Explicit class field theory in function fields: Gross-Stark units and Drinfeld modules

Alison Miller

April 23, 2008

Contents

Chapter 1

Introduction

Since the time of Euclid, mathematicians have studied the set of integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

and the set of rational numbers $\mathbb{Q}$, which contains all ratios p/q of pairs of integers p and q with $q \neq 0$. The sets $\mathbb{Z}$ and $\mathbb{Q}$ are endowed with additional structure due to the presence of certain arithmetic operations of addition on these sets. The set $\mathbb{Z}$ is called a *ring* because it is closed under the operations of addition, subtraction, and multiplication. However, the quotient of two integers p and q may be a rational number that is not an integer. On the other hand, the rational numbers are not only closed under addition, subtraction, and multiplication, but also under division by nonzero rationals; thus the rational numbers are called a *field*.

Ancient Greek mathematicians such as Euclid studied the structure of the integers and of the rationals. In particular, they showed that any positive integer can be uniquely factored as a product of prime numbers. However, they also discovered the limitations of the rational numbers: most famously, they proved that the square root of 2 is an irrational number. Algebraically, this is equivalent to saying that the equation $x^2 = 2$ has no solutions in $\mathbb{Q}$. In order to find solutions, one must work in the larger field $\mathbb{Q}(\sqrt{2})$ which contains all numbers of the form $a + b\sqrt{2}$, where a and b are rational numbers. As mathematicians attempted to solve higher-degree equations, they discovered that the key to understanding them was to understand the "number fields" in which the solutions of the equations lived. This idea was the core of Galois theory (see [1] for more historical background).

1.1 Class field theory

In the late 19th and early 20th century, a group of mathematicians, notably including Emil Artin, discovered a surprising connection known as class field theory [7] between the set of primes of a field F and the set of Galois extensions of F. Class field theory implies that given a base field F, such as $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{2})$, there exists a family of larger fields containing F and having certain algebraic properties (namely, the fields are Galois extensions of F with abelian

Galois group). Unfortunately, the elegant theoretical arguments showing the existence of these families did not actually give a recipe for constructing the families. However, there are a few cases in which we have a simple description of these families in terms of analytic functions. One of these is the case where the base field is the rationals. Then the fields shown to exist by class field theory are of the form $\mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{\frac{2\pi i}{n}}$ is a primitive nth root of unity: that is, $\zeta_n^n = 1$, but no smaller power of ζ_n equals 1. The fields $\mathbb{Q}(\zeta_n)$ can be constructed purely algebraically, but they can also be constructed analytically, because $\zeta_n = e^{\frac{2\pi i}{n}}$ is the value of the analytic function $e^{2\pi iz}$ given by the infinite sum

$$e^{2\pi iz} = 1 + \frac{2\pi iz}{1!} + \frac{(2\pi iz)^2}{2!} + \frac{(2\pi iz)^3}{3!} + \cdots$$

evaluated at the rational number $z = \frac{1}{n}$. This is, however, not the only way of constructing these fields analytically. For example, if we are only interested in the subset of the field $\mathbb{Q}(\zeta_n)$ that is contained in the real numbers, we can consider the closely related trigonometric function $\sin(\pi z)$, which has the infinite product expansion

$$\sin(\pi z) = \pi z \prod_{a=1}^{\infty} \left(1 - \frac{z}{a}\right)\left(1 + \frac{z}{a}\right). \tag{1.1}$$

When z is a rational number, the value of $\sin(\pi z)$ is algebraic. For example, when $z = \frac{1}{2}$, $\sin(\pi/2) = \frac{\sqrt{2}}{2}$ is an algebraic number. The analytic functions $e^{2\pi iz}$ and $\sin(\pi z)$ are then said to make class field theory "explicit" for the base field $\mathbb{Q}$.

The problem of finding analytic functions whose values generate the abelian extensions of an arbitrary base field is known as Hilbert's Twelfth Problem. Although the exponential construction for $\mathbb{Q}$ is elegant, it does not generalize to arbitrary base fields. In one other case, the case of imaginary quadratic fields such as $\mathbb{Q}(i)$, there is an analytic construction based on elliptic functions. Elliptic functions are similar to exponential and trigonometric functions in that they are periodic, but unlike trigonometric functions, they have two distinct complex-valued periods, not just one. For other base fields, including real quadratic base fields such as $\mathbb{Q}(\sqrt{2})$ as well as other more complicated fields, there is no known simple generalization of the exponential function.

However, there is hope that such a generalization might exist for certain fields F, thanks to a conjecture of Stark from the 1970s [13]. Stark's conjecture states that any finite abelian extension K of a base field F contains a special element known as a *Stark unit* which has close ties to certain *partial zeta-functions* associated to the extension. Partial zeta-functions are functions that generalize the Riemann zeta-function, defined for a complex variable s with $\mathrm{Re}(s) > 1$ by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{1.2}$$

The function $\zeta(s)$ can be extended by analytic continuation to the entire complex plane. Stark's conjecture states that the absolute values of the Stark unit are equal to certain linear combinations of the leading terms of the expansions of the partial zeta-functions at $s = 0$.

Stark's conjecture does not give an explicit formula for the Stark unit, but such an explicit formula was given in certain cases in refined conjectures by Gross [6] and Dasgupta [3]. Although these conjectures are known to be true when the base field is $\mathbb{Q}$ or an imaginary quadratic field, and they are supported by numerical evidence, it is still somewhat mysterious why they are true in general.

1.2 Function fields

Since explicit class field theory is difficult to tackle in number fields, it is natural to study a a similar, but simpler, setting in which to test and verify these conjectures. One such setting is the theory of function fields. Function fields are in many ways similar to number fields, but in many cases their theory is substantially easier. The set $\mathbb{C}[T]$ of polynomials in the variable T with complex-valued coefficients acts in many ways like the integers $\mathbb{Z}$. Like the integers, it is a ring: that is, it is closed under addition, subtraction, multiplication, and division. More interestingly, just as every integer has a unique factorization into primes, every polynomial has a unique factorization into irreducible (or "prime") polynomials. One defines a field of rational functions in complete analogy with the rational numbers: the field $\mathbb{C}(T)$ of rational functions over the complex numbers contains all quotients $P(T)/Q(T)$ of polynomials $P(T), Q(T) \in \mathbb{C}[T]$ with $Q(T) \neq 0$. The field $\mathbb{C}(T)$ is called a "function field" because any element of $\mathbb{C}(T)$ defines a meromorphic function on the complex numbers. We can construct larger field extensions of $\mathbb{C}(T)$ by adding in roots of polynomials, just as we constructed extensions of the rationals. These field extensions of $\mathbb{C}(T)$ are also function fields, but now their elements correspond to functions on a more general complex algebraic curve. For example, elements of the field

$$\mathbb{C}(T)[\sqrt{T^3+1}] = \{f(T) + g(T)\sqrt{T^3+1} \mid f(T), g(T) \in \mathbb{C}(T)\}$$

correspond to meromorphic functions on the algebraic curve defined by the equation

$$S^2 = T^3 + 1.$$

The advantage of function fields is that many properties of the arithmetic of the function field correspond directly to properties of the corresponding algebraic curve. For example, the Fundamental Theorem of Algebra states that any monic polynomial $P(T)$ with complex coefficients factors as

$$P(T - \alpha) = \prod_{\alpha} (T - \alpha)$$

where α ranges over the set of all roots of P (counted with appropriate multiplicity). Hence the irreducible factors of P are linear factors that correspond to the values α with $P(\alpha) = 0$. In other words, factoring a polynomial over $\mathbb{C}$ is equivalent to finding its roots in the complex numbers. Hence the primes in the function field $\mathbb{C}[T]$ correspond to points of $\mathbb{C}$. A more general statement is true: for the appropriate generalization of the notion of "prime" to an arbitrary function field, it is generally the case that primes of a function field correspond to points of the corresponding algebraic curve.

Although we have discussed the field $\mathbb{C}(T)$ of polynomials over the complex numbers for the sake of simplicity, the discussion above generalizes to the field of polynomials with coefficients in an arbitrary field. (It will no longer be the case that every polynomial factors as a product of linear factors, but one can still say that primes correspond to points of the curve for a slightly generalized definition of "points.") In fact, the field $\mathbb{C}(x)$ does not give the best analogy with the rational numbers, because the complex numbers are in some sense "too large". It turns out that to obtain the best analogue of $\mathbb{Z}$ and $\mathbb{Q}$, it is most convenient to use coefficient fields that are *finite*. The simplest finite field is the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of "integers mod p." One can also construct other finite fields algebraically. For every integer q that is a power of a prime, there is a unique field with exactly q elements denoted $\mathbb{F}_q$.

From now on "function field" will always mean "function field of an algebraic curve over $\mathbb{F}_q$." Many results that hold in the setting of number fields also hold in function fields, and in fact the proofs are often easier in the function field setting. In fact some statements that are only conjectured in the former setting are proven theorems in the latter. For example, one of the most important outstanding conjectures in number theory, the Riemann Hypothesis, has an analogous statement in function fields which has been proven. The Riemann hypothesis is a statement about the zeroes of the function $\zeta(s)$ defined above in (1.2). Statements about the distribution of these zeroes have implications for the distribution of primes in the integers, and in particular the Riemann hypothesis has many important consequences in number theory. If we now replace $\mathbb{Z}$ with $\mathbb{F}_q[T]$, the analogous zeta function has the following simple expansion:

$$\zeta_{\mathbb{F}_q[T]}(s) = \prod_{\substack{a \in \mathbb{F}_q[T] \\ a \text{ monic}}} \frac{1}{q^{(\deg a)s}} = \sum_{d=0}^{\infty} q^{d(1-s)} = \frac{1}{1-q^{1-s}} \tag{1.3}$$

This function is never zero. Hence we know precisely what the zeroes of the zeta function of $\mathbb{F}_q[T]$ are: there are none of them! As a result, the Riemann hypothesis for $\mathbb{F}_q[T]$ is trivial, and knowing the exact formula for $\zeta_{\mathbb{F}_q[T]}$ tells us a good deal about the distribution of prime elements in $\mathbb{F}_q[T]$. The generalizations of the Riemann hypothesis for function fields other than $\mathbb{F}_q[T]$ are less trivial, and have been proved by Weil [14].

Another famous unsolved problem in number theory, the Birch and Swinnerton-Dyer conjecture, also has an analogue over function fields. Although the Birch and Swinnerton-Dyer conjecture has not been proven in function fields, substantial progress has been made, and a number of special cases are known results. Like Stark's conjecture, both conjectures involve zeta functions or related functions called L-functions, which in general have simpler behavior in function fields. Hence it is reasonable to expect that Stark's conjecture and its refinements are tractable in function fields – and in fact they are!

The key to proving the function field analogues of these conjectures is an explicit class field theory for function fields developed by Drinfeld and elaborated by Hayes [10]. This theory constructs exponential-type functions defined on the appropriate function field analogue of the complex numbers. The special values of these exponential functions generate abelian extensions of function fields just as the special values $e^{2\pi i/n}$ generate abelian extensions of the rational numbers. These exponential functions are periodic, like ordinary exponential or trigonometric functions. They can be expressed analytically as a power series like that of e^z and also have an infinite product expansion similar to that of $\sin z$. The simplest example, the *Carlitz exponential* corresponding to the ring $\mathbb{F}_q[T]$, has the following product expansion:

$$e_{\mathbb{F}_q[T]}(z) = z \prod_{\substack{a\in\mathbb{F}_q[T] \\ a\neq 0}} \left(1 - \frac{z}{a}\right). \tag{1.4}$$

Note that this expansion is quite similar to the product expansion of $\sin(\pi z)$ given in (1.1).

Drinfeld's insight was to attach an algebraic structure known as a *Drinfeld module* to every such exponential function. This Drinfeld module was the link that joined the analytic exponential functions with the algebraic structures of class fields. Hayes elaborated on these ideas and showed that the explicit formulas coming from the exponential functions could be manipulated to define elements with the appropriate properties of Stark units. He thus proved the Stark conjecture in function fields. Hayes further showed that Gross's conjecture also held for these elements.

1.3 Outline

In this thesis, we will give an exposition of Hayes's proof of the conjectures of Stark and Gross. However, we will also go beyond what Hayes has done, and show that his formulas also imply a function field analogue of Dasgupta's conjecture. This result is original to this thesis.

Chapter 2 is a brief overview of terminology and notation. In Chapter 3, we introduce Stark's conjecture and its refinements by Gross and Dasgupta. The chapter culminates in the statement of a function field analogue of Dasgupta's conjecture, which gives a totally explicit formula for Stark's unit. This formula is the analogue of the formula in Dasgupta's conjecture for number fields. Chapter 4 is an exposition of the theory of rank-one Drinfeld modules over a function field as a means of obtaining an explicit class field theory. Finally, in Chapter 5, we apply the theory of Drinfeld modules to the conjectures stated in Chapter 3. We explain Hayes's proof [9] of Stark's conjecture and of Gross's refinement in function fields. We finally show that his methods can be extended to prove Dasgupta's refinement.

Chapter 2

Definitions and class fields

Let F be a global field with places at infinity $\infty_1, \ldots, \infty_n$, and let $\mathcal{O}$ be the ring of elements integral at all places other than $\infty_1, \ldots, \infty_n$. There are two kinds of global fields: number fields and function fields. In the case where F is a number field, we will be using the term "places at infinity" in its conventional meaning to denote places corresponding to archimedean valuations, so that $\mathcal{O}$ is the usual ring of integers $\mathcal{O}_F$. Furthermore, in the case that F is a number field, we will always assume that F is totally real.

However, in the case of function fields, all valuations are non-archimedean and no places are specially distinguished, so our choice of places $\infty_1, \ldots, \infty_n$ is somewhat arbitrary. The simplest example would be to consider $F = \mathbb{F}_q(T)$ and a single infinite place ∞ corresponding to the valuation $v_\infty(a) = -\deg a$, that is, corresponding to the point at infinity on the projective line over $\mathbb{F}_q$. A somewhat more general example would be to have F be a finite extension of $\mathbb{F}_q(T)$ and the places $\infty_1, \ldots, \infty_n$ correspond exactly to the places of F lying over the prime ∞ of $\mathbb{F}_q(T)$. This family of examples is the most closely analogous to the case of number fields, however, it is not the most general case, and all our formulas will work with arbitrary choices of places at infinity. Each place ∞_i has a degree $d_{\infty_i} = [k_{\infty_i} : \mathbb{F}_q]$, which may depend upon i. For each infinite place ∞_i, let $\mathbf{F}_{\infty_i}$ be the completion of F at the place ∞_i, and let $\boldsymbol{\mathcal{O}}_{\infty_i}$ be its ring of integers. (In our paper, we will use the convention that completions are written in bold.) Let k_{∞_i} be the field of constants of the local field $\mathbf{F}_{\infty_i}$, that is, the residue field of the ring of the local field $\mathbf{F}_{\infty_i}$. The field k_{∞_i} is also canonically isomorphic to the algebraic closure of $\mathbb{F}_q$ inside $\mathbf{F}_{\infty_i}$. Each completion $\mathbf{F}_{\infty_i}$ is a local field with a valuation map $v_{\infty_i} : \mathbf{F}_{\infty_i}^\times \to \mathbb{Z}$, which restricts to a valuation v_{∞_i} on $F^\times$. This valuation is normalized in the standard way, so that v_{∞_i} surjects onto $\mathbb{Z}$. This valuation can be used to define the ∞_i-adic absolute value on $\mathbf{F}_{\infty_i}$, defined by $|z|_{\infty_i} = q^{-d_{\infty_i} v_{\infty_i} z}$. Note that we can in the same way define valuations $v_\mathfrak{p}$ and $||_\mathfrak{p}$ for all places of F, not just the infinite ones.

We will associate a sign-function on $\mathbf{F}_{\infty_i}^\times$ to each infinite place ∞_i of F, which, in both the number field and function field cases, will be a surjective multiplicative homomorphism from $\mathbf{F}_{\infty_i}^\times$ to the group of roots of unity in $\mathbf{F}_{\infty_i}^\times$.

In the number field case, we have assumed that F is totally real. This means that for each infinite place ∞_i, the completion $\mathbf{F}_{\infty_i}$ is isomorphic to $\mathbb{R}$, and we have a canonical sign function: $\mathrm{sgn}_\infty : \mathbf{F}_\infty^\times \to \{\pm 1\}$ which is the same as the normal sign function on $\mathbb{R}^\times$.

Unlike with number fields, in the function field case, we have a choice of sign functions. Recall that k_{∞_i} is the field of constants of the local field $\mathbf{F}_{\infty_i}$. Then k_{∞_i} is a finite field, and $k_{\infty_i}^\times$ is exactly the group of roots of unity in $\mathbf{F}_{\infty_i}$. We first choose a uniformizer π_{∞_i} for $\mathbf{F}_{\infty_i}$. By definition of a uniformizer, any $x \in \mathbf{F}_{\infty_i}$ can be written as $\pi_{\infty_i}^f a_x$ for some a_x in the group $\boldsymbol{\mathcal{O}}_{\infty_i}^\times$ of units in $\boldsymbol{\mathcal{O}}_{\infty_i}$. We define $\mathrm{sgn}_{\infty_i}(x)$ to be the image of $a_x \in \boldsymbol{\mathcal{O}}_{\infty_i}^\times$ in the multiplicative group $k_{\infty_i}^\times$ of the residue field k_{∞_i}. Equivalently, the sign function sgn_{∞_i} is defined as the unique homomorphism $\mathbf{F}_{\infty_i}^\times \to k_{\infty_i}^\times$ such that the restriction $\mathrm{sgn}\,|_{\boldsymbol{\mathcal{O}}_{\infty_i}^\times}$ is the same as the reduction mod ∞_i map $\boldsymbol{\mathcal{O}}_{\infty_i}^\times \to k_{\infty_i}^\times$ and such that $\mathrm{sgn}(\pi_{\infty_i}) = 1$.

Definition. In both the number and function field case, we define $x \in \mathbf{F}_{\infty_i}$ to be *positive* if $x \in \ker \mathrm{sgn}_{\infty_i}$. Likewise, we say that $x \in F$ is *totally positive* and write $x \gg 0$ if, for each i, the image of x under the inclusion map $F \hookrightarrow \mathbf{F}_{\infty_i}$ is a positive element of $\mathbf{F}_{\infty_i}$.

In the function field case, we will also take advantage of our freedom to put arbitrary places at infinity. In particular, it will often be useful for us to work in a context where we will treat a single place $\mathfrak{p}$, distinct from our previously chosen places at infinity, as the only infinite place (this is, unfortunately, a freedom that we have only in function fields). In particular, we will consider the completion $\mathbf{F}_\mathfrak{p}$ of F at $\mathfrak{p}$: as in the previous paragraph, we can define a sign-function $\mathrm{sgn}_\mathfrak{p}$ on $\mathbf{F}_\mathfrak{p}$ as well. We choose a uniformizer $\varpi = \varpi_\mathfrak{p}$ for $\mathbf{F}_\mathfrak{p}$, and we let $\mathrm{sgn}_\mathfrak{p}$ be the unique sign-function which satisfies $\mathrm{sgn}_\mathfrak{p}(\varpi) = 1$. We let A be the ring of elements of F that are regular away from $\mathfrak{p}$. Note that, just as $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$, for each i, the place ∞_i corresponds to a prime ideal of A, namely, the set of those elements of A with positive ∞_i-adic valuation. Furthermore, there is a one-to-one correspondence between ideals of $\mathcal{O}$ relatively prime to $\mathfrak{p}$ and ideals of A relatively prime to $\infty = \infty_1 \cdots \infty_n$. We will switch between these two viewpoints in our paper – when it is important to disambiguate between ideals of $\mathcal{O}$ and ideals of A, we will, for example, refer to the ideal of A corresponding to the ideal $\beta \subset \mathcal{O}$ as the ideal βA.

