\mathfrak{m}|\mathfrak{m}'$.

Define the *support* of a fractional $\mathcal{O}_F$-ideal I to be

$$\mathrm{supp}(I) = \{v \text{ a non-archimedean place of } F : \mathrm{ord}_v(I) \neq 0\}.$$

If I is the integral ideal corresponding to a modulus $\mathfrak{m}$, define $\mathrm{supp}(\mathfrak{m}) = \mathrm{supp}(I)$ and $\mathrm{ord}_v(\mathfrak{m}) = \mathrm{ord}_v(I)$ if v is a non-archimedean.

The signature group Sgn_F of F is defined to be $\bigoplus_{\mathrm{real}\ v}\{1,-1\}$, where $\{1,-1\}$ is the group of units of $\mathbb{Z}$ (the direct sum is taken over all real archimedean places of F). We also define a signature map

$$\mathrm{sgn}_F : F^\times \to \mathrm{Sgn}_F : x \to (\mathrm{sign}(\phi_v(x)))_{\mathrm{real}\ v},$$

where ϕ_v is the embedding of F in $\mathbb{R}$ corresponding to v.

If $\mathfrak{m}$ is a modulus of F, define the modified signature group by

$$\mathrm{Sgn}_{F,\mathfrak{m}} = \bigoplus_{\mathrm{real}\ v|\mathfrak{m}} \{1,-1\},$$

where the direct sum is taken over all real archimedean places of F dividing $\mathfrak{m}$. The modified signature map $\mathrm{sgn}_{F,\mathfrak{m}} : F^\times \to \mathrm{Sgn}_{F,\mathfrak{m}}$ is defined analogously to sgn_F.

*If S is a set, $\#S$ denotes its cardinality.

Given an extension K/k, any valuation of K restricted to k is clearly a valuation of k. If w is a place of K which contains a valuation whose restriction to k is a element of the place v, then the same is true for all valuations in w, and we say that w divides, or lies above v, and write $w|_k = v$. For every place v of k there exists a finite, non-empty set of places of K which lie above v; we use the notation $\bar{v}$ to denote some fixed place of K dividing v.

Suppose w divides v. If w (and hence v) is non-archimedean, let $\mathfrak{p}$ and $\mathfrak{P}$ be the prime ideals of $\mathcal{O}_k$ and $\mathcal{O}_K$ corresponding to v and w respectively. Then $\mathcal{O}_k/\mathfrak{p}$ is canonically embedded in $\mathcal{O}_K/\mathfrak{P}$, and we define

$$f(w/v) = \dim_{\mathcal{O}_k/\mathfrak{p}}(\mathcal{O}_K/\mathfrak{P}) \ , \quad e(w/v) = \mathrm{ord}_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_K).$$

On the other hand, if v and w are archimedean, define

$$f(w/v) = 1 \ , \quad e(w/v) = \begin{cases} 2 & \text{if } v \text{ is real and } w \text{ is complex} \\ 1 & \text{otherwise} \end{cases} \dagger$$

This ensures that $|x|_v = |x|_w^{e(w/v)f(w/v)}$ for all $x \in k$. We say that w is ramified in K/k if $e(w/v) > 1$, and unramified otherwise, and that w splits completely in K/k iff it is unramified and $f(w/v) = 1$. If the extension K/k is Galois, then $e(w/v)$ and $f(w/v)$ depend only on v, and we talk about v being ramified or splitting completely in K/k if $\bar{v}$ is ramified or splits completely in K/k respectively.

If S is a set of places of k, then S_K denotes the set of places of K dividing those in S. Likewise, if $\mathfrak{m} = \prod_v v^{n_v}$ is a modulus of k such that all archimedean places dividing $\mathfrak{m}$ are unramified in K/k, define $\mathfrak{m}_K = \prod_v \left(\prod_{w|v} w^{e(w/v)}\right)^{n_v}$, which is then a modulus of K.

1.1.2 $R[G]$-modules and group representations

Let R and S be commutative unital rings, and suppose A and B are S-modules. If A is also an R-module, we give $A \bigotimes_S B$ an R-module structure by considering A as an R-S-bimodule and B as a left S-module. If G is a group and there is a representation $\rho : G \to \mathrm{Aut}_S(A)$, then A is naturally an $S[G]$-module. We write σa for $\rho(\sigma)(a)$ when the representation is clear from the context. If there are representations $\rho : G \to \mathrm{Aut}_R(A)$ and $\rho : G \to \mathrm{Aut}_S(B)$, we obtain a representation of G associated to $A \bigotimes_S B$ by defining $\sigma\cdot(a \otimes b) = (\sigma\cdot a) \otimes (\sigma\cdot b)$.

† See [Gra03] for a dissenting view.

For any abelian group A, we will write RA as short-hand for the R-module $R\bigotimes_{\mathbb{Z}} A$. We always give R the trivial G-action, so if A is an $\mathbb{Z}[G]$-module, $R[G]$ acts on RA by

$$\left(\sum_{\sigma\in G} r_\sigma\sigma\right)\cdot(r\otimes a) = \sum_{\sigma\in G} r_\sigma r\otimes\sigma\cdot a.$$

If $f : A \to B$ is a homomorphism, we will again write f for the homomorphism $1_R\bigotimes_{\mathbb{Z}} f : RA \to RB$. Although this notation is ambiguous, it should be clear from the context which function f refers to. We will usually take R to be a subring of $\mathbb{C}$, and will abbreviate $r\otimes a$ by ra.

Remark 1.1.1. If G is abelian and M is a left $\mathbb{Z}[G]$-module, we may regard $R[G]$ as an $R[G]-\mathbb{Z}[G]$-bimodule and form the left $R[G]$-module $R[G]\bigotimes_{\mathbb{Z}[G]} M$. This is isomorphic to the $R[G]$-module $RM = R\bigotimes_{\mathbb{Z}} M$, the isomorphism sending $(\sum_{\sigma\in G} r_\sigma\sigma)\otimes m$ to $\sum_{\sigma\in G} r_\sigma\otimes\sigma\cdot m$.

Let E be a subfield of $\mathbb{C}$. Suppose V is a (left) $E[G]$-module, of dimension n over E, corresponding to the representation $\rho : G \to \mathrm{Aut}_E(V)$. If α is a field embedding of E in $\mathbb{C}$, we define $\mathbb{C}_\alpha$ to be $\mathbb{C}$ with a $\mathbb{C}$-E-bimodule structure given by $\gamma\in\mathbb{C}$ acting on the left by $\gamma\cdot x = \gamma x$, and $\eta\in E$ acting on the right by $x\cdot\eta = x\alpha(\eta)$. We define $V^\alpha = \mathbb{C}_\alpha\bigotimes_E V$. If $\phi : V \to W$ is a homomorphism of E-vector spaces, we define $\phi^\alpha = 1_{\mathbb{C}_\alpha}\bigotimes_E\phi$.

If $f\in\mathrm{End}_E(V)$ corresponds to the matrix M_{ij} with respect to the basis $\{b_1,\ldots,b_n\}$ of V, then

$$f^\alpha(1\otimes b_i) = 1\otimes f(b_i) = \sum_{j=1}^{n} 1\otimes M_{ij}b_j = \sum_{j=1}^{n} M_{ij}^\alpha\cdot(1\otimes b_j),$$

so f^α corresponds to the matrix M_{ij}^α with respect to the basis $\{1\otimes b_1,\ldots,1\otimes b_n\}$ of V^α.

If ρ is the representation associated to V, then $\rho^\alpha : G \to \mathrm{Aut}_{\mathbb{C}}(V^\alpha)$ is defined by $\rho^\alpha(\sigma) = \rho(\sigma)^\alpha$ for $\sigma\in G$. Therefore if $\chi : G \to E$ is the character of ρ, $\chi^\alpha := \alpha\circ\chi : G \to \mathbb{C}$ is the character of ρ_α.

Any $\mathbb{Z}[G]$-module may also be regarded as a $\mathbb{Z}$-module/abelian group. To avoid constant repetition in chapters 4 and 5, we adopt the convention that when referring to a $\mathbb{Z}[G]$-module M, the word 'torsion' will mean $\mathbb{Z}$-torsion, and not $\mathbb{Z}[G]$-torsion. We use $\widetilde{M}$ to denote M modulo torsion, and we write $\widetilde{x}$ for the image of $x\in M$ under the natural map $M \to \widetilde{M}$. If M is torsion-free, we identify M with $\widetilde{M}$. If R is a unital commutative ring containing $\mathbb{Q}$, we will identify $\widetilde{M}$ with the image of M in RM. Since we will frequently be dealing with exterior powers modulo torsion, we use the notation $\rlap{-}\bigwedge_R^r M$ to denote $\widetilde{\bigwedge_R^r M}$.

If G is a finite group, we will use $\mathbf{1}_G$ to denote the trivial one-dimensional character of G (and *not* the identity element of G [‡]). We define $N_G = \sum_{\sigma\in G}\sigma \in \mathbb{Z}[G]$.

The map $\mathrm{aug}_G : \mathbb{Z}[G] \to \mathbb{Z} : \sum_{\sigma\in G} n_\sigma \sigma \mapsto \sum_{\sigma\in G} n_\sigma$ is called the augmentation map, and we denote its kernel by I_G. Define $M_G = M/I_G{\cdot}M$.

Results in the remainder of this section may be found in [Ser77]. Let G be a finite group, F a field. A finite-dimensional representation of G over F is a homomorphism $\rho : G \to \mathrm{Aut}_F(V)$, where V is a finite-dimensional F-vector space (we will refer to finite-dimensional representations as representations, it being understood that all representation we consider are finite-dimensional). If for $i = 1, 2$, $\rho_i : G \to V_i$ is a representation of G over F, a morphism from ρ_1 to ρ_2 is an F-linear map $\Phi : V_1 \to V_2$ such that $\Phi \circ (\rho_1(\sigma)) = \rho_2(\sigma) \circ \Phi$ for all $\sigma \in G$. Each representation χ gives a function $\chi = \mathrm{Tr} \circ \rho : G \to F$, called the character of the representation, and any two representations are isomorphic iff they have the same characters. We can form the direct sum of two representations of the same group, and a representation is said to be irreducible if it is not isomorphic to the direct sum of two non-zero representations. For any irreducible character χ of G, the central idempotent associated to χ is defined by

$$e_\chi = \frac{1}{\#G}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1} \in \mathbb{C}[G].$$

We now assume that F is algebraically closed. Every representation can then be uniquely written as the direct sum of irreducible representations (up to isomorphism and order). If χ and ψ are two characters of G, define

$$\langle \chi, \psi\rangle_G = \frac{1}{\#G}\sum_{\sigma\in G}\chi(\sigma)\psi(\sigma^{-1}).$$

If χ and ψ are irreducible, then

$$\langle \chi, \psi\rangle_G = \begin{cases} 1 & \chi = \psi \\ 0 & \chi \neq \psi \end{cases}$$

If $G \to \mathrm{Aut}_F V$ is a representation, with character ϕ, the idempotents e_χ (χ irreducible), can be used to give V a direct sum decomposition $V \cong \bigoplus_\chi e_\chi{\cdot}V$, where $\dim(e_\chi{\cdot}V) = \langle \chi, \phi\rangle_G$. This implies that $\langle \mathbf{1}_G, \phi\rangle_G = \dim_F V^G$.

Suppose H is a subgroup of G, and χ and ψ are characters of H and G respectively. Let $\mathrm{Ind}_H^G\chi$ be the character of $\mathrm{Ind}_H^G V$, where V is an $F[H]$-module giving rise to χ, and let $\mathrm{Res}_H^G\psi = \psi|_H$. Then

$$\left\langle \mathrm{Ind}_H^G\chi, \psi\right\rangle_G = \left\langle \chi, \mathrm{Res}_H^G\psi\right\rangle_H.$$

[‡]Note that if G is abelian, $\mathbf{1}_G$ is the identity element of the character group $\widehat{G}$.

1.1.3 Some conventions

If V is a finite-dimensional vector space and $f \in \mathrm{Aut}(V)$, then $\det(f|W)$ is the determinant of $f|_W : W \to W$[§]. We also write $W \xrightarrow{f} W$ when we mean $W \xrightarrow{f|_W} W$.

When A and B are modules as in the previous subsection, we sometimes abbreviate the R-module $A \bigotimes_S B$ by $A \bigotimes B$ when it is clear what S is.

Many objects we will deal with in this dissertation have a number of subscripts. At times we will omit the subscripts when it is clear from the context what they are. In some of the later sections we will give advance warning as to which subscripts will be omitted, but this will not always be done.

If G is a group and M is a left G-module which is written multiplicatively, we sometimes write m^α in place of $\alpha{\cdot}m$ ($\alpha \in \mathbb{Z}[G]$). Note that this implies $m^{(\alpha\beta)} = (m^\beta)^\alpha$. This should note be confused with M^G, which is the submodule of all $m \in M$ for which $\sigma{\cdot}m = m$ for all $\sigma \in G$.

The trivial group will be written as $\mathbb{1}$, while the identity morphism of an object X (in some category) will be denoted by 1_X.

Finally, $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$.

[§]This is purely for typographical reasons. It would be more natural to write $\det(f|_W)$, were it not for the fact that W may be given by a relatively complicated expression which would be awkward to read if it were a subscript.

Chapter 2

Preliminaries to Stark's conjecture

2.1 Artin L-functions

Let K/k be a finite normal extension of number fields with Galois group G. We turn the set of places of K into a G-set by defining

$$|x|_{\sigma w} = |\sigma^{-1}(x)|_w$$

for all $x \in K$, $\sigma \in G$. The action of G on the non-archimedean places corresponds to the action of G on prime ideals. If w lies above the place v of k, then so does $\sigma \cdot w$ for every $\sigma \in G$, and one can show that G acts transitively on set of places of K lying above v ([Tat67] proposition 1.2 (ii), p 163).

Let v be a place of k, and put $w = \bar{v}$. Define

$$D_w = \{\sigma \in G : \sigma \cdot w = w\}$$

to be the decomposition group of w. It is equal to the image of $\mathrm{Gal}(K_w/k_v)$ in G.

Suppose now that w is non-archimedean, corresponding to a prime ideal $\mathfrak{P}$. One sees that

$$D_w = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

We also denote this by $D_{\mathfrak{P}}$. If $i \in \mathbb{N}$, the i-th ramification group of w is

$$G_{w,i} = \left\{\sigma \in G : \sigma(x) - x \in \mathfrak{P}^{i+1} \quad (\forall x \in \mathcal{O}_K)\right\},$$

and we call $I_w := G_{w,0}$ the inertia group of w. Since all elements of D_w fix $\mathfrak{P}$, there is an obvious map $D_w \to \mathrm{Gal}(\mathbb{F}(w)/\mathbb{F}(v))$, which can be shown to be onto. Clearly the kernel of this map is I_w, so D_w/I_w is isomorphic to $\mathrm{Gal}(\mathbb{F}(w)/\mathbb{F}(v))$ which is cyclic of order $f(w/v)$ with generator $x \mapsto x^{\#\mathbb{F}(v)}$ (see [Sma] p 13, for example). The element of D_w/I_w that corresponds to $x \mapsto x^{\#\mathbb{F}(v)}$ will be denoted by $(w, K/k)$ and is called the Frobenius automorphism corresponding to w.

If $w' = \sigma w$ is another place extending v, then $D_{w'} = \sigma D_w \sigma^{-1}$ and $G_{w',i} = \sigma G_{w,i}\sigma^{-1}$. Thus if G is abelian, D_w and $G_{w,i}$ depend only on v, and we sometimes denote these subgroups by D_v and $G_{v,i}$, and write $(v, K/k)$ in place of $(w, K/k)$. If the extension K/k is clear from the context, we abbreviate $(w, K/k)$ by σ_w (or σ_v if $w|v$ and K/k is abelian).

Let $\rho : G \to \mathrm{Aut}_{\mathbb{C}}(V)$ be a complex finite-dimensional representation of G. Since I_w is a normal subgroup of D_w, V^{I_w} is a $\rho(D_w)$-invariant subspace of V. Thus we obtain a representation $G \to \mathrm{Aut}_{\mathbb{C}}(V^{I_w})$, whose kernel clearly contains I_w, and so we can define a representation

$$\rho_w : D_w/I_w \to \mathrm{Aut}_{\mathbb{C}}(V^{I_w}) : \sigma I_w \mapsto \rho(\sigma)|_{V^{I_w}}.$$

For any $s \in \mathbb{C}$ with $\Re(s) > 1$, the element

$$1 - \rho_w(\sigma_w) N v^{-s}$$

of $\mathrm{End}(V^{I_w})$ has an inverse

$$(1 - Nv^{-fs})^{-1} \sum_{r=0}^{f-1} \rho_w(\sigma_w)^r N v^{-rs}$$

(where $f = f(w/v)$ is the order of σ_w), and so its determinant is non-zero. This determinant is independent of the choice of w extending v.

Let S be a finite set of places of k including the archimedean ones. The function defined for $\{s \in \mathbb{C} : \Re(s) > 1\}$ by

$$s \mapsto \prod_{v \notin S} \det\left(1 - \rho_{\bar{v}}(\sigma_{\bar{v}}) N v^{-s}\right)^{-1}$$

(where v runs over the places of k not in S) can be analytically continued to a meromorphic function on $\mathbb{C}$. This only depends on the character χ of ρ, and we call this the Artin L-function of the extension K/k with respect to χ, and denote it by $L_S(s, \chi; K/k)$. We will also write $L_S(s, \chi)$ for $L_S(s, \chi; K/k)$ when it is not necessary to mention which extension we are dealing with. If S contains only the archimedean places, we will simply write $L(s, \chi)$ in place of $L_S(s, \chi)$. One can show that $L(s, \chi)$ is defined and non-zero at $s = 1$ if χ is a non-trivial irreducible character, while $L(s, \mathbf{1}_G)$ has a simple pole at $s = 1$.

Artin L-functions satisfy certain useful properties which we list below (proofs may be found in [Neu86] theorem 4.2, pp 123-124).

Additivity:

For any two characters χ_1 and χ_2 of G,

$$L_S(s, \chi_1 + \chi_2) = L_S(s, \chi_1) L_S(s, \chi_2)$$

Hence every Artin L-function may be written as a product of Artin L-functions corresponding to irreducible representations.

This also shows that $L_S(s, \chi)$ has a pole of order $\langle \mathbf{1}_G, \chi \rangle_G = \dim V^G$ at $s = 1$.

Induction:

If H is a subgroup of G and $F = K^H$ is the fixed field of H, then for a character χ of H,

$$L_{S_F}(s, \chi; K/F) = L_S(s, \mathrm{Ind}_H^G \chi; K/k).$$

Inflation:

If F is a Galois extension of k containing K, then there is a canonical surjection

$$\pi : \mathrm{Gal}(F/k) \to \mathrm{Gal}(K/k) : \sigma \mapsto \sigma|_K,$$

and any character χ of G gives a character $\mathrm{Infl}_G^H \chi := \chi \circ \pi$ of $H = \mathrm{Gal}(F/k)$. One can show that

$$L_S(s, \chi; K/k) = L_S(s, \mathrm{Infl}_G^H \chi; F/k).$$

Suppose χ is the character of the complex representation $\rho : G \to \mathrm{Aut}_{\mathbb{C}}(V)$. Then ρ factors through $\pi : G \to G/\ker(\rho)$ (i.e. $\rho = \rho' \circ \pi$, where $\rho' : G/\ker(\rho) \to \mathrm{Aut}_{\mathbb{C}}(V)$ is a (faithful) representation). Therefore if χ' is the character of ρ',

$$L_S(s, \chi'; K^{\ker(\rho)}/k) = L_S(s, \chi; K/k).$$

Thus every Artin L-function is equal to one defined by a faithful character. In particular, every L-function given by a one-dimensional character is equal to an L-function associated to a character of an abelian Galois group.

2.1.1 The Augmented Artin L-Function and the Functional Equation

We now introduce the augmented Artin L-function, following the exposition in [Mar77] and [Tat84]. Define

$$\Upsilon(s) = \pi^{-s/2} \Gamma(s/2),$$

a meromorphic function with a pole of order 1 at $s = 0$ (Here Γ is Euler's gamma function).

Let $\rho : G \to \mathrm{Aut}_{\mathbb{C}}(V)$ be a complex representation of G with character χ. If v is a real archimedean place of k, let

$$a_v = \dim V^{D_{\bar{v}}}, \qquad b_v = \mathrm{codim} V^{D_{\bar{v}}}$$

(these are independent of the choice of $\bar{v}$). We then define

$$\Upsilon_\chi^v(s) = \Upsilon(s)^{a_v}\Upsilon(s+1)^{b_v}.$$

If v is a complex archimedean place of k, define $\Upsilon_\chi^v(s) = [\Upsilon(s)\Upsilon(s+1)]^{\chi(1)}$. Finally, we define $\Upsilon_\chi(s) = \prod_{v \in S_\infty} \Upsilon_\chi^v(s)$.

Note that at $s = 0$, $\Upsilon_\chi^v(s)$ has a pole of order a_v if v is real, and of order $\chi(1) = \dim V = \dim V^{D_{\bar{v}}}$ if v is complex*. Thus $\Upsilon_\chi(s)$ has a pole of order

$$\sum_{v \text{ real}} a_v + \sum_{v \text{ complex}} \chi(1) = \sum_{v \text{ real}} \dim V^{D_{\bar{v}}} + \sum_{v \text{ complex}} \dim V^{D_{\bar{v}}} = \sum_{v \in S_\infty} \dim V^{D_{\bar{v}}}.$$

Also note that $\Upsilon_\chi(s)$ is defined and non-zero at $s = 1$.

Let v be a non-archimedean place of k. Define

$$n(\chi, v) = \frac{1}{\# I_{\bar{v}}} \sum_{i=0}^{\infty} \# G_{\bar{v},i} \mathrm{codim} V^{G_{\bar{v},i}}.$$

One can show that $n(\chi, v)$ is always an integer (see [Ser79], p100), and since $G_{\bar{v},i} = 0$ for almost all v and i, $n(\chi, v)$ is almost always zero. We then define $\mathfrak{f}(\chi)$, the *Artin conductor* of χ, by

$$\mathfrak{f}(\chi) = \prod_{v \nmid \infty} \mathfrak{p}_v^{n(\chi,v)},$$

where $\mathfrak{p}_v$ is the prime ideal corresponding to v. Finally, define $B(\chi) = |d_k|^{\chi(1)} N(\mathfrak{f}(\chi))$.

The augmented Artin L-function Λ is then defined by

$$\Lambda(s, \chi) = B(\chi)^{s/2}\Upsilon_\chi(s)L(s, \chi),$$

and satisfies the functional equation

$$\Lambda(s, \chi) = W(\chi)\Lambda(1 - s, \bar{\chi}),$$

where $W(\chi) \in \mathbb{C}$ is a constant with absolute value 1, the Artin root number (see [Mar77] p 14).

*If v is complex, $D_{\bar{v}}$ is trivial.

We may use this to determine the order of the zero of $L(s,\chi)$ at $s=0$; namely

$$\begin{aligned}\mathrm{ord}_{s=0}L(s,\chi) &= \mathrm{ord}_{s=1}L(s,\bar{\chi}) + \mathrm{ord}_{s=1}\Upsilon_{\bar{\chi}}(s) - \mathrm{ord}_{s=0}\Upsilon_{\chi}(s) \\ &= -\dim V^G + \sum_{v\in S_\infty} \dim V^{D_w}, \end{aligned} \tag{2.1.1}$$

since $\mathrm{ord}_{s=1}L(s,\bar{\chi}) = -\dim V^G$.

2.2 Brauer's Theorem

A character of a finite group G is said to be *monomial* if it is induced by a one-dimensional character of some subgroup of G. The following useful theorem is due to Brauer ([Bra47] theorem 1, p 503):

Theorem 2.2.1. *Every character of a finite group G can be written as a $\mathbb{Z}$-linear combination of monomial characters.*

Hence for any character χ of $G = \mathrm{Gal}(K/k)$, we can write $\chi = \sum_j n_j\Psi_j$, where $n_j \in \mathbb{Z}$ and $\Psi_j = \mathrm{Ind}_{H_j}^G(\psi_j)$ for a one-dimensional character ψ_j of a subgroup H_j of G. If we let $k_j = K^{H_j}$, then by the addition and induction properties of Artin L-functions,

$$\begin{aligned}L_S(s,\chi,K/k) &= L(s,\sum_j n_j\Psi_j;K/k) \\ &= \prod_j L_S(s,\mathrm{Ind}_{H_j}^G(\psi_j);K/k)^{n_j} \\ &= \prod_j L_{S_{k_j}}(s,\psi_j;K/k_j)^{n_j}.\end{aligned}$$

Replacing K/k_j by $K^{\ker\psi_j}/k_j$ expresses $L_S(s,\chi,K/k)$ is a product of integral powers of L-functions corresponding to abelian extensions. Thus we may often reduce questions about general L-functions to questions about L-functions corresponding to abelian extensions (with one-dimensional characters).

2.3 The Stark regulator

This section follows [Tat84], chapitre I. Let K/k be a finite normal extension of number fields, and let S be a finite set of places of k, including all the archimedean ones.

Let $Y_{K,S}$ be the free abelian group on S_K. This has a natural left G-action, induced by the action of G on S_K. If we give $\mathbb{Z}$ the trivial G-action, the augmentation map

$$\mathrm{aug}_K : Y_{K,S} \to \mathbb{Z} : \sum_{w\in S_K} n_w w \mapsto \sum_{w\in S_K} n_w$$

is a surjective G-module homomorphism with kernel

$$X_{K,S} = \left\{ \sum_{w \in S_K} n_w w \in Y_{K,S} : \sum_{w \in S_K} n_w = 0 \right\}.$$

To simplify the notation, we will omit the subscripts K and S at times. Tensoring the short exact sequence

$$0 \to X \to Y \to \mathbb{Z} \to 0$$

with $\mathbb{C}$ over $\mathbb{Z}$ gives a short exact sequence of $\mathbb{C}[G]$-modules

$$0 \to \mathbb{C}X \to \mathbb{C}Y \to \mathbb{C} \to 0.$$

By semi-simplicity, $\mathbb{C}Y \cong \mathbb{C}X \bigoplus \mathbb{C}$ (as $\mathbb{C}[G]$-modules), and so if χ_X and χ_Y are the characters of $\mathbb{C}X$ and $\mathbb{C}Y$ respectively, we have $\chi_Y = \chi_X + \mathbf{1}_G$.

Note that $Y \cong \bigoplus_{v \in S} Y_v$, where Y_v is the free abelian group generated by the places of K above v, and thus has character $\mathrm{Ind}_{D_{\bar{v}}}^G \mathbf{1}_{D_{\bar{v}}}$.

Definition 2.3.1. *If χ is the character of a finite-dimensional complex representation of G, define*

$$r_{K/k,S}(\chi) = \mathrm{ord}_{s=0} L_S(s, \chi; K/k).$$

We will usually omit the subscript K/k.