If F is a number field, class field theory implies that any abelian extension of F is contained in the narrow ray class field $H_\mathfrak{f}$ of conductor $\mathfrak{f}$ for some ideal $\mathfrak{f}$ of $\mathcal{O}$. This narrow ray class field is defined as the fixed field of the subgroup

$$F^\times \cdot \prod_{\infty_i} \ker \mathrm{sgn}_{\infty_i} \prod_{v|\mathfrak{f}} \mathbf{U}_{v,\mathfrak{f}} \prod_{v\nmid\infty\mathfrak{f}} \boldsymbol{\mathcal{O}}_v^\times \subset \mathbb{A}_F^\times$$

under the global Artin map (where $\mathbf{U}_{v,\mathfrak{f}}$ is the group of elements of $\mathcal{O}_v^\times$ that are congruent to 1 mod $\mathfrak{f}$), i.e. it is determined by

$$\mathrm{Gal}(H_\mathfrak{f}/F) = \mathbb{A}_F^\times / (F^\times \prod_{\infty_i} \ker \mathrm{sgn}_i \prod_{v|\mathfrak{f}} \mathbf{U}_{v,\mathfrak{f}} \prod_{v\nmid\infty\mathfrak{f}} \boldsymbol{\mathcal{O}}_v^\times). \tag{2.1}$$

The Galois group $\mathrm{Gal}(H_\mathfrak{f}/F)$ is canonically isomorphic to the narrow ray class group

$$\mathrm{Cl}_\mathfrak{f}^+(\mathcal{O}) := I_\mathfrak{f}(\mathcal{O})/P_\mathfrak{f}(\mathcal{O}),$$

where $I_{\mathfrak{f}}(\mathcal{O})$ is the group of fractional ideals of $\mathcal{O}$ relatively prime to $\mathfrak{f}$, and $P_{\mathfrak{f}}(\mathcal{O})$ is the group of principal fractional ideals generated by totally positive elements of $\mathcal{O}$ congruent to 1 mod $\mathfrak{f}$. It is a standard fact from class field theory that

Proposition 2.0.1. $\mathrm{Gal}(H_{\mathfrak{f}}/F) \cong \mathrm{Cl}_{\mathfrak{f}}^{+}(\mathcal{O})$.

However, any construction that depends purely upon $\mathfrak{p}$-adic limits must live in some field K that can be embedded in the completion $\mathbf{F}_{\mathfrak{p}}$. This is the case when the local Artin map at $\mathfrak{p}$ acts trivially on K. To this end, we let $H = H(\mathfrak{f};\mathfrak{p})$ be the fixed field of $H_{\mathfrak{f}}$ under the action of the group generated by the $\mathfrak{p}$-Frobenius element, with Galois group

$$\mathrm{Gal}(H/F) = \mathbb{A}_F^{\times}/(F^{\times}\prod_{\infty_i}\ker\mathrm{sgn}_i\prod_{v|\mathfrak{f}}\mathbf{U}_{v,\mathfrak{f}}\prod_{v\nmid\infty\mathfrak{f}\mathfrak{p}}\boldsymbol{\mathcal{O}}_v^{\times}\times\mathbf{F}_{\mathfrak{p}}^{\times}) \cong \mathrm{Cl}_{\mathfrak{f}}^{+}(\mathcal{O})/\langle\mathfrak{p}\rangle. \tag{2.2}$$

We now move to the function field setting. We can construct the fields $H_{\mathfrak{f}}$ and H in the same way as before, so that (2.1) and (2.2) both hold. However, it is now no longer the case that $H_{\mathfrak{f}}$ contains all abelian extensions of F unramified outside $\mathfrak{f}$. In the function field case, the Galois group of the the maximal abelian extension $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ is simply $\mathbb{A}_F/F^{\times}$, without the additional quotienting by $\prod_{\infty_i}\ker\mathrm{sgn}_i$. (If F is a number field, $\prod_{\infty_i}\ker\mathrm{sgn}_i$ is the connected component of the identity in $\mathbb{A}_F^{\times}$. However, if F is a function field, the connected component of the identity in $\mathbb{A}_F^{\times}$ is trivial.) This means that the requirement that $\ker\mathrm{sgn}_i$ fix $H_{\mathfrak{f}}$ for each i imposes a nontrivial condition on $H_{\mathfrak{f}}$.

We will sometimes want to consider extensions of F that are not fixed by $\prod_i\ker\mathrm{sgn}_i$. For $\mathfrak{p}$-adic constructions, the most natural family of fields to consider is the following. Let $\mathfrak{m}$ be an ideal of the ring A of elements integral away from $\mathfrak{p}$. Note that we are allowing $\mathfrak{m}$ to be divisible by the infinite primes, considered as prime ideals of A, and in fact, we will most often apply this to the case $\mathfrak{m} = \mathfrak{f}\infty$. Then we define a field $K_{\mathfrak{m}}$ by class field theory corresponding the the Galois group

$$\mathrm{Gal}(K_{\mathfrak{m}}/F) = \mathbb{A}_F^{\times}/(F^{\times}\prod_{v|\mathfrak{m}}\mathbf{U}_{v,\mathfrak{m}}\prod_{v\nmid\mathfrak{m}\mathfrak{p}}\boldsymbol{\mathcal{O}}_v^{\times}\times\mathbf{F}_{\mathfrak{p}}^{\times}). \tag{2.3}$$

This Galois group can also be expressed as a class group, this time a ray class group of the ring A of elements of F that are integral away from $\mathfrak{p}$. More precisely, define

$$\mathrm{Cl}_{\mathfrak{m}}(A) = I_{\mathfrak{m}}(A)/P_{\mathfrak{m}}(A), \tag{2.4}$$

where $I_{\mathfrak{m}}(A)$ is the group of fractional ideals of A relatively prime to $\mathfrak{m}$, and $P_{\mathfrak{m}}(A)$ is the group of principal fractional ideals of A generated by elements congruent to 1 mod $\mathfrak{m}$. Again, it is a standard fact from class field theory that

Proposition 2.0.2. $\mathrm{Gal}(K_{\mathfrak{m}}/F) \cong \mathrm{Cl}_{\mathfrak{m}}(A)$.

If we then set $\mathfrak{m} = \mathfrak{f}\infty$, we obtain

$$\mathrm{Gal}(K_{\mathfrak{f}\infty}/F) = \mathbb{A}_F^{\times}/(F^{\times}\prod_{v|\mathfrak{f}}\mathbf{U}_{v,\mathfrak{m}}\prod_{\infty_i}\mathbf{U}_{\infty_i,1}\prod_{v\nmid\mathfrak{m}\mathfrak{p}}\boldsymbol{\mathcal{O}}_v^{\times}\times\mathbf{F}_{\mathfrak{p}}^{\times}). \tag{2.5}$$

where $\mathbf{U}_{\infty_i,1}$ denotes the group of units in $\boldsymbol{\mathcal{O}}_{\infty_i}$ congruent to 1 mod ∞_i. By definition of our sign function sgn_i, the kernel $\ker \mathrm{sgn}_i$ contains $\mathbf{U}_{\infty_i}$, and it follows from this that $K_{\mathfrak{f}\infty}$ contains H. Furthermore, the relative Galois group $\mathrm{Gal}(K_{\mathfrak{f}\infty}/H)$ equals

$$\mathrm{Gal}(K_{\mathfrak{f}\infty}/H) = (F^\times \prod_{\infty_i} \ker \mathrm{sgn}_i \prod_{v|\mathfrak{f}} \mathbf{U}_{v,\mathfrak{f}} \prod_{v\nmid\infty\mathfrak{f}\mathfrak{p}} \boldsymbol{\mathcal{O}}_v^\times \times \mathbf{F}_{\mathfrak{p}}^\times)/(F^\times \prod_{v|\mathfrak{f}\infty} \mathbf{U}_{v,\mathfrak{f}\infty} \prod_{v\nmid\mathfrak{f}\infty\mathfrak{p}} \boldsymbol{\mathcal{O}}_v^\times \times \mathbf{F}_{\mathfrak{p}}^\times). \quad (2.6)$$

To simplify this expression, we make some auxiliary definitions. Let

$$\iota : F^\times \to \prod_{i=1}^{n} \mathbb{R}^{>0} \times k_{\infty_i}^\times$$

denote the map given by $\iota(z) = (|z|_{\infty_i}, \mathrm{sgn}_{\infty_i}(z))$. Note that, for function fields, this map is not injective, even though it would be in the case of number fields. Let $Q := \prod_{i=1}^n \mathbb{R}^{>0} \times 1$ be the "positive orthant" inside $\prod_{i=1}^n \mathbb{R}^{>0} \times k_{\infty_i}^\times$. Let $E_{\mathfrak{p}}(\mathfrak{f})$ denote the group of elements of $F^\times$ that are units at all places except $\mathfrak{p}$ and the infinite places, and are congruent to 1 mod $\mathfrak{f}$.

Proposition 2.0.3. *There is a canonical isomorphism* $\mathrm{Gal}(K_{\mathfrak{f}\infty}/H) \cong (\iota(F^\times) \cap Q)/\iota(E_{\mathfrak{p}})$.

Proof. By inspecting (2.6), we observe that any element of the quotient $\mathrm{Gal}(K_{\mathfrak{f}\infty}/H)$ has a representative in $\prod_{\infty_i} \ker \mathrm{sgn}_i$, that is, of the form $\{x_v\}$ where $x_{\infty_i} \in \ker \mathrm{sgn}_i$ for each i, and $x_v = 1$ for v non-infinite. We map this representative to $(\iota(F^\times) \cap Q)/\iota(E_{\mathfrak{p}})$ by $\iota\{x_v\} = \prod_{\infty_i} |x_{\infty_i}|_{\infty_i} \times 1$ (note that this agrees with our pre-existing defnition of ι on $F^\times$). This map is defined modulo the image

$$\iota\left(\ker \mathrm{sgn}_i \cap (F^\times \prod_{v|\mathfrak{m}} \mathbf{U}_{v,\mathfrak{f}\infty} \prod_{v\nmid\mathfrak{f}\infty\mathfrak{p}} \boldsymbol{\mathcal{O}}_v \times \mathbf{F}_{\mathfrak{p}}^\times)\right).$$

Since ι is trivial on $\prod_{v|\mathfrak{m}} \mathbf{U}_{v,\mathfrak{f}\infty} \prod_{v\nmid\mathfrak{f}\infty\mathfrak{p}} \boldsymbol{\mathcal{O}}_v \times \mathbf{F}_{\mathfrak{p}}^\times$, this image is the same as

$$\iota\left(F^\times \cap (\ker \mathrm{sgn}_i \prod_{v|\mathfrak{m}} \mathbf{U}_{v,\mathfrak{f}\infty} \prod_{v\nmid\mathfrak{f}\infty\mathfrak{p}} \boldsymbol{\mathcal{O}}_v \times \mathbf{F}_{\mathfrak{p}}^\times)\right),$$

which is $\iota(E_{\mathfrak{p}})$ by defintion of $E_{\mathfrak{p}}$.

This gives us a map $\iota : \mathrm{Gal}(K_{\mathfrak{f}\infty}/H) \to (\iota(F^\times) \cap Q)/\iota(E_{\mathfrak{p}})$. It is clearly surjective, since we can choose the x_i to have arbitrary absolute value, and it is also easily checked to be injective. □

Chapter 3

Stark's conjecture and its refinements

3.1 Stark's conjecture

We maintain the notation from the previous section: F is either a totally real number field, or an arbitrary function field. Let K be an abelian extension of F such that $\mathfrak{p}$ splits completely in K. Let S be a set of primes of F that contains $\infty_1, \ldots, \infty_n$, $\mathfrak{p}$, and all primes ramifying in K/F. We also require that $\#S \geq 3$, i.e., that S contains at least two primes other than $\mathfrak{p}$. Let R be the set $S - \{\mathfrak{p}\}$. Because K is unramified outside R, the Artin map $\mathbb{A}_F \to \mathrm{Gal}(K/F)$ induces a map from the group of fractional ideals relatively prime to S to the Galois group $\mathrm{Gal}(K/F)$. We will denote this map as sending an ideal $\mathfrak{a}$ to the corresponding Artin element $\sigma_{\mathfrak{a}}$. Also, for an ideal $\mathfrak{a}$ relatively prime to R, define $N\mathfrak{a} = [\mathcal{O} : \mathfrak{a}\mathcal{O}]$. Likewise, for an element α of $\mathfrak{a}$, we let $N\alpha$ denote $N(\alpha\mathcal{O})$. The norm map is multiplicative, and so we can extend N to the group of fractional ideals of $\mathcal{O}$.

In the function field case, one can show that $N\mathfrak{a} = \prod_{\infty_i} q^{-d_{\infty_i} v_{\infty_i}(\mathfrak{a})}$. Also in the function field case, if $\mathfrak{a}$ is also relatively prime to $\mathfrak{p}$, the quotient $\mathcal{O}/\mathfrak{a}\mathcal{O}$ is isomorphic to $A/\mathfrak{a}A$ (where A is the ring of elements integral away from $\mathfrak{p}$), so we can also write $N\mathfrak{a} = [A : N\mathfrak{a}]$.

Definition. For each $\sigma \in \mathrm{Gal}(K/F)$, define the partial zeta-function $\zeta_R(K/F, \sigma, s)$ as the following sum over ideals

$$\zeta_R(K/F, \sigma, s) = \sum_{\substack{(\mathfrak{a}, R) = 1 \\ \sigma_{\mathfrak{a}} = \sigma}} N\mathfrak{a}^{-s}. \tag{3.1}$$

for $\mathrm{Re}\, s \geq 1$. The function $\zeta_R(K/F, \sigma, s)$ extends by analytic continuation to a meromorphic function on the entire complex plane, with at most a simple pole at $s = 1$. Define $\zeta_S(K/F, \sigma, s)$ likewise.

Observe that $\zeta_S(K/F, \sigma, s) = (1 - N\mathfrak{p}^{-s})\zeta_R(K/F, \sigma, s)$. In particular, setting $s = 0$, we find that

$$\zeta_S(K/F, \sigma, 0) = 0, \tag{3.2}$$

a fact that we will find to be useful several times later on.

It is known that the special value $\zeta_R(K/F,\sigma,0)$ is always rational. However, we will want our zeta functions to have integral special values. The most general way of ensuring this is as follows. Let G be the Galois group $\mathrm{Gal}(K/F)$, and let $\mathbb{Z}[G]$ be the associated group ring. Then the set $\mu(K)$ of roots of unity in K has a natural $\mathbb{Z}[G]$-module structure: define $\mathrm{Ann}(K/F)$ as the submodule of elements of $\mathbb{Z}[G]$ that annihilate $\mu(K)$. Then it is more generally known [4] that, for any $A \in \mathrm{Ann}(K/F)$ of the form $A = \sum_{\gamma\in G} c_\gamma \cdot \gamma$ with coefficients $c_\gamma \in \mathbb{Z}$, the linear combination of special values

$$\sum_{\gamma\in G} c_\gamma \zeta_S(K/F,\sigma\gamma^{-1},0) \tag{3.3}$$

is integral. As a special case: let W_K be the order of the group μ_K. Then any element of μ_K is a W_Kth root of 1, so the element $W_K \in \mathbb{Z}[G]$ belongs to $\mathrm{Ann}(K/F)$. It follows that $W_K\zeta_S(K/F,\sigma\gamma^{-1},0) \in \mathbb{Z}$ for all $\sigma \in G$.

We are now ready to state the abelian form of Stark's Conjecture for non-archimedean primes $\mathfrak{p}$, as formulated by Tate in [13]. Pick a prime $\mathfrak{P}$ lying above $\mathfrak{p}$.

Conjecture 3.1.1 (Brumer-Stark Conjecture). *There exists an $\epsilon \in K$ such that*

(a) $|\epsilon|_{\mathfrak{P}'} = 1$ if $\mathfrak{P}'$ is a (possibly infinite) prime not dividing $\mathfrak{p}$.

(b) For all $\sigma \in \mathrm{Gal}(K/F)$, $\log|\epsilon^\sigma|_{\mathfrak{P}} = -W_K\zeta_S'(K/F,\sigma,0)$.

Furthermore, for λ such that $\lambda^{W_K} = \epsilon$, the extension $K(\lambda)/F$ is abelian.

Because any element of a global field which is a unit at every prime must be a root of unity, the Stark unit ϵ is defined up to multiplication by a root of unity.

We now restate the second condition of Stark's conjecture in a form that we will find more useful. First, note that, by definition of the $\mathfrak{P}$-adic valuation,

$$\log|\epsilon^\sigma|_{\mathfrak{P}} = \log(N\mathfrak{P}^{-v_{\mathfrak{P}}(\epsilon^\sigma)}) = -v_{\mathfrak{P}}(\epsilon^\sigma)\log(N\mathfrak{p})$$

using the fact that $\mathfrak{p}$ is totally split to replace $N\mathfrak{P}$ with $N\mathfrak{p}$. On the other hand, differentiating the expression $\zeta_S(K/F,\sigma,s) = (1-N\mathfrak{p}^{-s})(\zeta_R(K/F,\sigma,s))$ at $s=0$ yields

$$\zeta_S'(K/F,\sigma,0) = \log(N\mathfrak{p})\zeta_R(K/F,\sigma,0). \tag{3.4}$$

Putting these results together gives us the following reformulation of condition (b):

$$v_{\mathfrak{P}}(\epsilon^\sigma) = W_K\zeta_R(K/F,\sigma,0). \tag{3.5}$$

3.2 Shifted Stark units

We would like to be able to specify a unit that is actually well-defined, not just well-defined up to multiplication by a root of unity. Gross's refinement of Stark's conjecture is about such a specific unit, and it also gives more information. We first take a closer look at the structure of annihilators of roots of unity.

Lemma 3.2.1. *Let L be an abelian extension of F, and let $G = \mathrm{Gal}(L/F)$. Let S be a set of primes of F including the infinite ones, the ones that ramify in F, and, when L and F are number fields, the ones dividing the order W_L of the group μ_L. Then the annihilator $\mathrm{Ann}(L/F)$ in $\mathbb{Z}[G]$ of the $\mathbb{Z}[G]$-module $\mu(L)$ is generated as a $\mathbb{Z}$-module by the set of elements $\{\sigma_{\mathfrak{q}} - N\mathfrak{q}\}$ where $\mathfrak{q}$ ranges over the set of primes of F that are not in S.*

Proof. For simplicity, we prove the result assuming that L and F are function fields. The proof in the case of number fields follows the same lines (see [12] for a proof.)

The first thing we need to do is confirm that $\sigma_{\mathfrak{q}} - N\mathfrak{q}$ lies in the annihilator $\mathrm{Ann}(L/F)$, or equivalently, we need to show that, for any root of unity $\zeta \in \mu_L$, $\sigma_{\mathfrak{q}}(\zeta) = \zeta^{N\mathfrak{q}}$. Let B be the integral closure of A in L, and let $\mathfrak{Q}$ be a prime of L lying above the prime $\mathfrak{q}$ of F. By the definition of $\sigma_{\mathfrak{q}}$, we have $\sigma_{\mathfrak{q}}(\zeta) \equiv \zeta^{N\mathfrak{q}} \pmod{\mathfrak{Q}}$. If we can show that the roots of unity in L are all distinct mod $\mathfrak{Q}$, we will be done. But, since we are in finite characteristic, the roots of unity in L generate a finite subfield ℓ of L that consists entirely of units in B, and this finite subfield must inject into $B/\mathfrak{Q}$, so the roots of unity in L are all distinct mod $\mathfrak{Q}$.

Let M be the $\mathbb{Z}$-module generated by $\{\sigma_{\mathfrak{q}} - N\mathfrak{q} \mid \mathfrak{q} \notin S\}$. We have shown that $M \subset \mathrm{Ann}(L/F)$; we now need to show that M is actually equal to $\mathrm{Ann}(L/F)$.

By the Chebotarev Density Theorem, every $\sigma \in G$ is of the form $\sigma_{\mathfrak{q}}$ for some prime $\mathfrak{q}$ not in S, and it follows that every element of $\mathbb{Z}[G]$ is congruent mod M to an element of $\mathbb{Z}$. Hence it suffices to show that $M \cap \mathbb{Z} = \mathrm{Ann}(L/F) \cap \mathbb{Z}$. But μ_L is a cyclic $\mathbb{Z}$-module of order W_L, so $\mathrm{Ann}(L/F) \cap \mathbb{Z}$ consists exactly of the multiples of W_L, and it suffices to show that $W_L\mathbb{Z} = M \cap \mathbb{Z}$.

Note that $\mathrm{Ann}(L/F) \cap \mathbb{Z}$ contains all integers of the form $N\mathfrak{q} - 1$, where $\mathfrak{q}$ ranges over all prime ideals not in S such that $\sigma_{\mathfrak{q}}$ is trivial on L. Then let $N = \gcd\{N\mathfrak{q} - 1 : \mathfrak{q} \notin S, \sigma_{\mathfrak{q}}|_L = 1\}$. By definition, $N \in M$. We ultimately want to show that $N = W_L$, that is, that L contains the Nth roots of unity.