Proposition 2.3.1.

$$r_S(\chi) = \sum_{v \in S} \dim V^{D_{\bar{v}}} - \dim V^G = \langle \chi, \chi_X \rangle_G = \dim(V \bigotimes \mathbb{C}X_{K,S})^G$$

Proof.

$$\begin{aligned}
\langle \chi, \chi_X \rangle_G &= \left\langle \chi, \sum_{v \in S} \mathrm{Ind}_{D_{\bar{v}}}^G \mathbf{1}_{D_{\bar{v}}} - \mathbf{1}_G \right\rangle_G \\
&= \sum_{v \in S} \langle \chi, \mathrm{Ind}_{D_{\bar{v}}}^G \mathbf{1}_{D_{\bar{v}}} \rangle_G - \langle \chi, \mathbf{1}_G \rangle_G \\
&= \sum_{v \in S} \langle \mathrm{Res}_{D_{\bar{v}}}^G \chi, \mathbf{1}_{D_{\bar{v}}} \rangle_{D_{\bar{v}}} - \dim V^G \\
&= \sum_{v \in S} \dim V^{D_{\bar{v}}} - \dim V^G,
\end{aligned}$$

so the second equality holds. The third equality follows from

$$\dim(V \bigotimes_{\mathbb{C}} \mathbb{C}X)^G = \langle \chi\chi_X, \mathbf{1}_G \rangle_G = \langle \chi, \overline{\chi_X} \rangle_G = \langle \chi, \chi_X \rangle_G,$$

where the last equality comes from the fact that χ_X takes on integer values. It remains to show that

$$r_S(\chi) = \sum_{v\in S} \dim V^{D_{\bar{v}}} - \dim V^G. \tag{2.3.1}$$

Using Brauer's theorem we may assume that χ is one-dimensional. Note that in this case

$$\begin{aligned}\operatorname{ord}_{s=0} \det\left(1 - \rho_{\bar{v}}(\sigma_{\bar{v}})Nv^{-s}|V^{I_{\bar{v}}}\right) &= \begin{cases} 0 & \rho_{\bar{v}}(\sigma_{\bar{v}}) \neq 1_{V^{I_{\bar{v}}}} \\ 1 & \rho_{\bar{v}}(\sigma_{\bar{v}}) = 1_{V^{I_{\bar{v}}}} \end{cases} \\ &= \dim(V^{I_{\bar{v}}})^{D_{\bar{v}}/I_{\bar{v}}} = \dim(V^{D_{\bar{v}}}).\end{aligned}$$

By equation 2.1.1, 2.3.1 is true if $S = S_{\infty,k}$. Suppose the equality holds for a particular set S; if v is a place of k not in S, then

$$\begin{aligned}\operatorname{ord}_{s=0}L_{S\cup\{v\}}(s,\chi) &= \operatorname{ord}_{s=0}L_S(s,\chi) + \operatorname{ord}_{s=0} \det\left(1 - \rho_{\bar{v}}(\sigma_{\bar{v}})Nv^{-s}|V^{I_{\bar{v}}}\right) \\ &= \operatorname{ord}_{s=0}L_S(s,\chi) + \dim V^{D_{\bar{v}}},\end{aligned}$$

and so by induction 2.3.1 holds for all $S \supseteq S_{\infty,k}$. □

Remark 2.3.1. If V is one-dimensional, then $\dim V^{D_w}$ is 1 or 0 depending on whether χ is trivial on D_w or not, respectively, while $\dim V^G$ is 1 if $\chi = \mathbf{1}_G$, and zero otherwise. This shows that

$$r_S(\chi) = \begin{cases} \#\{v \in S : \chi|_{D_{\bar{v}}} = \mathbf{1}_{D_{\bar{v}}}\} & \text{if } \chi \neq \mathbf{1}_G \\ \#S - 1 & \text{if } \chi = \mathbf{1}_G \end{cases}$$

Suppose F is a number field, and S a finite set of places of F containing $S_{\infty,F}$. Let $U_{F,S} = \{x \in F^\times : |x|_w = 1\ (\forall w \notin S)\}$ be the group of S-units of F. Define the $\mathbb{R}$-linear map

$$\lambda_{F,S} : \mathbb{R}U_{F,S} \to \mathbb{R}X_{F,S} : ru \mapsto \sum_{w\in S} r \log|u|_w\, w^\dagger.$$

The proof of Dirichlet's units theorem can be modified to show that $\lambda_{F,S}$ is an isomorphism (see [Nar90] theorem 3.5, pp 101-103). The images of $\mathbb{Z}$-bases for $\widetilde{U_{F,S}}$ and $X_{F,S}$ in $\mathbb{R}U_{F,S}$ and $\mathbb{R}X_{F,S}$ give $\mathbb{R}$-bases for the respective vector spaces, and we define the S-regulator $R_{F,S}$ to be the determinant of $\lambda_{F,S}$ with respect to these bases.

†This is well-defined, since $\sum_{w\in S}\log|u|_w = \log\left(\prod_{w\in S}|u|_w\right) = \log 1 = 0$ by the product formula (see [Nar90] p 93, for example).

Dedekind's zeta function ζ_F is defined by

$$\zeta_F(s) = \sum_{\mathfrak{a}} (N\mathfrak{a})^{-s} \tag{2.3.2}$$

for $\Re(s) > 1$ (the sum running over integral ideal $\mathfrak{a}$), and defined on the rest of $\mathbb{C} \setminus \{1\}$ by analytic continuation. More generally, one defines the S-modified Dedekind zeta function $\zeta_{F,S}$ by restricting the sum in 2.3.2 to those integral ideals prime to the non-archimedean places in S. Alternatively, one may define it as taking the sum over integral $\mathcal{O}_{F,S}$-ideals, where

$$\mathcal{O}_{F,S} = \{x \in F : \mathrm{ord}_v(x) \geq 0 \text{ for all places } v \text{ of } F \text{ not in } S\}$$

is the ring of S-integers of F. The S-modified Dedekind zeta function has a product expansion

$$\zeta_{F,S}(s) = \prod_{\mathfrak{p} \notin S} (1 - N\mathfrak{p}^{-s})^{-1},$$

which is simply $L_S(s, \mathbf{1}_1; F/F)$.

By the Dirichlet class-number formula ([BS66]),

$$\lim_{s \to 0} s^{1-\#S_\infty} \zeta_F(s) = -\frac{h_F R_F}{w_F}.$$

Let $A_{F,S}$ denote the S-class group of F, that is, the quotient of the group of fractional $\mathcal{O}_{F,S}$-ideals by the subgroup of principal fractional $\mathcal{O}_{F,S}$-ideals. We claim that Dirichlet's class-number formula can be generalised as follows:

$$\lim_{s \to 0} s^{1-\#S} \zeta_{F,S}(s) = -\frac{h_{F,S} R_{F,S}}{w_F}. \tag{2.3.3}$$

where $h_{F,S} = \#A_{F,S}$. If $S = S_{\infty,F}$, this is just the usual formula. Suppose 2.3.3 holds for a set $S \supseteq S_{\infty,F}$, and let v be a place of F not in S, corresponding to the prime ideal $\mathfrak{p}$. Let d be the order $\mathfrak{p}$ in $A_{F,S}$, and let u be a generator of $\mathfrak{p}^d$. Then $h_{F,S\cup\{v\}} = h_{F,S}/d$, and $R_{F,S\cup\{v\}} = R_{F,S} \left|\log |u|_v\right| = R_{F,S} d \log Nv$. Since adding v to S increases the left-hand side of equation 2.3.3 by $\lim_{s \to 0} s^{-1}(1 - Nv^{-s}) = \log Nv$, the result follows by induction.

We consider again a normal extension of number fields K/k with Galois group G. If $S \supseteq S_{\infty,k}$ is a finite set of places of k, we write $U_{K,S} = U_{K,S_K}$, $\lambda_{K,S} = \lambda_{K,S_K}$, $\mathcal{O}_{K,S} = \mathcal{O}_{K,S_K}$, etc.

Let $j_{K/k,S} : Y_{k,S} \to Y_{K,S}$ be the $\mathbb{Z}[G]$-homomorphism defined by

$$j(v) = N_G \cdot \bar{v} = \#D_{\bar{v}} \sum_{\sigma D_{\bar{v}} \in G/D_{\bar{v}}} \sigma \cdot \bar{v}$$

for $v \in S$. Since $\mathrm{aug}_K \circ j = \#G\mathrm{aug}_k$, j restricts to a map $X_k \to X_K$, which we again denote by j. If $u \in U_{k,S}$, then

$$\lambda_K(\tilde{u}) = \sum_{w \in S_K} \log |u|_w w = \sum_{v \in S} \sum_{\sigma D_{\bar{v}} \in G/D_{\bar{v}}} \#D_{\bar{v}} \log |u|_v \sigma \cdot \bar{v}$$
$$= \sum_{v \in S} \log |u|_v j(v) = j(\lambda_k(\tilde{u})).$$

In other words,

$$\begin{array}{ccc} \mathbb{R}U_K & \xrightarrow{\lambda_K} & \mathbb{R}X_K \\ \uparrow & & \uparrow j_{K/k} \\ \mathbb{R}U_k & \xrightarrow{\lambda_k} & \mathbb{R}X_k \end{array} \qquad (2.3.4)$$

commutes. Likewise, if $u \in U_{K,S}$, then

$$\sum_{w|v} \log |u|_w = \frac{1}{\#D_{\bar{v}}} \sum_{\sigma \in G} \log |u|_{\sigma\bar{v}} = \sum_{\sigma \in G} \log |\sigma^{-1} \cdot u|_{\bar{v}}^{1/\#D_{\bar{v}}} = \log |N_{K/k}(u)|_v,$$

and thus $\lambda_K(\tilde{u})|_k = \sum_{v \in S} \sum_{w|v} \log |u|_w v = \sum_{v \in S} \log |N_{K/k}(u)|_v v = \lambda_k(N_{K/k}(u))$. Thus

$$\begin{array}{ccc} \mathbb{R}U_K & \xrightarrow{\lambda_K} & \mathbb{R}X_K \\ N_{K/k} \downarrow & & \downarrow |_k \\ \mathbb{R}U_k & \xrightarrow{\lambda_k} & \mathbb{R}X_k \end{array} \qquad (2.3.5)$$

is commutative.

Since $\lambda_{K,S}$ gives an $\mathbb{R}[G]$-isomorphism between $\mathbb{R}U$ and $\mathbb{R}X$, these two modules give rise to the same character. Tensoring a $\mathbb{Q}[G]$-module with $\mathbb{R}$ over $\mathbb{Q}$ leaves the character unchanged, so $\mathbb{Q}U$ and $\mathbb{Q}X$ have the same character and are thus isomorphic as $\mathbb{Q}[G]$-modules‡.

Hence we can find a $\mathbb{Q}[G]$-isomorphism $f : \mathbb{Q}X \to \mathbb{Q}U$, which after tensoring with $\mathbb{C}$ over $\mathbb{Q}$ gives a $\mathbb{C}[G]$-isomorphism $f : \mathbb{C}X \to \mathbb{C}U$.

Definition 2.3.2. *Let V be a $\mathbb{C}[G]$-module with character χ, and let $f : \mathbb{Q}X \to \mathbb{Q}U$ be a $\mathbb{Q}[G]$-isomorphism. The Stark regulator is defined to be*

$$R(\chi, f) = \det\left(1_V \otimes (\lambda \circ f) | (V \otimes \mathbb{C}X)^G\right).$$

‡although there does not seem to be a canonical way of choosing such an isomorphism.

Like the regulator of a number field, the Stark regulator is a combination of logarithms of normalised valuations of units.

Remark 2.3.2. We define $V^* = \mathrm{Hom}_{\mathbb{C}[G]}(V, \mathbb{C}[G])$, and give it the obvious $\mathbb{C}[G]$-module structure. Let $(\lambda \circ f)_V$ be the image of $\lambda \circ f$ under the functor $\mathrm{Hom}_G(V^*, \_)$, i.e.

$$(\lambda \circ f)_V : \mathrm{Hom}_{\mathbb{C}[G]}(V^*, \mathbb{C}X) \to \mathrm{Hom}_{\mathbb{C}[G]}(V^*, \mathbb{C}X) : h \mapsto \lambda \circ f \circ h.$$

$(V \bigotimes \mathbb{C}X)^G$ is naturally isomorphic to $\mathrm{Hom}_{\mathbb{C}[G]}(V^*, \mathbb{C}X)$ (see appendix A.1.1), and under this isomorphism, the restriction of $1_V \bigotimes (\lambda \circ f)$ to $(V \bigotimes \mathbb{C}X)^G$ corresponds to $(\lambda \circ f)_V$. Hence

$$R(\chi, f) = \det((\lambda \circ f)_V).$$

This is the definition used in the book by Tate ([Tat84] p 26).

Remark 2.3.3. Although the $\mathbb{Q}[G]$-modules $\mathbb{Q}X$ and $\mathbb{Q}U$ are isomorphic, this is not in general true of the $\mathbb{Z}[G]$ modules X and $\widetilde{U}$. For example, consider the case $K = \mathbb{Q}(\zeta)$, $k = \mathbb{Q}(\zeta^2)$, $S = S_\infty$, where $\zeta = i\sqrt[4]{3}$. The Galois group $\mathrm{Gal}(K/k)$ has order 2, and is generated by $\tau : \zeta \mapsto -\zeta$. The places in S_K correspond to the embeddings

$$w_1 : \zeta \mapsto \pm\zeta, \quad w_+ : \zeta \mapsto i\zeta, \quad w_- : \zeta \mapsto -i\zeta,$$

hence $\{w_1 - w_+, w_1 - w_-\}$ is a $\mathbb{Z}$-basis for X. Using PARI-GP, we find that the image of $\{\zeta^2 - 2, \zeta^3 + \zeta^2 + \zeta + 2\}$ in $\widetilde{U}$ gives a $\mathbb{Z}$-basis for $\widetilde{U}$. With respect to these integral bases, τ corresponds to the matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

respectively. One can easily show that these two matrices are not conjugate by an element of $GL_2(\mathbb{Z})$, hence no $\mathbb{Z}[G]$-isomorphism $f : X \to \widetilde{U}$ exists.

Remark 2.3.4. There is an alternative way of describing $R(\chi, f)$ when χ is one-dimensional. Let $(\lambda \circ f)_\chi$ be $\lambda \circ f$ with domain and codomain restricted to $e_{\bar{\chi}} \cdot \mathbb{C}X$. There is an isomorphism of $\mathbb{C}$-vector spaces

$$\xi_\chi : (V \bigotimes \mathbb{C}X)^G \to e_{\bar{\chi}}\mathbb{C}X : \gamma \otimes x \mapsto \gamma x^\S,$$

and since the diagram

$$\begin{array}{ccc} (V\otimes \mathbb{C}X)^G & \xrightarrow{1\otimes(\lambda\circ f)} & (V\otimes\mathbb{C}X)^G \\ \downarrow{\scriptstyle \xi_\chi} & & \downarrow{\scriptstyle\xi_\chi} \\ e_{\bar\chi}\cdot\mathbb{C}X & \xrightarrow{(\lambda\circ f)_\chi} & e_{\bar\chi}\cdot\mathbb{C}X \end{array}$$

commutes, $R(\chi, f) = \det(\lambda \circ f)_\chi$.

2.3.1 Behaviour under addition, induction and inflation of characters

Let us consider the general case again. We will show that $R_S(\chi, f)$ behaves similarly to $L_S(s, \chi)$ under addition, induction and inflation of characters.

Additivity

For any two characters χ_1 and χ_2 of G,

$$R_S(\chi_1 + \chi_2, f) = R_S(\chi_1, f)R_S(\chi_2, f).$$

The proof is straightforward, and therefore omitted.

Induction

Let L/k be a Galois subextension of K/k, let $H = \mathrm{Gal}(K/L)$, and let V be a $\mathbb{C}[H]$-module. There is a natural isomorphism

$$\mathrm{Hom}_{\mathbb{C}[H]}(V^*, \mathbb{C}X_{K,S_L}) \cong \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}_H^G V^*, \mathbb{C}X_{K,S})$$

(see A.1.2), so the diagram

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{C}[H]}(V^*, \mathbb{C}X_{K,S_L}) & \xrightarrow{(\lambda\circ f)_V} & \mathrm{Hom}_{\mathbb{C}[H]}(V^*, \mathbb{C}X_{K,S_L}) \\ \downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle\cong} \\ \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}_H^G V^*, \mathbb{C}X_{K,S}) & \xrightarrow{(\lambda\circ f)_{\mathrm{Ind}_H^G(V)}} & \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}_H^G V^*, \mathbb{C}X_{K,S}) \end{array}$$

commutes. The definition of $R(\chi, f)$ given by Tate (remark 2.3.2), and the fact that $\mathrm{Ind}_H^G V^* = (\mathrm{Ind}_H^G V)^*$, then shows that $R_{S_L}(\chi, f; K/L) = R_S(\mathrm{Ind}_H^G \chi, f; K/k)$.

[§]We identify the underlying $\mathbb{C}$ vector space of V with $\mathbb{C}$.

Inflation

Suppose E is a Galois extension of k containing K, and let $H = \mathrm{Gal}(E/k)$. Suppose we have a commutative diagram of the following form:

$$\begin{array}{ccc} \mathbb{Q}X_E & \xrightarrow{f_E} & \mathbb{Q}U_E \\ \Big\uparrow {\scriptstyle j_{E/K}} & & \Big\uparrow \\ \mathbb{Q}X_K & \xrightarrow{f_K} & \mathbb{Q}U_K \end{array} \tag{2.3.6}$$

where f_E and f_K are isomorphisms[¶]. If we regard $\mathbb{Q}X_K$ and $\mathbb{Q}X_K$ as H-modules via the restriction-to-K map $H \to G$, then $j_{E/k}$ is an H-homomorphism since the inclusion $\mathbb{Q}U_K \to \mathbb{Q}U_E$ is. Therefore, for any $\mathbb{C}[H]$-module V, $1_V \bigotimes j_{E/K}$ maps $(V \bigotimes \mathbb{C}X_K)^G = (V \bigotimes \mathbb{C}X_K)^H$ into $(V \bigotimes \mathbb{C}X_E)^H$. Combining 2.3.4 and 2.3.6 gives the following commutative diagram

$$\begin{array}{ccc} (V \bigotimes \mathbb{C}X_E)^H & \xrightarrow{1_V \bigotimes (\lambda_E \circ f_E)} & (V \bigotimes \mathbb{C}X_E)^H \\ \Big\uparrow {\scriptstyle 1_V \bigotimes j_{E/K}} & & \Big\uparrow {\scriptstyle 1 \bigotimes j_{E/K}} \\ (V \bigotimes \mathbb{C}X_K)^G & \xrightarrow{1 \bigotimes (\lambda_K \circ f)} & (V \bigotimes \mathbb{C}X_K)^G \end{array} \tag{2.3.7}$$

Since the L-functions satisfy the induction property,

$$\dim(V \bigotimes \mathbb{C}X_E)^H = r_S(\mathrm{Infl}_G^H \chi; E/k) = r_S(\chi; K/k) = \dim(V \bigotimes \mathbb{C}X_K)^G.$$

Therefore, since the vertical maps in diagram 2.3.7 are injective, they are isomorphisms, and so

$$R_S(\chi, f_K; K/k) = R_S(\mathrm{Infl}_G^H \chi, f_E, E/k).$$

Some final definitions before we are able to state Stark's conjecture: Let

$$c_S(\chi; K/k) = \lim_{s \to 0} s^{-r_S(\chi)} L_S(s, \chi)$$

be the leading coefficient in the Taylor expansion of $L_S(s, \chi)$ about $s = 0$.

[¶]Given an isomorphism $f_K : \mathbb{Q}X_K \to \mathbb{Q}U_K$, we can always find an isomorphism $f_E : \mathbb{Q}X_E \to \mathbb{Q}U_E$ to make the diagram commute, since the category of $\mathbb{Q}[G]$-modules is semi-simple.

Choose an isomorphism of $\mathbb{Q}[G]$-modules $f : \mathbb{Q}X_{K,S} \to \mathbb{Q}U_{K,S}$ and define

$$A_S(\chi, f; K/k) = \frac{R_S(\chi, f; K/k)}{c_S(\chi; K/k)}.$$

Since $R(\chi, f)$ and $c(\chi)$ satisfy the same additivity, induction and inflation properties, so does $A(\chi, f)$.

Chapter 3

Stark's conjecture

As in the previous section, most of the results in this chapter are taken from [Tat84] chapitre I.

3.1 Statement of Stark's principal conjecture

As before, let K/k be a Galois extension of number fields with Galois group G, let S be a finite set of places of k containing the archimedean ones, and choose an isomorphism of $\mathbb{Q}[G]$-modules $f : \mathbb{Q}X_{K,S} \to \mathbb{Q}U_{K,S}$.

Stark's principal conjecture, as reformulated by Tate, is

Conjecture 3.1.1. *For any complex character χ of G, and any $\alpha \in \mathrm{Aut}(\mathbb{C})$,*

$$A(\chi, f)^{\alpha} = A(\chi^{\alpha}, f).$$

This may not appear to be a generalisation of Dirichlet's class number formula (and in fact it isn't), but we will show that it generalises a weaker form of Dirichlet's formula. Define $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(G))$, and let ρ be a representation of G with character χ. If $\sigma \in G$, the eigenvalues of $\rho(\sigma)$ are g-th roots of unity (g $= \#G$), so $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\zeta)$, where ζ is a primitive g-th root of unity. Hence every embedding of $\mathbb{Q}(\chi)$ in $\mathbb{C}$ is the restriction of $\nu_a : \zeta \mapsto \zeta^a$ for some a coprime to g. Since $\nu_a(\chi(\sigma)) = \chi(\sigma^a) \in \mathbb{Q}(\chi)$ for every $\sigma \in G$, we see that $\mathbb{Q}(\chi)/\mathbb{Q}$ is normal.

Stark's conjecture implies that for any $\alpha \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}(\chi))$,

$$A(\chi, f)^{\alpha} = A(\chi^{\alpha}, f) = A(\chi, f),$$

and hence $A(\chi, f) \in \mathbb{Q}(\chi)$. One sees thus that Stark's conjecture is equivalent to:

$$\begin{cases} A(\chi, f) \in \mathbb{Q}(\chi), \\ A(\chi, f)^{\alpha} = A(\chi^{\alpha}, f) \quad (\forall \alpha \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})). \end{cases}$$

This implies that $c(\chi) = A(\chi, f)^{-1}R(\chi, f)$ is the product of an element of $\mathbb{Q}(\chi)$ and a combination of logarithms of normalised valuations of S_K-units, generalising the class number formula.

3.2 Independence of f

As it stands, it appears that the conjecture depends on the choice of the isomorphism $f : \mathbb{Q}X \to \mathbb{Q}U$. However, we shall show that if the conjecture holds for one choice of f, it holds for all others.

Suppose $f, f' : \mathbb{Q}X \to \mathbb{Q}U$ are $\mathbb{Q}[G]$-isomorphisms. It suffices to show that given any $\alpha \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$,

$$\frac{A(\chi, f')^\alpha}{A(\chi, f)^\alpha} = \frac{A(\chi^\alpha, f')}{A(\chi^\alpha, f)},$$

so if $\theta(\chi) = \frac{A(\chi,f')}{A(\chi,f)}$, we wish to show that $\theta(\chi)^\alpha = \theta(\chi^\alpha)$. Since

$$\begin{aligned}\theta(\chi) &= \frac{A(\chi, f')}{A(\chi, f)} = \frac{R(\chi, f')}{R(\chi, f)} = \frac{\det\left(1_V \bigotimes_{\mathbb{C}} (\lambda \circ f') | (V \bigotimes_{\mathbb{C}} \mathbb{C}X)^G\right)}{\det\left(1_V \bigotimes_{\mathbb{C}} (\lambda \circ f) | (V \bigotimes_{\mathbb{C}} \mathbb{C}X)^G\right)} \\ &= \det\left(1_V \bigotimes_{\mathbb{C}} (f^{-1} \circ f') \middle| (V \bigotimes_{\mathbb{C}} \mathbb{C}X)^G\right) = \det\left(1_V \bigotimes_{\mathbb{Q}} (f^{-1} \circ f') \middle| (V \bigotimes_{\mathbb{Q}} \mathbb{Q}X)^G\right),\end{aligned}$$

it remains to prove that for any $\mathbb{Q}[G]$-isomorphism $g : \mathbb{Q}X \to \mathbb{Q}X$,

$$\det\left(1_V \bigotimes g \,|(V \bigotimes \mathbb{Q}X)^G\right)^\alpha = \det\left(1_{V^\alpha} \bigotimes g \,|(V^\alpha \bigotimes \mathbb{Q}X)^G\right). \tag{3.2.1}$$

(We have omitted the subscript $\mathbb{Q}$ from $\bigotimes$). If $h : W \to W$ is an endomorphism of a finite-dimensional complex vector space W, then $\det(h|W)^\alpha = \det(h^\alpha|W^\alpha)$, hence the left-hand side of equation 3.2.1 is equal to

$$\det\left((1_V \bigotimes g)^\alpha \middle| ((V \bigotimes \mathbb{Q}X)^G)^\alpha\right) = \det\left((1_V \bigotimes g)^\alpha \middle| ((V \bigotimes \mathbb{Q}X)^\alpha)^G\right).$$

Since α leaves elements of $\mathbb{Q}$ fixed, there is a well-defined map

$$V^\alpha \bigotimes \mathbb{Q}X \to (V \bigotimes \mathbb{Q}X)^\alpha : (\gamma \otimes v) \otimes x \mapsto \gamma \otimes (v \otimes x),$$

which is clearly an isomorphism. Since the diagram

$$\begin{array}{ccc} V^\alpha \bigotimes \mathbb{Q}X & \xrightarrow{1_{V^\alpha} \bigotimes g} & V^\alpha \bigotimes \mathbb{Q}X \\ \cong \downarrow & & \downarrow \cong \\ (V \bigotimes \mathbb{Q}X)^\alpha & \xrightarrow{(1_V \bigotimes g)^\alpha} & (V \bigotimes \mathbb{Q}X)^\alpha \end{array}$$

commutes, 3.2.1 holds.

3.3 Independence of S

In this section, we prove that for a given extension, the truth of the conjecture is independent of the set S (so it suffices to prove it for $S = S_\infty$). By Brauer's theorem and the additivity, induction and inflation properties of $A_S(\chi, f)$, it is enough to prove this for faithful one-dimensional characters. Suppose $\chi(1) = 1$. To prove the independence of S, it is enough to show that if S is a finite set of places of k containing the archimedean ones, and v is a place of k not in S, then the conjecture is true for S if and only it is true for $S' = S \cup \{v\}$.

Let $U = U_S$, $X = X_S$, $U' = U_{S'}$, $X' = X_{S'}$. In general, we will use a prime to indicate that a quantity is defined using S', so for example $c'(\chi) = c_{S'}(\chi)$. Note that by proposition 2.3.1, $r'(\chi) = r(\chi) + \dim V^{D_{\bar{v}}}$.

Suppose $f : \mathbb{Q}X \to \mathbb{Q}U$ is a $\mathbb{Q}[G]$-isomorphism. By semi-simplicity, we may view $\mathbb{Q}X$ and $\mathbb{Q}U$ as direct summands of $\mathbb{Q}X'$ and $\mathbb{Q}U'$ respectively, so f can be extended to a $\mathbb{Q}[G]$-isomorphism $f' : \mathbb{Q}X' \to \mathbb{Q}U'$. It suffices to show that if

$$\Omega(\chi) = A(\chi, f)/A'(\chi, f'),$$

then $\Omega(\chi)^\alpha = \Omega(\chi^\alpha)$ for all $\alpha \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$.

Let $w = \bar{v}$. We consider two cases:

Case 1: D_w is non-trivial

Since the representation is faithful and V is one-dimensional, $V^{D_w} = \{0\}$, and so $r'(\chi) = r(\chi)$. We may view $\mathbb{C}X$ as a submodule of $\mathbb{C}X'$, and thus there is a canonical embedding of $(V \bigotimes \mathbb{C}X)^G$ in $(V \bigotimes \mathbb{C}X')^G$. Since these spaces have the same dimension over $\mathbb{C}$, this embedding is an isomorphism; since $\lambda' \circ f'$ with domain and codomain restricted to $\mathbb{C}X$ is $\lambda \circ f$, it is clear that $R(\chi, f) = R'(\chi, f')$. Therefore

$$\Omega(\chi) = c'(\chi)/c(\chi) = \det(1 - \sigma_w | V^{I_w}),$$

which is either $1 - \chi(\sigma_w)$ or 1, depending on whether V^{I_w} is V or $\{0\}$. In either case, $\Omega(\chi)^\alpha = \Omega(\chi^\alpha)$ for all $\alpha \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, and we are done.

Case 2: D_w is trivial

In this case, $\sigma_w = 1$, and $r'(\chi) = r(\chi) + 1$. Suppose w corresponds to the prime ideal $\mathfrak{P}$; then $\mathfrak{P}^{h_K} = \pi\mathcal{O}_K$ for some $\pi \in \mathcal{O}_K$. Pick any $w_0 \in S$, and define

$$x = w - e_{1_G} \cdot w_0 \in \mathbb{Q}X'.$$

Note that $\mathbb{Q}U' \cong \mathbb{Q}U \bigoplus \mathbb{Q}[G]\pi$ and $\mathbb{Q}X' \cong \mathbb{Q}X \bigoplus \mathbb{Q}[G]x$, and let $j : \mathbb{Q}[G]x \to \mathbb{Q}[G]\pi$ be the $\mathbb{Q}[G]$-module isomorphism that sends x to π. Since the truth of the Stark conjecture for S' is independent of the choice of f', we may assume that $f' = f \bigoplus j$.

Choose ordered $\mathbb{Q}$-bases for $\mathbb{Q}U$ and $\mathbb{Q}X$ and extend these to $\mathbb{Q}$-bases for $\mathbb{Q}U'$ and $\mathbb{Q}X'$ by adding $\{\sigma\cdot\pi : \sigma \in G\}$ and $\{\sigma\cdot x : \sigma \in G\}$ respectively (choose some ordering of G). We also view these as bases for the vector spaces obtained by tensoring with $\mathbb{C}$. For each $\sigma \in G$,

$$\begin{aligned}\lambda'(\sigma\cdot\pi) &= \lambda(\sigma\cdot\pi) + \sum_{\gamma\in G} \log|\sigma\cdot\pi|_{\gamma w}\gamma\cdot w = \lambda(\sigma\cdot\pi) + \log|\pi|_w \sigma\cdot w \\ &= \lambda(\sigma\cdot\pi) + \log|\pi|_w\sigma\cdot x + \log|\pi|_w e_{1_G}\cdot w_0 \equiv \log|\pi|_w\sigma\cdot x \pmod{\mathbb{C}X}.\end{aligned}$$

Therefore, if we let $M(\lambda)$ and $M(f)$ be the matrices corresponding to λ and f with respect to the chosen bases for $\mathbb{C}U$ and $\mathbb{C}X$ respectively, the matrices corresponding to λ' and f' with respect to the extended bases are respectively

$$M(\lambda') = \begin{pmatrix} M(\lambda) & * \\ 0 & \log|\pi|_w I_g \end{pmatrix} \quad \text{and} \quad M(f') = \begin{pmatrix} M(f) & 0 \\ 0 & I_g \end{pmatrix},$$

where I_g is the g $\times$ g identity matrix and $*$ represents some unspecified matrix. Because

$$(V \otimes \mathbb{C}X')^G \cong (V \otimes \mathbb{C}X)^G \bigoplus (V \otimes \mathbb{C}[G]\cdot x)^G,$$

where $(V \otimes \mathbb{C}[G]\cdot x)^G \cong \mathbb{C}e_{\bar{\chi}}\cdot x$ is one-dimensional, $R'(\chi, f') = \log|\pi|_w R(\chi, f)$. Finally, the fact that

$$\begin{aligned} c'(\chi) &= \lim_{s\to 0} s^{-r(\chi)-1}(1 - Nv^{-s})L_S(s,\chi) \qquad (\text{since } \sigma_w = 1) \\ &= \left(\lim_{s\to 0} s^{-1}(1 - Nv^{-s})\right)\left(\lim_{s\to 0} s^{-r(\chi)}L_S(s,\chi)\right) \\ &= \log Nv\, c(\chi) \end{aligned}$$

shows that $\Omega(\chi) = \log Nv/\log|\pi|_w = \log Nv/\log Nw^{-h} = -1/h$, and so $\Omega(\chi)^\alpha = \Omega(\chi^\alpha)$ for all $\alpha \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$.