To this end, consider the field $L(\zeta_N)$ produced by adjoining an Nth root of unity to L. By the Chebotarev Density Theorem for the extension $L(\zeta_N)/F$, any element of $\mathrm{Gal}(L(\zeta_N)/L)$ can be written $\sigma_{\mathfrak{q}}|_{L(\zeta_N)}$ for some prime $\mathfrak{q}$ of F not in S such that $\sigma_{\mathfrak{q}}|_L$ is trivial. By definition of N, any such prime $\mathfrak{q}$ must satisfy $N\mathfrak{q} \equiv 1 \pmod{N}$. Applying the argument used in the first half to the extension $L(\zeta_N)/F$, we see that $\sigma_{\mathfrak{q}} - N\mathfrak{q}$ annihilates the Nth roots of unity in $L(\zeta_N)$. Since $N\mathfrak{q} \equiv 1 \pmod{N}$, $N\mathfrak{q} - 1$ also annihilates the Nth roots of unity in $L(\zeta_N)$. Adding, we see that $\sigma_q - 1$ annihilates the Nth roots of unity in $L(\zeta_N)$. Hence σ fixes ζ_N, but σ is an element of the Galois group $L(\zeta_N)/L$, so σ must be the identity.

Since this is true for every $\sigma \in \mathrm{Gal}(L(\zeta_N)/L)$, the Galois group $\mathrm{Gal}(L(\zeta_N)/L)$ is trivial. It follows that $L(\zeta_N) = L$, so L contains the ζ_Nth roots of unity, and so $N \mid W_L$. Since $N \in M$, it follows that $W_L \in M \cap \mathbb{Z}$. Hence $W_L\mathbb{Z}$ contains $M \cap \mathbb{Z}$, and we already know the other containment, so $W_L\mathbb{Z} = M \cap \mathbb{Z}$. □

This result motivates the following statement of Gross's conjecture. As before, let K/F be an abelian extension of global fields such that $\mathfrak{p}$ splits completely in K, and let S be a set of primes containing the infinite primes, the prime $\mathfrak{p}$ and the primes that ramify in K. Let L be an auxiliary abelian extension of K that is unramified outside S.

We assume that the Brumer-Stark Conjecture 3.1.1 holds. Let $\epsilon \in K$ be the unit of the Brumer-Stark conjecture, and let λ be a W_Kth root of ϵ. By the Brumer-Stark conjecture, $K(\lambda)/F$ is abelian. Taking the compositum with L, we see that $L(\lambda)$ is also an abelian extension of F. Now, let η be a prime of F that is not in S: in the case of number fields, we also need to require that η does not divide W_L. Because λ is a unit at all places of K that do not divide $\mathfrak{p}$, the Kummer extension $K(\lambda)/K$ is only ramified at the primes dividing $\mathfrak{p}$, and, in the number field case, the primes dividing W_K (note that in the function field case, W_K is a number of the form $p^e - 1$, so it is a unit in characteristic $\mathfrak{p}$, and this result becomes unnecessary). Since K/F is by assumption only ramified at places in S, it follows that $K(\lambda)/F$ is only ramified at places that are in S or divide W_K. Likewise, $L(\lambda)/F$ is only ramified at places that are in S or divide W_L. In particular, neither field extension is ramified at η, so the Frobenius element σ_η is defined on both fields $K(\lambda)$ and $L(\lambda)$.

We now define a "shifted Stark unit" in K by

$$u_{K,\eta} = \lambda^{\sigma_\eta - N\eta}. \tag{3.6}$$

Proposition 3.2.2. *The shifted Stark unit $u_{K,\eta}$ is well-defined, independent of our choice of Stark unit ϵ and of our W_Kth root λ of ϵ.*

Proof. Suppose that we have λ_1 and λ_2 such that $\lambda_1^{W_K} = \epsilon_1$ and $\lambda_2^{W_K} = \epsilon_2$ are both Stark units for K. Since Stark units are unique up to roots of unity, ϵ_1/ϵ_2 is a root of unity in K, and so also λ_1/λ_2 is a root of unity in $K(\lambda_1, \lambda_2)$. The field $K(\lambda_1, \lambda_2)$ is the compositum of two extensions $K(\lambda_1)$ and $K(\lambda_2)$ of F that are unramified at η, so $K(\lambda_1, \lambda_2)$ is unramified at η. As a result, the Frobenius element σ_η is defined on $K(\lambda_1, \lambda_2)$, consistently with the definitions of the Frobenius elements on $K(\lambda_1)$ and $K(\lambda_2)$. Now, we apply Lemma 3.2.1 to the root of unity $\lambda_1/\lambda_2 \in K(\lambda_1, \lambda_2)$ to get $(\lambda_1/\lambda_2)^{\sigma_\eta - N\eta} = 1$. Rearranging, we find that $\lambda_1^{\sigma_\eta - N\eta} = \lambda_2^{\sigma_\eta - N\eta}$, hence $u_{K,\eta}$ is well-defined. $\square$

Note that we can construct well-defined Stark units shifted by any element of the annihilator of roots of unity. However, by Proposition 3.2.1, these units can be expressed as products of powers of Stark units already constructed, and so in some sense we gain nothing by considering them.

We can use the definition of ϵ to obtain a formula for the valuations of $u_{K,\eta}$. Before doing so, we define a shifted zeta function as follows:

Definition. For T a set of primes of F that are unramified in K, define partial zeta functions $\zeta_{S,T}(K/F, \sigma, s)$ for all $\sigma \in G = \mathrm{Gal}(K/F)$ so that the following equation holds in the group ring $\mathbb{C}[G]$:

$$\sum_{\sigma \in G} \zeta_{S,T}(K/F, \sigma, s)[\sigma] = \prod_{\eta \in T} ([\sigma_\eta]^{-1} - (N\eta)^{1-s}) \sum_{\sigma \in G} \zeta_S(K/F, \sigma, s)[\sigma]. \tag{3.7}$$

We will most often use this definition in the case T contains a single prime η, in which case we can write $\zeta_{S,\eta}(K/F, \sigma, s)$ explicitly as

$$\zeta_{S,\eta}(K/F, \sigma, s) = \zeta_S(K/F, \sigma\sigma_\eta, s) - (N\eta)^{1-s} \zeta_S(K/F, \sigma, s). \tag{3.8}$$

Remark. This shifting differs from that in Hayes [9], which has $[\sigma_\eta]^{-1} - N\eta$ in place of $[\sigma_\eta]^{-1} - (N\eta)^{1-s}$. However, the end result is the same upon setting $s = 0$. Our shifting is also not quite the same as that used in Dasgupta [3], who uses $1 - (N\eta)^{1-s}[\sigma_\eta]$.

Proposition 3.2.3. *Assume Conjecture 3.1.1. The Stark unit $u_{K,\eta}$ is the unique element of K possessing the following properties:*

(a) $|u_{K,\eta}|_{\mathfrak{P}'} = 1$ *if $\mathfrak{P}'$ is a (possibly infinite) prime not dividing $\mathfrak{p}$.*

(b) For all $\sigma \in \mathrm{Gal}(K/F)$, $\log |u^\sigma_{K,\eta}|_{\mathfrak{P}} = -\zeta'_{S,\eta}(K/F, \sigma, 0)$.

(c) $u_{K,\eta} \equiv 1 \pmod{\mathfrak{Q}}$ *for every prime $\mathfrak{Q}$ of K that lies over the prime η of F.*

Proof. Part (a) follows directly from the corresponding property of ϵ. Part (b) also follows directly from the corresponding property of ϵ, since, if we extend σ to an element of $\mathrm{Gal}(K(\lambda)/F)$, we can express the log of the absolute value of the shifted Stark unit as

$$\log |u^\sigma_{K,\eta}|_{\mathfrak{P}} = \log |(\epsilon^{\sigma\eta - N\eta})^\sigma|_{\mathfrak{P}} = \log |\epsilon^{\sigma\sigma_\eta}| - N\eta \log |\epsilon^\sigma| \tag{3.9}$$

which is $-\zeta'_S(K/F, \sigma\sigma_\eta, 0) + N\eta^{1-0}\zeta_S(K/F, \sigma, 0) = -\zeta'_{S,\eta}(K/F, \sigma, 0)$ as desired. Finally, part (c) follows from the definition of the Frobenius element. □

As in the non-shifted case, the second condition can be reformulated as

$$v_{\mathfrak{P}}(u^\sigma_{K,\eta}) = \zeta_{R,\eta}(K/F, \eta, 0). \tag{3.10}$$

Proposition 3.2.4. *Suppose we have a tower of fields $F \subset K \subset K'$. Then $u_{K,\eta} = N_{K'/K}u_{K',\eta}$.*

Proof. We need to show that $N_{K'/K}(u_{K',\eta})$ is a Stark unit for K. Conditions (a) and (c) for $N_{K'/K}(u_{K,\eta}) \in K'$ follow immediately from the analogous conditions for $u_{K,\eta}$ in Proposition 3.2.3. Let $\mathfrak{P}$ be a prime of K above F, and let P be a prime of K' above $\mathfrak{P}$. Choose $\sigma \in \mathrm{Gal}(K/F)$ and extend it to an element $\sigma \in \mathrm{Gal}(L/F)$ whose restriction to K/F is σ. Because $\mathfrak{P}$ splits completely in the extension K'/K, the $\mathfrak{P}$-adic valuation $v_{\mathfrak{P}}$ of $u^\sigma_{K,\eta}$ is

$$v_{\mathfrak{P}}(u^\sigma_{K,\eta}) = v_P(u^\sigma_{K,\eta}) = \sum_{\tau \in \mathrm{Gal}(L/K)} v_P(u^{\sigma\tau}_{K,\eta}) = \sum_{\tau \in \mathrm{Gal}(K'/F)} \zeta_{R,\eta}(K'/F, \sigma\tau, 0) \tag{3.11}$$

If we now change variables to $\sigma' = \sigma\tau \in \mathrm{Gal}(K'/F)$, we obtain

$$\sum_{\substack{\sigma' \in \mathrm{Gal}(K'/F) \\ \sigma'|_K = \sigma}} \zeta_{R,\eta}(K'/F, \sigma, 0) \tag{3.12}$$

which is easily seen to be the same as $\zeta_{R,\eta}(K'/F, \sigma, 0)$. □

3.3 Gross's refinement

We now state Gross's $\mathfrak{p}$-adic refinement of Stark's conjecture. Recall that $\mathbf{F}_\mathfrak{p}$ is the completion of F at the prime $\mathfrak{p}$. Because $\mathfrak{p}$ is completely split in K, the completion $\mathbf{K}_\mathfrak{P}$ is isomorphic to $\mathbf{F}_\mathfrak{p}$ as a local field. Local class field theory provides us with the Artin reciprocity map $\mathrm{rec} : \mathbf{K}_\mathfrak{P}^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, where K^{ab} is the maximal abelian extension of K. Restricting this reciprocity map to our auxiliary abelian extension L of K yields a homomorphism $\mathrm{rec} : \mathbf{F}_\mathfrak{p}^\times \cong \mathbf{K}_\mathfrak{P}^\times \to \mathrm{Gal}(L/K)$.

Conjecture 3.3.1 (Gross). *For any $\sigma \in \mathrm{Gal}(K/F)$, the image of the Stark unit $u_{K,\eta}^\sigma$ under the reciprocity map $\mathrm{rec} : \mathbf{K}_{\mathfrak{P}^\tau}^\times \to \mathrm{Gal}(L/K)$ is*

$$\mathrm{rec}(u_{K,\eta}^\sigma) = \prod_{\substack{\tau \in \mathrm{Gal}(L/F) \\ \tau|_K = \sigma}} \tau^{-\zeta_{S,\eta}(L/F,\tau,0)}. \tag{3.13}$$

Gross's conjecture, like Stark's conjecture, is compatible with taking norms from one field to another, though we will not prove this fact.

3.4 Gross's conjecture restated and $\mathfrak{p}$-adic integrals

We now restate Gross's conjecture in a way that brings it closer to being an explicit formula for $u_{K,\eta}$ and reinterpret it in terms of $\mathfrak{p}$-adic integrals. We specialize to the case where K is the field $H = H(\mathfrak{f};\mathfrak{p})$ defined in Section 3.1 as the maximal subfield H of the narrow ray class field $H_\mathfrak{f}$ such that H is totally split at $\mathfrak{p}$. In the case of number fields, any abelian extension of F which is totally split at $\mathfrak{p}$ is contained in $H(\mathfrak{f};\mathfrak{p})$ for some $\mathfrak{f}$. Since Stark units for subfields can be constructed by taking norms of the Stark units for the larger field, no generality is lost by restricting to this case. This is not quite true in the case of function fields, where the fields $K_\mathfrak{m}$ are not necessarily contained in fields of the form $H_\mathfrak{f}$. We will see that for $K = K_\mathfrak{m}$, Gross's conjecture yields an explicit $\mathfrak{p}$-adic formula for the unit $u_{K_\mathfrak{m},\eta}^\sigma$.

Let the field $H = H(\mathfrak{f};\mathfrak{p})$ play the role of K. In order to obtain a $\mathfrak{p}$-adic formula, we specialize to let L be the narrow ray class field $H_{\mathfrak{f}\mathfrak{p}^m}$ of H for some positive integer m. Recall that $\mathcal{O}$ is the ring of integers of F (i.e. elements integral at all places except $\infty_1, \dots, \infty_n$), and let $E_\mathfrak{p}(\mathfrak{f})$ be the subgroup of the group of units of $\mathcal{O}^\times$ consisting of the totally positive $\mathfrak{p}$-units congruent to 1 mod $\mathfrak{f}$.

Proposition 3.4.1. *The kernel of the local reciprocity map $\mathrm{rec} : \mathbf{F}_\mathfrak{p}^\times \to \mathrm{Gal}(H_{\mathfrak{f}\mathfrak{p}^m}/H)$ is exactly the subgroup of $\mathbf{F}_\mathfrak{p}^\times$ generated by $E_\mathfrak{p}(\mathfrak{f})$ and the subgroup $\mathbf{U}_{\mathfrak{p},m}$ of units of $\boldsymbol{\mathcal{O}}_\mathfrak{p}$ that are congruent to $1 \pmod{\mathfrak{p}^m}$.*

Proof. The ray class field $H_{\mathfrak{f}\mathfrak{p}^m}$ is defined via the global Artin map of class theory by

$$\mathrm{Gal}(H_{\mathfrak{f}\mathfrak{p}^m}/F) = \mathbb{A}_F^\times / (F^\times \prod_{\infty_i} \ker \mathrm{sgn}_i \prod_{v|\mathfrak{f}\mathfrak{p}^m} \mathbf{U}_{v,\mathfrak{f}\mathfrak{p}^m} \prod_{v\nmid\infty\mathfrak{f}\mathfrak{p}^m} \boldsymbol{\mathcal{O}}_v^\times).$$

Now, we can relate the global Artin map to the local Artin map as follows. Let $\iota_{\mathfrak{p}}$ be the natural inclusion map $\mathbf{F}_{\mathfrak{p}}^{\times} \to \mathbb{A}_F^{\times}$ that sends $a \in \mathbf{F}_{\mathfrak{p}}^{\times}$ to the ideal whose $\mathbf{F}_{\mathfrak{p}}^{\times}$ component equals a and whose other components all equal 1. We will identify $\mathbf{F}_{\mathfrak{p}}^{\times}$ with its image $\iota_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}}^{\times})$ inside $\mathbb{A}_F^{\times}$. Restricting the global Artin map $\mathbb{A}_F^{\times} \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ to $\mathbf{F}_{\mathfrak{p}}^{\times}$ yields a map that with our definitions is the reciprocal of the local Artin map: that is, for $a \in \mathbf{F}_{\mathfrak{p}}^{\times}$, the element $\mathrm{rec}(a) \in \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}^{\mathrm{ab}}/\mathbf{F}_{\mathfrak{p}})$ restricts to the element $\sigma_a^{-1} \in \mathrm{Gal}(F^{\mathrm{ab}}/F)$. Hence, for $a \in \mathbf{F}_{\mathfrak{p}}^{\times}$, the element $\mathrm{rec}(a) \in \mathrm{Gal}(H_{\mathfrak{f}\mathfrak{p}^m}/H)$ is the identity if and only if $\sigma_a \in \mathrm{Gal}(F^{\mathrm{ab}}/F)$ is the identity on $H_{\mathfrak{f}\mathfrak{p}^m}$, i.e., if and only if the element $a \in \mathbf{F}_{\mathfrak{p}}^{\times}$ lies in

$$(F^{\times} \prod_{\infty_i} \ker \mathrm{sgn}_i \prod_{v|\mathfrak{f}\mathfrak{p}^m} \mathbf{U}_{v,\mathfrak{f}\mathfrak{p}^m} \prod_{v\nmid\infty\mathfrak{f}\mathfrak{p}^m} \boldsymbol{\mathcal{O}}_v^{\times}) \cap \mathbf{F}_{\mathfrak{p}}^{\times}$$

If this is the case, there must be some $\alpha \in F^{\times} \subset \mathbb{A}_F$ such that α is congruent to $\iota_{\mathfrak{p}}(a) \in \mathbb{A}_F$ modulo $\ker \mathrm{sgn}_i \prod_{v|\mathfrak{f}\mathfrak{p}^m} \mathbf{U}_{v,\mathfrak{f}\mathfrak{p}^m} \prod_{v\nmid\infty\mathfrak{f}\mathfrak{p}^m} \boldsymbol{\mathcal{O}}_v^{\times}$. Because $\iota_{\mathfrak{p}}(a)$ is 1 at all places of A, looking at the components in the places other than $\mathfrak{p}$ tells us that $\alpha \in \ker \mathrm{sgn}_i \prod_{v|\mathfrak{f}} \mathbf{U}_{v,\mathfrak{f}} \prod_{v\nmid\infty\mathfrak{f}\mathfrak{p}^m} \boldsymbol{\mathcal{O}}_v^{\times}$. This is equivalent to saying that α is totally positive, congruent to 1 mod $\mathfrak{f}$, and a unit at all places except for $\mathfrak{p}$ and $\infty_1, \ldots, \infty_n$, that is, $\alpha \in E_{\mathfrak{p}}(\mathfrak{f})$. Finally, looking at the $\mathfrak{p}$-adic component, we see that a is congruent to α modulo the multiplicative subgroup $\mathbf{U}_{\mathfrak{p},m}$ of $\mathbf{F}_p^{\times}$.

We conclude that it is a necessary and sufficient condition for a to lie in $E_{\mathfrak{p}}(\mathfrak{f}) \cdot \mathbf{U}_{v,\mathfrak{f}\mathfrak{p}^m}$, as desired. □

Quotienting out by this kernel induces an injection $\mathrm{rec} : \mathbf{F}_{\mathfrak{p}}^{\times}/(\mathbf{U}_{\mathfrak{p},m} E_{\mathfrak{p}}(\mathfrak{f})) \to \mathrm{Gal}(H_{\mathfrak{f}}/H)$. Because H is the maximal subfield of $H_{\mathfrak{f}\mathfrak{p}^m}$ which is totally split at $\mathfrak{p}$, this map is also surjective, so it an isomorphism.