3.4 Reduction to special cases

Given a Galois extension of number fields K/k, let F be the normal closure of K over $\mathbb{Q}$, and put $H = \mathrm{Gal}(F/\mathbb{Q})$, $\Gamma = \mathrm{Gal}(F/k)$. Then

$$A(\chi, f; K/k) = A(\mathrm{Infl}_G^\Gamma\chi, \bar{f}; F/k) = A(\mathrm{Ind}_\Gamma^H \mathrm{Infl}_G^\Gamma\chi, \bar{f}; F/\mathbb{Q}).$$

Therefore Stark's conjecture is true if it holds for every Galois extension of $\mathbb{Q}$.

By Brauer's theorem, we see that Stark's conjecture is true if it holds for all irreducible characters of abelian Galois groups.

3.5 Proofs of Stark's conjecture in special cases

Stark's conjecture has been proven in a number of special cases, the most significant being in [Sta75], where Stark gives a proof of his conjecture in the case where the character takes on rational values (see also [Tat84] chapitre II and [Das] chapter 9). As this proof is rather long, we omit it, and prove the conjecture in some easier cases.

3.5.1 The trivial character

We will show that Stark's conjecture is true for the trivial character $\mathbf{1}_G$. Since

$$A(\mathbf{1}_G, f; K/k) = A(\mathrm{Infl}_{\mathbf{1}}^{G}\mathbf{1}_{\mathbf{1}}, f; K/k) = A(\mathbf{1}_{\mathbf{1}}, f_0; k/k),$$

(where $f : \mathbb{Q}X_K \to \mathbb{Q}U_K$ extends $f_0 : \mathbb{Q}X_k \to \mathbb{Q}U_k$), we may assume $K = k$. In this case the L-function concerned is just the Dedekind zeta function of k.

By Dirichlet's class number formula,

$$c(\mathbf{1}_G) = -\frac{h_k R_k}{w_k},$$

so if we can show that $R(\mathbf{1}_G, f)/R_k \in \mathbb{Q}$, we will be done.

We have defined R_k to be the absolute value of the determinant of $\lambda_k : \widetilde{U_k} \to X_k$ with respect to $\mathbb{Z}$-bases for $\widetilde{U_k}$ and X_k. If $f : \mathbb{Q}X_k \to \mathbb{Q}U_k$ is an isomorphism, then $R(\mathbf{1}_G, f) = \pm R_k \det(f)$, where $\det(f)$ is calculated with respect to $\mathbb{Z}$-bases for $\widetilde{U_k}$ and X_k, considered as $\mathbb{Z}$-bases for $\mathbb{Q}U_k$ and $\mathbb{Q}X_k$ respectively. Since f is a function between rational vector spaces, $\det(f) \in \mathbb{Q}$, completing the proof.

Remark 3.5.1. From the above result, we may easily prove that the conjecture holds for extensions K/k with $[K : k] = 2$. Let χ be the non-trivial irreducible representation of G. Then since $\mathbf{1}_G + \chi = \mathrm{Ind}_{\mathbf{1}}^{G}\mathbf{1}_{\mathbf{1}}$, we see by using the additivity, induction and inflation properties of $A(\, , \,)$ that

$$A(\mathbf{1}_{\mathbf{1}}, f', K/K) = A(\mathbf{1}_{\mathbf{1}}, f, k/k) A(\chi, f', K/k),$$

and so the conjecture is true for χ since it holds for the trivial character.

3.5.2 The symmetric group on 3 letters

Stark's conjecture holds for quadratic extensions since the non-trivial character can be built up out of trivial characters by applying the inflation, induction and additivity properties of L-functions, and clearly this is true in general. A somewhat more complicated example of this is given below (The core idea is taken from [San01] p 7).

Suppose K/k is a Galois extension of number fields with Galois group G isomorphic to $\mathcal{S}_3$, the symmetric group on three letters. Let τ be an element of G of order 2, let σ be an element of G of order 3, and let F be the subfield of K fixed by $\langle\tau\rangle$. The group G has three irreducible characters; let ϕ be the non-trivial one-dimensional character, and ψ be the irreducible two-dimensional character (the character table is given below).

	$\{1\}$	$\{\tau, \tau\sigma, \tau\sigma^2\}$	$\{\sigma, \sigma^2\}$
$\mathbf{1}_G$	1	1	1
ϕ	1	-1	1
ψ	2	0	-1

Let φ be the non-trivial character of $\mathrm{Gal}(K/F) = \langle\tau\rangle \cong \mathbb{Z}/2\mathbb{Z}$. The identities

$$\psi = \mathrm{Ind}_{\langle\tau\rangle}^{G} \mathbf{1}_{\langle\tau\rangle} - \mathbf{1}_G \quad \text{and} \quad \phi = \mathrm{Ind}_{\langle\tau\rangle}^{G} \varphi - \psi$$

show that Stark's conjecture holds for all characters of G. Since all characters of a symmetric group take on rational values ([JK81] theorem 1.2.17, p 15), this also follows from the theorem proved by Stark.

Let L be the subfield of K fixed by the elements of G of order 3, and let χ and $\overline{\chi}$ be the non-trivial irreducible characters of $H = \mathrm{Gal}(K/L) \cong \mathbb{Z}/3\mathbb{Z}$. Then

$$\mathrm{Ind}_H^G \chi = \mathrm{Ind}_H^G \overline{\chi} = \psi,$$

so Stark's conjecture holds for the cubic extension K/L as well*. However, there does not appear to be a proof of Stark's conjecture for general cubic extensions.

*In general, if K/k is a normal extension of number fields with Galois group G having a normal subgroup H, then Stark's conjecture holds for K/K^H and all characters of H if it holds for K/k and all characters of G. Likewise, Stark's conjecture holds for K^H/k and all characters of G/H if it holds for K/k and all characters of G.

Chapter 4

Preliminaries to the Rubin-Stark conjecture

4.1 $R[G]$-modules

Let G be a finite abelian group, R a commutative unital ring.

4.1.1 $R[G]$-lattices

Definition 4.1.1. *An* $R[G]$-lattice *is an* $R[G]$*-module whose underlying* R*-module is free on a finite number of generators.*

Let M be an $R[G]$-module, which we may also view as an R-module. Define $M^* = \mathrm{Hom}_{R[G]}(M, R[G])$. We have a natural isomorphism of $R[G]$-modules

$$\mathrm{Hom}_{R[G]}(M, R[G]) \cong \mathrm{Hom}_R(M, R)$$

(see appendix A.1.1 for this isomorphism and the $R[G]$-module structure on $\mathrm{Hom}_R(M, R)$). Suppose now that M is finitely generated* and that R is a principal ideal domain; by the structure theorem for finitely generated modules over principal ideal domains (see [Bly77] theorem 16.6, p 300), the underlying R-module of M is a direct sum of free and torsion. Thus the underlying R-module of M^* is free on a finite number of generators. Hence M^* is an $R[G]$-lattice, and we see that if M is an $R[G]$-lattice to begin with, M^{**} is naturally isomorphic to M.

We prove the following homological algebra lemma (based on [Pop02] lemma 5.2.1, pp 15 - 16) for later reference

*either as an $R[G]$-module or an R-module; G is finite so it makes no difference.

Lemma 4.1.1. *Let D be a Dedekind domain and M a finitely generated $D[G]$-module.*

i) If M is D-torsion-free, then $\mathrm{Ext}^n_{D[G]}(M, D[G]) = 0$ for all $n \geq 1$.

ii) $\mathrm{Ext}^n_{D[G]}(M, D[G]) = 0$ for all $n \geq 2$.

Proof. Let $\mathcal{U} : D[G]\text{-}\mathbf{Mod} \to D\text{-}\mathbf{Mod}$ be the forgetful functor. Since the functors $\mathcal{U}(\mathrm{Hom}_{D[G]}(\_, D[G]))$ and $\mathrm{Hom}_D(\mathcal{U}(\_), D)$ (from $D[G]$-**Mod** to D-**Mod**) are naturally isomorphic, the right derived functors of $\mathcal{U}(\mathrm{Hom}_{D[G]}(\_, D[G]))$ and $\mathrm{Hom}_D(\mathcal{U}(\_), D)$ are too. If P is a projective $D[G]$-module, then $\mathcal{U}(P)$ is a projective D-module†, so $\mathcal{U}$ applied to any projective resolution of M gives a projective resolution of $\mathcal{U}(M)$. Thus the right derived functors of $\mathrm{Hom}_D(\mathcal{U}(\_), D)$ are $\mathrm{Ext}^n_D(\mathcal{U}(\_), D)$ (up to natural isomorphism), and so there exist natural isomorphisms

$$\mathcal{U}(\mathrm{Ext}^n_{D[G]}(\_, D[G])) \cong \mathrm{Ext}^n_D(\mathcal{U}(\_), D).$$

Therefore it is enough to show that

i) If M is D-torsion-free, then $\mathrm{Ext}^n_D(\mathcal{U}(M), D) = 0$ for all $n \geq 1$.

ii) $\mathrm{Ext}^n_D(\mathcal{U}(M), D) = 0$ for all $n \geq 2$.

Part *i)* follows from the fact that D-torsion-free modules are projective D-modules ([Coh03] p 373). To show that *ii)* holds, let

$$0 \to F_1 \to F_0 \to M \to 0 \tag{4.1.1}$$

be a short exact sequence of D-modules, where F_1 and F_0 are D-torsion free (choose F_0 to be free and let F_1 be the kernel of $F_0 \to M$). The long exact sequence of Ext modules, together with *i)*, shows that *ii)* holds. □

Corollary 4.1.1. *If $0 \to A \to B \to C \to 0$ is an exact sequence of $\mathbb{Z}[G]$-lattices, then $0 \to C^* \to B^* \to A^* \to 0$ is also exact.*

4.1.2 Exterior powers

Let R be a commutative unital ring, M an R-module. We write $\bigwedge_R M$ for the exterior algebra of M. It has the structure of a $\mathbb{Z}$-graded R-algebra $\bigwedge_R M \cong \bigoplus_{r\in\mathbb{Z}} \bigwedge_R^r M$ (we use the convention that $\bigwedge_R^r M = \{0\}$ if $r < 0$). If $f : N \to M$ is a homomorphism of R-modules, there is a unique R-algebra homomorphism $\bigwedge_R f : \bigwedge_R N \to \bigwedge_R M$ which preserves grading and, when its domain and codomain are restricted to $\bigwedge_R^1 N \cong N$ and

†If $P \bigoplus P' \cong \coprod_S D[G]$, then $\mathcal{U}(P) \bigoplus \mathcal{U}(P') \cong \coprod_{S\times G} D$.

$\bigwedge_R^1 M \cong M$ respectively, coincides with f. We write $f^{(r)} : \bigwedge_R^r N \to \bigwedge_R^r M$ for the restriction of $\bigwedge_R f$.

If N and M are both free of rank r with bases $\{n_1, \ldots, n_r\}$ and $\{m_1, \ldots, m_r\}$ respectively, then $f^{(r)}(n_1 \wedge \ldots \wedge n_r) = \det(f) m_1 \wedge \ldots \wedge m_r$, where the determinant is taken with respect to the given bases.

One can show that

$$\bigwedge_R^r (M \bigoplus N) \cong \bigoplus_{i=0}^{r} \left(\bigwedge_R^{r-i} M \otimes_R \bigwedge_R^i N \right), \tag{4.1.2}$$

and that if M is an S-module, A an S-algebra, then

$$A \otimes_R \left(\bigwedge_R^r M \right) \cong \bigwedge_A^r (A \otimes_R M)$$

([Mat86] p 284). This isomorphism applied to the case where $R = \mathbb{Z}[G]$ and $A = \mathbb{Q}[G]$, together with remark 1.1.1, shows that

$$\mathbb{Q} \bigwedge_{\mathbf{Z}[G]}^r M \cong \bigwedge_{\mathbf{Z}[G]}^r \mathbb{Q} M.$$

In general, if N is a submodule of M, $\bigwedge_R^r N$ will *not* be a submodule of $\bigwedge_R^r M$ (unless $r = 0$ or 1). For example, if I is an ideal of R, then $\bigwedge_R^2 R = 0$, but $\bigwedge_R^2 I$ may not be zero if I is nonprincipal (see [Mat86] pp 283 - 284). However, in certain cases we will have inclusion. For example, if N is a direct summand of M, say $M \cong N \bigoplus N'$, then

$$\bigwedge_R^r M \cong \bigoplus_{i=0}^{r} \left(\bigwedge_R^{r-i} N \otimes_R \bigwedge_R^i N' \right) \cong \bigwedge_R^r N \bigoplus \left(\bigoplus_{i=1}^{r} \left(\bigwedge_R^{r-i} N \otimes_R \bigwedge_R^i N' \right) \right).$$

We will use the following proposition.

Proposition 4.1.1. *Suppose N is a submodule of the G-module M. Then for every $n \in \mathbb{N}$, $\rlap{\,-}\bigwedge_{\mathbf{Z}[G]}^n N$ may be identified with a submodule of $\rlap{\,-}\bigwedge_{\mathbf{Z}[G]}^n M$.*

Proof. $\mathbb{Q} \bigwedge_{\mathbf{Z}[G]}^n N \cong \bigwedge_{\mathbf{Q}[G]}^n \mathbb{Q} N$ is a submodule of $\mathbb{Q} \bigwedge_{\mathbf{Z}[G]}^n M \cong \bigwedge_{\mathbf{Q}[G]}^n \mathbb{Q} M$ since $\mathbb{Q} N$ is a direct summand of $\mathbb{Q} M$. But $\rlap{\,-}\bigwedge_{\mathbf{Z}[G]}^n N$ and $\rlap{\,-}\bigwedge_{\mathbf{Z}[G]}^n M$ are embedded in $\mathbb{Q} \bigwedge_{\mathbf{Z}[G]}^n N$ and $\mathbb{Q} \bigwedge_{\mathbf{Z}[G]}^n M$ respectively, so $\rlap{\,-}\bigwedge_{\mathbf{Z}[G]}^n N \to \rlap{\,-}\bigwedge_{\mathbf{Z}[G]}^n M$ must be injective. □

4.1.3 Rubin's modified exterior power

For any $r \in \mathbb{N}$, there is an R-linear map $\iota : M^* \to \mathrm{Hom}_R(\bigwedge_R M, \bigwedge_R M)$ defined by

$$\iota(\phi)(m_1 \wedge \ldots \wedge m_t) = \sum_{j=1}^{t} (-1)^{j+1} \phi(m_j) \cdot m_1 \wedge \ldots \wedge m_{j-1} \wedge m_{j+1} \wedge \ldots \wedge m_t$$

on monomials and extended R-linearly to all of $\bigwedge_R M$ (we use the convention that a sum from $j = 1$ to $j = 0$ is 0). Observe that if $f : M \to M'$ is an R-module isomorphism,

$$\iota(\phi \circ f^{-1})\left(f^{(t)}(\mathbf{m})\right) = f^{(t-1)}(\iota(\phi)(\mathbf{m})). \tag{4.1.3}$$

We extend ι to a function $\iota : \bigwedge_R M^* \to \operatorname{Hom}_R(\bigwedge_R M, \bigwedge_R M)$ by defining $\iota(\phi_1 \wedge \ldots \wedge \phi_r) = \iota(\phi_1) \circ \ldots \circ \iota(\phi_r)$[‡]. It is clear that for every $r, t \in \mathbb{N}$, if $\phi \in \bigwedge_R^r M^*$ and $\mathbf{m} \in \bigwedge_R^t M$, then $\iota(\phi)(\mathbf{m}) \in \bigwedge_R^{t-r} M$.

One can show that under the identification of $\bigwedge_R^0 M$ with R,

$$\iota(\phi_1 \wedge \ldots \wedge \phi_r)(m_1 \wedge \ldots \wedge m_r) = \det(\phi_i(m_j))$$

(cite) From now on we only consider the case where $R = \mathbb{Z}[G]$ and M is finitely generated. In [Rub96], Rubin defines the following modified exterior power:

$$\bigwedge_{\mathbf{Z}[G],0}^r M = \left(\iota\left(\bigwedge_{\mathbf{Z}[G]}^r M^*\right)\right)^*.$$

Let $\mathcal{C}$ be the cokernel of the inclusion $\iota\left(\bigwedge_{\mathbf{Z}[G]}^r M^*\right) \to \left(\bigwedge_{\mathbf{Z}[G]}^r M\right)^*$. By tensoring with $\mathbb{C}$ and writing $\mathbb{C}M = \bigoplus_{\chi \in \hat{G}} e_\chi \mathbb{C}M$, we see that $\mathbb{C}\mathcal{C} = 0$. Thus $\mathcal{C}$ is finite, and so $\mathcal{C}^* = 0$. Therefore by lemma 4.1.1 there is an exact sequence

$$0 \to \bigwedge_{\mathbf{Z}[G]}^r M \to \bigwedge_{\mathbf{Z}[G],0}^r M \to \operatorname{Ext}_{\mathbf{Z}[G]}^1(\mathcal{C}, \mathbb{Z}[G]) \to 0.$$

Since $\mathcal{C}$ is finite, so is $\operatorname{Ext}_{\mathbf{Z}[G]}^1(\mathcal{C}, \mathbb{Z}[G])$. It follows that we may identify $\bigwedge_{\mathbf{Z}[G],0}^r M$ with

$$\left\{\mathbf{m} \in \mathbb{Q}\bigwedge_{\mathbf{Z}[G]}^r M : \iota(\phi)(\mathbf{m}) \in \mathbb{Z}[G] \ \left(\forall \phi \in \bigwedge_{\mathbf{Z}[G]}^r M^*\right)\right\}.$$

Note that if $\phi \in \bigwedge_{\mathbf{Z}[G]}^t M^*$, then

$$\iota(\phi)\left(\bigwedge_{\mathbf{Z}[G],0}^r M\right) \subseteq \bigwedge_{\mathbf{Z}[G],0}^{r-t} M.$$

4.2 Basic definitions

Definition 4.2.1. *Let $\mathfrak{m}$ be a modulus of a number field F. We say that $\alpha \in F^\times$ is congruent to 1 mod $\mathfrak{m}$ (in symbols, $\alpha \equiv 1 \bmod^\times \mathfrak{m}$), if $\operatorname{ord}_v(\alpha - 1) \geq \operatorname{ord}_v(\mathfrak{m})$ for all $v \in \operatorname{supp}(\mathfrak{m})$, and if $\operatorname{sgn}_{F,\mathfrak{m}}(\alpha)$ is the identity of $\operatorname{Sgn}_{F,\mathfrak{m}}$.*

Given a set of places $S \supset S_{\infty,F}$ of a number field F, and a modulus $\mathfrak{m}$ of F such that $\operatorname{supp}(\mathfrak{m}) \cap S = \emptyset$, we define the following:

[‡] Of course one needs to check that this is well-defined.

- $F^{\mathfrak{m}} = \{x \in F^\times : \mathrm{ord}_v(x) = 0\ (\forall v \in \mathrm{supp}(\mathfrak{m}))\}$. Observe that this is a subgroup of $F^\times$.
- $F_1^{\mathfrak{m}} = \{x \in F^\times : x \equiv 1 \bmod^\times \mathfrak{m}\}$. Note that if $x \equiv 1 \bmod^\times \mathfrak{m}$, then $\mathrm{ord}_v(x) = \mathrm{ord}_v(1) = 0$ for all $v \in \mathrm{supp}(\mathfrak{m})$ (otherwise $\mathrm{ord}_v(x-1) = \min\{\mathrm{ord}_v(x), \mathrm{ord}_v(1)\} \leq 0$). Thus $F_1^{\mathfrak{m}}$ is a subgroup of $F^{\mathfrak{m}}$.
- $Q_{F,\mathfrak{m}} = F^{\mathfrak{m}}/F_1^{\mathfrak{m}}$[§]. We will give a more concrete description of $Q_{F,\mathfrak{m}}$ in due course.
- $\mathscr{I}_{F,S,\mathfrak{m}}$ is the free abelian group on the places of F not in $S \cup \mathrm{supp}(\mathfrak{m})$. There is a group homomorphism

$$\mathrm{div}_{F,S,\mathfrak{m}} : F_1^{\mathfrak{m}} \to \mathscr{I}_{F,S,\mathfrak{m}} : x \mapsto \sum_{v \notin S \cup \mathrm{supp}(\mathfrak{m})} \mathrm{ord}_v(x) v.$$

- $A_{F,S,\mathfrak{m}} = \mathrm{coker}(\mathrm{div}_{F,S,\mathfrak{m}}) = \mathscr{I}_{F,S,\mathfrak{m}}/\mathrm{div}_{F,S,\mathfrak{m}}(F_1^{\mathfrak{m}})$ – the 'S-ray class group modulo $\mathfrak{m}$'. One could also describe this as the group of fractional $\mathcal{O}_{F,S}$-ideals prime to the non-archimedean part of $\mathfrak{m}$, modulo the subgroup of principal fractional $\mathcal{O}_{F,S}$-ideals with a generator congruent to 1 mod $\mathfrak{m}$.
- $U_{F,S,\mathfrak{m}} = \ker(\mathrm{div}_{F,S,\mathfrak{m}}) = \{u \in F_1^{\mathfrak{m}} : \mathrm{ord}_v(u) = 0\ (\forall v \notin S)\} = F_1^{\mathfrak{m}} \cap U_{F,S}$. Thus there is an exact sequence

$$0 \to U_{F,S,\mathfrak{m}} \to F_1^{\mathfrak{m}} \to \mathscr{I}_{F,S,\mathfrak{m}} \to A_{F,S,\mathfrak{m}} \to 0 \tag{4.2.1}$$

- $\mu_{F,\mathfrak{m}}$ is the torsion subgroup of $U_{F,S,\mathfrak{m}}$, i.e. $\mu_{F,\mathfrak{m}} = \mu_F \cap U_{F,S,\mathfrak{m}} = \mu_F \cap F_1^{\mathfrak{m}}$. We also define $w_{F,\mathfrak{m}} = \#\mu_{F,\mathfrak{m}}$.

In appendix A.6, we show that there exists a long exact sequence

$$0 \to U_{F,S,\mathfrak{m}} \to U_{F,S} \to Q_{F,\mathfrak{m}} \to A_{F,S,\mathfrak{m}} \to A_{F,S} \to 0. \tag{4.2.2}$$

From this, we see that

$$[U_{F,S} : U_{F,S,\mathfrak{m}}]h_{F,S,\mathfrak{m}} = \#Q_{F,\mathfrak{m}}h_{F,S}\text{[¶]}. \tag{4.2.3}$$

Since $\lambda_{F,S,\mathfrak{m}}$ is $\lambda_{F,S}$ composed with the inclusion $U_{F,S,\mathfrak{m}}/\mu_{F,\mathfrak{m}} \hookrightarrow U_{F,S}/\mu_F$, the definition of $R_{F,S,\mathfrak{m}}$ gives

$$\begin{aligned} R_{F,S,\mathfrak{m}} &= [U_{F,S}/\mu_F : U_{F,S,\mathfrak{m}}/\mu_{F,\mathfrak{m}}]R_{F,S} \\ &= \frac{[U_{F,S} : U_{F,S,\mathfrak{m}}]}{[\mu_F : \mu_{F,\mathfrak{m}}]}R_{F,S} = \frac{[U_{F,S} : U_{F,S,\mathfrak{m}}]w_{F,\mathfrak{m}}}{w_F}R_{F,S}. \end{aligned} \tag{4.2.4}$$

[§]This is non-standard notation. The notation $(\mathcal{O}_K/\mathfrak{m})^\times$ is more commonly used.

[¶]We will compute $Q_{F,\mathfrak{m}}$ shortly, and show that it is finite.

Putting equations (2.3.3), (4.2.3) and (4.2.4) together gives

$$\#Q_{F,\mathfrak{m}} \lim_{s\to 0} s^{1-\#S}\zeta_{F,S}(s) = -\frac{h_{F,S,\mathfrak{m}}R_{F,S,\mathfrak{m}}}{w_{F,\mathfrak{m}}}. \tag{4.2.5}$$

For the rest of this dissertation, K/k will be a finite abelian extension of number fields with Galois group G, and all characters of G will be assumed to be one-dimensional.

Suppose $S \supseteq S_{\infty,k}$ is a finite set of places of k containing all places which ramify in K/k, and suppose $\mathfrak{m}$ is a modulus of k such that $\text{supp}(\mathfrak{m}) \cap S = \emptyset$, and such that no real archimedean place dividing $\mathfrak{m}$ is ramified in K/k. We then define $A_{K,S,\mathfrak{m}} = A_{K,S_K,\mathfrak{m}_K}$, $U_{K,S,\mathfrak{m}} = U_{K,S_K,\mathfrak{m}_K}$, $Q_{K,\mathfrak{m}} = Q_{K,\mathfrak{m}_K}$, etc. (In general, we replace S and $\mathfrak{m}$ by S_K and $\mathfrak{m}_K$). All the groups defined above have natural G-module structures, and all the group homomorphisms are G-homomorphisms.

Putting $F = k$ and $F = K$ in the exact sequence 4.2.1 gives two sequences which fit together to give the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_{K,S,\mathfrak{m}} & \longrightarrow & K_1^{\mathfrak{m}} & \longrightarrow & \mathscr{I}_{K,S,\mathfrak{m}} & \longrightarrow & A_{K,S,\mathfrak{m}} & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow{\scriptstyle i_{K/k}} & & \uparrow{\scriptstyle i^A_{K/k}} & & \\
0 & \longrightarrow & U_{k,S,\mathfrak{m}} & \longrightarrow & k_1^{\mathfrak{m}} & \longrightarrow & \mathscr{I}_{k,S,\mathfrak{m}} & \longrightarrow & A_{k,S,\mathfrak{m}} & \longrightarrow & 0
\end{array}$$

The first two vertical maps are the natural inclusions, $i_{K/k}$ sends $v \in \mathscr{I}_{k,S,\mathfrak{m}}$ to $\sum_{w|v} w \in \mathscr{I}_{K,S,\mathfrak{m}}$, and $i^A_{K/k}$ is induced by the previous ones. We use the map $i_{K/k} : \mathscr{I}_{k,S,\mathfrak{m}} \to \mathscr{I}_{K,S,\mathfrak{m}}$ to identify $\mathscr{I}_{k,S,\mathfrak{m}}$ with a submodule of $\mathscr{I}_{K,S,\mathfrak{m}}$.

We also have

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_{K,S,\mathfrak{m}} & \longrightarrow & K_1^{\mathfrak{m}} & \longrightarrow & \mathscr{I}_{K,S,\mathfrak{m}} & \longrightarrow & A_{K,S,\mathfrak{m}} & \longrightarrow & 0 \\
 & & {\scriptstyle N_{K/k}}\downarrow & & {\scriptstyle N_{K/k}}\downarrow & & {\scriptstyle N^{\mathscr{I}}_{K/k}}\downarrow & & {\scriptstyle N^A_{K/k}}\downarrow & & \\
0 & \longrightarrow & U_{k,S,\mathfrak{m}} & \longrightarrow & k_1^{\mathfrak{m}} & \longrightarrow & \mathscr{I}_{k,S,\mathfrak{m}} & \longrightarrow & A_{k,S,\mathfrak{m}} & \longrightarrow & 0
\end{array}$$

The two first two vertical maps are restrictions of $N_{K/k} : K^\times \to k^\times$, $N^{\mathscr{I}}_{K/k}$ sends $w \in \mathscr{I}_{K,S,\mathfrak{m}}$ to $N_G \cdot w = \#D_w \sum_{w'|v} w' = \#D_w i(v)$ (where $v = w|_k$), and $N^A_{K/k}$ is induced by the others.

4.2.1 The $\mathbb{Z}[G]$-module structure of $Q_{K,\mathfrak{m}}$

The following proposition shows that the calculation of $Q_{K,\mathfrak{m}}$ can be reduced to the case where $\mathfrak{m}$ is the power of a single place.