We now apply the inverse map $\mathrm{rec}^{-1} : \mathrm{Gal}(H_{\mathfrak{f}\mathfrak{p}^m}/H) \to \mathbf{F}_{\mathfrak{p}}^{\times}/(\mathbf{U}_{\mathfrak{p},m} E_{\mathfrak{p}}(\mathfrak{f}))$ to the equation (3.13) in the statement of Conjecture 3.3.1 for $K = H$, $L = H_{\mathfrak{f}\mathfrak{p}^m}$. However, we first apply the change of variables $x = \mathrm{rec}^{-1}(\tau^{-1}\sigma)$ (this is well-defined because $\tau\sigma^{-1} \in \mathrm{Gal}(H_{\mathfrak{f}}/H)$),

$$\mathrm{rec}_{\mathfrak{p}}(u_{H,\eta}^{\sigma}) = \prod_{x \in \mathbf{F}_{\mathfrak{p}}^{\times}/(\mathbf{U}_{\mathfrak{p},m} \cdot E_{\mathfrak{p}}(\mathfrak{f}))} (\sigma\, \mathrm{rec}(x)^{-1})^{-\zeta_{S,\eta}(H_{\mathfrak{f}\mathfrak{p}^m}/F, \sigma\, \mathrm{rec}(x)^{-1}, 0)}. \tag{3.14}$$

We now observe that the total exponent of σ in this product is $-\zeta_{S,\eta}(K/F, \sigma, 0)$, which is 0 by (3.2). After canceling the σ terms, we can then apply rec^{-1} to (3.14) to obtain

$$u_{H,\eta}^{\sigma} = \prod_{x \in \mathbf{F}_{\mathfrak{p}}^{\times}/(\mathbf{U}_{\mathfrak{p},m} \cdot E_{\mathfrak{p}}(\mathfrak{f}))} x^{\zeta_{S,\eta}(H_{\mathfrak{f}\mathfrak{p}^m}/F, \sigma\, \mathrm{rec}(x)^{-1}, 0)} \quad \text{in } \mathbf{F}_{\mathfrak{p}}^{\times}/\mathbf{U}_{\mathfrak{p},m} \cdot E_{\mathfrak{p}}(\mathfrak{f}) \tag{3.15}$$

If we take the limit as $m \to \infty$, we will obtain a formula for $u_{H,\eta}^{\sigma}$ in the projective limit $\lim_{\leftarrow} \mathbf{K}_{\mathfrak{p}}^{\times}/\mathbf{U}_{\mathfrak{p},m} \cdot E_{\mathfrak{p}}(\mathfrak{f}) = \mathbf{K}_{\mathfrak{p}}^{\times}/\widehat{E_{\mathfrak{p}}(\mathfrak{f})}$, where $\widehat{E_{\mathfrak{p}}(\mathfrak{f})}$ is the closure of $E_{\mathfrak{p}}(\mathfrak{f})$ in $\mathbf{K}_{\mathfrak{p}}^{\times}$. Also, Stark's conjecture tells us the $\mathfrak{p}$-adic valuation of $u_{H,\eta}^{\sigma}$ in $\mathbf{F}_{\mathfrak{p}}^{\times}$. Combining that with the information from Gross's conjecture determines $u_{H,\eta}$ modulo the elements of $E_{\mathfrak{p}}(\mathfrak{f})$ that are units at $\mathfrak{p}$, in other words, modulo the group $E_{\mathfrak{f}}$ of units of $\mathcal{O}$ that are congruent to 1 mod $\mathfrak{f}$.

The most convenient way of encapsulating such a formula is by use of $\mathfrak{p}$-adic integrals. We first give some preliminaries on $\mathfrak{p}$-adic integrals. The definitions we give can be extended to more general situations, but we will just state them in the case in which we need them. Let X be a compact totally disconnected Hausdorff space. For our purposes, X will always be a quotient of a subset of $\boldsymbol{\mathcal{O}}_{\mathfrak{p}}$. A $\mathbb{Z}$*-valued measure* on X is a function μ from the set of compact open subsets of X to $\mathbb{Z}$ such that for disjoint compact open sets U and V, $\mu(U \cup V) = \mu(U) + \mu(V)$.

Definition. For a continuous map $f : X \to \mathbf{F}_{\mathfrak{p}}^{\times}$ and a $\mathbb{Z}$-valued measure on X, we define the multiplicative integral

$$\times\!\!\!\!\!\!\int_X f \; d\mu = \lim_{m \to \infty} \prod_{x \in \mathbf{F}_{\mathfrak{p}}^{\times}/\mathbf{U}_{\mathfrak{p},m}} x^{\mu(f^{-1}(x))}. \tag{3.16}$$

The products inside the limit are all finite by compactness of X, and the limit converges because the sequence of products is evidently Cauchy.

We can restate Gross's conjecture as a $\mathfrak{p}$-adic integral. By finiteness of the class group, we know that for some positive e, the ideal $\mathfrak{p}^e$ is a principal ideal of $\mathcal{O}$ generated by a totally positive element π that is congruent to 1 mod $\mathfrak{f}$. Define $\mathbf{O} = \boldsymbol{\mathcal{O}}_{\mathfrak{p}} - \pi \boldsymbol{\mathcal{O}}_{\mathfrak{p}}$. If $\mathfrak{p} = (\pi)$, then $\mathbf{O}$ is the same as $\boldsymbol{\mathcal{O}}_{\mathfrak{p}}^{\times}$. Let $\widehat{E}_{\mathfrak{f}}$ be the topological closure of the group $E_{\mathfrak{f}}$ inside $\boldsymbol{\mathcal{O}}_{\mathfrak{p}}^{\times}$: equivalently, $\widehat{E}_{\mathfrak{f}} = \bigcap_{m=1}^{\infty} E_{\mathfrak{f}} \cdot \mathbf{U}_{\mathfrak{p},m}$. We now define a $\mathbb{Z}$-valued measure on $\mathbf{O}$ that encapsulates the information contained in the partial zeta functions.

We first slightly generalize our zeta functions. For a compact open subset U of $\mathbf{O}/\widehat{E}_{\mathfrak{f}}$ and an integral ideal $\mathfrak{b}$ of $\mathcal{O}$, define

$$\zeta_S(\mathfrak{b}, U, s) = \sum_{\substack{\mathfrak{a} \subset \mathcal{O}, (\mathfrak{a}, S) = 1 \\ \sigma_{\mathfrak{a}} \in \sigma_{\mathfrak{b}} \cdot \mathrm{rec}_{\mathfrak{p}}(U)^{-1}}} N\mathfrak{a}^{-s} = N\mathfrak{b}^{-s} \sum_{\substack{\alpha \in (\mathfrak{b}^{-1}\mathfrak{f}+1)/E_{\mathfrak{f}} \\ (\alpha, R) = 1 \\ \alpha \gg 0}} N\alpha^{-s} |\alpha|_{\mathfrak{p}}^{-s}, \tag{3.17}$$

where we use the fact that $\mathfrak{a}\mathfrak{b}^{-1}$ lies in the subgroup generated by $\mathfrak{p}$ and principal ideals to write $\mathfrak{a}\mathfrak{b}^{-1} = (\alpha)\mathfrak{p}^{-v_{\mathfrak{p}}(\alpha)}$. Note that $\zeta_S(\mathfrak{b}, U, s)$ can be written as a finite sum of partial zeta functions, and so can be meromorphically extended to the entire complex plane.

We can define shifted zeta functions $\zeta_{S,T}(\mathfrak{b}, U, s)$ similarly to before. Define shifting coefficients $c_{\mathfrak{a}}(s)$, where $\mathfrak{a}$ ranges over the fractional ideals of $\mathcal{O}$, by the following equation

$$\prod_{\eta \in T} ([\eta^{-1}]1 - N\eta^{1-s}) = \sum_{\mathfrak{a}} c_{\mathfrak{a}}(s)[\mathfrak{a}].$$

Then define

$$\zeta_{S,T}(\mathfrak{b}, U, s) = \sum_{\mathfrak{a}} c_{\mathfrak{a}}(s) \zeta_S(\mathfrak{a}^{-1}\mathfrak{b}, U, s). \tag{3.18}$$

Now define a measure $\mu(\mathfrak{b})$ on $\mathbf{O}/\widehat{E}_{\mathfrak{f}}$ by

$$\mu(\mathfrak{b}, U) = \zeta_{S,T}(\mathfrak{b}, U, 0). \tag{3.19}$$

Additivity of $\mu(\mathfrak{b})$ follows immediately from the definitions, and $\mu(\mathfrak{b})$ is $\mathbb{Z}$-valued because shifted partial zeta functions take on integer values at 0. We note also that the measure of the entire space $\mathbf{O}/E_{\mathfrak{f}}$ is $\mu(\mathfrak{b}, \mathbf{O}/E_{\mathfrak{f}}) = \zeta_{S,T}(H/F, \sigma_{\mathfrak{b}}, 0) = 0$.

Proposition 3.4.2. *Gross's conjecture implies the following:*

$$u_{H,\eta}^{\sigma_{\mathfrak{b}}} \equiv \pi^{\zeta_{R,T}(H_{\mathfrak{f}}/F,\mathfrak{b},0)} \times\!\!\!\!\!\!\int_{\mathcal{O}/\widehat{E_{\mathfrak{f}}}} x \, d\mu(\mathfrak{b}, x) \pmod{\widehat{E}_{\mathfrak{f}}} \tag{3.20}$$

for all integral ideals $\mathfrak{b}$ *of* $\mathcal{O}$.

Proof. Restating (3.15) as an integral, we find that

$$u_{H,\eta}^{\sigma_{\mathfrak{b}}} = \times\!\!\!\!\!\!\int_{\mathcal{O}/\widehat{E_{\mathfrak{f}}}} x \, d\mu(\mathfrak{b}, x) \text{ in } F_p^{\times}/\widehat{E_{\mathfrak{p}}(\mathfrak{f})}. \tag{3.21}$$

Since the group $\widehat{E_{\mathfrak{p}}(\mathfrak{f})}$ also contains all integer powers of π, the two sides of (3.20) are congruent mod $\widehat{E_{\mathfrak{p}}(\mathfrak{f})}$. By Proposition 3.2.3, the two sides of (3.20) also have the same $\mathfrak{p}$-adic valuation. The result follows, since the group $E_{\mathfrak{f}}$ contains exactly those elements of $E_{\mathfrak{p}}(\mathfrak{f})$ that are units at $\mathfrak{p}$. ☐

As noted before, in the function field case, we can also look at the larger field $K_{\mathfrak{m}}$ where $\mathfrak{m} = \mathfrak{f}\infty$. In this case, the role of the auxiliary extension field L is played by the field $L_{\mathfrak{m}\mathfrak{p}^m}$ that is defined to have Galois group

$$\mathrm{Gal}(L_{\mathfrak{m}\mathfrak{p}^m}/F) = \mathbb{A}_F^{\times}/(F^{\times} \prod_{v|\mathfrak{m}} \mathbf{U}_{v,\mathfrak{m}} \prod_{v\nmid\mathfrak{m}\mathfrak{p}} \boldsymbol{\mathcal{O}}_v^{\times} \times \mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}}) \tag{3.22}$$

where $\varpi^{\mathbb{Z}}$ is the multiplicative group generated by our chosen positive uniformizer ϖ for $\mathbf{F}_{\mathfrak{p}}$. (Note that this extension depends upon our choice of ϖ.)

By a similar argument to Proposition 3.4.1, we can show

Proposition 3.4.3. *The kernel of the local reciprocity map* $\mathrm{rec} : \mathbf{F}_{\mathfrak{p}}^{\times} \to \mathrm{Gal}(L_{\mathfrak{m}\mathfrak{p}^m}/F)$ *is exactly the subgroup* $\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}} \subset \mathbf{F}_{\mathfrak{p}}^{\times}$.

It follows from this that $\mathrm{Gal}(L_{\mathfrak{m}\mathfrak{p}^m}/L) = \mathbf{F}_{\mathfrak{p}}^{\times}/\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}} \cong (\boldsymbol{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{p}^m)^{\times}$, and the same manipulations that gave us (3.15) tell us that

$$u_{K_{\mathfrak{m}},\eta}^{\sigma} = \prod_{x \in \mathbf{F}_{\mathfrak{p}}^{\times}/(\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}}} x^{\zeta_{S,\eta}(L_{\mathfrak{m}\mathfrak{p}^m}/F, \sigma\,\mathrm{rec}(x)^{-1}, 0)} \quad \text{in } \mathbf{K}_{\mathfrak{p}}^{\times}/\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}}. \tag{3.23}$$

From this and Stark's conjecture on the $\mathfrak{p}$-adic valuation of $u_{K_{\mathfrak{m}},\eta}^{\sigma}$, we can derive a complete $\mathfrak{p}$-adic formula for $u_{K_{\mathfrak{m}},\eta}^{\sigma}$. This formula can also be rewritten as a $\mathfrak{p}$-adic integral; however, we will not actually need to use it in that form.

Additionally, since $N_{K_{\mathfrak{m}}/H}(u_{K_{\mathfrak{m}},\eta}) = u_{H,\eta}$, we can use the explicit formula for $u_{K_{\mathfrak{m}},\eta}$ and its conjugates to obtain an explicit formula for $u_{H,\eta}$: we will do this in Chapter 5. This formula could also be derived by applying Gross's conjecture with $L = K_{\mathfrak{m}}$ and $K = H$.

3.5 Shintani domains and Dasgupta's refinement for number fields

In order to give an exact formula for $u_{H,\eta}$, not just one only defined mod $E_{\mathfrak{f}}$, we must choose canonical representatives for each of the cosets of $E_{\mathfrak{f}}$. That is, we must choose a canonical domain for the action of $E_{\mathfrak{p}}(\mathfrak{f})$ on $\mathbf{O}$. We first discuss Shintani domains and formulate Dasgupta's refinement in the number field case, and then we transfer everything over to function fields.

Let F be a totally real number field, with notation as above. Since F is totally real, the tensor product $F \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{i=1}^{n} \mathbf{F}_{\infty_i}$ is isomorphic to $\mathbb{R}^n$. This gives us a natural embedding of F into $\mathbb{R}^n$. Also, $F^\times$ acts on $\mathbb{R}^n$ by multiplication on the left factor of $F \otimes_{\mathbb{Q}} \mathbb{R}$. Let Q be the positive orthant $(\mathbb{R}^{>0})^n \subset \mathbb{R}^n$. The group of totally positive elements of F acts on Q. In particular, the group $E_{\mathfrak{f}}$ of totally positive units of $\mathcal{O}$ congruent to 1 mod $\mathfrak{f}$ acts on Q. It follows from Dirichlet's unit theorem that $E_{\mathfrak{f}}$ acts properly discontinuously on Q, so it makes sense to look for a fundamental domain.

For linearly independent vectors $v_1, \dots, v_r$ in Q, define the *simplicial cone* $C(v_1, \dots, v_r)$ in Q by

$$C(v_1, \dots, v_r) = \left\{ \sum_{i=1}^{r} c_i v_i \mid c_i > 0 \right\}. \tag{3.24}$$

In the case when all v_i belong to $F \cap Q$, we say that the simplicial cone is a *Shintani cone*. Furthermore, a *Shintani set* is a subset of Q that can be written as a disjoint union of Shintani cones. Define a *Shintani domain* for $E_{\mathfrak{f}}$ to be a Shintani set $\mathcal{D}$ that is a fundamental domain for Q under the action of $E_{\mathfrak{f}}$.

Theorem 3.5.1 (Shintani, [11]). *A Shintani domain exists.*

We now define Shintani zeta functions. First we state some technical conditions that will be needed for our Shintani zeta functions to be well-defined and have integral special values. We say that a prime η of F is *good* for a Shintani cone C if (i) $N\eta$ is a rational prime and (ii) C can be written as $C(v_1, \dots, v_n)$ such that each $v_i \in \mathcal{O}$ but no v_i is divisible by η. We also say that a set of primes T is *good* for a Shintani set $\mathcal{D}$ if $\mathcal{D}$ can be decomposed as the disjoint union of Shintani cones C_i such that, for each C_i, it is the case either that there are two primes in T of different residue characteristic that are good for C_i, or that there is one prime η in T that is good for C_i and satisfies $N\eta \geq n+2$.

Assume that no prime of S has the same residue characteristic as any prime of T, and that no two primes of T have the same residue characteristic. Let $\mathcal{D}$ be a Shintani set (not necessarily a fundamental domain) such that T is good for $\mathcal{D}$.

Now, for each integral ideal $\mathfrak{b}$ of $\mathcal{O}$ relatively prime to S, and each compact open subset $U \subset \mathcal{O}_{\mathfrak{p}}$, define a zeta function $\zeta_R(\mathfrak{b}, \mathcal{D}, U, s)$ by

$$\zeta_R(\mathfrak{b}, \mathcal{D}, U, s) = N\mathfrak{b}^{-s} \sum_{\substack{\alpha \in (\mathfrak{b}^{-1}\mathfrak{f}+1) \cap \mathcal{D} \\ \alpha \in U, (\alpha, R)=1}} N\alpha^{-s}. \tag{3.25}$$

More generally, we can define a shifted zeta function $\zeta_{R,T}(\mathfrak{b}, \mathcal{D}, U, s)$ as in (3.7).

It can be shown under the assumptions given above (see [11] and [3]) that $\zeta_{R,T}(\mathfrak{b}, \mathcal{D}, U, s)$ extends to a meromorphic function on $\mathbb{C}$ and that $\zeta_{R,T}(\mathfrak{b}, \mathcal{D}, U, 0) \in \mathbb{Z}$. Hence we can define a $\mathbb{Z}$-valued measure $\nu(\mathfrak{b}, \mathcal{D})$ on $\boldsymbol{\mathcal{O}}_{\mathfrak{p}}$ by

$$\nu(\mathfrak{b}, \mathcal{D}, U) = \zeta_{R,T}(\mathfrak{b}, \mathcal{D}, U, 0). \tag{3.26}$$

It follows from comparing definitions that if we restrict ν to $\mathbf{O}$ and then push forward to $\mathbf{O}/\widehat{E}_{\mathfrak{f}}$, we obtain the measure μ defined in the previous section. Hence the measure ν is a natural candidate to use to obtain an explicit formula that refines Gross's formula for the Stark unit.

Recall that we have defined an element π such that $(\pi) = \mathfrak{p}^e$ for the minimal e for which $\mathfrak{p}^e$ is a principal ideal of $\mathcal{O}$ generated by a totally positive element π that is $1 \mod \mathfrak{f}$. We first consider the case in which $\pi\mathcal{D} = \mathcal{D}$ – this will happen in the case where the absolute value $|\pi_{\infty_i}|$ is independent of i, which, since π is totally positive, is equivalent to requiring that π is rational.

Conjecture 3.5.2 (Dasgupta's refinement, number fields, first version). *Suppose that $\pi \in \mathbb{Q}$. Then for any integral ideal $\mathfrak{b}$ of $\mathcal{O}$ that is relatively prime to S, the Stark unit $u_H^{\sigma_{\mathfrak{b}}}$ can be expressed as*

$$u_H^{\sigma_{\mathfrak{b}}} = \pi^{\zeta_{R,T}(H/F, \mathfrak{b}, 0)} \times\!\!\!\!\!\!\int_{\mathbf{O}} x \; d\nu(\mathfrak{b}, \mathcal{D}, x). \tag{3.27}$$

for any Shintani domain $\mathcal{D}$ such that T is good for $\mathcal{D}$ and $\pi\mathcal{D} = \mathcal{D}$.

In the case where $\pi\mathcal{D} \neq \mathcal{D}$, the above formula needs a correction term. Define

$$\epsilon(\mathfrak{b}, \mathcal{D}, \pi) = \prod_{\epsilon \in E_{\mathfrak{f}}} \epsilon^{\nu(\mathfrak{b}, \epsilon\mathcal{D} \cap \pi^{-1}\mathcal{D}, \boldsymbol{\mathcal{O}}_{\mathfrak{p}})}. \tag{3.28}$$

(The product can be shown to be finite by compactness.) Then we can modify our previous conjecture by

Conjecture 3.5.3 (Dasgupta's refinement, number fields, general version). *For any integral ideal $\mathfrak{b}$ of $\mathcal{O}$ that is relatively prime to S, the Stark unit $u_H^{\sigma_{\mathfrak{b}}}$ can be expressed as*

$$u_H^{\sigma_{\mathfrak{b}}} = \epsilon(\mathfrak{b}, \mathcal{D}, \pi) \cdot \pi^{\zeta_{R,T}(H/F, \mathfrak{b}, 0)} \times\!\!\!\!\!\!\int_{\mathbf{O}} x \; d\nu(\mathfrak{b}, \mathcal{D}, x). \tag{3.29}$$

for any Shintani domain $\mathcal{D}$ such that T is good for $\mathcal{D}$.

3.6 Shintani zeta functions in function fields

We now switch to the case where F is a function field. Recall that we have defined a map $\iota : F^\times \to \prod_{i=1}^n \mathbb{R}^{>0} \times k_i^\times$ by $\iota(z) = (|x|_{\infty_i}, \mathrm{sgn}_i(x))$. Then $F^\times$ acts on the codomain $\prod_{i=1}^n \mathbb{R}^{>0} \times k_i^\times$ by componentwise multiplication after applying ι. Recall that we have defined a “totally positive orthant” $Q = \prod_{1=1}^{n} \mathbb{R}^{>0} \times 1 \subset \prod_{i=1}^{n} \mathbb{R}^{>0} \times k_i^\times$, which contains the images under ι of all totally positive elements of $F^\times$. In particular, the group $E_\mathfrak{f}$ of totally positive elements of $\mathcal{O}^\times$ congruent to 1 mod $\mathfrak{f}$ acts on Q.