Proposition 4.2.1. *If* $\mathfrak{m}$ *and* $\mathfrak{n}$ *are relatively prime*[‖] *moduli of* k, *then* $Q_{K,\mathfrak{mn}} \cong Q_{K,\mathfrak{m}} \bigoplus Q_{K,\mathfrak{n}}$

Proof. There is an obvious map $Q_{K,\mathfrak{mn}} \to Q_{K,\mathfrak{m}} \bigoplus Q_{K,\mathfrak{n}}$, which is injective since $x \equiv 1 \bmod^{\times} \mathfrak{m}_K$ and $x \equiv 1 \bmod^{\times} \mathfrak{n}_K$ imply $x \equiv 1 \bmod^{\times} \mathfrak{m}_K\mathfrak{n}_K$.

We now show that the map is onto. Let a and b be representatives of elements of $Q_{K,\mathfrak{m}}$ and $Q_{K,\mathfrak{n}}$ respectively. By theorem A.3.1, we can find $x \in K$ such that:

- $\mathrm{ord}_w(x - b/a) \geq \mathrm{ord}_w(\mathfrak{n}_K) - \mathrm{ord}_w(a)$ for all $w \in \mathrm{supp}(\mathfrak{n}_K)$,
- $\mathrm{ord}_w(x - 1) \geq \mathrm{ord}_w(\mathfrak{m}_K)$ for all $w \in \mathrm{supp}(\mathfrak{m}_K)$,
- $\mathrm{sgn}_{K,\mathfrak{n}}(x) = \mathrm{sgn}_{K,\mathfrak{n}}(a/b)$,
- $\mathrm{sgn}_{K,\mathfrak{m}}(x)$ is the identity element of $\mathrm{Sgn}_{K,\mathfrak{m}}$.

For all $w \in \mathrm{supp}(\mathfrak{n}_K)$,

$$\mathrm{ord}_w(ax/b - 1) = \mathrm{ord}_w(x - b/a) + \mathrm{ord}_w(a) - \mathrm{ord}_w(b) \geq \mathrm{ord}_w(\mathfrak{n}_K),$$

since $\mathrm{ord}_w(b) = 0$. Also, $\mathrm{sgn}_{K,\mathfrak{n}}(ax/b)$ is the identity of $\mathrm{Sgn}_{K,\mathfrak{n}}$, so $y := ax/b \in K_1^{\mathfrak{n}}$. By construction, $x \in K_1^{\mathfrak{m}}$. Therefore $ax = by \in K^{\mathfrak{m}_K} \cap K^{\mathfrak{n}_K} = K^{\mathfrak{m}_K\mathfrak{n}_K}$, and it is clear that the equivalence class of $ax = by$ gets mapped to the equivalence classes of a and b in $Q_{K,\mathfrak{m}}$ and $Q_{K,\mathfrak{n}}$ respectively. □

Suppose now that $\mathfrak{m} = v^n$, where v is a place of k and $n \in \mathbb{N}^+$. We consider two cases:

Case 1: v archimedean

In this case $K^{\mathfrak{m}} = K^{\times}$. The natural map $K^{\mathfrak{m}} \to \mathrm{Sgn}_{K,\mathfrak{m}}$ is onto by proposition A.3.1, and has kernel $K_1^{\mathfrak{m}}$. Thus $Q_{K,\mathfrak{m}} \cong \mathrm{Sgn}_{K,\mathfrak{m}} \cong \bigoplus_{w|v} \mathbb{Z}/2\mathbb{Z}$ as an abelian group, and if we consider the natural action of G on $\bigoplus_{w|v} \mathbb{Z}/2\mathbb{Z}$, we see that $Q_{K,\mathfrak{m}} \cong (\mathbb{Z}/2\mathbb{Z})[G] \cong \mathbb{Z}[G]/2\mathbb{Z}[G]$ as a G-module.

Case 2: v non-archimedean

First we show that every element of $Q_{K,\mathfrak{m}}$ has a representative in $\mathcal{O}_K$. Given $x \in K^{\mathfrak{m}}$, the approximation theorem A.3.1 implies that we can find $y \in K^{\times}$ such that

- $\mathrm{ord}_w(y - 1) \geq \mathrm{ord}_w(\mathfrak{m})$ for all $w \in \mathrm{supp}(\mathfrak{m}_K)$,
- $\mathrm{ord}_w(y) \geq -\mathrm{ord}_w(x)$ for all non-archimedean $w \notin \mathrm{supp}(\mathfrak{m}_K)$,

[‖]We say that two moduli are relatively prime if no place divides both.

- $\mathrm{sgn}_{K,\mathfrak{m}}(y)$ is the identity of $\mathrm{Sgn}_{K,\mathfrak{m}}$.

Then $y \in K_1^{\mathfrak{m}}$ and $xy \in \mathcal{O}_K$.

Let $\mathfrak{p}$ be the ideal of $\mathcal{O}_k$ corresponding to v. Because every element of $Q_{K,\mathfrak{m}}$ has a representative in $\mathcal{O}_K$, $Q_{K,\mathfrak{m}}$ can be described as the multiplicative monoid $\mathcal{O}_K \cap K^{\mathfrak{m}} = \bigcap_{\mathfrak{P}|\mathfrak{p}}(\mathcal{O}_K \setminus \mathfrak{P})$ modulo the congruence

$$\begin{aligned} x \sim y \quad &\Leftrightarrow \quad \mathrm{ord}_w(x/y - 1) \geq n \text{ for all } w|v \\ &\Leftrightarrow \quad \mathrm{ord}_w(x - y) \geq n \text{ for all } w|v \text{ (since } \mathrm{ord}_w(y) = 0) \\ &\Leftrightarrow \quad x - y \in \mathfrak{p}^n\mathcal{O}_K. \end{aligned}$$

Any representative of an element of $(\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times$ must lie in $\bigcap_{\mathfrak{P}|\mathfrak{p}}(\mathcal{O}_K \setminus \mathfrak{P})$, so $Q_{K,\mathfrak{m}} \cong (\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times$.

4.2.2 Fitting ideals

Let R be a commutative unital ring, and let M be a finitely generated R-module. Choose a free presentation

$$F_1 \xrightarrow{f} F_0 \longrightarrow M \longrightarrow 0\,, \tag{4.2.6}$$

where F_0 has finite rank, equal to to n. The first Fitting ideal $\mathrm{Fitt}_R(M)$ is defined to be the image of

$$f^{(n)} : \textstyle\bigwedge_R^n F_1 \to \bigwedge_R^n F_0 \cong R.$$

It is clear that this is an ideal of R, and independent of the choice of isomorphism $\bigwedge_R^n F_0 \cong R$, but it takes more work to show that $\mathrm{Fitt}_R(M)$ does not depend on the choice of the presentation (see [Nor] theorem 1, p 58). One can define other Fitting ideals, but we will not make use of them and will thus refer to the first Fitting ideal as simply the Fitting ideal. Some properties of Fitting ideals can be found in appendix A.2.

Fitting ideals of a number of Galois module occur in connection with the Rubin-Stark conjecture, and it appears that the Fitting ideal of $Q_{K,\mathfrak{m}}$ plays a part. In appendix A.5.1 we show that

$$\delta_{K,v^n} := \begin{cases} (1 - \sigma_v^{-1}Nv)Nv^{n-1} & \text{if } v \text{ is non-archimedean} \\ 2 & \text{if } v \text{ is archimedean} \end{cases}$$

is a generator of $\mathrm{Fitt}_{\mathbb{Z}[G]}(Q_{K,v^n})$.

To define $\delta_{K,\mathfrak{m}}$ in general, write $\mathfrak{m} = \prod_{v|\mathfrak{m}} \mathfrak{a}_v$, where $\mathfrak{a}_v = v^{n_v}$, $n_v \in \mathbb{N}^+$. We then define $\delta_{K,\mathfrak{m}} = \prod_{v|\mathfrak{m}} \delta_{K,\mathfrak{a}_v}$, and the direct sum decomposition of $Q_{K,\mathfrak{m}}$, together with the fact that $\mathrm{Fitt}_{\mathbb{Z}[G]}$ is multiplicative on direct sums (see appendix A.2), shows that $\mathrm{Fitt}_{\mathbb{Z}[G]}(Q_{K,\mathfrak{m}})$ is generated by $\delta_{K,\mathfrak{m}}$.

Remark 4.2.1. By checking cases, one sees that $|\mathrm{aug}_G(\delta_{K,\mathfrak{m}})| = \#Q_{k,\mathfrak{m}}$. One could also prove this using the fact that $Q_{K,\mathfrak{m}}$ is cohomologically trivial (proposition A.5.1), and that for a cohomologically trivial G-module A, $\pi\left(\mathrm{Fitt}_{\mathbb{Z}[G]}(A)\right) = \mathrm{Fitt}_{\mathbb{Z}[G/H]}(A^H)$, where H is a normal subgroup of G and $\pi : \mathbb{Z}[G] \to \mathbb{Z}[G/H]$ is the ring homomorphism coming from the quotient map $G \to G/H$ (take $H = G$, and observe that $Q^G_{K,\mathfrak{m}} \cong Q_{k,\mathfrak{m}}$, as one sees by checking cases or by using lemma A.6.2).

4.3 The Stickelberger function

Let S be a finite set of places of k containing all archimedean places. We define the S-modified Stickelberger function by

$$\Theta_S(s;K/k) = \sum_{\chi\in\widehat{G}} L_S(s,\bar{\chi})e_\chi \in \mathbb{C}[G] \qquad (s \in \mathbb{C}\setminus\{1\}). \tag{4.3.1}$$

If S also contains all places which ramify in K/k, there is another way of defining $\Theta_S(s;K/k)$:

Proposition 4.3.1. *([Tat84] proposition 1.6, p 86) For $s \in \mathbb{C}$ with $\Re(s) > 1$,*

$$\Theta_S(s;K/k) \quad = \quad \prod_{v\notin S} \left(1 - Nv^{-s}\sigma_v^{-1}\right)^{-1}\,^{**}. \tag{4.3.2}$$

Proof. For every $\chi \in \widehat{G}$, extended by linearity to $\mathbb{C}[G]$,

$$\begin{aligned}\chi(\Theta_S(s)) = L_S(s,\chi) &= \prod_{v\notin S} \det\left(1 - Nv^{-s}\sigma_v^{-1}|V\right)^{-1} \\ = \prod_{v\notin S} \chi\left(1 - Nv^{-s}\sigma_v^{-1}\right)^{-1} &= \chi\left(\prod_{v\notin S}(1 - Nv^{-s}\sigma_v^{-1})^{-1}\right).\end{aligned}$$

The last equality comes from the fact that $\chi : \mathbb{C}[G] \to \mathbb{C}$ is continuous, as one can easily verify. □

Let H be a subgroup of $G = \mathrm{Gal}(K/k)$, with L the fixed field of H. Let $\pi : \mathbb{C}[G] \to \mathbb{C}[G/H]$ be the $\mathbb{C}$-algebra homomorphism induced by the quotient map $G \to G/H$.

** $\mathbb{C}[G]$ with the norm $\|\sum_{\sigma\in G} n_\sigma\sigma\| = \sqrt{g\sum_{\sigma\in G}|n_\sigma|^2}$ is a Banach algebra.

Proposition 4.3.2. *([Tat84] proposition 1.8, p 87) With the notation as above,*

$$\pi(\Theta_S(s;K/k)) \quad = \quad \Theta_S(s;L/k)$$

Proof. For every $\chi \in \widehat{G/H}$,

$$\chi(\pi(\Theta_S(s;K/k))) = L_S(s, \mathrm{Infl}\chi; K/k) = L_S(s,\chi;L/k) = \chi(\Theta_S(s;L/k)),$$

and so $\pi(\Theta_S(s;K/k)) = \Theta_S(s;k'/k)$.

□

The S-modified Stickelberger function $\Theta_S(s)$ extends to a meromorphic function on $\mathbb{C}$ which is analytic at $s = 0$††. Define

$$r_{K/k,S} = \mathrm{ord}_{s=0}\Theta_S(s;K/k) = \min\{r_{K/k,S}(\chi) : \chi \in \widehat{G}\},$$

and for $r = 0, 1, \ldots, r_{K/k,S}$, define

$$\Theta^{(r)}_{K/k,S} = \lim_{s\to 0} s^{-r}\Theta_S(s;K/k) = \frac{1}{r!}\frac{d^r}{ds^r}\Theta_S(s;K/k)\bigg|_{s=0} \in \mathbb{C}[G],$$

and $\Theta^{(r)}_{K/k,S,\mathfrak{m}} = \delta_{K,\mathfrak{m}}\Theta^{(r)}_{K/k,S}$ ‡‡. We shall usually omit the subscript K/k when there is no confusion as to the extension concerned.

Remark 4.3.1. We could define $\Theta_{S,\mathfrak{m}}(s)$ by defining an analytic $\mathbb{C}[G]$-valued function $\delta_{\mathfrak{m}}(s)$ which is equal to $\delta_{\mathfrak{m}} \in \mathbb{C}[G]$ (as we have defined it) at $s = 0$. When $\mathfrak{m}$ is the product of distinct non-archimedean places, which is essentially the case considered by Rubin in [Rub96], one defines $\delta_{\mathfrak{m}}(s) = \prod_{v|\mathfrak{m}}(1 - \sigma_v^{-1}Nv^{1-s})$. This ensures that $\Theta_{S,\mathfrak{m}}(-n) \in \mathbb{Z}[G]$ for all $n \in \mathbb{N}$, thanks to a theorem of Deligne and Ribet (see [DR80]). However, since we are only interested in the value of $\Theta_S(s)$ at $s = 0$, we will not be concerned with extending the definition of $\delta_{\mathfrak{m}}(s)$ to the case where $\mathfrak{m}$ is not the product of distinct non-archimedean places.

A final definition: Let $\lambda_{K,S,\mathfrak{m}} : \mathbb{R}U_{K,S,\mathfrak{m}} \to \mathbb{R}X_{K,S}$ be the restriction of $\lambda_{K,S}$, and for any $r \in \mathbb{N}$, let

$$\lambda^{(r)}_{K,S,\mathfrak{m}} : \mathbb{R}\bigwedge^r_{\mathbb{Z}[G]}U_{K,S,\mathfrak{m}} \cong \bigwedge^r_{\mathbb{R}[G]}\mathbb{R}U_{K,S,\mathfrak{m}} \to \bigwedge^r_{\mathbb{R}[G]}\mathbb{R}X_{K,S} \cong \mathbb{R}\bigwedge^r_{\mathbb{Z}[G]}X_{K,S}$$

be the isomorphism induced by $\lambda_{K,S,\mathfrak{m}}$.

††We may identify the underlying topological space of $\mathbb{C}[G]$ with $\mathbb{C}^g$; the terms meromorphic and analytic are used in this sense.

‡‡Of course, $\Theta^{(r)}_{K/k,S,\mathfrak{m}} = \Theta^{(r)}_{K/k,S} = 0$ if $r < r_{K/k,S}$. It should be noted that in most of the relevent literature, $\Theta^{(r)}_{K/k,S}$ is usually denoted by $\Theta^{(r)}_{K/k,S}(0)$. Since we will not be concerned with the value of $\Theta^{(r)}_{K/k,S}(s)$ at any point other than $s = 0$, we have opted to simplify the notation by omitting the (0).

Chapter 5

Rubin's refinement of Stark's conjecture in the abelian case

In [Sta80], Stark made some refined conjectures about the first derivatives of Artin L-functions in the case where the extension K/k was abelian and all L-functions associated to irreducible characters of the Galois group had order of vanishing at least 1. In cases where the order of vanishing of all L-functions is strictly greater than 1, the first derivatives are zero, and these conjectures are trivial. In [Rub96], Rubin extended Stark's refined conjectures for abelian extensions to give not-necessarily-trivial statements about higher-order derivatives of the corresponding L-functions.

5.1 Statement of Rubin's conjecture

We will in fact state a slightly more general version of Rubin's integral refinement of Stark's conjecture, although, as we shall see, this follows from Rubin's original conjecture in most cases.

Consider the following hypotheses:

Hypotheses $\mathbf{H}(K/k, S, \mathfrak{m}, r)$:

i) S is a finite set of places of k containing all archimedean places and all places ramified in K/k.

ii) $\mathfrak{m}$ is a modulus of k, such that $\operatorname{supp}(\mathfrak{m}) \cap S = \emptyset$, and such that no real archimedean place dividing $\mathfrak{m}$ is ramified in K/k.

iii) $U_{K,S,\mathfrak{m}}$ is torsion-free.

iv) At least r places of S split completely in K/k.

v) $r \leq \#S - 1$.

Remark 5.1.1. Condition iii) is easily satisfied. For example, if there is an archimedean place dividing $\mathfrak{m}$, then K has a real archimedean place, whence $\mu_K = \{1, -1\}$ and $\mu_{F,\mathfrak{m}} = \{1\}$.

Alternatively, if ζ is an non-trivial root of unity in $U_{K,S,\mathfrak{m}}$,

$$N_{K/\mathbf{Q}}(1-\zeta) = N_{\mathbf{Q}(\zeta)/\mathbf{Q}}\left(N_{K/\mathbf{Q}(\zeta)}(1-\zeta)\right) = N_{\mathbf{Q}(\zeta)/\mathbf{Q}}\left(1-\zeta\right)^{[K:\mathbf{Q}(\zeta)]},$$

and since

$$N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(1-\zeta) = \begin{cases} p & n \text{ is a power of } p \\ 1 & \text{otherwise} \end{cases} \tag{5.1.1}$$

(see [Was82] for example), one simply needs to choose $\mathfrak{m} = v$, a non-archimedean place where the characteristic of $\mathbb{F}(v)$ is prime to w_K, or choose $\mathfrak{m} = v_1 v_2$ where $\mathbb{F}(v_1)$ and $\mathbb{F}(v_2)$ have different characteristics. Even if the characteristic of $\mathbb{F}(v)$ is not prime to w_K, one could put $\mathfrak{m} = v^\ell$, where ℓ is chosen sufficiently large.

At times we will work with a subset of the five conditions above, and we write $\mathrm{H}(K/k, S)$ for i), $\mathrm{H}(K/k, S, \mathfrak{m})$ for i) – iii), and $\mathrm{H}(K/k, S, r)$ for i), iv) and v) of the hypotheses above.

Note that by remark 2.3.1, iv) and v) imply $r \leq r_{K/k,S}$, so $\Theta^{(r)}_{S,\mathfrak{m}}$ is well-defined. An (apparently) slightly stronger version of the conjecture put forward by Rubin ([Rub96] conjecture B, p 39) is:

Conjecture 5.1.1. $\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ *If hypotheses $\mathrm{H}(K/k, S, \mathfrak{m}, r)$ are satisfied, then*

$$\Theta^{(r)}_{K/k,S,\mathfrak{m}} \cdot \bigwedge{}^{r}_{\mathbf{Z}[G]} X_{K,S} \subseteq \lambda^{(r)}_{K,S,\mathfrak{m}}\left(\bigwedge{}^{r}_{\mathbf{Z}[G],0} U_{K,S,\mathfrak{m}}\right) \tag{5.1.2}$$

We will refer to this as the r-th order Rubin-Stark conjecture. Note that because $\delta_{K,\mathfrak{m}}$ generates $\mathrm{Fitt}_{\mathbf{Z}[G]}(Q_{K,\mathfrak{m}})$, 5.1.2 is equivalent to

$$\mathrm{Fitt}_{\mathbf{Z}[G]}(Q_{K,\mathfrak{m}}) \cdot \Theta^{(r)}_{K/k,S} \cdot \bigwedge{}^{r}_{\mathbf{Z}[G]} X_{K,S} \subseteq \lambda^{(r)}_{K,S,\mathfrak{m}}\left(\bigwedge{}^{r}_{\mathbf{Z}[G],0} U_{K,S,\mathfrak{m}}\right).$$

Remark 5.1.2. The conjecture proposed by Rubin in [Rub96] amounts to $\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ with the extra condition that $\mathfrak{m}$ be a product of distinct non-archimedean places.

Remark 5.1.3. It may happen that, given S and $\mathfrak{m}$ as above, the maximum r for which hypotheses $\mathrm{H}(K/k, S, \mathfrak{m}, r)$ are satisfied is strictly less than $r_{K/k,S}$, in which case Rubin's conjecture is trivially true. One may hope to generalise $\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ by conjecturing that if hypotheses $\mathrm{H}(K/k, S, \mathfrak{m})$ are satisfied, then 5.1.2 holds with $r = r_{K/k,S}$. However, according to Popescu ([Pop]), this is false. Instead, Popescu conjectures that a certain cyclic $\mathbb{Z}[G]$-submodule of

$$\Theta^{(r)}_{K/k,S,\mathfrak{m}} \cdot \bigwedge\nolimits^{r}_{\mathbb{Z}[G]} X_{K,S}, \quad r = r_{K/k,S}$$

is contained in the right-hand side of 5.1.2*. This submodule is generated by a certain element $\mathbf{w}_{S_{min}} \in \bigwedge^{r}_{\mathbb{Z}[G]} X_{K,S}$, which is a free generator of $e_S \cdot \mathbb{C} \bigwedge^{r}_{\mathbb{Z}[G]} X_{K,S}$ as an $e_S \cdot \mathbb{C}[G]$-module†.

5.1.1 An equivalent formulation

It is often more convenient to work with another version of Rubin's conjecture, which we derive in this subsection.

If hypotheses $\mathrm{H}(K/k, S, \mathfrak{m}, r)$ are satisfied, let $\Xi_{S,r}$ be the set of all characters $\chi \in \widehat{G}$ such that $r_S(\chi) = r$. Define

$$e_{S,r} = \sum_{\chi \in \Xi_{S,r}} e_\chi,$$

and note that $e_{S,r}\Theta^{(r)}_S = \Theta^{(r)}_S$.

Lemma 5.1.1. *([Rub96] lemma2.6 (ii), pp 41 - 42) Suppose hypotheses $H(K/k, S, r)$ are satisfied, and let $\{v_1, \ldots, v_r\}$ be a set of r places of S which split completely. If w is a place of S_K not dividing any v_i, then*

$$e_{S,r} \cdot w = \begin{cases} 0 & \text{if } \mathbf{1}_G \notin \Xi_{S,r} \\ e_{\mathbf{1}_G} \cdot w & \text{if } \mathbf{1}_G \in \Xi_{S,r} \end{cases}$$

Proof. If $\chi \in \Xi_{S,r} \setminus \{e_{\mathbf{1}_G}\}$, then by remark 2.3.1, $\chi|_{D_w} \neq \mathbf{1}_{D_w}$. Thus

$$\begin{aligned} e_\chi \cdot w &= \frac{1}{g} \sum_{\sigma \in G} \bar{\chi}(\sigma)\sigma \cdot w \\ &= \frac{1}{g} \sum_{\mu \in D_w} \sum_{\sigma D_w \in G/D_w} \bar{\chi}(\sigma\mu)\sigma\mu \cdot w \\ &= \frac{1}{g} \sum_{\mu \in D_w} \bar{\chi}(\mu) \sum_{\sigma D_w \in G/D_w} \bar{\chi}(\sigma)\sigma \cdot w \\ &= 0. \end{aligned}$$

*This is under the assumption that $\mathfrak{m}$ is the product of distinct non-archimedean places, although this assumption does not appear to be necessary.

†Here e_S is the sum of the idempotents e_χ associated to those characters $\chi \in \widehat{G}$ for which $r_S(\chi) = r_{K/k,S}$. The definition of $\mathbf{w}_{S_{min}}$ can be found in [Emm06], while the proof that it is a free generator will appear in a forthcoming paper by Popescu.

□

Let $W = (w_0, w_1, \ldots, w_r)$ be an $(r+1)$-tuple of places of S_K, no two of which lie over the same place of k, and such that $w_1, \ldots, w_r$ split completely in K/k. Throughout the rest of this dissertation, whenever the symbol W reappears, it will be defined in this way. Define $\mathbf{x}_{K,S,W}$ to be the image of $(w_1 - w_0) \wedge \ldots \wedge (w_r - w_0)$ in $\Lambda\!\!\!\!-^{r}_{\mathbb{Z}[G]} X_{K,S}$.

Lemma 5.1.2. *([Rub96] lemma 2.6 (ii), pp 41 - 42) Under hypotheses $H(K/k, S, \mathfrak{m}, r)$, the $\mathbb{Z}[G]$-module $\Theta^{(r)}_{S,\mathfrak{m}} \Lambda\!\!\!\!-^{r}_{\mathbb{Z}[G]} X_S \subseteq \mathbb{C} \bigwedge^{r}_{\mathbb{Z}[G]} X_S$ is cyclic, generated by $\Theta^{(r)}_{S,\mathfrak{m}} \cdot \mathbf{x}_{S,W}$.*

Proof. It will be sufficient to show that $e_{S,r} \Lambda\!\!\!\!-^{r}_{\mathbb{Z}[G]} X_S$ is generated by $e_{S,r} \cdot \mathbf{x}_{S,W}$. Put $v_i = w_i|_k$ for $i = 1, \ldots, r$, and let $T = S \setminus \{v_1, \ldots, v_r\}$. Every $x \in X_S$ can be written as

$$x = \sum_{i=1}^{r} \alpha_i \cdot (w_i - w_0) + \sum_{v \in T} \beta_v \cdot \bar{v},$$

for some $\alpha_i, \beta_v \in \mathbb{Z}[G]$. Observe that $\sum_{v \in T} \mathrm{aug}_G(\beta_v) = \mathrm{aug}_K\left(\sum_{v \in T} \beta_v \cdot \bar{v}\right) = 0$.

Suppose $\mathbf{1}_G \in \Xi_{S,r}$. Then $\#S = r + 1$ and so the sum $\sum_{v \in T} \beta_v \cdot \bar{v}$ consists of only one term, say $\beta_v \cdot \bar{v}$. By lemma 5.1.1 and the observation above,

$$e_{S,r} \cdot (\beta_v \cdot \bar{v}) = \beta_v e_{\mathbf{1}_G} \cdot \bar{v} = \mathrm{aug}_G(\beta_v) e_{\mathbf{1}_G} \cdot \bar{v} = 0.$$

Therefore if $x_1 \wedge \ldots \wedge x_r$ is a monomial in $\bigwedge^{r}_{\mathbb{Z}[G]} X_S$,

$$e_{S,r} \cdot (x_1 \wedge \ldots \wedge x_r) = (e_{S,r} \cdot x_1) \wedge \ldots \wedge (e_{S,r} \cdot x_r) = \alpha \cdot (w_1 - w_0) \wedge \ldots \wedge (w_r - w_0)$$

for some $\alpha \in \mathbb{Z}[G]$.

Now suppose $\mathbf{1}_G \notin \Xi_{S,r}$. Every monomial $x_1 \wedge \ldots \wedge x_r \in \bigwedge^{r}_{\mathbb{Z}[G]} X_S$ can be written in the form

$$\alpha \cdot (w_1 - w_0) \wedge \ldots \wedge (w_r - w_0) + \sum_{\mathbf{y}} \alpha_{\mathbf{y}} \cdot \mathbf{y},$$

where each $\mathbf{y}$ is a monomial containing at least one element of T_K. By lemma 5.1.1, $e_{S,r} \cdot \mathbf{y} = 0$. □

Suppose hypotheses $\mathrm{H}(K/k, S, \mathfrak{m}, r)$ are satisfied, and let W be as before. Define $\varepsilon_{K,S,W} \in \mathbb{C} \bigwedge^{r}_{\mathbb{Z}[G]} U_{K,S}$ by

$$\varepsilon_{K,S,W} = \Theta^{(r)}_{K/k,S} \cdot (\lambda^{-1}_{K,S})^{(r)}(\mathbf{x}_{K,S,W}).$$

Observe that

$$\begin{aligned} & \Theta^{(r)}_{K/k,S,\mathfrak{m}} \cdot \Lambda\!\!\!\!-^{r}_{\mathbb{Z}[G]} X_{K,S} \subseteq \lambda^{(r)}_{K,S,\mathfrak{m}} \left(\bigwedge^{r}_{\mathbb{Z}[G],0} U_{K,S,\mathfrak{m}} \right) \\ \Leftrightarrow \quad & \Theta^{(r)}_{K/k,S,\mathfrak{m}} \cdot \mathbf{x}_{K,S,W} \in \lambda^{(r)}_{S,\mathfrak{m}} \left(\bigwedge^{r}_{\mathbb{Z}[G],0} U_{K,S,\mathfrak{m}} \right) \\ \Leftrightarrow \quad & \delta_{K,\mathfrak{m}} \cdot \varepsilon_{K,S,W} = \Theta^{(r)}_{K/k,S,\mathfrak{m}} \cdot (\lambda^{-1}_{S,\mathfrak{m}})^{(r)}(\mathbf{x}_{K,S,W}) \in \bigwedge^{r}_{\mathbb{Z}[G],0} U_{K,S,\mathfrak{m}}, \end{aligned}$$

and so we have the following formulation of Rubin's conjecture:

Conjecture 5.1.2. *RS* $(K/k, S, \mathfrak{m}, r)$ If hypotheses $H(K/k, S, \mathfrak{m}, r)$ are satisfied, then*

$$\delta_{K,\mathfrak{m}}\cdot\varepsilon_{K,S,W} \in \bigwedge^r_{\mathbb{Z}[G],0} U_{K,S,\mathfrak{m}}.$$

Note that this is independent of the choice of W.