The definitions of Shintani cones and Shintani sets in Q continue to apply here. As in the previous section, we define a *Shintani domain* $\mathcal{D}$ for $E_\mathfrak{f}$ to be a Shintani set that is a fundamental domain for the action of $E_\mathfrak{f}$ on Q.

We now define Shintani zeta functions for F in a manner analogous to the number field case. Let $\mathcal{D}$ be a Shintani set, and let $\mathfrak{b}$ be an integral ideal of $\mathcal{O}$. Then we define

$$\zeta_R(\mathfrak{b}, \mathcal{D}, U, s) = N\mathfrak{b}^{-s} \sum_{\substack{\alpha \in (\mathfrak{b}^{-1}\mathfrak{f}+1), \iota(\alpha) \in \mathcal{D} \\ \alpha \in U, (\alpha, R)=1}} N\alpha^{-s}. \tag{3.30}$$

Alternatively, we can write this zeta function in a different way. Define a degree function $\deg_\infty$ on $F^\times$ by $\deg_\infty(\alpha) = \log_q N(\alpha\mathcal{O})$, which is also equal to $-\sum_i d_{\infty_i} v_{\infty_i}(\alpha)$. Let $A_N(\mathfrak{b})$ denote the set of totally positive elements $\alpha \in \mathfrak{b}^{-1}\mathfrak{f} + 1$ relatively prime to R such that $\iota(\alpha) \in \mathcal{D}$ and $\deg_\infty(\alpha) = N$. Define a sequence $a_N(\mathfrak{b}, U)$ by $a_N(\mathfrak{b}, U) = \#(A_N(\mathfrak{b}) \cap U)$. Then, grouping terms by degree, we can rewrite $\zeta_R(\mathfrak{b}, \mathcal{D}, U, s)$ as

$$\zeta_R(\mathfrak{b}, \mathcal{D}, U, s) = N\mathfrak{b}^{-s} \sum_{N=-\deg_\infty \mathfrak{b}}^{\infty} a_N(\mathfrak{b}, U) q^{-Ns}. \tag{3.31}$$

We can also define a shifted zeta function $\zeta_{R,T}(\mathfrak{b}, \mathcal{D}, U, s)$ in the same manner as before. We conveniently no longer need any technical conditions on the set T in order to ensure integrality of the zeta functions. This will follow from the fact that in the function field case shifted Shintani zeta functions are really finite sums. To prove that fact, we will need the following lemma, which is a version of the Riemann-Roch theorem:

Lemma 3.6.1. *Let F be a function field over $\mathbb{F}_q$. Then there are numbers g and M depending only on the field F, such that the following holds: Let S be a set of primes of F and $\{r_\mathfrak{q} \mid \mathfrak{q} \in S\}$ be integers subject to the condition that $\sum_{\mathfrak{q} \in S} r_\mathfrak{q} d_\mathfrak{q} \geq M$ (where $d_\mathfrak{q}$ is the degree of the place $\mathfrak{q}$). For each $\mathfrak{q} \in S$, let $x_\mathfrak{q}$ be an element of $\mathfrak{q}$, and let $B_\mathfrak{q}(x_\mathfrak{q}, -r_\mathfrak{q})$ denote the $\mathfrak{q}$-adic ball $\{x \in F_\mathfrak{q} \mid x \equiv x_\mathfrak{q} \pmod{\mathfrak{q}^{-r_\mathfrak{q}}}\}$. Define a subset $\mathcal{A}$ of $\mathbb{A}_F$ by*

$$\mathcal{A} = \prod_{\mathfrak{q} \in S} B_\mathfrak{q}(x_\mathfrak{q}, -r_\mathfrak{q}) \prod_{\mathfrak{q} \notin S} \mathcal{O}_\mathfrak{q}. \tag{3.32}$$

Then $F \cap \mathcal{A}$ has $q^{(\sum_\mathfrak{q} r_\mathfrak{q} d_\mathfrak{q}) - g + 1}$ elements.

Proof. We will take g to the genus of the algebraic curve corresponding to the function field F, and we will take $M = g + 1$.

Let $\mathcal{L} = \prod_{\mathfrak{q} \in S} \mathfrak{q}^{-r_q} \mathcal{O}_\mathfrak{q} \prod_{q \notin S} \mathcal{O}_q$. Since $\mathcal{A}$ is a coset of the $\mathbb{F}_q$-vector space $\mathcal{L}$, $F \cap \mathcal{A}$ is a coset of the $\mathbb{F}_q$-vector space $F \cap \mathcal{L}$, provided that it is nonempty. Since $\sum_\mathfrak{q} r_\mathfrak{q} d_\mathfrak{q} \geq M > g$, the Riemann-Roch theorem for function fields implies that the dimension of this vector space is $\sum_{\mathfrak{q}} r_{\mathfrak{q}} d_{\mathfrak{q}} - g + 1$. Hence $F \cap \mathcal{A}$ will have the correct number of elements, assuming that $F \cap \mathcal{A}$ is nonempty.

To show that $F \cap \mathcal{A}$ is nonempty, for each $\mathfrak{q}$, let $s_{\mathfrak{q}} = -v_{\mathfrak{q}}(x_{\mathfrak{q}})$, and define $\mathcal{L}' = \prod_{\mathfrak{q}\in S} \mathfrak{q}^{-r_q} \mathcal{O}_{\mathfrak{q}} \prod_{q \notin S} \mathcal{O}_{\mathfrak{q}}$. Then the quotient $F \cap \mathcal{L}'/F \cap \mathcal{L}$ of $\mathbb{F}_q$-vector spaces injects into the quotient $\mathcal{L}'/\mathcal{L} \cong \prod_{\mathfrak{q}\in S} \mathfrak{q}^{-s_{\mathfrak{q}}}/\mathfrak{q}^{-r_{\mathfrak{q}}}$. The dimension of the latter vector space is $\sum_{\mathfrak{q}\in S}(s_{\mathfrak{q}} - r_{\mathfrak{q}}) d_{\mathfrak{q}}$, and by Riemann-Roch on $F \cap \mathcal{L}'$ and $F \cap \mathcal{L}$, the dimension of $F \cap \mathcal{L}'/F \cap \mathcal{L}$ is exactly the same. Hence we have a bijection $F \cap \mathcal{L}'/F \cap \mathcal{L} \to \mathcal{L}'/\mathcal{L}$, and the preimage under this map of the reduction of the element $\prod_{\mathfrak{q}\in S} x_{\mathfrak{q}} \in \prod_{\mathfrak{q}\in S} \mathfrak{q}^{-s_{\mathfrak{q}}}/\mathfrak{q}^{-r_{\mathfrak{q}}} = \mathcal{L}'/\mathcal{L}$ is exactly the coset $F \cap \mathcal{A}$. Hence $F \cap \mathcal{A}$ is nonempty and has size $q^{(\sum_{\mathfrak{q}} r_{\mathfrak{q}} d_{\mathfrak{q}}) - g + 1}$. □

This lemma can also be interpreted in terms of sizes of solution sets to simultaneous congruences, and that is how we will use it below.

Proposition 3.6.2. *For any nonempty set T of primes, any Shintani set $\mathcal{D}$, any compact open set U of $\mathbf{O}$, and any integral ideal $\mathfrak{b}$ of $\mathcal{O}$ that is relatively prime to both S and T, the Shintani zeta function $\zeta_{R,T}(\mathfrak{b}, \mathcal{D}, U, s)$ is a finite Dirichlet series in s with integral coefficients.*

Proof. Without loss of generality, we may assume that T contains a single prime η, since zeta functions shifted by larger sets of primes can be written as linear combinations of zeta functions shifted by a single prime. By equation (3.31), we can express $\zeta_{R,\eta}(\mathfrak{b}, \mathcal{D}, U, s) = \zeta_{R,\eta}(\mathfrak{b}\eta, \mathcal{D}, U, s) - N\eta^{1-s}\zeta_{R,\eta}(\mathfrak{b}, \mathcal{D}, U, s)$ as

$$\zeta_{R,\eta}(\mathfrak{b}, \mathcal{D}, U, s) = \sum_{N=-\deg_\infty(\mathfrak{b})}^{\infty} (a_N(\mathfrak{b}\eta, U) - N\eta \cdot a_{N-\deg_\infty(\eta)}(\mathfrak{b}, U)) q^{-Ns}. \tag{3.33}$$

The coefficients $a_N(\mathfrak{b}\eta, U) - N\eta \cdot a_{N-\deg_\infty(\eta)}(\mathfrak{b}, U)$ are manifestly integral, so it will suffice to show that, for N sufficiently large, $a_N(\mathfrak{b}\eta, U) = N\eta \cdot a_{N-\deg_\infty(\eta)}(\mathfrak{b}, U)$. We use the notation $B(a, r)$ for the $\mathfrak{p}$-adic open ball $a + \mathfrak{p}^r \mathcal{O}_{\mathfrak{p}}$ in $\mathcal{O}_{\mathfrak{p}}$. Any compact open subset U of $\mathcal{O}_{\mathfrak{p}}$ can be expressed as a finite union of such $\mathfrak{p}$-adic open balls (for each $a \in U$ we can use openness of U to find a p-adic ball $B(a, r_a)$ contained in U and finitely many of those will cover U by compactness of U). Since any two $\mathfrak{p}$-adic open balls are either disjoint or nested, after eliminating redundant balls, we can express U as a disjoint union of finitely many $\mathfrak{p}$-adic open balls. By additivity, this means that we can reduce to the case where $U = B(a, r)$ is a $\mathfrak{p}$-adic open ball.

We now partition the set $A_N(\mathfrak{b}) \cap U$ as follows. Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_m$ be the non-infinite places of S. For every n-tuple of integers $w = (w_1, \ldots, w_n)$ with $\sum_i d_{\infty_i} w_i = N$, and every sequence $x = (x_1, \ldots, x_m)$ such that x_j is an element of the multiplicative group $(\mathcal{O}_{\mathfrak{q}_j}/\mathfrak{q}_j \mathcal{O}_{\mathfrak{q}_j})^\times$ of the residue field at $\mathfrak{q}_j$, let

$$A_{N,w,x}(\mathfrak{b}) = \\ \{\alpha \in A_N(\mathfrak{b}) \mid v_{\infty_i}(\alpha) = -w_i \text{ for } i = 1, \ldots, n \text{ and } \alpha \equiv x_j \pmod{\mathfrak{q}_j} \text{ for } j = 1, \ldots, m\}$$

Define $A_{N,w,x}(\mathfrak{b}\eta)$ likewise. The sets $A_{N,w,x}(\mathfrak{b})$ partition $S_N(\mathfrak{b})$, and likewise the sets $A_{N,w,k}(\mathfrak{b}\eta)$ partition $A_N(\mathfrak{b}\eta)$. Hence it will suffice to show that, provided that N is sufficiently large,

$$\#A_{N,w,x}(\mathfrak{b}\eta) \cap B(x,r) = N\eta \cdot \#A_{N,w,x}(\mathfrak{b}) \cap B(x,r).$$

We now note that the two conditions that $v_{\infty_i}(\alpha) = -w_i$ and that α is positive at ∞_i are equivalent to the single condition $\alpha \equiv \pi_{\infty_i}^{-w_i} \pmod{\pi_{\infty_i}^{-w_i+1}}$. Using this and the definition of $A_N(\mathfrak{b})$, we can write

$$A_{N,w,x}(\mathfrak{b}) \cap B(a,r) =$$
$$\{\alpha \in F \mid \alpha \equiv \pi_{\infty_i}^{-w_i} \pmod{\pi_{\infty_i}^{-w_i+1}}, \alpha \equiv x_j \pmod{\mathfrak{q}_j}, \alpha \equiv 1 \pmod{\mathfrak{b}^{-1}\mathfrak{f}}, \alpha \equiv a \pmod{\mathfrak{p}^r}\}.$$

More succinctly, we can write $A_{N,w,x}(\mathfrak{b}) \cap B(a,r) = F \cap \mathcal{A}$ where $\mathcal{A} \subset \mathbb{A}_K$ is the elementary open subset

$$\mathcal{A} = \prod_i B_{\infty_i}(\pi_{\infty_i}^{-w_i}, -w_i+1) \prod_j B_{q_j}(x_j, 1), \prod_{q \mid \mathfrak{b}^{-1}\mathfrak{f}} B_q(1, v_q(\mathfrak{b}^{-1}\mathfrak{f})) \times B_{\mathfrak{p}}(a,r).$$

We may now apply Lemma 3.6.1 to conclude that, for N sufficiently large,

$$\begin{aligned} \#(A_{N,w,x}(\mathfrak{b}) \cap B(x,r)) &= q^{N\sum_{i=1}^{n}(d_{\infty_i}(w_i-1)) - \sum_{\mathfrak{q}_i} d_{\mathfrak{q}_i} - \deg_\infty(\mathfrak{b}^{-1}\mathfrak{f}) - r d_{\mathfrak{p}} - g + 1} \\ &= q^{N + \deg_{\infty_i} \mathfrak{b} - \kappa}, \end{aligned} \tag{3.34}$$

where κ is an integer independent of our choices of N, w, x and $\mathfrak{b}$. Likewise,

$$\#(A_{N,w_1,\ldots,w_n,x_1,\ldots,x_m}(\mathfrak{b}\eta) \cap B(x,r)) = q^{N + \deg_\infty(\mathfrak{b}\eta) - \kappa}$$

for the same κ. Since $N\eta = q^{\deg_\infty \eta}$, we conclude that

$$\#(A_{N,w_1,\ldots,w_n,x_1,\ldots,x_m}(\mathfrak{b}\eta) \cap B(x,r)) = N\eta \cdot \#(A_{N,w_1,\ldots,w_n,x_1,\ldots,x_m}(\mathfrak{b}) \cap B(x,r)).$$

Summing over all possible w and x yields the desired result. □

As a corollary, we can deduce an analogous fact for other types of shifted zeta functions:

Corollary 3.6.3. *For any nonempty set T of primes, any compact open subset U of $\mathbf{O}/\widehat{E}_{\mathfrak{f}}$, and any ideal $\mathfrak{b}$, the zeta function $\zeta_{R,T}(\mathfrak{b}, U, s)$ is a finite Dirichlet series in s with integral coefficients. As a special case, we obtain that our original shifted zeta functions $\zeta_{R,T}(K/F, \sigma, s)$ are finite Dirichlet series.*

Proof. Let $\mathcal{D}$ be a Shintani domain. Because $\mathcal{D}$ is a fundamental domain for the action of $\widehat{E}_{\mathfrak{f}}$, it follows that $\zeta_{R,T}(\mathfrak{b}, U, s) = \zeta_{R,T}(\mathfrak{b}, \mathcal{D}, U, s)$ is a finite Dirichlet series. □

We now return to integration. For any Shintani set $\mathcal{D}$, we can define, as before, a measure $\nu(\mathfrak{b}, \mathcal{D}, U)$ by

$$\nu(\mathfrak{b}, \mathcal{D}, U) = \zeta_{R,T}(\mathfrak{b}, \mathcal{D}, U, 0).$$

3.7 A formulation of Dasgupta's refinement in function fields

We can now formulate exact function field analogues of the number field conjectures from Section 3.5.2. We first formulate the conjecture supposing that, with π as before, the absolute value $|\pi|_{\infty_i}$ is the same for all i. Note that this is a less restrictive condition in the function field setup, because the absolute value map $\mathcal{O}_{\infty_i} \to \mathbb{Z}$ is no longer an injection, and the image of $||_i$ is constrained to the subset of powers of q^{-1}.

Because, as we will see below, Stark's conjecture is a known fact in function fields, we will not need to assume the truth of Stark's conjecture in order to make conjectures about the Stark unit in function fields.

Theorem 3.7.1 (Function fields, first version). *Suppose that the absolute value $|\pi|_{\infty_i}$ is the same regardless of the infinite place ∞_i. Then for any integral ideal $\mathfrak{b}$ of $\mathcal{O}$ relatively prime to S, the Stark unit $u_{H_\mathfrak{f}}^{\sigma_\mathfrak{b}}$ can be expressed as*

$$u_H^{\sigma_\mathfrak{b}} = \pi^{\zeta_{R,T}(H/F,\mathfrak{b},0)} \times\!\!\!\!\!\!\int_{\mathbf{O}} x \; d\nu(\mathfrak{b}, \mathcal{D}, x). \tag{3.35}$$

for any Shintani domain $\mathcal{D}$ in Q.

We will prove this conjecture in Chapter 5. As in the number field case, we can also make a more general statement of Dasgupta's refinement, without the assumption that $|\pi|_{\infty_i}$ is the same for all infinite places ∞_i. We define a correction term $\epsilon(\mathfrak{b}, \mathcal{D}, U)$ by (3.28) exactly as in the number field case. We state the following result.

Theorem 3.7.2 (Function fields, general version). *For any integral ideal $\mathfrak{b}$ of $\mathcal{O}$ that is relatively prime to S, the Stark unit $u_H^{\sigma_\mathfrak{b}}$ can be expressed as*

$$u_H^{\sigma_\mathfrak{b}} = \epsilon(\mathfrak{b}, \mathcal{D}, \pi) \cdot \pi^{\zeta_{R,T}(H/F,\mathfrak{b},0)} \times\!\!\!\!\!\!\int_{\mathbf{O}} x \; d\nu(\mathfrak{b}, \mathcal{D}, x). \tag{3.36}$$

for any Shintani domain $\mathcal{D}$.

This version can also be handled by methods similar to those used in the proof of Theorem 3.7.1, however, for simplicity, we will restrict ourselves to proving the first version only.

Chapter 4

Exponential functions of lattices and the theory of Drinfeld modules

4.1 The exponential function of a lattice

We now switch gears and approach the explicit class field theory of function fields from a different direction. Instead of proposing analogues of the conjectural constructions of Stark units, we now build up an algebraic apparatus that will give us an analogue of the better-understood theories of cyclotomic fields and of elliptic curves with complex multiplication.

Let F be a global function field with field of constants equal to $\mathbb{F}_q$, and let $\mathfrak{p}$ be a place of F. Then F embeds into the completion $\mathbf{F}_\mathfrak{p}$ of F at $\mathfrak{p}$, and the ring A of elements integral away from $\mathfrak{p}$ is contained as a discrete subring of $\mathbf{F}_\mathfrak{p}$. Let $\mathbf{C}_\mathfrak{p}$ be the completion of the algebraic closure of $\mathbf{F}_\mathfrak{p}$: it is a well-known fact from the theory of local fields (see Proposition 2.1 of [5]) that $\mathbf{C}_\mathfrak{p}$ is algebraically closed.

We define a degree function $\deg_\mathfrak{p}$ on F by $\deg_\mathfrak{p}(z) = -d_\mathfrak{p} v_\mathfrak{p}(z)$, where $d_\mathfrak{p}$ is the degree of the place $\mathfrak{p}$. The degree function also extends to all of $\mathbf{C}_\mathfrak{p}$ In the case where $z \in A$ the product formula implies that

$$\deg_\mathfrak{p}(z) = \sum_{\mathfrak{p}'} d_{\mathfrak{p}'} v_{\mathfrak{p}'}(z),$$

where $\mathfrak{p}'$ ranges over all places other than $\mathfrak{p}$. In particular, $\deg_\mathfrak{p}(z)$ is non-negative for every $z \in A$. Also, since the ideal $(z) \in A$ factorizes as $\prod_{\mathfrak{p}'} (\mathfrak{p}')^{v_{\mathfrak{p}'}(z)}$, we have

$$[A : zA] = \prod_{\mathfrak{p}'} q^{v_{\mathfrak{p}'}(z) d_{\mathfrak{p}'}} = q^{\deg_\mathfrak{p}(z)}.$$

Since A is discrete in $\mathbf{F}_\mathfrak{p}$, for every positive integer N, there are only finitely many $z \in A$ with $\deg_\mathfrak{p}(z) \le N$.