Lemma 5.1.2 shows that $\Theta^{(r)}_{S,\mathfrak{m}}\cdot\bigwedge^r_{\mathbb{Z}[G]} X_S$ is a cyclic $\mathbb{Z}[G]$-module, and so it is a cyclic $e_{S,r}\mathbb{Z}[G]$-module. It turns out that more is true. The set S_K is by definition a $\mathbb{Z}$-basis for the free abelian group $Y_{K,S}$. This gives us a dual basis $\mathbb{Z}$-basis $\{w^\circ : w \in S_K\}$ for $\mathrm{Hom}_{\mathbb{Z}}(Y_{K,S}, \mathbb{Z})$, and we define w^* to be the image of w° under the natural isomorphism $\mathrm{Hom}_{\mathbb{Z}}(Y_{K,S}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}[G]}(Y_{K,S}, \mathbb{Z}[G])$ (see equation A.1.3). In other words,

$$w^*(w') = \sum_{\sigma\in G} w^\circ(\sigma\cdot w')\sigma^{-1}.$$

Let W be as above. Define $\phi_{K,S,W} = \iota(w_1^*\wedge\ldots\wedge w_r^*) \in \left(\bigwedge^r_{\mathbb{Z}[G]} Y_{K,S}\right)^* = \left(\bigwedge^r_{\mathbb{Z}[G]} Y_{K,S}\right)^*$. Then $\phi_{K,S,W}(\mathbf{x}_{K,S,W}) = 1$ (we may regard $\mathbf{x}_{K,S,W}$ as an element of $\bigwedge^r_{\mathbb{Z}[G]} Y_{K,S}$ by proposition 4.1.1). Thus, for any $\alpha \in \mathbb{Z}[G]$, $\alpha\cdot\mathbf{x}_{K,S,W} = 0 \Rightarrow \alpha = 0$. This shows that $\Theta^{(r)}_{S,\mathfrak{m}}\cdot\bigwedge^r_{\mathbb{Z}[G]} X_S$ is a free rank 1 $e_{S,r}\mathbb{Z}[G]$-module.

Remark 5.1.4. Rubin and other authors define a $\mathbb{Z}[G]$-lattice

$$\Lambda_{S,\mathfrak{m}} = \left\{u \in \bigwedge^r_{\mathbb{Z}[G],0} U_{S,\mathfrak{m}} : e_{S,r}\cdot u = u\right\},$$

and a so-called regulator map: $\eta_W := \phi_{K,S,W} \circ \lambda^{(r)}_{K,S} : \mathbb{C}\Lambda_{S,\mathfrak{m}} \to e_{S,r}\mathbb{C}[G]$, which can be shown to be an isomorphism of $\mathbb{C}[G]$-modules. One can show that $\varepsilon_{K,S,W,\mathfrak{m}} := \delta_{K,\mathfrak{m}}\cdot\varepsilon_{K,S,W}$ is the unique element of $\mathbb{C}\Lambda_{S,\mathfrak{m}}$ that gets mapped to $\Theta^{(r)}_{S,\mathfrak{m}} \in e_{S,r}\mathbb{C}[G]$ by η_W, and an equivalent formulation of the Rubin-Stark conjecture would be to conjecture that $\varepsilon_{K,S,W,\mathfrak{m}} \in \Lambda_{S,\mathfrak{m}}$ (we identify $\Lambda_{S,\mathfrak{m}}$ with its image in $\mathbb{C}\Lambda_{S,\mathfrak{m}}$).

5.2 Relation to Stark's principal conjecture

Let $\mathbb{Q}\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ be $\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ with $\lambda^{(r)}_{K,S,\mathfrak{m}}\left(\bigwedge^r_{\mathbb{Z}[G],0} U_{K,S,\mathfrak{m}}\right)$ replaced by $\mathbb{Q}\lambda^{(r)}_{K,S,\mathfrak{m}}\left(\bigwedge^r_{\mathbb{Z}[G],0} U_{K,S,\mathfrak{m}}\right)$ in equation 5.1.2.

The following proposition shows how Stark's principal conjecture is related to Rubin's refinement.

Proposition 5.2.1. *([Rub96] proposition 2.3, p 41) Let K/k be an abelian extension with Galois group G. Under hypotheses $H(K/k, S, \mathfrak{m}, r)$, conjecture $\mathbb{Q}RS(K/k, S, \mathfrak{m}, r)$ is true if and only if Stark's principal conjecture is true for all $\chi \in \Xi_{S,r}$.*

Proof. Firstly, note that since $\bigwedge^r_{\mathbf{Z}[G]} U_{S,\mathfrak{m}}$ is of finite index in $\bigwedge^r_{\mathbf{Z}[G],0} U_{S,\mathfrak{m}}$ and $U_{S,\mathfrak{m}}$ is of finite index in U_S,

$$\mathbb{Q}\lambda^{(r)}_{S,\mathfrak{m}}\left(\bigwedge\nolimits^r_{\mathbf{Z}[G],0} U_{S,\mathfrak{m}}\right) = \mathbb{Q}\lambda^{(r)}_S\left(\bigwedge\nolimits^r_{\mathbf{Z}[G]} U_S\right).$$

Since $\Theta^{(r)}_{S,\mathfrak{m}}$ is equal to $\Theta^{(r)}_S$ multiplied by an invertible element of $\mathbb{Q}[G]$, $\mathbb{Q}\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ is equivalent to

$$\Theta^{(r)}_S \cdot \mathbf{x}_{S,W} \in \mathbb{Q}\lambda^{(r)}_S\left(\bigwedge\nolimits^r_{\mathbf{Z}[G]} U_S\right).$$

Let $f : \mathbb{Q}X_S \to \mathbb{Q}U_S$ be a $\mathbb{Q}[G]$-isomorphism. Since every $\chi \in \widehat{G}$ is one-dimensional, $R(\chi, f) = \det(\lambda_S \circ f)_\chi$ (see remark 2.3.4). Define

$$\begin{aligned} a_S(\chi, f) &= \lim_{s\to 0} s^{-r} L_S(s,\chi)/R_S(\chi, f) \\ &= \begin{cases} A_S(\chi, f)^{-1} & \text{if } \chi \in \Xi_{S,r} \\ 0 & \text{if } \chi \notin \Xi_{S,r} \end{cases} \\ &= \begin{cases} c_S(\chi)/\det(\lambda_S \circ f)_\chi & \text{if } \chi \in \Xi_{S,r} \\ 0 & \text{if } \chi \notin \Xi_{S,r} \end{cases}, \end{aligned}$$

and put

$$\theta = \sum_{\chi\in\widehat{G}} a_S(\chi, f) e_{\bar{\chi}} = \sum_{\chi\in\Xi_{S,r}} a_S(\chi, f) e_{\bar{\chi}} \in \mathbb{C}[G].$$

Any $\alpha \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ acts on $\mathbb{C}[G]$ in the obvious way, and one sees immediately that $e^\alpha_{\bar{\chi}} = e_{\bar{\chi}^\alpha} = e_{\bar{\chi^\alpha}}$. Note that

$$\begin{aligned} &\text{Stark's conjecture is true for all } \chi \in \Xi_r \\ \Leftrightarrow\ & a_S(\chi, f)^\alpha = a_S(\chi^\alpha, f) \qquad (\forall\chi \in \Xi_r)\ (\forall\alpha \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})) \\ \Leftrightarrow\ & \theta^\alpha = \sum_{\chi\in\Xi_{S,r}} a_S(\chi, f)^\alpha e^\alpha_{\bar{\chi}} = \sum_{\chi\in\Xi_{S,r}} a_S(\chi^\alpha, f) e_{\bar{\chi^\alpha}} = \theta \qquad (\forall\alpha \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})) \\ \Leftrightarrow\ & \theta \in \mathbb{Q}[G]. \end{aligned}$$

If $\chi \in \Xi_{S,r}$, then $r = r_S(\chi) = \dim(e_{\bar{\chi}} \cdot \mathbb{C}X_S)$ and $\{e_{\bar{\chi}} \cdot (w_1 - w_0), \ldots, e_{\bar{\chi}} \cdot (w_r - w_0)\}$ is a basis for $e_{\bar{\chi}} \cdot \mathbb{C}X_S$. Therefore $(\lambda_S \circ f)^{(r)}(e_{\bar{\chi}} \cdot \mathbf{x}_{S,W}) = \det(\lambda_S \circ f)_\chi e_{\bar{\chi}} \cdot \mathbf{x}_{S,W}$, and so

$$\begin{aligned} \lambda^{(r)}_S \circ f^{(r)}(\theta \cdot \mathbf{x}_{S,W}) &= \theta \sum_{\chi\in\widehat{G}} (\lambda_S \circ f)^{(r)}(e_{\bar{\chi}} \cdot \mathbf{x}_{S,W}) \\ &= \left(\sum_{\chi\in\widehat{G}} a(\chi, f) e_{\bar{\chi}}\right)\left(\sum_{\chi\in\widehat{G}} \det(\lambda_S \circ f)_\chi e_{\bar{\chi}} \cdot \mathbf{x}_{S,W}\right) \\ &= \sum_{\chi\in\widehat{G}} \lim_{s\to 0} s^{-r} L_S(s,\chi) e_{\bar{\chi}} \cdot \mathbf{x}_{S,W} \\ &= \Theta^{(r)}_S \cdot \mathbf{x}_{S,W}. \end{aligned} \tag{5.2.1}$$

Suppose $\mathbb{Q}\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ holds true. Then

$$\lambda_S^{(r)} \circ f^{(r)}(\theta \cdot \mathbf{x}_{S,W}) = \Theta_S^{(r)} \cdot \mathbf{x}_{S,W} \in \mathbb{Q}\lambda_S^{(r)} \left(\bigwedge{}^r_{\mathbf{Z}[G]} U_S \right).$$

Therefore, since $\lambda_S^{(r)}$ is injective,

$$\theta \cdot \mathbf{x}_{S,W} \in \mathbb{Q}(f^{(r)})^{-1} \left(\bigwedge{}^r_{\mathbf{Z}[G]} U_S \right) = \mathbb{Q}\bigwedge{}^r_{\mathbf{Z}[G]} X_S,$$

so $\theta = \phi_{S,W}(\theta \cdot \mathbf{x}_{S,W}) \in \phi_{S,W}\left(\mathbb{Q} \bigwedge{}^r_{\mathbf{Z}[G]} X_S \right) \subseteq \mathbb{Q}[G]$.

Conversely, if $\theta \in \mathbb{Q}[G]$, then by equation 5.2.1, $\Theta_S^{(r)} \cdot \mathbf{x}_{S,W} = \lambda_S^{(r)} \circ f^{(r)}(\theta \mathbf{x}_{S,W}) \in \mathbb{Q}\lambda_S^{(r)} \left(\bigwedge{}^r_{\mathbf{Z}[G]} U_S \right)$, and so $\mathbb{Q}\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ is true. □

Remark 5.2.1. One seemingly unsatisfactory thing about this proposition is that the truth of Rubin's conjecture for the set of data $(K/k, S, r)$ only implies the validity of Stark's conjecture for characters χ satisfying $r_S(\chi) = r$. However, if the Rubin-Stark conjecture is true in general, then Stark's conjecture is true in general. We have shown that the principal Stark conjecture is true if it is true for all faithful characters, so let χ be a faithful character (of the Galois group of an abelian extension of number fields). Since Stark's conjecture is true for the trivial character, we may assume $\chi \neq \mathbf{1}_G$. Thus

$$r_S(\chi) = \#\{v \in S : \chi|_{D_v} = \mathbf{1}_{D_v}\} = \#\{v \in S : v \text{ splits completely in } K/k\}$$

Now let S be the set of archimedean places, those ramified in K/k, and some additional place which does not split completely in K/k [‡], so that $\#S \geq r_S(\chi) + 1$. It is easy to find $\mathfrak{m}$ such that hypotheses $\mathrm{H}(K/k, S, \mathfrak{m}, r_S(\chi))$ are satisfied (see remark 5.1.1), and by the previous proposition, Stark's principal conjecture is true for χ if $\mathbb{Q}\mathrm{RS}(K/k, S, \mathfrak{m}, r_S(\chi))$ is true.

5.3 Changing S

We wish to look at how increasing the set S affects the truth of the conjecture. It will suffice to consider the effect of adding a single place to S, so suppose v is place of k not in S, and put $S' = S \cup \{v\}$. In this section, K and $\mathfrak{m}$ will be fixed, so we omit them from the subscripts.

[‡]Our assumption that $\chi \neq \mathbf{1}_G$ implies that $K \neq k$, so by the Čebotarev density theorem (see [Nar90] theorem 7.11, p 382, for example) it is possible to find a non-archimedean, unramified place which does not split completely.

Proposition 5.3.1. *([Rub96] proposition 3.6, p 49) If hypotheses $H(K/k, S, \mathfrak{m}, r)$ are satisfied, then with the notation as above,*

$$RS(K/k, S, \mathfrak{m}, r) \Rightarrow RS(K/k, S', \mathfrak{m}, r).$$

Proof. Suppose $\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ holds. If we identify $\bigwedge^r_{\mathbb{Z}[G]} X_S$ with a submodule of $\bigwedge^r_{\mathbb{Z}[G]} X_{S'}$ (which we may do by proposition 4.1.1), then $\mathbf{x}_{S',W} = \mathbf{x}_{S,W}$. Consequently

$$\begin{aligned}\Theta_{S'}^{(r)} \cdot \mathbf{x}_{S',W} &= (1-\sigma_v)\Theta_S^{(r)} \cdot \mathbf{x}_{S,W} \\ &\in \lambda_S^{(r)}\left(\bigwedge^r_{\mathbb{Z}[G],0} U_S\right) \subseteq \lambda_{S'}^{(r)}\left(\bigwedge^r_{\mathbb{Z}[G],0} U_{S'}\right),\end{aligned}$$

and we are done by lemma 5.1.2. □

If v splits completely in K/k, then the order of vanishing of each L-function increases by one, so $\mathrm{RS}(K/k, S', \mathfrak{m}, r)$ is trivially true. One might hope to show that in this case $\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ implies $\mathrm{RS}(K/k, S', \mathfrak{m}, r+1)$, but it appears that stronger hypotheses are necessary for this to be true (see [Rub96], theorem 5.3, (iii)). However, the reverse implication does hold, namely

Proposition 5.3.2. *([Rub96] theorem 5.3 (i)) With the notation as above, if v splits completely, then*

$$RS(K/k, S', \mathfrak{m}, r+1) \Rightarrow RS(K/k, S, \mathfrak{m}, r).$$

Proof. Recall the definition of $w^* \in Y_S^*$ for $w \in S_K$ given in subsection 5.1.1. Let $\gamma = (\log Nv)^{-1}$, and define

$$\Phi_{\bar{v}} = \gamma \bar{v}^* \circ \lambda_{S'} : \mathbb{R}U_{S'} \to \mathbb{R}[G].$$

For every $u \in U_{S'}$,

$$\Phi_{\bar{v}}(\tilde{u}) = \gamma \bar{v}^* \left(\sum_{w \in S'_K} \log |u|_w w \right) = \gamma \sum_{w|v} \log |u|_w \bar{v}^*(w) = -\sum_{w|v} \mathrm{ord}_w(u) \bar{v}^*(w) \in \mathbb{Z}[G],$$

so we may regard restrict the domain and codomain of $\Phi_{\bar{v}}$ to obtain an element of $U_{S'}^*$. Define $W' = (w_0, w_1, \ldots, w_r, \bar{v})$, and note that if $\mathbf{x}_{S,W} = \tilde{\mathbf{x}}$, then $\mathbf{x}_{S',W'}$ is equal to the image of $\mathbf{x} \wedge (\bar{v} - w_0)$ in $\bigwedge^{r+1}_{\mathbb{Z}[G]} X_{S'}$. Therefore $\iota(\bar{v}^*)(\mathbf{x}_{S',W'}) = \pm \mathbf{x}_{S,W}$ §, and so

$$\begin{aligned}\iota(\bar{v}^* \circ \lambda_{S'})\left(\left(\lambda_{S'}^{-1}\right)^{(r+1)}(\mathbf{x}_{S',W'})\right) &= \left(\lambda_{S'}^{-1}\right)^{(r)}\left(\iota(\bar{v}^*)(\mathbf{x}_{S',W'})\right) \quad \text{(see eqn 4.1.3)} \\ &= \pm\left(\lambda_{S'}^{-1}\right)^{(r)}(\mathbf{x}_{S,W}) \\ &= \pm\left(\lambda_S^{-1}\right)^{(r)}(\mathbf{x}_{S,W}).\end{aligned}$$

§ the sign depends on the parity of r, but is irrelevant for our purposes.

Thus, since $\Theta_{S'}^{(r+1)} = \log Nv\Theta_S^{(r)} = \gamma^{-1}\Theta_S^{(r)}$,

$$\begin{aligned}\varepsilon_{S,W} &= \Theta_S^{(r)}\cdot\left(\lambda_S^{-1}\right)^{(r)}(\mathbf{x}_{S,W})\\ &= \pm\gamma\Theta_{S'}^{(r+1)}\cdot\iota(\bar{v}^*\circ\lambda_{S'})\left(\left(\lambda_{S'}^{-1}\right)^{(r+1)}(\mathbf{x}_{S',W'})\right)\\ &= \pm\iota(\gamma\bar{v}^*\circ\lambda_{S'})\left(\Theta_{S'}^{(r+1)}\cdot\left(\lambda_{S'}^{-1}\right)^{(r+1)}(\mathbf{x}_{S',W'})\right)\\ &= \pm\iota(\Phi_{\bar{v}})(\varepsilon_{S',W'}).\end{aligned}$$

If RS$(K/k,S,\mathfrak{m},r+1)$ holds, $\varepsilon_{S',W'}\in\bigwedge_{\mathbb{Z}[G],0}^{r+1}U_{S'}$ and so $\varepsilon_{S,W}\in\bigwedge_{\mathbb{Z}[G],0}^{r}U_{S'}$. It is not hard to show that $U_{S'}/U_S$ is torsion-free, so corollary 4.1.1 implies that $U_{S'}^*\to U_S^*$ is onto. Therefore, given $\phi\in\bigwedge_{\mathbb{Z}[G]}^{r}U_S^*$, we can find $\phi'\in\bigwedge_{\mathbb{Z}[G]}^{r}U_{S'}^*$ such that

$$\iota(\phi)(\varepsilon_{S,W}) = \iota(\phi')(\varepsilon_{S,W})\in\mathbb{Z}[G].$$

Thus $\varepsilon_{S,W}\in\bigwedge_{\mathbb{Z}[G],0}^{r}U_S$. □

5.4 Changing $\mathfrak{m}$

Since K and S will be fixed in this section, we omit them from subscripts in most cases, and write $Q_\mathfrak{m}=Q_{K,\mathfrak{m}}$, $U=U_{K,S}$, $U_\mathfrak{m}=U_{K,S,\mathfrak{m}}$, etc. We will show that it is sufficient to prove the Rubin-Stark conjecture for minimal moduli $\mathfrak{m}$; in other words,

Proposition 5.4.1. *Suppose* $\mathfrak{m}|\mathfrak{m}'$, *and that hypotheses* $H(K/k,S,\mathfrak{m},r)$ *and* $H(K/k,S,\mathfrak{m}',r)$ *are satisfied. Then*

$$RS(K/k,S,\mathfrak{m},r)\Rightarrow RS(K/k,S,\mathfrak{m}',r)$$

Proof. (basic ideas taken from [Pop02] proposition 5.3.1, pp 17 - 18). It will be sufficient to show this under the assumption $\mathfrak{m}'=v\mathfrak{m}$, v a place of k.

Let $\Delta_{\mathfrak{m}'}^{\mathfrak{m}}$ be the kernel of the canonical homomorphism $Q_{\mathfrak{m}'}\to Q_\mathfrak{m}$. By looking at the direct sum decomposition of $Q_\mathfrak{m}$, one sees that $\Delta_{\mathfrak{m}'}^{\mathfrak{m}}$ is the kernel of the homomorphism $Q_{v^{n+1}}\to Q_{v^n}$, where n is the largest power of v dividing $\mathfrak{m}$ (which may be 0). If $n=0$, then $\Delta_{\mathfrak{m}'}^{\mathfrak{m}}\cong Q_v$, which is either $\mathbb{Z}[G]/2\mathbb{Z}[G]$ or $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^\times\cong\mathbb{Z}[G]/\delta_v\mathbb{Z}[G]$¶, depending on whether v is archimedean or non-archimedean. If $n>0$, then v is non-archimedean and $\Delta_{\mathfrak{m}'}^{\mathfrak{m}}$ is the kernel of

$$(\mathcal{O}_K/\mathfrak{p}^{n+1}\mathcal{O}_K)^\times\to(\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times$$

($\mathfrak{p}$ the prime ideal of $\mathcal{O}_k$ corresponding to v), and this can be shown to be isomorphic to $\bigoplus_{i=1}^{f}\mathbb{Z}[G]/p\mathbb{Z}[G]$, where p is the characteristic of $\mathbb{F}(v)$ and $f=f(\mathfrak{p}/p\mathbb{Z})$ (see equation A.5.3). Observe that in each case, $\mathrm{Ext}^1_{\mathbb{Z}[G]}(\Delta_{\mathfrak{m}'}^{\mathfrak{m}},\mathbb{Z}[G])\cong\Delta_{\mathfrak{m}'}^{\mathfrak{m}}$.

¶See appendix A.5.1.

Let $\mathcal{I}_{\mathfrak{m}}$ and $\mathcal{I}_{\mathfrak{m}'}$ be the images of U in $Q_{\mathfrak{m}}$ and $Q_{\mathfrak{m}'}$ respectively (under the map in the long exact sequence 4.2.2), so that we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_{\mathfrak{m}'} & \longrightarrow & U & \longrightarrow & \mathcal{I}_{\mathfrak{m}'} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow = & & \downarrow & & \\ 0 & \longrightarrow & U_{\mathfrak{m}} & \longrightarrow & U & \longrightarrow & \mathcal{I}_{\mathfrak{m}} & \longrightarrow & 0 \end{array}$$

Define

$$\mathcal{I}^{\mathfrak{m}}_{\mathfrak{m}'} = U_{\mathfrak{m}}/U_{\mathfrak{m}'} \cong \ker(\mathcal{I}_{\mathfrak{m}'} \to \mathcal{I}_{\mathfrak{m}}) \subseteq \Delta^{\mathfrak{m}}_{\mathfrak{m}'}.$$

Since $\Delta^{\mathfrak{m}}_{\mathfrak{m}'}$ is finite, $\left(\mathcal{I}^{\mathfrak{m}}_{\mathfrak{m}'}\right)^* = 0$. By lemma 4.1.1, we have the exact sequences

$$0 \to U^*_{\mathfrak{m}} \to U^*_{\mathfrak{m}'} \to \mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathcal{I}^{\mathfrak{m}}_{\mathfrak{m}'}, \mathbb{Z}[G]) \to 0,$$
$$\mathrm{Ext}^1_{\mathbb{Z}[G]}(\Delta^{\mathfrak{m}}_{\mathfrak{m}'}, \mathbb{Z}[G]) \to \mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathcal{I}^{\mathfrak{m}}_{\mathfrak{m}'}, \mathbb{Z}[G]) \to 0.$$

Thus $U^*_{\mathfrak{m}'}/U^*_{\mathfrak{m}}$ may be identified with a quotient module of $\mathrm{Ext}^1_{\mathbb{Z}[G]}(\Delta^{\mathfrak{m}}_{\mathfrak{m}'}, \mathbb{Z}[G]) \cong \Delta^{\mathfrak{m}}_{\mathfrak{m}'}$, and so

$$\mathrm{Fitt}_{\mathbb{Z}[G]}(\Delta^{\mathfrak{m}}_{\mathfrak{m}'}) \subseteq \mathrm{Fitt}_{\mathbb{Z}[G]}(U^*_{\mathfrak{m}'}/U^*_{\mathfrak{m}})$$

(see proposition A.2.1).

Lemma A.2.2 applied to the short exact sequence

$$0 \to U^*_{\mathfrak{m}} \to U^*_{\mathfrak{m}'} \to U^*_{\mathfrak{m}'}/U^*_{\mathfrak{m}} \to 0$$

gives

$$\mathrm{Fitt}_{\mathbb{Z}[G]}(\Delta^{\mathfrak{m}}_{\mathfrak{m}'}) \cdot \bigwedge\nolimits^r_{\mathbb{Z}[G]} U^*_{\mathfrak{m}'} \subseteq \bigwedge\nolimits^r_{\mathbb{Z}[G]} U^*_{\mathfrak{m}}. \tag{5.4.1}$$

In appendix A.5.1, we show that $\mathrm{Fitt}_{\mathbb{Z}[G]}(\Delta^{\mathfrak{m}}_{\mathfrak{m}'})\mathrm{Fitt}_{\mathbb{Z}[G](Q_{\mathfrak{m}})} = \mathrm{Fitt}_{\mathbb{Z}[G](Q_{\mathfrak{m}'})}$, so $\mathrm{Fitt}_{\mathbb{Z}[G]}(\Delta^{\mathfrak{m}}_{\mathfrak{m}'})$ is generated by $\delta_{\mathfrak{m}'}/\delta_{\mathfrak{m}}$. Therefore 5.4.1 is equivalent to

$$\delta^{\mathfrak{m}}_{\mathfrak{m}'} \cdot \bigwedge\nolimits^r_{\mathbb{Z}[G]} U^*_{\mathfrak{m}'} \subseteq \bigwedge\nolimits^r_{\mathbb{Z}[G]} U^*_{\mathfrak{m}}.$$

Thus for any $\phi \in \bigwedge^r_{\mathbb{Z}[G]} U^*_{\mathfrak{m}'}$, we have $\delta^{\mathfrak{m}}_{\mathfrak{m}'} \cdot \phi \in \bigwedge^r_{\mathbb{Z}[G]} U^*_{\mathfrak{m}}$, and so

$$\iota(\phi)(\delta_{\mathfrak{m}'} \cdot \varepsilon_W) = \iota(\delta^{\mathfrak{m}}_{\mathfrak{m}'} \cdot \phi)(\delta_{\mathfrak{m}} \cdot \varepsilon_W) \in \mathbb{Z}[G].$$

□

Remark 5.4.1. *This shows that the only cases where conjecture RS($K/k, S, \mathfrak{m}, r$) might not follow from Rubin's original conjecture is where an archimedean place v divides $\mathfrak{m}$ and $\mathfrak{m}/v$, or where v^n ($n > 1$) divides $\mathfrak{m}$. Remark 5.1.1 implies that if the original Rubin-Stark conjecture holds, one need only check finitely many values of $\mathfrak{m}$ to determine whether RS($K/k, S, \mathfrak{m}, r$) holds for all $\mathfrak{m}$.*

5.5 Subextensions

We will show that the truth of the r-th order Rubin-Stark conjecture for K/k implies its truth for all normal subextensions.

Let H be a subgroup of G, and put $L = K^H$.

For the rest of this subsection, we omit the subscripts S and $\mathfrak{m}$, since these will be fixed. Thus $U_K = U_{K,S,\mathfrak{m}}$, $U_L = U_{L,S,\mathfrak{m}}$, etc. We will need the following lemma for the next proposition and the proof of the Rubin-Stark conjecture for quadratic extensions.

Lemma 5.5.1. *([Hay04] lemma 3.1, p 105)If hypotheses $H(K/k, S, \mathfrak{m}, r)$ are satisfied, then U_K/U_L is torsion-free.*

Proof. Let $u \in U_K$ be a representative of a torsion element of U_K/U_L. Then $u^n \in U_L$ for some non-zero integer n. But then for every $\sigma \in H$, $(u^{\sigma-1})^n = (u^n)^{\sigma-1} = 1$. Thus $u^{\sigma-1}$ is a torsion element of U_K, so $u^{\sigma-1} = 1$, and as this is true of all $\sigma \in H$, we have $u \in U_L$. □

Proposition 5.5.1. *With K, L and k as above, if hypotheses $H(K/k, S, \mathfrak{m}, r)$ are satisfied, then*

$$RS(K/k, S, \mathfrak{m}, r) \Rightarrow RS(L/k, S, \mathfrak{m}, r).$$

Proof. ([Hay04, Tat84]) It is clear that H$(K/k, S, \mathfrak{m}, r) \Rightarrow$ H$(L/k, S, \mathfrak{m}, r)$. Let $\Gamma = G/H$. By proposition 4.3.2, if $\pi : \mathbb{Z}[G] \to \mathbb{Z}[\Gamma]$ is the ring homomorphism coming from the quotient map $G \to G/H$, then $\pi\left(\Theta^{(r)}_{K/k}\right) = \Theta^{(r)}_{L/k}$. Note that we may identify the G-modules $\bigwedge^r_{\mathbb{Z}[G]} U_L$ and $\bigwedge^r_{\mathbb{Z}[\Gamma]} U_L$, if we give the latter a G-module structure using π. The same goes for $\bigwedge^r_{\mathbb{Z}[G]} X_L$ and $\bigwedge^r_{\mathbb{Z}[\Gamma]} X_L$. If $W = (w_0, w_1, \ldots, w_r)$, let $W|_L = (w_0|_L, w_1|_L, \ldots, w_r|_L)$. We will use the ad-hoc notation restr_L to denote the map $X_K \to X_L : x \mapsto x|_L$. Since $\Theta^{(r)}_{K/k} \cdot \mathbf{x}_{K,W} = \lambda^{(r)}_K(\varepsilon_{K,W})$, the commutative diagram 2.3.5 shows that

$$\begin{aligned} \Theta^{(r)}_{L/k} \cdot \mathbf{x}_{K,W|_L} &= \pi\left(\Theta^{(r)}_{K/k}\right) \cdot \mathbf{x}_{K,W|_L} \\ &= \mathrm{restr}^{(r)}_L\left(\Theta^{(r)}_{K/k} \cdot \mathbf{x}_{K,W}\right) = \mathrm{restr}^{(r)}_L\left(\lambda^{(r)}_K(\varepsilon_{K,W})\right) = \lambda^{(r)}_L\left(N^{(r)}_{K/L}(\varepsilon_{K,W})\right), \end{aligned}$$

and therefore $\varepsilon_{L,W|_L} = N^{(r)}_{K/L}(\varepsilon_{K,W})$.

By lemma 5.5.1,

$$0 \to U_L \to U_K \to U_K/U_L \to 0$$

is an exact sequence of $\mathbb{Z}[G]$-lattices. Corollary 4.1.1 implies that there is a surjective homomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(U_K, \mathbb{Z}[G]) \to \mathrm{Hom}_{\mathbb{Z}[G]}(U_L, \mathbb{Z}[G]),$$

and composing this with the isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(U_L, \mathbb{Z}[G]) \cong \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_L, \mathbb{Z}[\Gamma])$$

(see equation A.1.4) gives a surjection

$$\mathcal{N}_{K/L} : \mathrm{Hom}_{\mathbb{Z}[G]}(U_K, \mathbb{Z}[G]) \to \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_L, \mathbb{Z}[\Gamma]) : \varphi \mapsto (u \mapsto \pi(\varphi(u)_0)),$$

where $N_H \cdot \varphi(u)_0 = \varphi(u)$. Pick $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U_K, \mathbb{Z}[G])$, then for every $u \in U_K$,

$$\left[\mathcal{N}_{K/L}(\varphi) \circ N_{K/L}\right](u) = \mathcal{N}_{K/L}(\varphi)(N_H \cdot u) = \pi(\varphi(u)).$$

It follows that

$$\iota\left(\mathcal{N}^{(r)}_{K/L}(\varphi)\right)\left(N^{(r)}_{K/L}(\boldsymbol{u})\right) = \pi(\iota(\varphi)(\boldsymbol{u}))$$

for all $\varphi \in \bigwedge^r_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_K, \mathbb{Z}[G])$ and all $\boldsymbol{u} \in \bigwedge^r_{\mathbb{Z}[G]} U_K$.

Let $\phi \in \bigwedge^r_{\mathbb{Z}[\Gamma]} \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_L, \mathbb{Z}[\Gamma]) \cong \bigwedge^r_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_L, \mathbb{Z}[\Gamma])$ be given. Since $\mathcal{N}_{K/L}$ is surjective, there exists $\varphi \in \bigwedge^r_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_K, \mathbb{Z}[G])$ such that $\mathcal{N}^{(r)}_{K/L}(\varphi) = \phi$. The result follows from

$$\iota(\phi)(\varepsilon_{L,W|_L}) = \iota\left(\mathcal{N}^{(r)}_{K/L}(\varphi)\right)\left(N^{(r)}_{K/L}(\varepsilon_{K,W})\right) = \pi(\iota(\varphi)(\varepsilon_{K,W})) \in \pi(\mathbb{Z}[G]) = \mathbb{Z}[\Gamma].$$

□

5.6 Proofs of the Rubin-Stark conjecture in special cases

5.6.1 More than r places of S split completely

We follow [Rub96] proposition 3.1, pp 44 - 45. If more than r places split completely, remark 2.3.1 shows that for all $\chi \neq \mathbf{1}_G$ we have $r_S(\chi) > r$, and so $\lim_{s\to 0} s^{-r} L_S(s, \chi) = 0$. If $r < \#S - 1$, then $\lim_{s\to 0} s^{-r} L_S(s, \mathbf{1}_G) = 0$ as well and the conjecture is trivial. Thus we may suppose that $r = \#S - 1$, in which case all places in S split completely in K/k.

In this subsection, S and $\mathfrak{m}$ will be fixed, so we omit them from subscripts. Thus $U_k = U_{k,S,\mathfrak{m}}$, $R_K = R_{K,S,\mathfrak{m}}$, $h_K = h_{K,S,\mathfrak{m}}$, $\Theta^{(r)} = \Theta^{(r)}_{S,\mathfrak{m}}$, etc.

Let $S = \{v_0, v_1, \ldots, v_r\}$, and for $i = 1, \ldots, r$, define $x_i = v_i - v_0 \in X_k$ and $\bar{x}_i = \bar{v}_i - \bar{v}_0 \in X_K$. Let $\{u_i : i = 1, \ldots, r\}$ be a $\mathbb{Z}$-basis for U_k; then from the definition of the regulator,

$$\lambda^{(r)}_k(u_1 \wedge \ldots \wedge u_r) = \pm R_k x_1 \wedge \ldots \wedge x_r.$$

From the commutative diagram 2.3.4, we see that

$$\begin{aligned} \lambda^{(r)}_K(u_1 \wedge \ldots \wedge u_r) &= j^{(r)}_{K/k} \circ \lambda^{(r)}_k(u_1 \wedge \ldots \wedge u_r) \\ &= j^{(r)}_{K/k}(\pm R_k x_1 \wedge \ldots \wedge x_r) = \pm R_k (N_G \cdot \bar{x}_1) \wedge \ldots \wedge (N_G \cdot \bar{x}_r) \\ &= \pm R_k N_G^r \cdot \bar{x}_1 \wedge \ldots \wedge \bar{x}_r = \pm R_k \mathrm{g}^r e_{\mathbf{1}_G} \cdot \mathbf{x}_W, \end{aligned} \tag{5.6.1}$$

where $W = (\bar{v}_0, \ldots, \bar{v}_r)$. By remark 4.2.1 and equation 4.2.5,

$$\Theta^{(r)} = \delta_K \lim_{s \to 0} s^{-r} \zeta_k(s) e_{1_G} = \pm h_k R_k e_{1_G},$$

and this, together with 5.6.1, shows that

$$\varepsilon_W = \pm \frac{h_k}{g^r} u_1 \wedge \ldots \wedge u_r.$$

If $\phi \in \mathrm{Hom}_{\mathbb{Z}}(U_K, \mathbb{Z})$, let $\hat{\phi}$ be the image of ϕ under the isomorphism $\mathrm{Hom}_{\mathbb{Z}}(U_K, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}[G]}(U_K, \mathbb{Z}[G])$. To show that $\varepsilon_W \in \bigwedge^r_{\mathbb{Z}[G],0} U_K$, it is enough to show that if $\{\phi_i : i = 1, \ldots, r\}$ is a set of elements of $\mathrm{Hom}_{\mathbb{Z}}(U_K, \mathbb{Z})$, then

$$\frac{h_k}{g^r} \det\left(\hat{\phi}_j(u_i)\right) \in \mathbb{Z}[G].$$

Since G acts trivially on u_i, $\hat{\phi}_j(u_i) = \sum_{\sigma \in G} \phi_j(\sigma \cdot u_i)\sigma^{-1} = \phi_j(u_i) N_G$, and so

$$\begin{aligned} \frac{h_k}{g^r} \det\left(\hat{\phi}_i(u_j)\right) &= \frac{h_k}{g^r} \det\left(\phi_j(u_i) N_G\right) \\ &= \frac{h_k}{g^r} N_G^r \det\left(\phi_j(u_i)\right) = \frac{h_k}{g} N_G \det\left(\phi_j(u_i)\right). \end{aligned}$$

Since S contains all places which ramify, and all places in S split completely, K/k is unramified. Therefore g divides h_k by class-field theory‖, and we are done.

Note that this gives another proof of Stark's principal conjecture for trivial characters.

5.6.2 The case $r = 0$

Proposition 5.6.1. *If hypotheses $H(K/k, S, \mathfrak{m})$ are satisfied, then $\delta_{K,\mathfrak{m}} \in \mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)$.*

Proof. Condition iii) of hypotheses $H(K/k, S, \mathfrak{m})$, together with the exact sequence (4.2.2), implies that μ_K is embedded in $Q_{K,\mathfrak{m}}$. Thus

$$\delta_{K,\mathfrak{m}} \in \mathrm{Fitt}_{\mathbb{Z}[G]}(Q_{K,\mathfrak{m}}) \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(Q_{K,\mathfrak{m}}) \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)$$

(see appendix A.2 for the first inclusion). □

We consider the conjecture $RS(K/k, S, \mathfrak{m}, 0)$. If a place in S splits completely, we are done by the result of the previous subsection; otherwise, no places split completely, in which case k is totally real, K totally complex. The following theorem is a consequence of results in [DR80]:

‖see [Gra03].

Theorem 5.6.1. *If k is totally real and K is totally complex,*

$$\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)\cdot\Theta_{K/k,S}(0) \subseteq \mathbb{Z}[G].$$

Thus, by proposition 5.6.1,

$$\Theta^{(0)}_{K/k,S,\mathfrak{m}} = \delta_{K,\mathfrak{m}}\Theta_{K/k,S}(0) \in \mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)\cdot\Theta_{K/k,S}(0) \subseteq \mathbb{Z}[G]. \tag{5.6.2}$$

Since $\bigwedge^0_{\mathbb{Z}[G]} X_{K,S} \cong \lambda^{(0)}_{K,S,\mathfrak{m}}\left(\bigwedge^0_{\mathbb{Z}[G],0} U_{K,S,\mathfrak{m}}\right) \cong \mathbb{Z}[G]$, the Rubin-Stark conjecture follows. This shows that Stark's principal conjecture is true for characters χ with $r_S(\chi) = 0$, a fact which also follows from results of Siegel and Klingen ([Sie70]), and Shintani ([Shi76]).

If S satisfies hypotheses $\mathrm{H}(K/k, S)$, define

$$\mathcal{M}_{K/k,S} = \{\mathfrak{m} : \text{Hypotheses } \mathrm{H}(K/k, S, \mathfrak{m}) \text{ are satisfied}\}.$$

While we do not need it here, we will prove the following proposition for later reference:

Proposition 5.6.2. *([Tat84] lemme 1.1, p 82) If hypotheses $H(K/k, S)$ are satisfied, then $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)$ is generated as a $\mathbb{Z}[G]$-module by $\{\delta_{K,\mathfrak{m}} : \mathfrak{m} \in \mathcal{M}_{K/k,S}\}$.*

Proof. We will prove that $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)$ is equal to the $\mathbb{Z}[G]$-ideal $\mathcal{A}$ generated by

$$\{\delta_{K,v} : v \in \mathcal{M}_{K/k,S}, v \text{ a non-archimedean place of } k\}.$$

By proposition 5.6.1, $\mathcal{A} \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)$. For each $\sigma \in G$ we may find a non-archimedean place $v_\sigma \in \mathcal{M}_{K/k,S}$ whose Frobenius automorphism is σ[**]. Let $\sum_{\sigma\in G} a_\sigma\sigma$ be an element of $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)$. Then since

$$\sum_{\sigma\in G} a_\sigma\sigma = \sum_{\sigma\in G}(a_\sigma N v_\sigma + a_\sigma(\sigma - N v_\sigma)) = \sum_{\sigma\in G} a_\sigma N v_\sigma + \sum_{\sigma\in G} a_\sigma\sigma\delta_{v_\sigma},$$

it is enough to show that $\sum_{\sigma\in G} a_\sigma N v_\sigma \in \mathcal{A}$. But proposition 5.6.1 implies that $\sum_{\sigma\in G} a_\sigma N v_\sigma \in \mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)$, so must be a multiple of $w_K = \#\mu_K$ since μ_K is cyclic as an abelian group. Thus it remains to show that $w_K \in \mathcal{A}$.

Let d be the greatest common divisor of

$$\{\delta_v : v \in \mathcal{M}_{K/k,S}, v \text{ non-arch}, \sigma_v = 1\} = \{1 - Nv : v \in \mathcal{M}_{K/k,S}, v \text{ non-arch}, \sigma_v = 1\},$$

and let ζ be a primitive d-th root of unity. Let τ be an element of $\mathrm{Gal}(K(\zeta)/K) \subseteq \mathrm{Gal}(K(\zeta)/k)$[††]. Let S' be the union of S and all places of k which ramify in $K(\zeta)/k$.

[**]This follows from remark 5.1.1 and the Čebotarev density theorem.

[††]$K(\zeta)/k$ is Galois (in fact abelian), since $K(\zeta)$ is the compositum of K and $k(\zeta)$.

Then $\tau = (v, K(\zeta)/k)$ for some non-archimedean place $v \in \mathcal{M}_{K(\zeta)/k,S'}{}^{**}$. Note that by proposition 5.6.1, $\zeta^{1-Nv\tau^{-1}} = 1$. Since $(v, K/k) = \tau|_K = 1$, it follows that $d|1 - Nv$, and consequently $\zeta^{\tau} = \zeta^{Nv} = \zeta$. Thus τ is trivial on $K(\zeta)$, so $K(\zeta) = K$ and hence $\zeta \in K$. Therefore $d|w_K$, and we are done. □

5.6.3 Quadratic extensions

This proof follows [Rub96] theorem 3.5, pp 47 - 48. We consider extensions with Galois group $G \cong \mathbb{Z}/2\mathbb{Z}$. In this subsection, S and $\mathfrak{m}$ will be fixed, so we omit the subscripts S and $\mathfrak{m}$, and write $U_K = U_{K,S,\mathfrak{m}}$, $U_k = U_{k,S,\mathfrak{m}}$, $h_K = h_{K,S,\mathfrak{m}}$, $\varepsilon_{K,W} = \varepsilon_{K,S,W,\mathfrak{m}}$, etc.

Lemma 5.6.1. *([Rub96] lemma 3.4, p 46) Suppose that hypotheses $H(K/k, S, \mathfrak{m})$ hold, and in addition that G is cyclic and S contains an element v such that $D_v = G$. Then*

a) h_k divides h_K,

b) $\#H^1(G, U_K)$ divides h_k,

c) If G is a p-group (p prime) and $\widehat{H}^0(G, U_K) = H^1(G, U_K) = 0$, then h_K/h_k is prime to p iff h_k is prime to p.

Proof. Put $S' = S \setminus \{\text{real } v'|\mathfrak{m}\}$, and note that $v \in S'$ since any real archimedean place dividing $\mathfrak{m}$ splits completely in K/k. Let H_K (resp. H_k) be the $(S'_K, \mathfrak{m}_K)$-ray class field of K (resp. the $(S', \mathfrak{m})$-ray class field of k), so that we have isomorphisms $\mathrm{Gal}(H_K/K) \cong A_K$ and $\mathrm{Gal}(H_k/k) \cong A_k$†. Since all places in S' split completely in H_k, $H_k \cap K = k$ (otherwise v would split completely and be inert in a proper field extension of k). Therefore we have an onto map $\mathrm{Gal}(H_K/K) \to \mathrm{Gal}(H_k/k)$, which proves *i*).

The exact sequence

$$0 \to H^1(G, U_K) \to A_k \to A_K^G \to \widehat{H}^0(G, U_K) \tag{5.6.3}$$

(derived in appendix A.6) shows that *ii*) holds.

Under the assumptions of *iii*), 5.6.3 shows that $A_k \cong A_K^G$, and so we may view A_k as a subgroup of A_K.

Suppose $p|h_k$. Since $N^A_{K/k} : A_K \to A_k$ is corresponds to the map $\mathrm{Gal}(H_K/K) \to \mathrm{Gal}(H_k/k)$, it is surjective. Therefore to show that $p|(h_K/h_k)$, it suffices to show that p divides $\#\ker(N_{K/k})$. If $\check{N}_{K/k} : A_k \to A_k$ is the restriction of $N_{K/k}$ to A_k, then $\check{N}_{K/k}$ is

†If F is a number field, $H_{F,S,\mathfrak{m}}$ is defined to be maximum subextension of $H_{F,\mathfrak{m}}$ in which all places in S split completely. Details can be found in the book by Georges Gras ([Gra03]), but note that in his notation $H_{F,S,\mathfrak{m}} = F^{\bar{S}}_{(\mathfrak{m}_0)}$, where $\mathfrak{m}_0$ is the integral ideal corresponding to $\mathfrak{m}$ and $\bar{S} = S \setminus \{\text{complex archimedean places of } F\}$.

simply multiplication by g (if write A_k additively), and so $\#\ker(\check{N}_{K/k}) = \#\text{coker}(\check{N}_{K/k})$ is divisible by p (recall that g is a power of p). Since $\ker(\check{N}_{K/k})$ is a subgroup of $\ker(N_{K/k})$, the result follows.

Conversely, if $p|(h_K/h_k)$, then $p|h_K = \#A_K$, and since G is a p-group, $p|\#(A_K^G) = h_k$ (we use the fact that if a p-group Γ acts on a finite set B, then $\#B \equiv \#(B^\Gamma) \bmod p$ – see [Ser79] p138 for example). □

We wish to show that $\mathrm{RS}(K/k, S, \mathfrak{m}, r)$ holds if $[K/k] = 2$. Without loss of generality, we may assume $r = r_{K/k,S}$. Let χ be the non-trivial character of $\mathrm{Gal}(K/k) \cong \mathbb{Z}/2\mathbb{Z}$. If $r(\mathbf{1}_G) < r(\chi)$, then $r+1$ places split completely, so the conjecture is true by the result of subsection 5.6.1. Thus we may suppose $r(\mathbf{1}_G) \geq r(\chi)$, and that exactly r places split. Note that this implies $D_v = G$ for some $v \in S$. Define $d = \#(S) - r - 1$, so that $\#(S_K) = \#S + r = d + 2r + 1$.

By lemma 5.5.1, $U_K \cong U_k \bigoplus U_K/U_k$ (as abelian groups), so we may choose a $\mathbb{Z}$-basis $\{u_i : i = 1, \ldots, d+2r\}$ for U_K such that $\{u_i : i = 1, \ldots, d+r\}$ is a $\mathbb{Z}$-basis for U_k. By lemma A.7.1, we may assume that if $H^1(G, U_K) \neq 0$, then $N_{K/k}(u_{d+r+1}) = 1$.

Write $S = \{v_i : i = 1, \ldots, d+r+1\}$, and choose the numbering so that the places v_i, for $i = d+1, \ldots, d+r$, split completely. Write $S_K = \{w_i : i = 1, \ldots, d+2r+1\}$, and choose the numbering so that w_i is the unique place of K dividing v_i for $i = 1, \ldots, d$, w_i and w_{i+r} are the two places of K dividing v_i for $i = d+1, \ldots, d+r$, and w_{d+2r+1} is the unique place of K dividing v_{d+r+1}. With respect to the ordered $\mathbb{Z}$-bases $\{u_i : i = 1, \ldots, d+2r\}$ and $\{w_i - w_{d+2r+1} : i = 1, \ldots, d+2r\}$, λ_K is represented by the matrix $(\log|u_j|_{w_i})_{1\leq i,j\leq d+2r}$, which we can write in the form

$$\begin{pmatrix} A & B & B \\ C & D & E \end{pmatrix}^T$$

where A is $(d+r) \times d$, B is $(d+r) \times r$, C is $r \times d$, etc. Therefore

$$R_K = \pm\det\begin{pmatrix} A & B & B \\ C & D & E \end{pmatrix} = \pm\det\begin{pmatrix} A & B & 0 \\ C & D & E-D \end{pmatrix} = \pm\det(A\ B)\det(E-D).$$

Note that, for all $u \in U_k$, $|u|_{w_j} = |u|_{v_j}^2$ for $j = 1, \ldots, d$ and $|u|_{w_j} = |u|_{v_j}$ for $j = d+1, \ldots, d+r$. Therefore

$$\det(A\ B) = \det(\log|u_i|_{w_j})_{1\leq i,j\leq d+r} = 2^d\det(\log|u_i|_{v_j})_{1\leq i,j\leq d+r} = \pm 2^d R_k,$$

and so $R_K/R_k = \pm 2^d\det(E-D)$. Let σ be the non-trivial element of G. Since $w_{j+r} = \sigma\cdot w_j$ for $j = d+1, \ldots, d+r$,

$$\begin{aligned}\det(E-D) &= \det(\log|u_i|_{\sigma w_j} - \log|u_i|_{w_j})_{d+r<i,j\leq d+2r} \\ &= \det\left(\log|u_i^{\sigma-1}|_{w_j}\right)_{d+r<i,j\leq d+2r},\end{aligned}$$

Let ε_- be the image of $u_{d+r+1} \wedge \ldots \wedge u_{d+2r}$ in $\bigwedge^r_{\mathbb{Z}[G]} U_K$, so that

$$\begin{aligned}\lambda_K^{(r)}(e_\chi \cdot \varepsilon_-) &= \det\left(\log|u_i^{e_\chi}|_{w_j} + \log|u_i^{e_\chi}|_{\sigma w_j}\sigma\right)_{d+r<i,j\le d+2r} \cdot \mathbf{x}_W \\ &= \det\left(\log|u_i^{1-\sigma}|_{w_j} e_\chi\right)_{d+r<i,j\le d+2r} \cdot \mathbf{x}_W = \pm\det(E-D)e_\chi \cdot \mathbf{x}_W,\end{aligned}$$

where $W = (w_{d+2r+1}, w_{d+r+1}, \ldots, w_{d+2r})$.

We consider two cases:

Case 1: $r(\mathbf{1}_G) > r(\chi)$:

In this case $\Theta_{K/k}^{(r)} = \frac{h_K R_K}{h_k R_k} e_\chi = \pm\frac{2^d h_K}{h_k}\det(E-D)e_\chi$, and so

$$\varepsilon_W = \pm\frac{2^d h_K}{h_k} e_\chi \cdot \varepsilon_- \in \bigwedge{}^r_{\mathbb{Z}[G]} U_K \subseteq \bigwedge{}^r_{\mathbb{Z}[G],0} U_K$$

by $i)$ of lemma 5.6.1.

Case 2: $r(\mathbf{1}_G) = r(\chi)$:

In this case,

$$\Theta_{K/k}^{(r)} = h_k R_k e_{1_G} + \frac{h_K R_K}{h_k R_k} e_\chi$$

and $d = 0$. Because $N_{K/k}(U_K)$ is a subgroup of the free abelian group U_k, it is free abelian, and we can find $\breve{u}_i \in U_K$ so that $\{N_{K/k}(\breve{u}_i) : i = 1, \ldots, r\}$ is a $\mathbb{Z}$-basis for $N_{K/k}(U_K)$. By lemma A.7.2, we may assume that if $\widehat{H}^0(G, U_K) \neq 0$, then $\breve{u}_1 \in U_k$. If we let ε_+ be the image of $\breve{u}_1 \wedge \ldots \wedge \breve{u}_r$ in $\bigwedge^r_{\mathbb{Z}[G]} U_K$, then

$$\begin{aligned}\lambda_K^{(r)}(e_{1_G} \cdot \varepsilon_+) &= \det((\log|\breve{u}_i|_{w_j} + \log|\breve{u}_i^\sigma|_{w_j}\sigma)e_{1_G})_{1\le i,j\le r} \cdot \mathbf{x}_W \\ &= \det(\log|\breve{u}_i^{1+\sigma}|_{w_j})_{1\le i,j\le r} e_{1_G} \cdot \mathbf{x}_W \\ &= \det(\log|N_{K/k}(\breve{u}_i)|_{w_j})_{1\le i,j\le r} e_{1_G} \cdot \mathbf{x}_W,\end{aligned}$$

Note that $\det(\log|N_{K/k}(\breve{u}_i)|_{v_j})_{1\le i,j\le r}$ is the determinant of $\lambda_k \circ \iota : N_{K/k}(U_K) \to \mathbb{R}X_k$, where $\iota : N_{K/k}(U_K) \to U_k$ is the inclusion, taken with respect to $\mathbb{Z}$-bases for $N_{K/k}(U_K)$ and $X_k \subseteq \mathbb{R}X_k$. Thus

$$\lambda_K^{(r)}(e_{1_G} \cdot \varepsilon_+) = \pm R_k[U_k : N_{K/k}(U_K)]e_{1_G} \cdot \mathbf{x}_W = \pm R_k \#\widehat{H}^0(G, U_K)e_{1_G} \cdot \mathbf{x}_W,$$

and hence

$$\lambda_K^{(r)}\left(\frac{\pm h_k}{\#\widehat{H}^0(G, U_K)} e_{1_G} \cdot \varepsilon_+ \pm \frac{h_K}{h_k} e_\chi \cdot \varepsilon_-\right) = \Theta_{K/k}^{(r)} \cdot \mathbf{x}_W,$$

$$\varepsilon_W = \frac{\pm h_k}{\#\widehat{H}^0(G, U_K)} e_{1_G} \cdot \varepsilon_+ \pm \frac{h_K}{h_k} e_\chi \cdot \varepsilon_-.$$

Since all places in S except one split completely, $\mathbb{Q}U_K \cong \mathbb{Q}X_K \cong \mathbb{Q}[G]^r$, so we may find an embedding of U_K in $\mathbb{Z}[G]^r$ with finite cokernel $\mathscr{C}$. Since $\widehat{H}^n(G, \mathbb{Z}[G]^r) = 0$ for all $n \in \mathbb{Z}$, the long exact Tate cohomology sequence applied to

$$0 \to U_K \to \mathbb{Z}[G]^r \to \mathscr{C} \to 0$$

shows that $\widehat{H}^0(G, U_K) \cong \widehat{H}^{-1}(G, \mathscr{C})$ and $H^1(G, U_K) \cong \widehat{H}^0(G, \mathscr{C})$. Since G is cyclic and $\mathscr{C}$ is finite, $\#\widehat{H}^0(G, U_K) = \#\widehat{H}^{-1}(G, \mathscr{C}) = \#\widehat{H}^0(G, \mathscr{C}) = \#H^1(G, U_K)$ (see appendix A.1.2).

Suppose $\widehat{H}^0(G, U_K) \neq 0$. Recall that we assume that $N_{K/k}(u_{r+1}) = N_{K/k}(u_{d+r+1}) = 1$ and $\check{u}_1 \in U_k$; hence $e_\chi \cdot \varepsilon_- = \varepsilon_-$ and $e_{1_G} \cdot \varepsilon_+ = \varepsilon_+$. Therefore

$$\varepsilon_W = \frac{\pm h_k}{\#H^1(G, U_K)} \varepsilon_+ \pm \frac{h_K}{h_k} \varepsilon_- \in \bigwedge{}^r_{\mathbb{Z}[G]} U_K \subseteq \bigwedge{}^r_{\mathbb{Z}[G],0} U_K$$

by lemma 5.6.1 *i*) and *ii*).

Now suppose $\widehat{H}^0(G, U_K) = 0$. Then by a theorem of Reiner (see the remarks after theorem A.7.1 in appendix A.7), $U_K \cong \mathbb{Z}[G]^r$. Therefore $\{u_i : i = r+1, \ldots, 2r\}$ is a $\mathbb{Z}[G]$-basis for U_K, and $\{N_{K/k}(u_i) : i = r+1, \ldots, 2r\}$ is a $\mathbb{Z}$-basis for $N_{K/k}(U_K) = U_k$[‡]. Since $\{N_{K/k}(\check{u}_i) : i = 1, \ldots, r\}$ is also a $\mathbb{Z}$-basis for U_k, it follows that $e_{1_G} \cdot \varepsilon_- = \pm e_{1_G} \cdot \varepsilon_+$. Hence

$$\varepsilon_W = \left(\pm h_k e_{1_G} \pm \frac{h_K}{h_k} e_\chi \right) \cdot \varepsilon_-.$$

Lemma 5.6.1 *iii*) shows that h_k and h_K/h_k have the same parity, whence

$$\varepsilon_W \in \bigwedge{}^r_{\mathbb{Z}[G]} U_K \subseteq \bigwedge{}^r_{\mathbb{Z}[G],0} U_K.$$

[‡]WLOG we may assume that, under the identification of U_K with $\mathbb{Z}[G]^r$, $u_{r+1} = (1, 0, 0, \ldots)$, $u_{r+2} = (0, 1, 0, \ldots)$ etc., and that $u_i = (1 + \sigma) \cdot u_{r+i}$ for $i = 1, \ldots, r$.

Appendix A

Appendices

A.1 G-modules

A.1.1 Hom groups

We begin with some general nonsense. Let $\alpha : R \to S$ be a homomorphism of commutative unital rings, and let R-**Mod** (resp. S-**Mod**) be the category of R-modules (resp. S-modules). Any S-module M can be given an R-module structure via α, which we call ${}_\alpha M$, and this association gives a 'forgetful' functor from S-**Mod** to R-**Mod**.