Definition. A *rank-r lattice* Γ in $\mathbf{C}_\mathfrak{p}$ is a discrete sub-A-module of $\mathbf{C}_\mathfrak{p}$ such that the F-vector space $\Gamma \otimes_A F$ is r-dimensional.

For the purposes of this thesis, we will be concerned only with the case $r = 1$; however, much of the theory presented below does generalize to larger values of r. We observe that A, being discrete in $\mathbf{C}_\mathfrak{p}$, satisfies the conditions to be a rank-1 lattice, as does any ideal or fractional ideal of A. More generally, for any $\zeta \in \mathbf{C}_\mathfrak{p}^\times$ and any fractional ideal $\mathfrak{a}$ of A, the A-module $\zeta\mathfrak{a}$ is discrete in A, and $\zeta\mathfrak{a} \otimes_A F = \zeta F$ is 1-dimensional, so $\zeta\mathfrak{a}$ is a rank-1 lattice. The following proposition states that any rank-1 lattice in $\mathbf{C}_\mathfrak{p}^\times$ is of this form.

Proposition 4.1.1. *Any rank-one lattice Γ in $\mathbf{C}_\mathfrak{p}$ can be written in the form $L = \zeta\mathfrak{a}$ for $\zeta \in \mathbf{C}_\mathfrak{p}^\times$ and a fractional ideal $\mathfrak{a}$ of A.*

Proof. Choose any nonzero $\zeta \in \Gamma$. Then $F \otimes_A \Gamma$ is a one-dimensional F-vector space containing ζ, so $F \otimes_A \Gamma = \zeta F$. It follows that $\zeta^{-1}F$ is a discrete A-submodule of $F \subset \mathbf{C}_\mathfrak{p}$ which contains A. Since $\zeta^{-1}F$ is discrete in $\mathbf{C}_\mathfrak{p}$, it is also discrete in the completion $\mathbf{F}_\mathfrak{p}$ of F in $\mathbf{C}_\mathfrak{p}$. It is well known that the quotient $\mathbf{F}_\mathfrak{p}/A$ of topological groups is compact. The image of $\zeta^{-1}F$ in $\mathbf{F}_\mathfrak{p}/A$ is also discrete in $\mathbf{F}_\mathfrak{p}/A$, so, by compactness of the quotient, it follows that $\zeta^{-1}F/A$ is finite. Hence A has finite index in $\zeta^{-1}F$, which implies that $\zeta^{-1}F$ is a fractional ideal of A, yielding the desired result. □

Definition. Two rank-one lattices Γ_1 and Γ_2 in $\mathbf{C}_\mathfrak{p}$ are *homothetic* if there exists $\alpha \in \mathbf{C}_\mathfrak{p}^\times$ such that $\Gamma_1 = \alpha\Gamma_2$.

It follows from the definition that two rank-one lattices Γ_1 and Γ_2 are homothetic if and only if they have isomorphic structure as A-modules.

Because homothety is an equivalence relation, we can consider equivalence classes of lattices up to homothety. Then Proposition 4.1.1 can be re-interpreted as giving a one-to-one correspondence between the set of homothety classes of lattices in $\mathbf{C}_\mathfrak{p}$ and the ideal class group of A. However, instead of viewing of the set of homothety classes of lattices as identified with the ideal class group $\mathrm{Cl}(A)$ of A, it will be more productive for us to view it as a *principal homogeneous space* for $\mathrm{Cl}(A)$, that is, a set with a transitive free $\mathrm{Cl}(A)$-action. First of all, the group of fractional ideals of A acts on the set of one-dimensional lattices by $\mathfrak{a} * \Gamma = \mathfrak{a}^{-1}\Gamma$, where $\mathfrak{a}^{-1}\Gamma$ is the lattice generated as an A-module by the set $\{\alpha z \mid \alpha \in \mathfrak{a}^{-1}, z \in \Gamma\}$. (One could equally well multiply by $\mathfrak{a}$ instead of $\mathfrak{a}^{-1}$, but for reasons that we will see below, it will be most convenient to use $\mathfrak{a}^{-1}$.) After quotienting out by the action of principal ideals, this action descends to an action of $\mathrm{Cl}(A)$ on the set of homothety classes of lattices.

Proposition 4.1.2. *The action $(\mathfrak{a}, \Gamma) \mapsto \mathfrak{a}^{-1}\Gamma$ endows the set of homothety classes of lattices with the structure of a principal homogeneous space for* $\mathrm{Cl}(A)$.

Proof. We have already seen that the set of homothety classes of lattices is in one-to-one correspondence with the class group $\mathrm{Cl}(A)$, and $\mathrm{Cl}(A)$ is clearly a principal homogeneous space for itself under the action $\mathfrak{a} \star \mathfrak{b} = \mathfrak{a}^{-1}\mathfrak{b}$. □

However, we are interested more generally in the ray class groups of A, which arose in Chapter 2 as the Galois groups corresponding to our ray class fields (see Proposition 2.0.2).

We now give a definition that will eventually help us interpret ray class groups in terms of lattices. First note that for a lattice Γ, we can consider the quotient $\mathbf{C}_\mathfrak{p}/\Gamma$. Since $\mathbf{C}_\mathfrak{p}$ and Γ are both A-modules, $\mathbf{C}_\mathfrak{p}/\Gamma$ inherits a natural A-module structure as a quotient of $\mathbf{C}_\mathfrak{p}/\Gamma$.

Definition. If Γ is a lattice and $\mathfrak{m}$ is an ideal of A, an $\mathfrak{m}$-division point of Γ is a point z of the quotient $\mathbf{C}_\mathfrak{p}/\Gamma$ such that $\mathfrak{m}z = 0$ in $\mathbf{C}_\mathfrak{p}/\Gamma$, or equivalently, that $mz \in \Gamma$ for all $m \in \mathfrak{m}$.

We note that the set of $\mathfrak{m}$-division points of Γ is exactly $\mathfrak{m}^{-1}\Gamma/\Gamma$.

Proposition 4.1.3. *The set $\mathfrak{m}^{-1}\Gamma/\Gamma$ of $\mathfrak{m}$-division points of Γ is an A-module isomorphic to $A/\mathfrak{m}$.*

Proof. By Proposition 4.1.1, every lattice is homothetic to a fractional ideal of A, so it suffices to show this result when $\Gamma = \mathfrak{b}$ is a fractional ideal of A. By scaling, we can reduce to the case that $\mathfrak{b}$ is an integral ideal relatively prime to $\mathfrak{m}$.

Hence it suffices to show that for relatively prime ideals $\mathfrak{b}$ and $\mathfrak{m}$, $\mathfrak{b}/\mathfrak{b}\mathfrak{m} \cong A/\mathfrak{m}$ as A-modules. By the Chinese Remainder Theorem, we have a canonical isomorphism of A-modules $\phi : A/(\mathfrak{b}\mathfrak{m}) \cong (A/\mathfrak{b}) \times (A/\mathfrak{m})$. The preimage $\phi^{-1}(\{0\} \times A/\mathfrak{m})$ is exactly $\mathfrak{b}/\mathfrak{b}\mathfrak{m}$, so the restriction of ϕ is an isomorphism $\mathfrak{b}/\mathfrak{b}\mathfrak{m} \to A/\mathfrak{m}$, as desired. □

Proposition 4.1.4. *The set of all homothety classes of pairs (Γ, z) such that Γ is a rank-one lattice in $\mathbf{C}_\mathfrak{p}$ and z is an A-module generator of $\mathfrak{m}^{-1}\Gamma/\Gamma$ can be given the structure of a principal homogeneous space for $\mathrm{Cl}_\mathfrak{m}(A)$, as follows: the ideal class $[\mathfrak{a}]$ of an integral ideal $\mathfrak{a}$ acts on the pair (Γ, z) by $[\mathfrak{a}](\Gamma, z) = (\mathfrak{a}^{-1}\Gamma, z)$.*

Proof. Since $\mathfrak{a}$ is an integral ideal, $\mathfrak{m}z \subset \Gamma \subset \mathfrak{a}^{-1}\Gamma$, so z is still an $\mathfrak{m}$-division point of Γ, as needed. We now show that an ideal $\mathfrak{a}$ acts trivially on a pair (Γ, z) if and only if $\mathfrak{a}$ represents the trivial class in $\mathrm{Cl}_\mathfrak{m}(A)$. If $\mathfrak{a}$ represents the trivial class in $\mathrm{Cl}_\mathfrak{m}(A)$, then we may write $\mathfrak{a} = (\alpha)$ where $\alpha \equiv 1 \pmod{\mathfrak{m}}$. Then $[\mathfrak{a}](\Gamma, z) = (\alpha^{-1}\Gamma, \alpha^{-1}z)$ is homothetic to $(\Gamma, \alpha z)$, and because $\alpha \equiv 1 \pmod{\mathfrak{m}}$, $\alpha z = z$ in $\mathbf{C}_\mathfrak{p}/\Gamma$.

Conversely, suppose that the pairs (Γ, z) and $[\mathfrak{a}](\Gamma, z)(\mathfrak{a}^{-1}\Gamma, z)$ are homothetic: this means that there exists $\xi \in \mathbf{C}_\mathfrak{p}$ such that $\Gamma = \xi\mathfrak{a}^{-1}\Gamma$ and $z \equiv \xi z \pmod{\Gamma}$. By Proposition refprincipal homogeneous Cl(A), the former fact implies that $\mathfrak{a}$ equals the principal ideal (ξ). The second fact is equivalent to saying that $(\xi - 1)z = 0$ in $m^{-1}\Gamma/\Gamma$: because z is a generator of $\mathfrak{m}^{-1}\Gamma/\Gamma$, this happens only when $\xi \equiv 1 \pmod{\mathfrak{m}}$. □

We now define the exponential function associated to a lattice Γ. This is an entire function of $\mathbf{C}_\mathfrak{p}$ and is periodic with respect to the lattice Γ.

Definition. Let $e_\Gamma(z) : \mathbf{C}_\mathfrak{p} \to \mathbf{C}_\mathfrak{p}$ be given by

$$e_\Gamma(z) = z \prod_{\alpha \in \Gamma - \{0\}} \left(1 - \frac{z}{\alpha}\right). \tag{4.1}$$

Proposition 4.1.5. *The product in (4.1) converges for all z to define an entire function $e_\Gamma(z)$ on $\mathbf{C}_\mathfrak{p}$, that is, $e_\Gamma(z)$ can be expressed as an everywhere convergent power series on $\mathbf{C}_\mathfrak{p}$.*

Proof. Since Γ is discrete, for any enumeration $\{\alpha_1, \alpha_2, \dots\}$ of $\Gamma - \{0\}$, we have $\|\alpha_i\|_{\mathfrak{p}} \to \infty$ as $i \to \infty$ and so $1 - \frac{z}{\alpha_i} \to 1$ as $i \to \infty$. Since $\mathbf{C}_{\mathfrak{p}}$ is an ultrametric space, this implies that the product

$$z \prod_{\alpha \in \Gamma - \{0\}} \left(1 - \frac{z}{\alpha}\right)$$

can be expanded out into a power series in z that converges for all z. □

Lemma 4.1.6. *For all $\zeta \in \mathbf{C}_{\mathfrak{p}}^{\times}$, we have*

$$e_{\zeta\Gamma}(\zeta z) = \zeta e_{\Gamma}(z). \tag{4.2}$$

Proof. This follows directly by comparing the products for the two sides. □

The first property of $e_{\Gamma}(z)$ that we establish is its additivity. This will in turn imply its periodicity. We will show that $e_{\Gamma}(z_1 + z_2) = e_{\Gamma}(z_1) + e_{\Gamma}(z_2)$ for any z_1 and z_2 in $\mathbf{C}_{\mathfrak{p}}$. This is somewhat similar to the usual exponential function on the complex numbers $\mathbb{C}$, which is a homomorphism from the additive group $\mathbb{C}^{+}$ to the multiplicative group $\mathbb{C}^{\times}$. Our exponential function e_{Γ} is actually a homomorphism from the additive group $\mathbf{C}_{\mathfrak{p}}^{+}$ to itself. In fact, even more is true: our e_{Γ} is an endomorphism of $\mathbf{C}_{\mathfrak{p}}$ as an $\mathbb{F}_q$-vector space. In order to demonstrate this fact, we will first build up the theory of $\mathbb{F}_q$-linear polynomials, a theory that will be also important for the theory of Drinfeld modules developed in the next section.

Definition. Let K be a field containing $\mathbb{F}_q$, and let $\overline{K}$ be an algebraic closure of K. A polynomial $P(z) \in K[z]$ is called $\mathbb{F}_q$*-linear* if the function given by $P : \overline{K} \to \overline{K}$ is an $\mathbb{F}_q$-linear map.

Proposition 4.1.7. *A polynomial $P(z) \in K[z]$ with no repeated roots in $\overline{K}$ is $\mathbb{F}_q$-linear if and only if the set of roots of P is an $\mathbb{F}_q$-vector subspace of $\overline{K}$.*

Proof. One direction is immediate: the kernel of an $\mathbb{F}_q$-linear map is an $\mathbb{F}_q$-linear subspace.

On the other hand, suppose that the set W of roots of P is closed under addition and multiplication by elements of $\mathbb{F}_q$. Then, for any root $w \in W$, the polynomials $P(z)$ and $P(z+w)$ have the same leading coefficient and the same set of roots, so $P(z) = P(z+w)$ for all $w \in W$.

Now, for arbitrary fixed $a \in \overline{K}$, consider the polynomial $Q(z) = P(z+a) - P(z) - P(a)$ in $\overline{K}[z]$. We observe that the leading terms of $P(z)$ and $P(z+a)$ cancel each other out, so $\deg Q < \deg P$. By the previous paragraph, for any root w of P, we have

$$Q(w) = P(w+a) - P(w) - P(a) = P(a) - 0 - P(a) = 0, \tag{4.3}$$

so w is a root of Q. But P has $\deg P$ distinct roots in the algebraic closure $\overline{K}$, and Q has degree strictly less than $\deg P$, so this can only happen if Q is the zero polynomial. Plugging in $z = b$, we obtain $P(b+a) = P(b) + P(a)$ for all $b \in \overline{K}$. But a was arbitrary, so it follows that in fact, $P(a+b) = P(a) + P(b)$ for all $a, b \in \overline{K}$.

It remains to show that P is $\mathbb{F}_q$-linear. If the set of roots of P is an $\mathbb{F}_q$-vector space, this means that the number of roots of P, which is equal to $\deg P$, is of the form q^d for some positive integer d. Hence the leading term of $P(z)$ is of the form az^{q^d} for $a \in K^\times$. We now compare the polynomials $cP(z)$ and $P(cz)$ for $c \in \mathbb{F}_{\mathfrak{q}}^\times$. They have the same degree, and, since the set of roots of P is stable under multiplication by c, the same set of roots. Furthermore, the leading term of $P(cz)$ is $a(cz)^{q^d} = acz^{q^d}$, because $c \in \mathbb{F}_q$ is fixed by the qth power map. Hence $P(cz)$ also has the same leading term as $cP(z)$. This implies that $P(cz) = cP(z)$ and concludes the proof. □

Proposition 4.1.8. *For a lattice $\Gamma \subset \mathbf{C}_\mathfrak{p}$, the function $e_\Gamma(z) : \mathbf{C}_\mathfrak{p} \to \mathbf{C}_\mathfrak{p}$ is $\mathbb{F}_q$-linear.*

Proof. We express $e_\Gamma(z)$ as a limit of $\mathbb{F}_q$-linear polynomials. For each positive integer N, let

$$E_{\Gamma,N}(z) := z \prod_{\substack{\alpha \in \Gamma - \{0\} \\ v_\mathfrak{p}(\alpha) > -N}} \left(1 - \frac{z}{\alpha}\right). \tag{4.4}$$

Since $E_{\Gamma,N}(z)$ is a polynomial in z, by the previous proposition, it suffices to show that the set $\{\alpha \in \Gamma - \{0\} \mid v_\mathfrak{p}(\alpha) > -N)\} \cup \{0\}$ of roots of $E_{\Gamma,N}$ is an $\mathbb{F}_q$-vector space. On the one hand, Γ is an A-module, and A contains $\mathbb{F}_q$, so Γ is also an $\mathbb{F}_q$-vector space. On the other the strong $\mathfrak{p}$-adic triangle inequality on valuations implies that if $v_\mathfrak{p}(\alpha), v_\mathfrak{p}(\beta) > -N$, then $v_\mathfrak{p}(\alpha+\beta) \geq \min(v_\mathfrak{p}(\alpha), v_\mathfrak{p}(\beta)) > -N$ as well. Multiplying by elements of $\mathbb{F}_q$ does not affect $\mathfrak{p}$-adic valuation, so the set of α with $v_\mathfrak{p}(\alpha) > -N$ is also an $\mathbb{F}_q$-vector space. Hence the set of roots of $E_{\Gamma,N}$ is an $\mathbb{F}_q$-vector space, and we conclude that $E_{\Gamma,N}(z)$ is $\mathbb{F}_q$-linear.

By the definition of $e_\Gamma(z)$ as an infinite product, $e_\Gamma(z) = \lim_{N\to\infty} E_{N,\Gamma}(z)$. Since each of the convergents $E_{\Gamma,N}(z)$ is $\mathbb{F}_q$-linear it follows that $e_\Gamma(z)$ is $\mathbb{F}_q$-linear as well. □

We state without proof the following useful lemma from $\mathfrak{p}$-adic analysis. For a proof, see Chapter 2 of [5].

Lemma 4.1.9. *Any non-constant entire function $\mathbf{C}_\mathfrak{p} \to \mathbf{C}_\mathfrak{p}$ is surjective.*

Corollary 4.1.10. *The function $e_\Gamma(z)$ is periodic with respect to the lattice Γ, that is, for any $w \in \Gamma$, we have $e_\Gamma(z+w) = e_\Gamma(z)$. Furthermore e_Γ induces a bijective map from $\mathbf{C}_\mathfrak{p}/\Gamma$ to $\mathbf{C}_\mathfrak{p}$.*

Proof. The first part follows immediately from the previous proposition and the fact that $e_\Gamma(w) = 0$ for $w \in \Gamma$. This means that $e_\Gamma(z)$ only depends upon the coset of z in $\mathbf{C}_\mathfrak{p}/\Gamma$ and e_Γ induces a map, which we also call e_Γ, from $\mathbf{C}_\mathfrak{p}/\Gamma$ to $\mathbf{C}_\mathfrak{p}$. Since, for any given z, all but finitely many terms in the product for $e_\Gamma(z)$ are $\mathfrak{p}$-adic units, $e_\Gamma(z) = 0$ only when one of the factors is 0, and the kernel of the original map $e_\Gamma : \mathbf{C}_\mathfrak{p} \to \mathbf{C}_\mathfrak{p}$ is exactly Γ. Hence e_Γ induces a injective map from $\mathbf{C}_\mathfrak{p}/\Gamma$ to $\mathbf{C}_\mathfrak{p}$. By Lemma 4.1.9, the non-constant entire function $e_\Gamma : \mathbf{C}_\mathfrak{p} \to \mathbf{C}_\mathfrak{p}$ is surjective, so the induced map on $\mathbf{C}_\mathfrak{p}/\Gamma$ is surjective as well as injective, hence bijective. □

There is another corollary of Lemma 4.1.9 that will be very helpful later:

Lemma 4.1.11. *If f and g are entire functions on $\mathbf{C}_\mathfrak{p}$ that have the same zeroes (counting multiplicity), then f is a constant multiple of g.*

Proof. Consider the function f/g. By the assumption, f/g is entire and never zero, which means that f/g is not surjective. By Lemma 4.1.9, the only possibility is that f/g is constant. $\square$

We have shown that e_Γ is an isomorphism of $\mathbb{F}_q$-vector spaces $\mathbf{C}_\mathfrak{p}/\Gamma \to \mathbf{C}_\mathfrak{p}$. However, $\mathbf{C}_\mathfrak{p}/\Gamma$ is not merely an $\mathbb{F}_q$-vector space: it also has an A-module structure inherited from $\mathbf{C}_\mathfrak{p}$.