If N is an R-module and M is an S-module, we define $\mathrm{Hom}_R({}_\alpha M, N)$ to be the abelian group of R-homomorphisms from ${}_\alpha M$ to N. This group has an S-module structure given by $s \cdot f : m \mapsto f(s \cdot m)$. The association $N \mapsto \mathrm{Hom}_R({}_\alpha S, N)$ defines a functor from R-**Mod** to S-**Mod**, and one can check that this is right adjoint to the forgetful functor. The natural isomorphism of Hom sets is given by

$$\mathrm{Hom}_R({}_\alpha M, N) \to \mathrm{Hom}_S(M, \mathrm{Hom}_R({}_\alpha S, N)) : f \mapsto (m \mapsto (s \mapsto f(s \cdot m))), \qquad \text{(A.1.1)}$$

and one may verify that this is an isomorphism of S-modules.

We can give S an S-R-bimodule structure, which allows us to define the S-module $S \bigotimes_R M$, given an R-module M. The association $M \mapsto S \bigotimes_R M$ defines a functor from R-**Mod** to S-**Mod**, and one can check that this is left adjoint to the forgetful functor. The natural isomorphism of Hom sets is given by

$$\mathrm{Hom}_R(M, {}_\alpha N) \to \mathrm{Hom}_S(S \bigotimes_R M, N) : f \mapsto (s \otimes m \mapsto f(s \cdot m)), \qquad \text{(A.1.2)}$$

and again one may verify that this is an isomorphism of S-modules.

Consider the case where H is a finite index subgroup of the abelian group G, A is a commutative unital ring, $R = A[H]$, $S = A[G]$ and $\alpha = \iota$ is the inclusion. If M is an

$A[G]$-module, there is an isomorphism of $A[G]$-modules

$$\mathrm{Hom}_{A[H]}({}_\iota A[G], A[H]) \to A[G] : f \mapsto \sum_{\sigma H \in G/H} \sigma^{-1} f(\sigma)$$

with inverse $a \mapsto (b \mapsto \mathrm{pr}_H(ab))$, where $\mathrm{pr}_H(\sum_{\sigma \in G} c_\sigma \sigma) = \sum_{\sigma \in H} c_\sigma \sigma$. Thus for any $A[G]$-module M, equation A.1.1 gives an isomorphism of $A[G]$-modules

$$\mathrm{Hom}_{A[H]}({}_\iota M, A[H]) \cong \mathrm{Hom}_{A[G]}(M, A[G]). \tag{A.1.3}$$

The case we will be interested in is where G is finite and H is trivial.

Now consider the case where $\alpha = \pi : G \to \Gamma$ is a surjective group homomorphism with finite kernel H (again we assume G to be abelian). Let $s : \Gamma \to G$ be a section of π. We also write $\pi : \mathbb{Z}[G] \to \mathbb{Z}[\Gamma]$ and $s : \mathbb{Z}[\Gamma] \to \mathbb{Z}[G]$ for the canonical associated maps.

We wish to show that there is an isomorphism

$$\mathrm{Hom}_{A[G]}({}_\pi A[\Gamma], A[G]) \to A[\Gamma].$$

If $f \in \mathrm{Hom}_{A[G]}(A[\Gamma], A[G])$, then for every $\sigma \in H$ and every $a \in A[\Gamma]$, $\sigma f(a) = f(\sigma{\cdot}a) = f(a)$. Thus f takes its values in $A[G]^H = N_H A[G]$, and so we can find a function $f_0 : A[\Gamma] \to A[G]$ (not necessarily a homomorphism) such that $f = N_H{\cdot}f_0$. The isomorphism sends f to $\pi(f_0(1))$, and this is easily seen to be independent of the choice of f_0. The inverse of this isomorphism sends $b \in A[\Gamma]$ to the function in $\mathrm{Hom}_{A[G]}(A[\Gamma], A[G])$ which takes c to $N_H s(bc)$.

Thus equation A.1.1 shows that for any $A[\Gamma]$-module M, there is an isomorphism of G-modules

$$\mathrm{Hom}_{A[G]}({}_\pi M, A[G]) \cong \mathrm{Hom}_{A[\Gamma]}(M, A[\Gamma]). \tag{A.1.4}$$

To be more explicit, this isomorphism takes $f \in \mathrm{Hom}_{A[G]}(M, A[G])$ to $\pi \circ f_0 \in \mathrm{Hom}_{A[\Gamma]}(M, A[\Gamma])$, where $f = N_H \cdot f_0$, as above.

We will usually omit the subscripts ι and π.

A.1.2 Cohomology of G-modules

Let G be a finite group. We list here a collection of facts concerning the cohomology of G-modules. Proofs of these statements can be found in [AW67].

Let M be a G-module. Define $H^q(G, M)$ ($q \in \mathbb{N}$) to be the right derived functors of the left-exact functor $M \mapsto M^G$, and define $H_q(G, M)$ ($q \in \mathbb{N}$) to be the left derived functors of the right-exact functor $M \mapsto M_G$ (see subsection 1.1.2 for the definition of M_G).

The Tate cohomology groups are defined as follows: For any G-module M there is a map $\mathcal{N}_G : M_G \to M^G : m + I_G \cdot M \mapsto N_G \cdot m$. The Tate cohomology groups are defined to be

$$\widehat{H}^q(G,M) = \begin{cases} H^q(G,M) & q > 0 \\ \operatorname{coker}\mathcal{N}_G & q = 0 \\ \ker \mathcal{N}_G & q = -1 \\ H_{-q-1}(G,M) & q < -1 \end{cases} \tag{A.1.5}$$

The snake lemma applied to the following exact diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \widehat{H}^0(G,A) & & \widehat{H}^0(G,B) & & \widehat{H}^0(G,C) & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & 0 \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & \longrightarrow & H^1(G,A) \longrightarrow \ldots \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
\ldots \longrightarrow & H_1(G,C) \longrightarrow & A_G & \longrightarrow & B_G & \longrightarrow & C_G & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \widehat{H}^{-1}(G,A) & & \widehat{H}^{-1}(G,B) & & \widehat{H}^{-1}(G,C) & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

shows that the Tate cohomology groups fit into a long exact sequence

$$\ldots \to \widehat{H}^{q-1}(G,C) \to \widehat{H}^q(G,A) \to \widehat{H}^q(G,B) \to \widehat{H}^q(G,C) \to \widehat{H}^{q+1}(G,A) \to \ldots$$

If G is cyclic, $\widehat{H}^q(G,M) \cong \widehat{H}^{q+2}(G,M)$ for all $q \in \mathbb{Z}$. If, in addition, M is finite, $\#\widehat{H}^0(G,M) = \#\widehat{H}^1(G,M)$. Consequently, if G is cyclic and M is finite, all Tate cohomology groups have the same order.

If H is a subgroup of the finite group G and M is an H-module, define $\mathrm{Ind}_H^G M = \mathbb{Z}[G] \bigotimes_{\mathbb{Z}[H]} M$. Shapiro's lemma states that for all $q \in \mathbb{Z}$, $\widehat{H}^q\left(G, \mathrm{Ind}_H^G M\right) \cong \widehat{H}^q(H,M)$.

A G-module M is said to be *cohomologically trivial* if $\widehat{H}^q(H,M) = 0$ for all subgroups H of G, and all $q \in \mathbb{Z}$.

Proposition A.1.1. *If* $0 \to A \to B \to C \to 0$ *is a short exact sequence of* G*-modules and two of* A, B *or* C *are cohomologically trivial, then so is the third.*

Proof. Follows from the long exact Tate cohomology sequence. □

Corollary A.1.1. *If a G-module M has a finite free resolution, it is cohomologically trivial.*

Proof. We can split the resolution

$$0 \to F_n \to F_{n-1} \to \ldots \to F_0 \to M \to 0$$

up into short exact sequences $0 \to Z_{i+1} \to F_i \to Z_i \to 0$, $i = 0, \ldots, n-1$, where $Z_n = F_n$ and $Z_0 = M$. The result follows by induction. □

A.2 Fitting ideals

Most of the results in this section can be found in the book by Northcott ([Nor]). We list some properties of Fitting ideals, and prove a lemma which is required in the proof of proposition 5.4.1. For the definition of the Fitting ideal, see subsection 4.2.2.

Proposition A.2.1. *If* $0 \to A \to B \to C \to 0$ *is a short exact sequence of finitely generated R-modules, then*

$$\mathrm{Fitt}_R(A)\mathrm{Fitt}_R(C) \subseteq \mathrm{Fitt}_R(B) \subseteq \mathrm{Fitt}_R(C). \tag{A.2.1}$$

Remark A.2.1. The proof relies on the fact that if A, B and C are as above, and $F'_A \to F_A \to A \to 0$ and $F'_C \to F_C \to C \to 0$ are free presentations of A and C respectively, then there exists a free presentation of B of the form $F'_A \bigoplus F'_C \to F_A \bigoplus F_C \to B \to 0$.

If the short exact sequence splits, then the first inclusion in equation A.2.1 is an equality, and so by induction

$$\mathrm{Fitt}_R\left(\bigoplus_{i=1}^{m} M_i\right) = \prod_{i=1}^{m} \mathrm{Fitt}_R(M_i).$$

The Fitting ideal is closely related to the annihilator ideal $\mathrm{Ann}_R(M)$. If M has n generators, then $\mathrm{Ann}_R(M)^n \subseteq \mathrm{Fitt}_R(M) \subseteq \mathrm{Ann}_R(M)$. In particular, if M is cyclic, $\mathrm{Fitt}_R(M) = \mathrm{Ann}_R(M)$.

It follows easily from the definition of the Fitting ideal that if S is a subring of R (both unital and commutative) and M is a finitely generated S, then

$$\mathrm{Fitt}_R(R \bigotimes_S M) \cong R\mathrm{Fitt}_S(M) \tag{A.2.2}$$

A proof of the following lemma may be found in [CG98] (lemma 3, 462).

Lemma A.2.1. *If $F'_C \to F_C \to C \to 0$ is a free presentation of a finitely generated R-module C, where F'_C and F_C have the same finite rank, then for any short exact sequence $0 \to A \to B \to C \to 0$ of finitely generated R-modules, the first inclusion in equation A.2.1 is an equality.*

The next lemma is needed in the proof of proposition 5.4.1.

Lemma A.2.2. *Suppose*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0,$$

is a short exact sequence of finitely generated R-modules. Then for any $r \in \mathbb{N}$,

$$\mathrm{Fitt}_R(C)\cdot {\textstyle\bigwedge}_R^r B \subseteq f^{(r)}\left({\textstyle\bigwedge}_R^r A\right). \tag{A.2.3}$$

Proof. Let $\{c_1, \ldots, c_n\}$ be a set of n non-zero generators of C, and for each $j = 1, \ldots, n$, choose $b_i \in B$ mapping to c_i. Then B is generated by $A \cup \{b_1, \ldots, b_n\}$ (we identify A with its image in B). Thus $\bigwedge_R^r B$ is generated by monomials $x_1 \wedge \ldots \wedge x_r$, where at most n of the x_i's are in $\{b_1, \ldots, b_n\}$, and the rest are in A. On the other hand, $\mathrm{Fitt}_R(C)$ is generated by $\det(r_{ij})$, where $\sum_{j=1}^n r_{ij}\cdot c_j = 0$ for every i. Hence it will be sufficient to show that for such monomials and elements of $\mathrm{Fitt}_R(C)$,

$$\det(r_{ij})\cdot x_1 \wedge \ldots \wedge x_r \in f^{(r)}\left({\textstyle\bigwedge}_R^r A\right). \tag{A.2.4}$$

Firstly, note that we may assume $r \geq n$. To see this, choose $n' \geq \max\{n, r\}$, and let D be a free R-module of rank $n' - r$. Suppose we have shown that the theorem holds holds with $r = n'$ for all short exact sequences $0 \to A' \to B' \to C' \to 0$ where C' has n generators. Since

$$0 \longrightarrow A \bigoplus D \xrightarrow{f \bigoplus 1_D} B \bigoplus D \xrightarrow{g \bigoplus 0} C \longrightarrow 0,$$

is such a short exact sequence, we deduce that

$$\mathrm{Fitt}_R(C)\cdot \bigoplus_{i=1}^{n'} \left[\left({\textstyle\bigwedge}_R^i B\right) \otimes_R \left({\textstyle\bigwedge}_R^{n'-i} D\right)\right] \subseteq \bigoplus_{i=1}^{n'} \left[f^{(i)}\left({\textstyle\bigwedge}_R^i A\right) \otimes_R {\textstyle\bigwedge}_R^{n'-i} D\right]$$

(see 4.1.2). Looking at the r-th summand shows that

$$\begin{aligned}\mathrm{Fitt}_R(C)\cdot {\textstyle\bigwedge}_R^r B &\cong \mathrm{Fitt}_R(C)\cdot \left({\textstyle\bigwedge}_R^r B\right) \otimes_R \left({\textstyle\bigwedge}_R^{n'-r} D\right) \\ &\subseteq f^{(r)}\left({\textstyle\bigwedge}_R^r A\right) \otimes_R \left({\textstyle\bigwedge}_R^{n'-r} D\right) \cong f^{(r)}\left({\textstyle\bigwedge}_R^r A\right).\end{aligned}$$

Secondly, we may assume $r = n$, since if A.2.4 holds in this case, it holds with $r \geq n$ (recall that we assume at most n of $x_1, \ldots, x_r$ are in $\{b_1, \ldots, b_n\}$).

If $m \in \mathbb{N}$, define $[{m \atop n}]$ to be the set of all strictly increasing functions from $\{1,\ldots,n\}$ to $\{1,\ldots,m\}$. For any $\beta_1,\ldots,\beta_m \in B$ and any $\gamma_{ij} \in R$, we have the following equality in $\bigwedge_R^n B$:

$$\left(\sum_{j=1}^{m} \gamma_{1j}\cdot\beta_j\right) \wedge \ldots \wedge \left(\sum_{j=1}^{m} \gamma_{nj}\cdot\beta_j\right) = \sum_{\phi\in[{m \atop n}]} \det(\gamma_{i\phi(j)})\cdot\beta_{\phi(1)} \wedge \ldots \wedge \beta_{\phi(n)}. \quad \text{(A.2.5)}$$

We will prove A.2.4 by induction on the number of the x_i's which are not in $\{b_1,\ldots,b_n\}$. Call this number ℓ. When $\ell = 0$, we may assume $x_j = b_j$ for $j = 1,\ldots,n$, and equation A.2.5 shows that

$$\det(r_{ij})\cdot b_1 \wedge \ldots \wedge b_n = \left(\sum_{j=1}^{n} r_{1j}\cdot b_j\right) \wedge \ldots \wedge \left(\sum_{j=1}^{n} r_{nj}\cdot b_j\right).$$

Since g maps $\sum_{j=1}^n r_{ij}\cdot b_j$ to $\sum_{j=1}^n r_{ij}\cdot c_j = 0$ for $i = 1,\ldots,n$, this is an element of A, and we have proven A.2.4 for $\ell = 0$.

Now suppose $d \leq n-1$ is a positive integer and A.2.4 holds for all $\ell \leq d-1$. We wish to show that A.2.4 holds with $\ell = d$. Without loss of generality we may assume that $x_j = a_j$ for $j = 1,\ldots,d$ and $x_j = b_j$ for $j = d+1,\ldots,n$, where the a_j's are arbitrary elements of A. We apply equation A.2.5 with

$$\gamma_{ij} = \begin{cases} r_{ij} & 1 \leq j \leq d \\ r_{i,j-d} & d+1 \leq j \leq d+n \end{cases} \qquad \beta_j = \begin{cases} a_j & 1 \leq j \leq d \\ b_{j-d} & d+1 \leq j \leq d+n \end{cases}$$

The left-hand side of A.2.5 is the wedge product of terms of the form $\sum_{j=1}^d r_{ij}\cdot a_j + \sum_{j=1}^n r_{ij}\cdot b_j$, which are all in A. Any term in the sum on the right-hand side for which $\phi \in [{d+n \atop n}]$ takes on the value i and $i+d$, for $1 \leq i \leq d$, will be zero. By the pigeon-hole principle, all non-zero terms must correspond to functions ϕ which satisfy $\phi(j) = j+d$ for $j = d+1,\ldots,n$. Such a term can have at most d x_j's not in $\{b_1,\ldots,b_n\}$, and in fact the only term which has exactly d x_j's not in $\{b_1,\ldots,b_n\}$ is

$$\det(r_{ij})\cdot\beta_1 \wedge \ldots \wedge \beta_d \wedge \beta_{2d+1} \wedge \ldots \wedge \beta_{n+d} = \det(r_{ij})\cdot a_1 \wedge \ldots \wedge a_d \wedge b_{d+1} \wedge \ldots \wedge b_n.$$

By our inductive hypothesis, it must be in $f^{(n)}\left(\bigwedge_{\mathbb{Z}[G]}^n A\right)$. □

A.3 An approximation theorem

A proof of the following proposition can be found in [Nar90] (proposition 2.1, pp 44-45).

Proposition A.3.1. *Let F be a number field, I an integral ideal of $\mathcal{O}_F$, and R an element of $\mathcal{O}_F/I$. Then the restriction of the signature map* $\mathrm{sgn}_F : F^\times \to \mathrm{Sgn}_F$ *to* $R \smallsetminus \{0\}$ *is onto.*

The following theorem can be thought of as a variation on the strong approximation theorem.

Theorem A.3.1. *Let F be a number field. Then for any finite set S of non-archimedean places of F, any $\{a_v \in F : v \in S\}$, $N \in \mathbb{N}$, and $s \in \mathrm{Sgn}_F$, there exists $x \in F^\times$ such that:*

- $\mathrm{ord}_v(x - a_v) \geq N$ *for all* $v \in S$,
- $\mathrm{ord}_v(x) \geq 0$ *for all non-archimedean places of F not in S,*
- $\mathrm{sgn}_F(x) = s$.

We first prove the theorem in a simple case:

Lemma A.3.1. *The theorem is true if $a_v = 1$ for all $v \in S$.*

Proof. Let I be an integral ideal satisfying $\mathrm{ord}_v(I) \geq N$ for all $v \in S$. By proposition A.3.1, there exists a non-zero $y \in 1 + I$ such that $\mathrm{sgn}_F(y) = s$, and such a y satisfies the conditions of the theorem. □

Proof. (of theorem A.3.1) The strong approximation theorem implies that the first two conditions can be satisfied, say by $y \in F$. By the lemma above, we can find $z \in F^\times$ such that:

- $\mathrm{ord}_v(z - 1) \geq N - \mathrm{ord}_v(y)$ for all $v \in S$,
- $\mathrm{ord}_v(z) \geq 0$ for all non-archimedean places of F not in S,
- $\mathrm{sgn}_F(z) = s\,\mathrm{sgn}_F(y)$.

Since $\mathrm{ord}_v(yz - a_v) = \mathrm{ord}_v(y(z-1) + (y - a_v)) \geq N$, $x = yz$ satisfies the conditions of the theorem. □

A.4 Unit and Picard groups of commutative rings

This section is not essential for the study of Stark's conjectures, but some of the results will be used in the remaining appendices. Most of the results in this section can be found in the exercises in [Wei].

Let A be a commutative ring (possibly without a unit), and let R be a commutative ring with unit. If A has an R-algebra structure, we may form the R-algebra $A +_1 R$, whose underlying R-module is the direct sum of the underlying R-modules of A and R, but where multiplication is defined by

$$(a,r)(a',r') = (aa' + ra' + r'a, rr').$$

This is a unital R-algebra $A +_1 R$, the unit being $(0, 1_R)$. The R-algebra homomorphism $R \to A +_1 R : r \mapsto (0,r)$ has a left inverse $A +_1 R \to R : (a,r) \mapsto r$, so under the units functor $R^\times \to (A +_1 R)^\times$ has a left inverse. We define the extended group of units $A^\times$ to be the cokernel of $R^\times \to (A +_1 R)^\times$, or equivalently (up to canonical isomorphism), the kernel of $(A +_1 R)^\times \to R^\times$. If A *does* have a unit, then there is an isomorphism of R-algebras

$$A +_1 R \to A \bigoplus R : (a,r) \mapsto (a + r1_A, r).$$

The composite $A \bigoplus R \to A +_1 R \to R$ is then projection onto R, and the units functor takes this to the projection of $(A \bigoplus R)^\times \cong A^\times \bigoplus R^\times$ onto $R^\times$. Hence $A^\times$ as we have just defined it is isomorphic to the group of units of A, the isomorphism sending a to $a + 1_A$. This justifies our notation.

It is not hard to see that

$$A^\times \cong \{a \in A : \exists a' \in A, aa' + a + a' = 0\},$$

where the group operation is $a * b = ab + a + b$. Thus $A^\times$ is independent of the R-module structure on A.

There are two special cases which we will make use of. Firstly, if A is an ideal I of R, then $I^\times \cong R^\times \cap (1 + I)$. Secondly, if the product of any two elements of A is zero, then since $a(-a) + a + (-a) = 0$ and $a * b = ab + a + b = a + b$, $A^\times$ is isomorphic to the underlying additive group of A.

We may define the extended Picard group $\text{Pic}(A)$ in an analogous way to $A^\times$: $\text{Pic}(A) = \ker[\text{Pic}(A +_1 R) \to \text{Pic}(R)]$, and one can verify that this is also independent of the R-algebra structure on A and coincides with the usual Picard group when A is unital. The (usual) Picard group of a finite commutative unital ring is zero *. In fact the same is true for the extended Picard group of a finite commutative ring. To see this, note that a finite ring A has non-zero characteristic, say n, so we may view it as a $\mathbb{Z}/n\mathbb{Z}$-algebra. Since $\text{Pic}(A)$ is the kernel of $\text{Pic}(A +_1 (\mathbb{Z}/n\mathbb{Z})) \to \text{Pic}(\mathbb{Z}/n\mathbb{Z})$, it is zero.

Finally, one can show that if I is an ideal of R, there is an exact sequence

$$0 \to I^\times \to R^\times \to (R/I)^\times \to \text{Pic}(I) \to \text{Pic}(R) \to \text{Pic}(R/I). \qquad \text{(A.4.1)}$$

*Finite rings are direct sums of local rings ([Lam01] p 340), and the Picard group of a local ring is trivial ([Mat86] p 166).

A.5 Algebraic number theory calculations

Our standing assumptions for the remaining three chapters are that K/k is an abelian extension of number fields with Galois group G, and that hypotheses $\mathrm{H}(K/k, S, \mathfrak{m})$ are satisfied.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$. We wish to calculate the $\mathbb{Z}[G]$-module structure of $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.

Let $\mathfrak{P}$ be a prime of $\mathcal{O}_K$ dividing $\mathfrak{p}$, let p be the characteristic of the residue field $\mathcal{O}_k/\mathfrak{p}$, and let $f = f(\mathfrak{p}/p\mathbb{Z})$ (p and f will always be defined this way in this appendix). By the normal basis theorem ([Rom95] theorem 8.7.2, p 169), there exists $\mathfrak{a} \in \mathcal{O}_K/\mathfrak{P}$ such that $\{\sigma(\mathfrak{a}) : \sigma \in D_\mathfrak{p}\}$ is a basis for the $\mathcal{O}_k/\mathfrak{p}$-vector space $\mathcal{O}_K/\mathfrak{P}$. Let $\{\mathfrak{b}_1, \dots, \mathfrak{b}_f\}$ be a $\mathbb{Z}/p\mathbb{Z}$-basis for $\mathcal{O}_k/\mathfrak{p}$. Then $\{\mathfrak{b}_i\sigma(\mathfrak{a}) : i = 1, \dots, f; \sigma \in D_\mathfrak{p}\}$ is a $\mathbb{Z}/p\mathbb{Z}$-basis for $\mathcal{O}_K/\mathfrak{P}$, so $\{\mathfrak{b}_i\mathfrak{a} : i = 1, \dots, f\}$ is a $(\mathbb{Z}/p\mathbb{Z})[D_\mathfrak{p}]$-basis for $\mathcal{O}_K/\mathfrak{P}$. Therefore

$$\mathcal{O}_K/\mathfrak{P} \cong \bigoplus_{i=1}^{f} \mathbb{Z}[D_\mathfrak{p}]/p\mathbb{Z}[D_\mathfrak{p}],$$

and so

$$\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \cong \mathbb{Z}[G]\otimes_{\mathbb{Z}[D_\mathfrak{p}]}(\mathcal{O}_K/\mathfrak{P}) \cong \bigoplus_{i=1}^{f} \mathbb{Z}[G]/p\mathbb{Z}[G] \tag{A.5.1}$$

(Note that these are isomorphisms of G-modules, not of rings).

Proposition A.5.1. *Let $Q_{K,\mathfrak{m}}$ be as defined in chapter 4. Then $Q_{K,\mathfrak{m}}$ is cohomologically trivial.*

Proof. WLOG we may assume that $\mathfrak{m} = v^n$ for some non-complex place v of k, and $n \in \mathbb{N}^+$. If v is real, $Q_{K,\mathfrak{m}} \cong \mathbb{Z}[G]/2\mathbb{Z}[G]$ is cohomologically trivial since it has a free resolution of length 2. So suppose v and $\bar{v}$ are non-archimedean, corresponding to the prime ideals $\mathfrak{p}$ and $\mathfrak{P}$ of $\mathcal{O}_k$ and $\mathcal{O}_K$ respectively. We first show that $\widehat{H}^q(G, Q_{K,\mathfrak{m}}) = 0$ for all $q \in \mathbb{Z}$ (which is all we really need).

$$Q_{K,\mathfrak{m}} \cong (\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times \cong \mathbb{Z}[G]\otimes_{\mathbb{Z}[D_\mathfrak{p}]}(\mathcal{O}_K/\mathfrak{P}^n)^\times,$$

so by Shapiro's lemma,

$$\widehat{H}^q(G, Q_{K,\mathfrak{m}}) \cong \widehat{H}^q(D_\mathfrak{p}, (\mathcal{O}_K/\mathfrak{P}^n)^\times).$$

For each positive integer ℓ, the units-Pic sequence A.4.1 applied to

$$0 \to \mathfrak{P}^\ell/\mathfrak{P}^{\ell+1} \to \mathcal{O}_K/\mathfrak{P}^{\ell+1} \to \mathcal{O}_K/\mathfrak{P}^\ell \to 0$$

gives a short exact sequence of $D_\mathfrak{p}$-modules

$$0 \to \left(\mathfrak{P}^\ell/\mathfrak{P}^{\ell+1}\right)^\times \to \left(\mathcal{O}_K/\mathfrak{P}^{\ell+1}\right)^\times \to \left(\mathcal{O}_K/\mathfrak{P}^\ell\right)^\times \to 0. \tag{A.5.2}$$

Since the product of any two elements of $\mathfrak{P}^\ell/\mathfrak{P}^{\ell+1}$ is zero, the remarks in appendix A.4 show that $\left(\mathfrak{P}^\ell/\mathfrak{P}^{\ell+1}\right)^\times$ is isomorphic to the additive $D_\mathfrak{p}$-module $\mathfrak{P}^\ell/\mathfrak{P}^{\ell+1}$, which in turn is isomorphic† to $\mathcal{O}_K/\mathfrak{P} \cong \bigoplus_{i=1}^f \mathbb{Z}[D_\mathfrak{p}]/p\mathbb{Z}[D_\mathfrak{p}]$. This has a free resolution of length 2, and is therefore cohomologically trivial. The sequence A.5.2 then shows that the Tate cohomology of $\left(\mathcal{O}_K/\mathfrak{P}^\ell\right)^\times$ is independent of ℓ.

Since $\mathcal{O}_K/\mathfrak{P}$ is a Galois field extension of $\mathcal{O}_k/\mathfrak{p}$ with Galois group isomorphic to $D_\mathfrak{p}$, Hilbert's theorem 90 ([Rom95] theorem 11.1.2, p 211) shows that $\widehat{H}^1(D_\mathfrak{p}, (\mathcal{O}_K/\mathfrak{P})^\times) = 0$. Since $D_\mathfrak{p}$ is cyclic and $(\mathcal{O}_K/\mathfrak{P})^\times$ is finite, all Tate cohomology groups are trivial.

To show that $(\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times$ is cohomologically trivial, let H be a subgroup of G, put $L = K^H$, and write $\mathfrak{p}\mathcal{O}_L = \prod_i \mathfrak{p}_i$, where the $\mathfrak{p}_i$'s are distinct primes of $\mathcal{O}_L$. Then for any integer q,

$$\begin{aligned} \widehat{H}^q(H, (\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times) &\cong \widehat{H}^q\left(H, \bigoplus_i (\mathcal{O}_K/\mathfrak{p}_i^n\mathcal{O}_K)^\times\right) \\ &\cong \bigoplus_i \widehat{H}^q(\mathrm{Gal}(K/L), (\mathcal{O}_K/\mathfrak{p}_i^n\mathcal{O}_K)^\times), \end{aligned}$$

and the result follows since all the groups in the direct sum on the right are zero by the result proved above. □

A.5.1 A generator of $\mathrm{Fitt}_{\mathbb{Z}[G]}(Q_{K,v^n})$

We wish to show that if v^n is a modulus of k, then δ_{K,v^n} generates $\mathrm{Fitt}_{\mathbb{Z}[G]}(Q_{K,v^n})$. We will use the notation of subsection 5.4, where we defined

$$\delta_{K,v^n} = \begin{cases} (1 - \sigma_v^{-1} N v) N v^{n-1} & \text{if } v \text{ is non-archimedean} \\ 2 & \text{if } v \text{ is archimedean} \end{cases}$$

If v is archimedean, then $Q_{K,v} \cong \mathbb{Z}[G]/2\mathbb{Z}[G]$, and clearly $\mathrm{Fitt}_{\mathbb{Z}[G]}(Q_{K,v})$ is generated by $\delta_{K,v} = 2$.