Let Γ and Γ' be a pair of lattices with $\Gamma \subset \Gamma'$ such that the index $[\Gamma' : \Gamma]$ is finite. We define a polynomial $P_{\Gamma'/\Gamma}(t)$ in t by

$$P_{\Gamma'/\Gamma}(t) = t \prod_{\sigma \in e_\Gamma(\Gamma') - \{0\}} \left(1 - \frac{t}{\sigma}\right). \tag{4.5}$$

This product is finite because Γ has finite index in Γ'. By construction, the set of roots of $P_{\Gamma'/\Gamma}(t)$ is $e_\Gamma(\Gamma')$, which is an $\mathbb{F}_q$-vector space, so $P_{\Gamma'/\Gamma}(t)$ is an $\mathbb{F}_q$-linear polynomial. The polynomial $P_{\Gamma'/\Gamma}(t)$ is important because of the following identity:

Proposition 4.1.12. *The exponential functions e_Γ and $e_{\Gamma'}$ are related by:*

$$e_{\Gamma'}(z) = P_{\Gamma'/\Gamma}(e_\Gamma(z)). \tag{4.6}$$

Proof. Both sides of the equality (4.6) are entire functions on $\mathbf{C}_\mathfrak{p}$. The left hand side has zeroes exactly at the points of Γ'. The right hand side is zero exactly when $e_\Gamma(z) \in e_\Gamma(\Gamma')$: since e_Γ maps $\mathbf{C}_\mathfrak{p}/\Gamma$ injectively to $\mathbf{C}_\mathfrak{p}$, this is the case exactly when $z \in \Gamma'$. Furthermore, all these zeroes are simple, so the two functions $e_{\Gamma'(z)}$ and $P_{\Gamma'/\Gamma}(e_\Gamma(z))$ have the same zeroes to the same order. By Lemma 4.1.11, the two sides of (4.6) must then be the same up to multiplication by a constant. However, if we expand both sides as power series in z, both sides have the coefficient of z equal to 1, so they must be identical. $\square$

There are two cases of this construction that will be especially useful to us. For one, we note that if $\Gamma' = \mathfrak{m}^{-1}\Gamma$, then the roots of polynomial $P_{\mathfrak{m}^{-1}\Gamma/\Gamma}$ are exactly the values of e_Γ at the $\mathfrak{m}$-division points of Γ. This polynomial will be important in showing that in special cases these division values are algebraic conjugates of each other.

For another, we consider the case where $\Gamma' = a^{-1}\Gamma$. Then $e_{\Gamma'(z)} = e_{a^{-1}\Gamma}(z) = a^{-1}e_\Gamma(az)$. Then Proposition 4.1.12 tells us that

$$e_\Gamma(az) = a^{-1}e_{a^{-1}\Gamma}(z) = P_{a^{-1}\Gamma/\Gamma}(e_\Gamma(z)). \tag{4.7}$$

We now introduce the notation $\phi_a^\Gamma := aP_{a^{-1}\Gamma/\Gamma}$. We have just shown

Proposition 4.1.13. *The two functions $e_\Gamma(z)$ and $e_\Gamma(az)$ are related by $e_\Gamma(az) = \phi_a^\Gamma(e_\Gamma(z))$.*

The map $a \mapsto \phi_a^\Gamma$ is called the "Drinfeld module" of Γ. We will work out some basic properties of this map before we give the abstract definition of a Drinfeld module.

Proposition 4.1.14. *Let Γ be a lattice, and let $a, b \in A$. The following statements hold:*

(a) If $a \in \mathbb{F}_q$, then $\phi_a^\Gamma(t) = at$.

(b) $\phi_{a+b}^\Gamma(t) = \phi_a^\Gamma(t) + \phi_b^\Gamma(t)$.

(c) $\phi_a^\Gamma(\phi_b^\Gamma(t)) = \phi_{ab}^\Gamma(t)$.

Proof. The first statement follows directly from the fact that $a\Gamma = \Gamma$ for $a \in \mathbb{F}_q$.

For the purposes of the second two parts, we may use surjectivity of e_Γ to set $t = e_\Gamma(z)$. By Proposition 4.1.13, $\phi_{a+b}^\Gamma(t) = e_\Gamma((a+b)z)$, and $\phi_a^\Gamma(t) + \phi_b^\Gamma(t) = e_\Gamma(az) + e_\Gamma(bz) = e_\Gamma(az + bz)$ by additivity of e_Γ. This shows (ii); a similar argument shows that both sides of (iii) are equal to $e_\Gamma(abz)$. $\square$

One way of rephrasing Proposition 4.1.14 is to say that the map $(a, t) \mapsto \phi_a^\Gamma(t)$ gives the $\mathbb{F}_q$-vector space $\mathbf{C}_\mathfrak{p}/\Gamma$ an A-module structure. Another interpretation is as follows.

The correspondence $a \mapsto \phi_a^\Gamma$ is a map from A to the set of $\mathbb{F}_q$-linear polynomials over $\mathbf{C}_\mathfrak{p}$. The set of $\mathbb{F}_q$-linear polynomials over $\mathbf{C}_\mathfrak{p}$ can be given the structure of a (non-commutative) $\mathbb{F}_q$-algebra, where the element $a \in \mathbb{F}_q$ corresponds to the additive polynomial ax, and the multiplication law is given by composition of polynomials. Then Proposition 4.1.14 says that the map $a \mapsto \phi_a^\Gamma$ is a homomorphism of $\mathbb{F}_q$-algebras. This homomorphism has the following special properties.

Proposition 4.1.15. *If Γ is a rank-one lattice, the degree of the polynomial $\phi_a^\Gamma(t) \in \mathbf{C}_\mathfrak{p}[t]$ is $q^{\deg_\mathfrak{p}(a)}$, and the coefficient of t in $\phi_a^\Gamma(t)$ is equal to a.*

Proof. Both statements follow from (4.5). The first statement comes from the fact that $\phi_a^\Gamma(t) = aP_{a^{-1}\Gamma/\Gamma}(t)$ is the product of $[a^{-1}\Gamma : \Gamma] = q^{\deg_\mathfrak{p} a}$ terms, and the second follows from the fact that the coefficient of t in $P_{a^{-1}\Gamma/\Gamma}(t)$ equals 1. $\square$

4.2 The theory of rank-one Drinfeld modules

As before, let A be the ring of elements of F that are integral away from $\mathfrak{p}$.

Definition. A *field over A* is a field K containing $\mathbb{F}_q$ equipped with a map $\iota : A \to K$ that is a morphism of $\mathbb{F}_q$-algebras (that is, ι is a ring homomorphism that is the identity on $\mathbb{F}_q$).

For our purposes, the field K will always be a field containing A, and $\iota : A \to K$ will be the inclusion map. However, it is also useful to consider cases in which $K = A/\mathfrak{q}$ for some prime ideal $\mathfrak{q}$ of A, and ι will be the map given by reduction mod $\mathfrak{q}$. This latter is central to the reduction theory of Drinfeld modules, a topic that this thesis will not discuss, but that is necessary to prove some of the results that we will use without proof.

We first go through some preliminaries on the algebra of $\mathbb{F}_q$-linear polynomials over K. Let τ be the polynomial $\tau(x) = x^q$. Because τ is a power of the Frobenius map $x \mapsto x^p$, τ is additive, and because τ also acts as the identity on $\mathbb{F}_q$, τ is $\mathbb{F}_q$-linear. Hence the algebra of $\mathbb{F}_q$-linear polynomials over K contains the noncommutative algebra $K\{\tau\}$ defines as the algebra of "twisted polynomials" the form $P = a_0 + a_1\tau + a_2\tau^2 + \cdots + a_m\tau^m$ which, when expressed as a polynomials of x are

$$\begin{aligned} P(x) &= a_0x + a_1\tau(x) + a_2\tau(\tau(x)) + \cdots + a_m\tau^m(x) \\ &= a_0x + a_1x^q + a_2x^{q^2} + \cdots + a_mx^{q^m}. \end{aligned} \tag{4.8}$$

Note that multiplication in $K\{\tau\}$ corresponds to composition of polynomials, so it is not the same as multiplication in $K[x]$. Multiplication in $K\{\tau\}$ is not commutative, but

$$\tau(ax) = a^qx^q = a^q\tau(x),$$

so we do have the identity that, for $\tau \cdot a = a^q\tau$ for $a \in K$, More generally, $\tau^i \cdot a = a^{q^i}\tau^i$. This implies that $K\{\tau\}$ is in fact closed under multiplication. The ring $K\{\tau\}$ is also called the "ring of twisted polynomials."

We now claim that all $\mathbb{F}_q$-linear polynomials are of the type described above: for a proof, see Chapter 1 of [5].

Proposition 4.2.1. *The ring of $\mathbb{F}_q$-linear polynomials over K is equal to $K\{\tau\}$.*

We introduce some notation: if $P(x) \in K[x]$ is an $\mathbb{F}_q$-linear polynomial, let $P(\tau)$ denote its representation in $K\{\tau\}$. Conversely, for $P(\tau) \in K\{\tau\}$, let $P(x)$ be the corresponding polynomial in x. (Caution: $P(\tau)$ is not obtained simply by setting $x = \tau$ in $P(x)$!)

Now, for nonzero $P(\tau) \in K\{\tau\}$ of the form $\sum_i a_i\tau^i$, define $\deg P$ to be the largest i such that the coefficient a_i of τ^i in $P(\tau)$ is nonzero. We observe that the degree of the corresponding polynomial $P(x)$ in x is $\deg P(x) = q^{\deg P(\tau)}$. Furthermore, degree is compatible with multiplication in $K\{\tau\}$: for $P(\tau)$, $Q(\tau) \in K\{\tau\}$ we have $\deg PQ = \deg P + \deg Q$. This implies that the product of two nonzero elements of $K\{\tau\}$ is nonzero, and therefore that left and right cancellation laws hold in $K\{\tau\}$.

Also, we define a morphism of $\mathbb{F}_q$-algebras $D : K\{\tau\} \to K$ that maps a polynomial in τ to its constant term i.e., $D(\sum_i a_i\tau^i) = a_0$. This map can be thought of as a "derivative at 0" map, since for $P(\tau)$ in $K\{\tau\}$, the coefficient of x in the corresponding polynomial $P(x)$ is the same as the constant term of $P(\tau)$, so $D(P)$ is the value of the (formal) derivative of $P(x)$ at the point $x = 0$.

With these definitions in hand, we are now ready to define a Drinfeld module.

Definition. Let K be a field over A. A Drinfeld A-module over K is an $\mathbb{F}_q$-algebra homomorphism $\phi : A \to K\{\tau\}$ such that (1) $D \circ \phi = \iota$, and (2) the image of ϕ is not contained in the subfield $K \subset K\{\tau\}$ of constant polynomials in τ.

We will use the notation ϕ_a for the image of an element $a \in A$ under the Drinfeld module homomorphism ϕ. The terminology "Drinfeld module" comes from the fact that any Drinfeld module A defined over K gives a structure of K as an A-module, where multiplication by an element $a \in A$ corresponds to application of the polynomial ϕ_a. (Note that this module structure does not agree with the standard A-module structure on K in which the multiplication map is the same as multiplication in K!)

We have seen an example of a Drinfeld module in the previous section:

Proposition 4.2.2. *For any lattice* Γ *in* $\mathbf{C}_\mathfrak{p}$*, the* $\mathbb{F}_q$*-algebra homomorphism* ϕ^Γ *given by* $a \mapsto \phi_a^\Gamma$ *is a Drinfeld module over* A*.*

Proof. This is a direct consequence of Propositions 4.1.14 and 4.1.15. □

There is a definition of the "rank" of a Drinfeld module, which turns out to correspond to that of the rank of a lattice. For our purposes, we will only need the definition of a rank-one Drinfeld module.

Definition. A Drinfeld A-module over K is said to be *a rank-one Drinfeld module* if, for every $a \in A$, $\deg(\phi_a) = \deg_\mathfrak{p}(a)$, where $\deg(\phi_a)$ denotes the degree of the twisted polynomial $\phi_a(\tau) \in K\{\tau\}$.

Proposition 4.2.3. *For any rank-one lattice* Γ *in* $\mathbf{C}_\mathfrak{p}$*, the associated Drinfeld module* ϕ^Γ *is also rank-one.*

Proof. This follows from Proposition 4.1.15 and the fact that $\deg \phi_a(\tau) = q^{\deg \phi_a(x)}$. □

It is an important theorem, which we state without proof, that the map $\Gamma \mapsto \phi^\Gamma$ is a one-to-one correspondence between rank-one lattices in $\mathbb{C}_\mathfrak{p}$ and rank-one Drinfeld modules over $\mathbb{C}_\mathfrak{p}$.

Theorem 4.2.4 (Uniformization theorem for rank-one Drinfeld modules). *Any rank-one Drinfeld module over* $\mathbb{C}_\mathfrak{p}$ *is the Drinfeld module* ϕ^Γ *of a uniquely determined rank-one lattice* $\Gamma \subset \mathbb{C}_\mathfrak{p}$*.*

Proof. For a proof, see [5]. □

We transfer some basic operations on lattices to the Drinfeld module setting. The set of rank-one lattices in $\mathbf{C}_\mathfrak{p}$ can be given the structure of a category in the following way. For lattices Γ and Γ', let the set of morphisms $\mathrm{Hom}(\Gamma, \Gamma')$ correspond to the set of $c \in \mathbf{C}_\mathfrak{p}$ such that $c\Gamma \subset \Gamma'$. Then composition of morphisms corresponds to multiplication of scalars: this is defined because if $c\Gamma \subset \Gamma'$ and $c'\Gamma' \subset \Gamma''$, then $cc'\Gamma \subset c'\Gamma' \subset \Gamma''$.

The definition of the category of Drinfeld modules is slightly more complicated, but we will show that the two are isomorphic.

Definition. If ϕ and ϕ' are Drinfeld modules, then a morphism from ϕ to ϕ', usually called an *isogeny*, is a twisted polynomial $P(\tau) \in K\{\tau\}$ such that $P\phi_a = \phi'_a P$ for all $a \in A$.

Note that if P is an isogeny from ϕ to ϕ' and P' is an isogeny from ϕ' to ϕ'', for all $a \in A$, $P'P\phi_a = P'\phi'_a P = \phi''_a P'P$, so the product $P'P$ is an isogeny from ϕ to ϕ''. It follows that Drinfeld modules and isogenies form a category. We now show that this category is isomorphic to the category of lattices already defined.

Proposition 4.2.5. *If* Γ*,* Γ' *are rank-one lattices in* $\mathbf{C}_\mathfrak{p}$ *and* ϕ^Γ*,* $\phi^{\Gamma'}$ *are the corresponding rank-one Drinfeld modules, there is a one-to-one correspondence between morphisms from* Γ *to* Γ' *and isogenies from* ϕ^Γ *to* $\phi^{\Gamma'}$*.*

Proof. In one direction, let $c \in \mathbf{C}$ be a morphism from Γ to Γ'. This means that $\Gamma \subset c^{-1}\Gamma'$, and, since they are both homothetic to ideals of A, Γ is a finite index sublattice of $c^{-1}\Gamma'$. Define the additive polynomial $P(x) = cP_{c^{-1}\Gamma'/\Gamma}(x)$ (where $P_{c^{-1}\Gamma'/\Gamma}(x)$ is defined as in (4.5)), and let $P(\tau)$ be the corresponding twisted polynomial in τ. By Proposition 4.1.12, the polynomial $P(x)$ satisfies $P(e_\Gamma(z)) = ce_{c^{-1}\Gamma'}(z) = e_{\Gamma'}(cz)$, and, since exponential functions are surjective, this relation uniquely determines P.

Now we must show that for any a, $P(\phi_a(x)) = \phi'_a(P(x))$ in $\mathbf{C}_\mathfrak{p}[x]$. Make the substitution $x = e_\Gamma(z)$. Then

$$P(\phi_a(x)) = P(\phi_a(e_\Gamma(z))) = P(e_\Gamma(az)) = e_{\Gamma'}(caz) = \phi'_a e_{\Gamma'}(cz) = \phi'_a P(e_\Gamma(z)) = \phi'_a(P(x))$$

as desired.

The other direction, although similar, is substantially more complicated, and we omit the proof. See Goss [5], Proposition 4.3.5 for a proof. □

The main concepts from the theory of lattices and exponential functions that we will need to carry over are the ideas of division points of a lattice and of the action of the class group of A on the set of homothety classes of lattices.

Definition. For an abstract Drinfeld module ϕ and an ideal $\mathfrak{a}$ of A, we can define an $\mathfrak{a}$-*division value* of A to be a value $x \in \mathbf{C}_\mathfrak{p}$ such that $\phi_a(x) = 0$ for all $a \in A$.

We note that if ϕ is the Drinfeld module ϕ^Γ associated to a rank-one lattice $\Gamma \in \mathbf{C}_\mathfrak{p}$, then the set of $\mathfrak{a}$-division values of ϕ are exactly the values $\{e_\Gamma(z) \mid z \in \mathfrak{a}^{-1}\Gamma\}$, which are in one-to-one correspondence with the points of $\mathfrak{a}^{-1}\Gamma/\Gamma$. Hence the number of $\mathfrak{a}$-division values of ϕ^Γ is exactly $\#(\mathfrak{a}^{-1}\Gamma/\Gamma) = N\mathfrak{a}$. By Theorem 4.2.4, this is true for any rank-one Drinfeld module ϕ.

Now, one way of determining the $\mathfrak{a}$-division values of Γ is to observe that x is a common root of ϕ_a for all $a \in \mathfrak{a}$ if and only if x is a root of the ideal generated by all such ϕ_a, or equivalently, by the unique monic generator of this ideal (which has no repeated roots because the ϕ_a all have no repeated roots). This generator, which we will call $\phi_\mathfrak{a}$, will be important in constructing ray class fields. We now present a more elegant way of constructing this polynomial, from the point of view of the twisted polynomial ring $K\{\tau\}$ rather than $K[x]$.

Recall that a *left ideal* of the noncommutative ring $K\{\tau\}$ is a subset of $K\{\tau\}$ that is closed under addition and left multiplication by elements of $K\{\tau\}$ i.e., that is a left $K\{\tau\}$-submodule of $K\{\tau\}$. Although $K\{\tau\}$ is noncommutative, it still remains some nice algebraic properties of commutative polynomial rings in one variable. In particular:

Proposition 4.2.6. *Any left ideal of $K\{\tau\}$ is principal.*

Proof. See [5], Chapter 1. The proof is almost exactly the same as in the commutative setting. □

Now, similarly to above, we consider the left $K\{\tau\}$-ideal $I_{\mathfrak{a},\phi}$ generated by the elements $\{\phi_a : a \in \mathfrak{a}\}$. By Proposition 4.2.6, this ideal has a unique monic generator, which we call $\phi_{\mathfrak{a}}$. Note that for twisted polynomials $P_1(\tau)$, $P_2(\tau)$, if we let P be the product P_1P_2 in $K\{\tau\}$, then since 0 is automatically a root of the polynomial $P_1(x)$, every root of P_2 is also a root of P. It follows by the same logic as in the commutative case that the roots of $\phi_{\mathfrak{a}}$ are exactly the $\mathfrak{a}$-division values of ϕ.

Also, note that when $\mathfrak{a} = aA$ is a principal ideal, $I_{\mathfrak{a},\phi}$ is generated by the element ϕ_a: however, ϕ_a is not generally monic. Define $\mu_\phi(a)$ to be the leading coefficient of ϕ_a. Then $\phi_{\mathfrak{a}} = \mu_\phi(a)^{-1}\phi_a$ is the monic normalization of ϕ_a.

We now relate our construction of $\phi_{\mathfrak{a}}$ back to exponential functions of lattices.