†The isomorphism $\mathcal{O}_K/\mathfrak{P} \cong \mathfrak{P}^\ell/\mathfrak{P}^{\ell+1}$ arises as follows: pick $a \in k$ with $\mathrm{ord}_\mathfrak{p}(a) = \ell$; then since $\mathfrak{p}$ is unramified in K/k, $\mathrm{ord}_\mathfrak{P}(a) = \mathrm{ord}_\mathfrak{p}(a) = \ell$. The map

$$\mathcal{O}_K/\mathfrak{P} \to \mathfrak{P}^\ell/\mathfrak{P}^{\ell+1} : x + \mathfrak{P} \mapsto ax + \mathfrak{P}^{\ell+1}$$

is an isomorphism of abelian groups (see [Nar90] p 11), and the fact that a is fixed by $D_\mathfrak{p}$ shows that this is an isomorphism of $D_\mathfrak{p}$-modules.

Now suppose v is non-archimedean, corresponding to the prime ideal $\mathfrak{p}$. Since

$$Q_{K,v^n} \cong (\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times \cong \mathbb{Z}[G]\bigotimes_{\mathbb{Z}[D_v]}(\mathcal{O}_K/\mathfrak{P}^n)^\times$$

for any $\mathfrak{P}$ lying above $\mathfrak{p}$, equation A.2.2 implies that it is sufficient to show that if $\hat{Q}_{K,v^n} = (\mathcal{O}_K/\mathfrak{P}^n)^\times$, $\mathrm{Fitt}_{\mathbb{Z}[D_v]}(\hat{Q}_{K,v^n})$ is generated by δ_{K,v^n}. If $n = 1$, then $(\mathcal{O}_K/\mathfrak{P}^n)^\times$ is cyclic and so $\mathrm{Fitt}_{\mathbb{Z}[D_v]}(\hat{Q}_{K,v^n}) = \mathrm{Ann}_{\mathbb{Z}[D_v]}\left((\mathcal{O}_K/\mathfrak{P})^\times\right) \cong (\sigma_v - Nv)\mathbb{Z}[D_v]$. Thus $\mathrm{Fitt}_{\mathbb{Z}[G]}(\hat{Q}_{K,v})$ is generated by $\delta_{K,v} = 1 - \sigma_v^{-1}Nv$. If $n > 1$, we have the exact sequence A.5.2

$$0 \to \bigoplus_{i=1}^{f} \mathbb{Z}[D_v]/p\mathbb{Z}[D_v] \to \left(\mathcal{O}_K/\mathfrak{P}^{\ell+1}\right)^\times \to \left(\mathcal{O}_K/\mathfrak{P}^{\ell}\right)^\times \to 0. \tag{A.5.3}$$

Since $\bigoplus_{i=1}^{f} \mathbb{Z}[D_v]/p\mathbb{Z}[D_v]$ and $\hat{Q}_v \cong \mathbb{Z}[D_v]/(1-\sigma_v^{-1}Nv)\mathbb{Z}[D_v]$ have free presentations with terms of equal rank, it follows by induction that the same is true of $\hat{Q}_{v^n}$ for all integers $n > 1$ (see remark A.2.1). By lemma A.2.1,

$$\begin{aligned}\mathrm{Fitt}_{\mathbb{Z}[D_v]}(\hat{Q}_{K,v^n}) &= \mathrm{Fitt}_{\mathbb{Z}[D_v]}\left(\bigoplus_{i=1}^{f} \mathbb{Z}[D_v]/p\mathbb{Z}[D_v]\right)\mathrm{Fitt}_{\mathbb{Z}[D_v]}(\hat{Q}_{K,v^{n-1}}) \\ &= p^f\,\mathrm{Fitt}_{\mathbb{Z}[D_v]}(\hat{Q}_{K,v^{n-1}}) = Nv\,\mathrm{Fitt}_{\mathbb{Z}[D_v]}(\hat{Q}_{K,v^{n-1}})\end{aligned}$$

for all integers $n > 1$, and we see by induction that $\mathrm{Fitt}_{\mathbb{Z}[G]}(\hat{Q}_{K,v^n})$ is generated by $\delta_{K,v^n} = (1-\sigma_v^{-1}Nv)Nv^{n-1}$.

A.6 Some exact sequences

In this appendix we will show how the exact sequences 4.2.2 and 5.6.3 arise.

A.6.1 The exact sequence 4.2.2

This is similar to the derivation of the exact sequence on page 472 of [Aok04]. A more direct proof can be found in [Coh00] (proposition 3.2.3, p 137). Let $\mathscr{I}_{K,S} = \mathscr{I}_{K,S,1}$ be the free abelian group on the places of K not in S_K. We may also think of this as the group of fractional $\mathcal{O}_S$-ideals. Let $\mathcal{F}_{K,\mathfrak{m}}$ be the free abelian group on $\mathrm{supp}(\mathfrak{m}_K)$. We give these groups their natural G-module structures.

Clearly $K_1^{\mathfrak{m}}$ is in the kernel of the map

$$K^\times \to \mathcal{F}_{K,\mathfrak{m}} : x \mapsto \sum_{w\in \mathrm{supp}(\mathfrak{m}_K)} \mathrm{ord}_w(x)w,$$

so we have a map $\mathrm{div}_K^{\mathfrak{m}} : K^\times/K_1^{\mathfrak{m}} \to \mathcal{F}_{K,\mathfrak{m}}$ (this is not to be confused with the map $\mathrm{div}_{K,S,\mathfrak{m}}$ given in section 4.2). Since $Q_{K,\mathfrak{m}} = K^{\mathfrak{m}}/K_1^{\mathfrak{m}}$, it is clear that

$$0 \to Q_{K,\mathfrak{m}} \longrightarrow K^\times/K_1^{\mathfrak{m}} \longrightarrow \mathcal{F}_{K,\mathfrak{m}} \to 0,$$

is exact. We construct a splitting for $K^\times/K_1^{\mathfrak{m}} \to \mathcal{F}_{K,\mathfrak{m}}$ as follows. For each $v \in \mathrm{supp}(\mathfrak{m})$, choose $a_v \in k^\times$ with $\mathrm{ord}_v(a_v) = 1$. By theorem A.3.1, we can find $b_v \in K^\times$ such that

- $\mathrm{ord}_w(b_v - 1) \geq \mathrm{ord}_w(\mathfrak{m}_K)$ for all $w \in \mathrm{supp}(\mathfrak{m}_K) \smallsetminus \{\bar{v}\}$,
- $\mathrm{ord}_{\bar{v}}(b_v - a_v) \geq \mathrm{ord}_{\bar{v}}(\mathfrak{m}_K) + 1$,
- $\mathrm{sgn}_{K,\mathfrak{m}}(b_v)$ is the identity of $\mathrm{Sgn}_{K,\mathfrak{m}}$.

Note that for any $\sigma \in D_v$, the above remain true if b_v is replaced by b_v^σ. Also note that $\mathrm{ord}_w(b_v) = 0$ for all $w \in \mathrm{supp}(\mathfrak{m}_K) \smallsetminus \{\bar{v}\}$ and $\mathrm{ord}_{\bar{v}}(b_v) = \mathrm{ord}_{\bar{v}}(a_v) = 1$. Since

$$\mathrm{ord}_w(b_v^{\sigma-1} - 1) = \mathrm{ord}_w(b_v^\sigma - b_v) = \mathrm{ord}_w(b_v^\sigma - 1 - (b_v - 1)) \geq \mathrm{ord}_w(\mathfrak{m}_K)$$

for all $w \in \mathrm{supp}(\mathfrak{m}_K) \smallsetminus \{\bar{v}\}$ and

$$\mathrm{ord}_{\bar{v}}(b_v^{\sigma-1} - 1) = \mathrm{ord}_{\bar{v}}(b_v^\sigma - b_v) - 1 = \mathrm{ord}_w(b_v^\sigma - a_v - (b_v - a_v)) - 1 \geq \mathrm{ord}_w(\mathfrak{m}_K),$$

we have $b_v^{1-\sigma} \in K_1^{\mathfrak{m}}$. Thus we may define a $\mathbb{Z}[G]$-homomorphism

$$\mathbb{Z}[G] \bigotimes_{\mathbb{Z}[D_v]} \mathbb{Z} \to K^\times/K_1^{\mathfrak{m}} : \tau \otimes n \mapsto b_v^{n\tau} K_1^{\mathfrak{m}},$$

where $\mathbb{Z}$ has trivial D_v action. Since $\mathcal{F}_{K,\mathfrak{m}} \cong \bigoplus_{v \in \mathrm{supp}(\mathfrak{m})} \mathbb{Z}[G] \bigotimes_{\mathbb{Z}[D_v]} \mathbb{Z}$, we obtain a homomorphism $\mathcal{F}_{K,\mathfrak{m}} \to K^\times/K_1^{\mathfrak{m}}$, which is easily seen to be a splitting map. Hence there is a short exact sequence

$$0 \longrightarrow K_1^{\mathfrak{m}} \longrightarrow K^\times \longrightarrow Q_{K,\mathfrak{m}} \bigoplus \mathcal{F}_{K,\mathfrak{m}} \to 0. \tag{A.6.1}$$

Consider the commutative diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_{K,S,\mathfrak{m}} & \longrightarrow & U_{K,S} & \longrightarrow & Q_{K,\mathfrak{m}} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K_1^{\mathfrak{m}} & \longrightarrow & K^\times & \longrightarrow & Q_{K,\mathfrak{m}} \bigoplus \mathcal{F}_{K,\mathfrak{m}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathscr{I}_{K,S,\mathfrak{m}} & \longrightarrow & \mathscr{I}_{K,S} & \longrightarrow & \mathcal{F}_{K,\mathfrak{m}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & A_{K,S,\mathfrak{m}} & \longrightarrow & A_{K,S} & \longrightarrow & 0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

The snake lemma then shows that there is an exact sequence

$$0 \to U_{K,S,\mathfrak{m}} \to U_{K,S} \to Q_{K,\mathfrak{m}} \to A_{K,S,\mathfrak{m}} \to A_{K,S} \to 0.$$

Remark A.6.1. In the case where $\mathfrak{m}$ is not supported on any archimedean places (so that we may regard it as an integral $\mathcal{O}_k$-ideal), this exact sequence is a case of the units-Pic sequence A.4.1 with $R = \mathcal{O}_{K,S}$, $I = \mathfrak{m}\mathcal{O}_{K,S}$. It is clear that $I^\times = U_{K,S,\mathfrak{m}}$, $(R/I)^\times = Q_{K,\mathfrak{m}}$; and $\mathrm{Pic}(R/I) = 0$ since the R/I is finite. Using Milnor's patching theorem (see [Wei] theorem 2.7, p 11), one can show that $\mathrm{Pic}(I) = A_{K,S,\mathfrak{m}}$, but this is more difficult.

A.6.2 The exact sequence 5.6.3

This derivation is adapted from results in a paper by Rim ([Rim65]).

Suppose the extension K/k is cyclic.

Lemma A.6.1. $H^1(G, \mathscr{I}_{K,S,\mathfrak{m}}) = 0$

Proof. Note that $\mathscr{I}_{K,S,\mathfrak{m}} \cong \coprod_{v \notin S \cup \mathrm{supp}(\mathfrak{m})} \left(\mathbb{Z}[G] \bigotimes_{\mathbb{Z}[D_v]} \mathbb{Z}\right)$, where $\mathbb{Z}$ has the trivial D_v-action. By Shapiro's lemma, $H^1(G, \mathscr{I}_{K,S}) \cong \coprod_{v \notin S \cup \mathrm{supp}(\mathfrak{m})} H^1(D_v, \mathbb{Z}) = 0$. □

Lemma A.6.2. $H^1(G, K_1^{\mathfrak{m}}) = 0$

Proof. The exact sequence A.6.1, together with Hilbert's theorem 90 and the fact that $Q_{K,\mathfrak{m}}$ is cohomologically trivial, implies that

$$\widehat{H}^0(G, K^\times) \to \widehat{H}^0(G, \mathcal{F}_{K,\mathfrak{m}}) \to H^1(G, K_1^{\mathfrak{m}}) \to 0$$

is short exact. Note that for all $x \in k^\times$,

$$\mathrm{div}_K^{\mathfrak{m}}(x) = \sum_{w \in \mathrm{supp}(\mathfrak{m}_K)} \mathrm{ord}_w(x) w = \sum_{v \in \mathrm{supp}(\mathfrak{m})} \mathrm{ord}_v(x) \sum_{w|v} w \,^{\ddagger},$$

which is simply $\mathrm{div}_k^{\mathfrak{m}}(x)$ under the identification of $v \in \mathrm{supp}(\mathfrak{m})$ with $\sum_{w|v} w$. Thus the restriction of $\mathrm{div}_K^{\mathfrak{m}}$ to $k^\times \to \mathcal{F}_{k,\mathfrak{m}}$ is $\mathrm{div}_k^{\mathfrak{m}}$, which is onto. Hence

$$\widehat{H}^0(G, K^\times) = k^\times / N_{K/k}(K^\times) \to \mathcal{F}_{k,\mathfrak{m}} / N_G \cdot \mathcal{F}_{K,\mathfrak{m}} = \widehat{H}^0(G, \mathcal{F}_{K,\mathfrak{m}})$$

is onto, and so $H^1(G, K_1^{\mathfrak{m}}) = 0$. □

‡ we use the fact that all $v \in \mathrm{supp}(\mathfrak{m})$ are unramified.

For any Galois extension F/k, we have exact sequences of $\mathrm{Gal}(F/k)$-modules

$$0 \to U_{F,S,\mathrm{m}} \to F_1^{\mathrm{m}} \to F_1^{\mathrm{m}}/U_{F,S,\mathrm{m}} \to 0, \qquad \text{(A.6.2)}$$

$$0 \to F_1^{\mathrm{m}}/U_{F,S,\mathrm{m}} \to \mathscr{I}_{F,\mathrm{m}} \to A_{F,S,\mathrm{m}} \to 0. \qquad \text{(A.6.3)}$$

(see 4.2.1.) From A.6.2 with $F = K$ and lemma A.6.2 we obtain the exact sequence

$$0 \to U_{k,S,\mathrm{m}} \to k_1^{\mathrm{m}} \to (K_1^{\mathrm{m}}/U_{K,S,\mathrm{m}})^G \to H^1(G, U_{K,S,\mathrm{m}}) \to 0, \qquad \text{(A.6.4)}$$

Recall the map $i^A = i^A_{K/k} : A_{k,S,\mathrm{m}} \to A_{K,S,\mathrm{m}}$ defined in section 4.2. Clearly the image of i^A is contained in $A^G_{K,S,\mathrm{m}}$, and we again write i^A for i^A with codomain restricted to $A^G_{K,S,\mathrm{m}}$.

In the commutative diagram below, the top row is exact by A.6.3 with $F = k$, the bottom row is exact by lemma A.6.1, and the column on the left is exact by A.6.4.

$$
\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & 0 & & 0 & & \ker(i^A) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & k_1^{\mathrm{m}}/U_{k,S,\mathrm{m}} & \longrightarrow & \mathscr{I}_{k,S,\mathrm{m}} & \longrightarrow & A_{k,S,\mathrm{m}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle i^A} & & \\
0 & \longrightarrow & (K_1^{\mathrm{m}}/U_{K,S,\mathrm{m}})^G & \longrightarrow & \mathscr{I}^G_{K,S,\mathrm{m}} & \longrightarrow & A^G_{K,S,\mathrm{m}} & \longrightarrow & H^1(G, K_1^{\mathrm{m}}/U_{K,S,\mathrm{m}}) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & H^1(G, U_{K,S,\mathrm{m}}) & & 0 & & \mathrm{coker}(i^A) & & \\
 & & \downarrow & & & & \downarrow & & \\
 & & 0 & & & & 0 & &
\end{array}
$$

Applying the snake lemma gives the exact sequence

$$0 \to \ker(i^A) \to H^1(G, U_{K,S,\mathrm{m}}) \to 0 \to \mathrm{coker}(i^A) \to H^1(G, K_1^{\mathrm{m}}/U_{K,S,\mathrm{m}}) \to 0$$

and so under the resulting isomorphisms, the third column above becomes

$$0 \to H^1(G, U_{K,S,\mathrm{m}}) \to A_{k,S,\mathrm{m}} \to A^G_{K,S,\mathrm{m}} \to H^1(G, K_1^{\mathrm{m}}/U_{K,S,\mathrm{m}}) \to 0.$$

Finally, A.6.2 and lemma A.6.2 show that

$$0 \to H^1(G, K_1^{\mathrm{m}}/U_{K,S,\mathrm{m}}) \to H^2(G, U_{K,S,\mathrm{m}})$$

is exact, and splicing the last two exact sequences together shows that 5.6.3 is exact ($H^2(G, U_{K,S,\mathrm{m}}) \cong \widehat{H}^0(G, U_{K,S,\mathrm{m}})$ since G is assumed to be cyclic).

A.7 Some results required for the proof of the Rubin-Stark conjecture for quadratic extensions.

We will use the convention in subsection 5.6.3 that the subscripts S and $\mathfrak{m}$ will be omitted. Our standing assumptions are that U_K is torsion-free, that $\{u_i : i = 1, \ldots, d+2r\}$ and $\{u_i : i = 1, \ldots, d+r\}$ are $\mathbb{Z}$-bases for U_K and U_k respectively, and that, in the case where $r(1_G) = r(\chi)$, $\{N_{K/k}(\tilde{u}_i) : i = 1, \ldots, r\}$ is a $\mathbb{Z}$-basis for $N_{K/k}(U_K)$.

Lemma A.7.1. *If $H^1(G, U_K) \neq 0$, we may assume that $N_{K/k}(u_{d+r+1}) = 1$.*

Proof. ([Hay04] lemma 4.3, p 10) Since $H^1(G, U_K) = \ker(N_{K/k})/U_K^{1-\sigma}$, we can find $u \in \ker(N_{K/k}) \smallsetminus U_K^{1-\sigma}$. Write $u = \epsilon \prod u_i^{m_i}$, where $\epsilon \in U_k$, $m_i \in \mathbb{Z}$, and the product runs from $i = d+r+1$ to $i = d+2r$. Since $u_i^2 = u_i^{1+\sigma} u_i^{1-\sigma}$, we can write $u = \epsilon_1 \epsilon_2 \prod u_i^{n_i}$, where $\epsilon_1 \in U_k$, $\epsilon_2 \in U_K^{1-\sigma}$, and $n_i = 0$ or 1. If all the n_i's are zero, then $1 = N_{K/k}(u) = N_{K/k}(\epsilon_1) = \epsilon_1^2$, and so $\epsilon_1 = 1$ since U_k is torsion-free. But this implies $u = \epsilon_2 \in U_K^{1-\sigma}$, a contradiction. Therefore, without loss of generality, we may assume $n_{d+r+1} = 1$, and replacing u_{d+r+1} by $u\epsilon_2^{-1} = \epsilon_1 \prod u_i^{n_i}$ gives the desired basis. □

Lemma A.7.2. *If $\widehat{H}^0(G, U_K) \neq 0$, we may assume that $\tilde{u}_1 \in U_k$.*

Proof. Since $\widehat{H}^0(G, U_K) = U_k/N_{K/k}(U_K)$, we can find $u \in U_k \smallsetminus N_{K/k}(U_K)$. Write $N_{K/k}(u) = \prod N_{K/k}(\tilde{u}_i)^{m_i}$, where $m_i \in \mathbb{Z}$ and the product runs from $i = 1$ to $i = r$. Then $u = \epsilon \prod \tilde{u}_i^{m_i}$ for some $\epsilon \in \ker(N_{K/k})$. Since $\tilde{u}_i^2 = \tilde{u}_i^{1-\sigma} \tilde{u}_i^{1+\sigma}$, we may write $u = \epsilon_1 \epsilon_2 \prod \tilde{u}_i^{n_i}$ where $\epsilon_1 \in \ker(N_{K/k})$, $\epsilon_2 \in N_{K/k}(U_K)$ and $n_i = 0$ or 1. If all the n_i's are zero, then $u^2 = N_{K/k}(u) = N_{K/k}(\epsilon_2) = \epsilon_2^2$. Since U_k is torsion-free, $u = \epsilon_2 \in N_{K/k}(U_K)$, a contradiction. Therefore, without loss of generality, we may assume $n_1 = 1$, and replacing $\tilde{u}_1$ by $u\epsilon_2^{-1} = \epsilon_1 \prod \tilde{u}_i^{n_i}$ gives the desired basis. □

We will need the following result of Reiner in proving the Rubin-Stark conjecture for quadratic extensions. Suppose $G = \langle \sigma \rangle$ is a group of prime order p, with ζ a primitive p-th root of unity. Consider the following types of G-modules M:

Type 1) $M = \mathbb{Z}$ with trivial G-action.

Type 2) $M = \mathfrak{U}$, an ideal of $\mathbb{Z}[\zeta]$, with G-action given by $\sigma \cdot u = \zeta u$.

Type 3) Those M for which there exists a non-split extension

$$0 \to \mathfrak{U} \to M \to \mathbb{Z} \to 0,$$

where $\mathfrak{U}$ and $\mathbb{Z}$ are as in 2) and 1) respectively.

Theorem A.7.1 (Reiner). *(see [Swa70] theorem 4.19, pp 73-74) Every finitely generated G-module is isomorphic to*

$$M_1 \bigoplus M_2 \bigoplus M_3,$$

where each M_i is a direct sum of G-modules of type i. Furthermore, the number of summands in each M_i is unique.

The case we are interested in is $p = 2$; in this case a module of type 2 is isomorphic to $\mathbb{Z}$, with $\sigma \cdot n = -n$, and it is not hard to see that any module of type 3 is isomorphic to $\mathbb{Z}[G]$. Note that if M_i is of type i ($i = 1, 2$), then $H^1(G, M_1)$ and $\widehat{H}^0(G, M_2)$ are both $\mathbb{Z}/2\mathbb{Z}$. Thus if M is a finitely generated G-module with $\widehat{H}^0(G, M) = H^1(G, M) = 0$, M must be a direct sum of modules of type 3 only, hence free.

Bibliography

[Aok04] Noboru Aoki. On Tate's refinement for a conjecture of Gross and its generalization. *Journal de Théorie des Nombres de Bordeaux*, 16:457–486, 2004.

[AW67] M. F. Atiyah and C. T. C. Wall. Cohomology of Groups. In J. W. S. Cassels & A. Frölich., editor, *'Algebraic Number Fields', Proceedings of the Brighton Symposium 1965*. Academic Press London, 1967.

[Bly77] T. S. Blyth. *Module Theory*. Clarendon Press, 1977.

[Bra47] Richard Brauer. On Artin's L-Functions with General Group Characters. *The Annals of Mathematics*, 48(2):502–514, April 1947.

[BS66] Z. I. Borevich and I. R. Shafarevich. *Number Theory*. Number 20 in Pure and Applied Mathematics: A Series of Monographs and Textbooks. Academic Press, 1966.

[Bur07] David Burns. Congruences between derivatives of abelian L-functions at $s = 0$. *Inventiones Math.*, 169:451–499, 2007.

[Cas67] J. W. S. Cassels. Global Fields. In J. W. S. Cassels & A. Frölich., editor, *'Algebraic Number Fields', Proceedings of the Brighton Symposium 1965*. Academic Press London, 1967.

[CG98] P. Cornacchia and C. Greither.. Fitting ideals of class groups of real fields with prime power conductor. *J. Number Th.*, 73:459–471, 1998.

[Coh00] Henri Cohen. *Advanced Topics in Computational Number Theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, 2000.

[Coh03] P. M. Cohn. *Basic Algebra: Groups, Rings and Fields*. Springer-Verlag, 2003.

[Das] Samit Dasgupta. Stark's Conjectures. Honours thesis, Harvard, 1999.

[DR80] P. Deligne and K. Ribet. Values of abelian L-functions at negative integers over totally real fields. *Invent. Math.*, 59:227–286, 1980.

[Emm06] Caleb Emmons. *Higher Order Integral Stark-Type Conjectures*. PhD thesis, University of California, San Diego, 2006.

[Gra03] Georges Gras. *Class Field Theory: From Theory to Practice*. Springer Monographs in Mathematics. Springer-Verlag, 2003.

[Gro88] B. H. Gross. On the values of abelian L-functions at $s = 0$. *J. Fac. Sci. Univ. Tokyo*, 35:177–197, 1988.

[Hay04] A. Hayward. A class-number formula for higher derivatives of abelian L-functions. *Compositio Mathematica*, 140:99–129, 2004.

[JK81] Gordon James and Adalbert Kerber. *The Representation Theory of the Symmetric Group*. Encyclopedia of Mathematics and its Applications. Addison-Wesley Publishing Company, 1981.

[Lam01] Tsit-Yuen Lam. *A First Course in Non-Commutative Rings*. Number 131 in Graduate Texts in Mathematics. Springer-Verlag, 2 edition, 2001.

[Mar77] J. Martinet. Character Theory and Artin L-functions. In A. Frölich., editor, *'Algebraic Number Fields', Proceedings of the Durham Symposium 1975*. Academic Press London, 1977.

[Mat86] Hideyuki Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1986.

[Nar90] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer-Verlag, second edition, 1990.

[Neu86] Jürgen Neukirch. *Class Field Theory*, volume 280 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1986.

[Nor] D. G. Northcott. *Finite Free Resolutions*, volume 71 of *Cambridge Tracts in Mathematics*. Cambridge University Press.

[Pop] Cristian Popescu. personal communication.

[Pop02] Cristian Popescu. Base change for Stark-type conjectures "over $\mathbb{Z}$". *J. Reine Angew. Math*, 524:85–111, 2002.

[Rim65] D. S. Rim. An Exact Sequence in Galois Cohomology. *Proc. Amer. Math. Soc.*, 16(4):4837–840, 1965.

[Rom95] Steven Roman. *Field Theory*. Number 158 in Graduate Texts in Mathematics. Springer-Verlag, 1995.

[Rub92] K. Rubin. Stark units and Kolyvagin's 'Euler systems'. *J. Reine Angew. Math*, 452:141–154, 1992.

[Rub96] K. Rubin. A Stark Conjecture 'over $\mathbb{Z}$' for Abelian L-functions with multiple zeros. *Annales de l'institute Fourier*, 46:33–62, 1996.

[San01] J. Sands. Stark's question and Popescu's conjecture for abelian L-functions. In M. Jutila and T. Metsänkylä, editors, *Number Theory: Proceedings of the Turku Symposium in Memory of K. Inkeri*, pages 305–315. Walter de Gruyter, Berlin, 2001.

[Ser77] J.-P. Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics*. Springer-Verlag, 1977.

[Ser79] J.-P. Serre. *Local Fields*. Number 67 in Graduate Texts in Mathematics. Springer-Verlag, 1979.

[Shi76] T. Shintani. On the evaluation of zeta functions of totally real algebraic fields at non-positive integers. *J. Fac. Sci. Univ. Tokyo*, 23:393–417, 1976.

[Sie70] C. L. Siegel. Über die Fourierschen Koeffizienten von Modulformen. *Nach. Akad. Wiss. Göttingen*, 3:15–56, 1970.

[Sma] Charles Small. *Arithmetic of Finite Fields*, volume 148 of *Pure and Applied Mathematics: A Program of Monographs, Textbooks, and Lecture Notes.* Marcel Dekker, Inc.

[Sol02] D. Solomons. p-Adic Abelian Stark Conjectures at $s = 1$. *Annales de l'institute Fourier*, 52(2):379–417, 2002.

[Sta71] H. M. Stark. Values of L-Functions at $s = 1$. I. L-Functions for quadratic forms. *Advances in Mathematics*, 7:301–343, 1971.

[Sta75] H. M. Stark. L-Functions at $s = 1$. II. Artin L-Functions with Rational Characters. *Advances in Mathematics*, 17:60–92, 1975.

[Sta76] H. M. Stark. L-Functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem. *Advances in Mathematics*, 22(1):64–84, 1976.

[Sta80] H. M. Stark. L-Functions at $s = 1$. IV. First derivatives at $s = 0$. *Advances in Mathematics*, 35:197–235, 1980.

[Swa70] R. Swan. *K-Theory of Finite Groups and Orders*, volume 149 of *Lecture Notes in Mathematics.* Springer-Verlag, 1970.

[Tat67] J. Tate. Global Class Field Theory. In J. W. S. Cassels & A. Frölich., editor, *'Algebraic Number Fields', Proceedings of the Brighton Symposium 1965.* Academic Press London, 1967.

[Tat84] J. Tate. *Les Conjectures de Stark sur les Fonctions L d'Artin en* $s = 0$, volume 47 of *Progress in Mathematics.* Birkhäuser, 1984.

[Was82] L. C. Washington. *Introduction to Cyclotomic Fields.* Number 83 in Graduate Texts in Mathematics. Springer-Verlag, 1982.

[Wei] C. Weibel. *K-Theory.*