Lemma 4.2.7. *For a rank-one lattice* Γ *and an ideal* $\mathfrak{a}$ *of* A*, the following identity holds:*

$$e_{\mathfrak{a}^{-1}\Gamma}(z) = D(\phi^{\Gamma}_{\mathfrak{a}})^{-1}\phi^{\Gamma}_{\mathfrak{a}}(e_\Gamma(z)). \tag{4.9}$$

Proof. We observe that both sides of the equation have simple zeroes exactly at the points of $\mathfrak{a}^{-1}\Gamma$. Also, each side has derivative 1 at $z = 0$, so they must be equal. □

We can now construct an action of the ideal class group on the set of rank-one Drinfeld modules:

Proposition 4.2.8. *Let* ϕ *be a rank-one Drinfeld module over* K*, and* $\mathfrak{a}$ *be an ideal of* A*. Then there is a unique rank-one Drinfeld module over* K*, which we denote* $\mathfrak{a} * \phi$*, such that the twisted polynomial* $\phi_{\mathfrak{a}}$ *is an isogeny from* ϕ *to* $\mathfrak{a} * \phi$*.*

Proof. We first show that for any $b \in A$, $I_{\mathfrak{a},\phi}\phi_b \subset I_{\mathfrak{a},\phi}$. By definition, an arbitrary element of $I_{\mathfrak{a},\phi}$ can be written in the form $\psi = P_1\phi_{a_1} + P_2\phi_{a_2} + \cdots + P_m\phi_{a_m}$ for $P_1, \ldots, P_m \in K\{\tau\}$ and $a_1, \ldots, a_m \in \mathfrak{a}$. By the definition of a Drinfeld module and the commutativity of A, we have

$$\phi_a\phi_b = \phi_{ab} = \phi_{ba} = \phi_b\phi_a$$

for any $a, b \in A$, so

$$\begin{aligned}\psi\phi_b =& P_1\phi_{a_1}\phi_b + P_2\phi_{a_2}\phi_b + \cdots + P_m\phi_{a_m}\phi_b \\ =& (P_1\phi_b)\phi_{a_1} + (P_2\phi_b)\phi_{a_2} + \cdots + (P_m\phi_b)\phi_{a_m} \in I_{\mathfrak{a},\phi}\phi_b\end{aligned}$$

as desired.

Thus $I_{\mathfrak{a},\phi}\phi_b \subset I_{\mathfrak{a},\phi}$. In particular, since $\phi_{\mathfrak{a}} \in I_{\mathfrak{a},\phi}$, we have $\phi_{\mathfrak{a}}\phi_b \in I_{\mathfrak{a},\phi}$. But also, $I_{\mathfrak{a},\phi} = K\{\tau\}\phi_{\mathfrak{a}}$ by definition of $\phi_{\mathfrak{a}}$. This implies that there is a unique ϕ'_b such that $\phi_{\mathfrak{a}}\phi_b = \phi'_b\phi_{\mathfrak{a}}$.

We now need to check that ϕ' is a Drinfeld module. The fact that the map $b \mapsto \phi'_b$ is a homomorphism follows directly from the facts that

$$\phi_a(\phi_{b_1+b_2}) = \phi_a\phi_{b_1} + \phi_a\phi_{b_2} = \phi'_{b_1}\phi_a + \phi'_{b_2}\phi_a = (\phi'_{b_1} + \phi'_{b_2})\phi_a,$$

and likewise

$$\phi_a\phi_{b_1b_2} = \phi_a\phi_{b_1}\phi_{b_2} = (\phi'_{b_1}\phi'_{b_2})\phi_a.$$

To check that $D \circ \phi' = \iota$, we observe that

$$D(\phi_{\mathfrak{a}})D(\phi_b) = D(\phi_{\mathfrak{a}}\phi_b) = D(\phi'_b\phi_{\mathfrak{a}}) = D(\phi'_b)D(\phi_{\mathfrak{a}})$$

in K. Since $\phi_{\mathfrak{a}}$ does not have a double zero at 0, we can cancel $D(\phi_{\mathfrak{a}})$, and we get that $D(\phi'_b) = D(\phi(b)) = \iota(b)$ as needed. Finally, to check that ϕ' is rank-one, we take degrees of both sides of the equation $\phi_{\mathfrak{a}}\phi_b = \phi'_b\phi_{\mathfrak{a}}$ and use additivity of degree.

Also, $\phi_{\mathfrak{a}}$ is an isogeny from ϕ to ϕ' by construction. So we can take $\mathfrak{a} * \phi$ to be the Drinfeld module ϕ' constructed above, and we are done. $\square$

We now show that, up to a scaling factor, this operation corresponds to the action of fractional ideals of A on rank-one lattices in $\mathbf{C}_{\mathfrak{p}}$.

Proposition 4.2.9. *Let Γ be a rank-one lattice in $\mathbf{C}_{\mathfrak{p}}$, and let $\mathfrak{a}$ be an ideal in A. Let $\phi' = \mathfrak{a} * \phi^{\Gamma}$, and let $\Gamma' = D(\phi^{\Gamma}_{\mathfrak{a}}) \cdot \mathfrak{a}^{-1}\Gamma$. Then $\phi' = \phi^{\Gamma'}$.*

Proof. We need to show that for any $b \in A$, $e_{\Gamma'}(bz) = \phi'(e'_{\Gamma}(z))$. For brevity of notation, write Δ for $e_{D(\phi^{\Gamma}_{\mathfrak{a}})}$. We now manipulate and apply Lemma 4.2.7:

$$e_{\Gamma'}(bz) = e_{\Delta\cdot\mathfrak{a}^{-1}\Gamma}(bz) = \Delta \cdot e_{\mathfrak{a}^{-1}\Gamma}(\Delta^{-1}bz) = \phi^{\Gamma}_{\mathfrak{a}}(e_{\Gamma}(\Delta^{-1}bz)) = \phi^{\Gamma}_{\mathfrak{a}}\phi^{\Gamma}_{b}e_{\Gamma}(\Delta^{-1}z) \tag{4.10}$$

Now, using the definition of the action $*$, we have $\phi^{\Gamma}_{\mathfrak{a}}\phi^{\Gamma}_{b}e_{\Gamma}(\Delta^{-1}z) = (\mathfrak{a} * \phi^{\Gamma})_b\phi_{\mathfrak{a}}e_{\Gamma}(\Delta^{-1}z)$, and doing the same manipulations as in (4.10) backwards, we obtain $\phi_{\mathfrak{a}}e_{\Gamma}(\Delta^{-1}z) = e_{\Gamma'}(z)$. Putting it all together gives $e_{\Gamma'}(bz) = (\mathfrak{a} * \phi^{\Gamma})_b(e_{\Gamma'}(z))$, as desired. $\square$

Lemma 4.2.10. *For integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A, the following equalities hold:*

(a) $\phi_{\mathfrak{a}\mathfrak{b}} = (\mathfrak{b} * \phi)_{\mathfrak{a}}\phi_{\mathfrak{b}}$

(b) $\mathfrak{a} * (\mathfrak{b} * \phi) = (\mathfrak{a}\mathfrak{b}) * \phi$.

Proof. For part (a), note that both sides are monic, so it suffices to show that they generate the same left ideal of $K\{\tau\}$. By definition, we know that $\phi_{\mathfrak{a}\mathfrak{b}}$ is the unique monic generator of the left ideal generated by the elements ϕ_c for $c \in \mathfrak{a}\mathfrak{b}$. By definition of the product $\mathfrak{a}\mathfrak{b}$, this is the same as the left $K\{\tau\}$-ideal generated by all elements of the form $\phi_a\phi_b$ for $a \in \mathfrak{a}$, $b \in \mathfrak{b}$.

On the other hand, the left ideal generated by $(\mathfrak{b} * \phi)_{\mathfrak{a}}$ is the left ideal generated by the elements $(\mathfrak{b}*\phi)_a$ for all $a \in \mathfrak{a}$. Hence the left $K\{\tau\}$-ideal given by $K\{\tau\}(\mathfrak{b}*\phi)_{\mathfrak{a}}\phi_{\mathfrak{b}}$ is generated by the set of elements of the form $(\mathfrak{b} * \phi)_a\phi_{\mathfrak{b}} = \phi_{\mathfrak{b}}\phi_a$. By defintion,we know that $K\{\tau\}\phi_{\mathfrak{b}}$ is also the left $K\{\tau\}$ ideal generated by elements ϕ_b with $b \in \mathfrak{b}$. Putting this together, we conclude that $K\{\tau\}(\mathfrak{b} * \phi)_{\mathfrak{a}}\phi_{\mathfrak{b}}$ is generated by the set of elements of the form $\phi_b\phi_a$ for $b \in \mathfrak{b}$ and $a \in \mathfrak{a}$. Since $\phi_b\phi_a = \phi_a\phi_b$, this is the same as the left ideal $K\{\tau\}\phi_{\mathfrak{a}\mathfrak{b}}$, as desired.

The second part then follows: by definition of $(\mathfrak{a}\mathfrak{b}) * \phi$, we need to show that $\phi_{\mathfrak{a}\mathfrak{b}}\phi_y = \mathfrak{a} * (\mathfrak{b} * \phi)_y\phi_{\mathfrak{a}\mathfrak{b}}$ for all $y \in A$. By the first part, the right hand side can be rewritten as

$$\mathfrak{a} * (\mathfrak{b} * \phi)_y(\mathfrak{b} * \phi)_{\mathfrak{a}}\phi_{\mathfrak{b}} = (\mathfrak{b} * \phi)_{\mathfrak{a}}(\mathfrak{b} * \phi)_y\phi_{\mathfrak{b}} = (\mathfrak{b} * \phi)_{\mathfrak{a}}\phi_{\mathfrak{b}}\phi_y = \phi_{\mathfrak{a}\mathfrak{b}}\phi_y$$

as needed. $\square$

Corollary 4.2.11. *The group of fractional ideals of A acts on the set of rank-one Drinfeld modules for A defined over $\mathbf{C}_\mathfrak{p}$. This action descends to give an action of the class group* $\mathrm{Cl}(A)$ *on the set of isomorphism classes of rank-one Drinfeld modules over A; this set exhibits the set of isomorphism classes of rank-one Drinfeld module as a principal homogeneous space for* $\mathrm{Cl}(A)$.

Proof. The first statement follows from Lemma 4.2.10. By Proposition 4.2.9, the action of the group of fractional ideals of A on the set of isomorphism classes of rank-one Drinfeld modules is the same as its action on the set of homothety classes of rank-one lattices. In particular, this means that principal ideals of A act trivially on the set of isomorphism classes of rank-one Drinfeld modules, and so induce an action of $\mathrm{Cl}(A)$ on this set of isomorphism classes which is identical to the action of $\mathrm{Cl}(A)$ on homothety classes of rank-one lattices. The second part then follows from Proposition 4.1.2. $\square$

We now fix an ideal $\mathfrak{m}$ of A. For any rank-one Drinfeld module ϕ, define $\Lambda_\phi(\mathfrak{m})$ to be the set of $\mathfrak{m}$-division values of ϕ, that is, the set of roots of the polynomial $\phi_\mathfrak{m}$.

Proposition 4.2.12. *The Drinfeld module ϕ induces an A-module structure on $\Lambda_\phi(\mathfrak{m})$, such that $\Lambda_\phi(\mathfrak{m}) \cong A/\mathfrak{m}$ as A-modules.*

Proof. By uniformization we may write $\phi = \phi^\Gamma$ as the Drinfeld module of a lattice Γ. Then we know already that the $\mathfrak{m}$-division values of Γ are exactly the values $\{e_\Gamma(z) \mid z \in \mathfrak{m}^{-1}\Gamma/\Gamma\}$. Furthermore, by Proposition , $\mathfrak{m}^{-1}\Gamma/\Gamma$ is a an A-module isomorphic to $A/\mathfrak{m}$, and this A-module structure corresponds to the A-module structure on $\Lambda_\phi(\mathfrak{m})$. $\square$

We now extend $*$ to an action of the integral ideals of A relatively prime to $\mathfrak{m}$ on the set of pairs (ϕ, λ) such that ϕ is a rank-one Drinfeld module over $\mathbf{C}_\mathfrak{p}$ and λ is a generator of the A-module $\Lambda_\phi(\mathfrak{m})$. To do this, we use the following lemma:

Lemma 4.2.13. *Let ϕ be a rank-one Drinfeld module and $\mathfrak{a}$ an integral ideal of A. The map $x \mapsto \phi_\mathfrak{a}(x)$ maps the A-module $\Lambda_\phi(\mathfrak{m})$ isomorphically to the A-module $\Lambda_{\mathfrak{a}*\phi}(\mathfrak{m})$. Consequently, it sends the set of generators of $\Lambda_\phi(\mathfrak{m})$ bijectively to the set of generators of $\Lambda_{\mathfrak{a}*\phi}(\mathfrak{m})$.*

Proof. First of all, we know that for any integral ideal $\mathfrak{a}$ relatively prime to $\mathfrak{m}$, the twisted polynomial $\phi_\mathfrak{a}$ is an isogeny from ϕ to $\mathfrak{a} * \phi$. We first show that that for any $\lambda \in \Lambda_\mathfrak{a}(\mathfrak{m})$, $\phi_\mathfrak{a}(\lambda)$ is an $\mathfrak{m}$-division value of $\mathfrak{a} * \phi$. Indeed, for any $m \in \mathfrak{m}$, $(\mathfrak{a} * \phi)_m(\phi_\mathfrak{a}(\lambda)) = \phi_\mathfrak{a}(\phi_m(\lambda))$.

Hence $\phi_\mathfrak{a}$ maps $\Lambda_\phi(\mathfrak{m})$ to $\Lambda_{\mathfrak{a}*\phi}(\mathfrak{m})$, and this map is a homomorphism of A-modules because $\phi_\mathfrak{a}$ is an isogeny. We claim that it fact it is an isomorphism. We know that the two sets $\Lambda_\phi(\mathfrak{m})$ and $\Lambda_{\mathfrak{a}*\phi}(\mathfrak{m})$ both have the same size, so it suffices to show that $\phi_\mathfrak{a}$ is injective. Suppose not: then there would be some nonzero $\lambda \in \Lambda_\phi(\mathfrak{m})$ such that $\phi_\mathfrak{a}(\lambda) = 0$. By definition, this means that $\phi_a(\lambda) = 0$ for all $a \in \mathfrak{a}$. Likewise, we know that $\phi_m(\lambda) = 0$ for all $m \in \mathfrak{m}$. But we have assumed that the two ideals $\mathfrak{a}$ and $\mathfrak{m}$ are relatively prime, so there exists some $a \in \mathfrak{a}$ and some $\mathfrak{m} \in m$ such that $a + m = 1$. This means that $\lambda = \phi_1(\lambda) = \phi_a(\lambda) + \phi_m(\lambda) = 0$. Hence the kernel of the map $\phi_\mathfrak{a} : \Lambda_\phi(\mathfrak{m}) \to \Lambda_{\mathfrak{a}*\phi}(\mathfrak{m})$ is trivial.

Hence the map $\phi_\mathfrak{a} : \Lambda_\phi(\mathfrak{m}) \to \Lambda_{\mathfrak{a}*\phi}(\mathfrak{m})$ is an isomorphism. In particular, this means that $\phi_\mathfrak{a}$ maps generators of $\Lambda_\phi(\mathfrak{m})$ to generators of $\Lambda_{\mathfrak{a}*\phi}(\mathfrak{m})$. $\square$

This motivates us to look at the following action:

Definition. For an integral ideal $\mathfrak{a}$ of A relatively prime to $\mathfrak{m}$ and a pair (ϕ, λ) such that λ is a generator of $\Lambda_\phi(\mathfrak{m})$, define

$$\mathfrak{a} * (\phi, \lambda) = (\mathfrak{a} * \phi, \phi_{\mathfrak{a}}(\lambda)). \tag{4.11}$$

The action given here is in fact an action because

$$\mathfrak{a} * (\mathfrak{b} * (\phi, \lambda)) = \mathfrak{a} * (\mathfrak{b} * \phi, \phi_{\mathfrak{b}}(\lambda)) = (\mathfrak{a} * (\mathfrak{b} * \phi), (\mathfrak{b} * \phi)_{\mathfrak{a}}(\lambda)) = (\mathfrak{a}\mathfrak{b} * \phi, \phi_{\mathfrak{a}\mathfrak{b}}(\lambda))$$

by Lemma 4.2.10.

We have an analogue of Proposition 4.2.9 which relates this action of ideals back to the action of $I_{\mathfrak{m}}(A)$ on lattices.

Proposition 4.2.14. *Let (Γ, z) be a pair consisting of a rank-one lattice Γ in $\mathbf{C}_{\mathfrak{p}}$ and an $\mathfrak{m}$-division point z of Γ. Let $\Gamma' = D(\phi^\Gamma_{\mathfrak{a}}) \cdot \mathfrak{a}^{-1}\Gamma$ and $z' = D(\phi^\Gamma_{\mathfrak{a}}) \cdot z$. Then for any ideal $\mathfrak{a}$ of A relatively prime to $\mathfrak{m}$,*

$$\mathfrak{a} * (\phi^\Gamma, e_\Gamma(z)) = (\phi^{\Gamma'}, e_{\Gamma'}(z')). \tag{4.12}$$

Proof. Proposition 4.2.9 states that $\mathfrak{a} * \phi^\Gamma = \phi^{\Gamma'}$, and Proposition 4.2.7 states that

$$\phi^\Gamma_{\mathfrak{a}}(e_\Gamma(z)) = D(\phi^\Gamma_{\mathfrak{a}})e_{\mathfrak{a}^{-1}\Gamma}(z) = e_{D(\phi^\Gamma_{\mathfrak{a}})\mathfrak{a}^{-1}\Gamma}(D(\phi^\Gamma_{\mathfrak{a}})z) = e_{\Gamma'}(z').$$

The result follows. □

4.3 Hayes's theory of sgn-normalized Drinfeld modules

In the previous section we showed, via the correspondence with lattices, that the action of any principal ideal of A sends any Drinfeld module ϕ to another isomorphic Drinfeld module ϕ. We now work out explicitly what this isomorphic Drinfeld module is. Recall that for $a \in A$, we have defined $\mu_\phi(a)$ as the leading coefficient of ϕ_a.

Lemma 4.3.1. *If $\mathfrak{a} = (a)$ is a principal ideal of A, then $\mathfrak{a} * \phi = \mu_\phi(a)^{-1}\phi\mu_\phi(a)$.*

Proof. We need to check that for any $b \in A$, we have $\phi_{\mathfrak{a}}\phi_b = \mu_\phi(a)^{-1}\phi_b\mu_\phi(a)\phi_{\mathfrak{a}}$. However, we have previously shown that $\phi_{\mathfrak{a}} = \mu_a^{-1}\phi_a$, and the twisted polynomials ϕ_a and ϕ_b commute, so

$$\phi_{\mathfrak{a}}\phi_b = \mu_a^{-1}\phi_a\phi_b = \mu^{-1}\phi_b\phi_{\mathfrak{a}} = \mu_\phi(a)^{-1}\phi_b\mu_\phi(a)\phi_{\mathfrak{a}}$$

as desired. □

This gives us hope that if we can control the function $\mu_\phi(a)$, we can better understand the action of fractional ideals on specific Drinfeld modules. Recall that we have chosen a sign function $\mathrm{sgn}_{\mathfrak{p}}$ on $\mathbf{F}_{\mathfrak{p}}$, which takes values in the field of constants $k_{\mathfrak{p}}$ of $\mathbf{F}_{\mathfrak{p}}$. For the purposes of this section, $\mathrm{sgn}_{\mathfrak{p}}$ will be the only sign function we consider, so we will drop the subscript and write sgn where there is no ambiguity. For an element σ of the Galois group $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_q)$, define the *twisting of* sgn *by* σ to be the function $\sigma \circ \mathrm{sgn} : \mathbf{F}_{\mathfrak{p}} \to k_{\mathfrak{p}}$. The function $\sigma \circ \mathrm{sgn}$ is called a *twisted sign function.*

Definition. A rank-one Drinfeld module ϕ is said to be sgn-*normalized* if the map $\mu_\phi : A \to k_\mathfrak{p}$ is the restriction to A of a twisting of sgn.

Let X denote the set of rank-one sgn-normalized Drinfeld modules over A. For convenience, we will adopt the notation in [5] of calling such a module a *Hayes-module* for sgn. We now invoke the following result, which says that there are Hayes-modules, and tells us how many exist. For a proof, see sections 12 and 13 of Hayes [10].

Proposition 4.3.2. *Any rank-one Drinfeld module over A is isomorphic to a Hayes-module, and every isomorphism class contains exactly* $\frac{q^{\deg \mathfrak{p}}-1}{q-1} = W_{\mathbf{F}_\mathfrak{p}}/W_F$ sgn-*normalized Drinfeld modules.*

The sgn-normalized Drinfeld modules enjoy several nice properties, some of which we will state below. For example:

Proposition 4.3.3. *If ϕ is a rank-one* sgn-*normalized Drinfeld module defined over a finite extension K of F, then for all $a \in A$, the coefficients of ϕ_a lie in the integral closure B of A in K.*

For a proof of this result, see [5].

Let $X_\mathfrak{m}$ be the set of all pairs (ϕ, λ) where ϕ is a Hayes-module and λ is a generator of $\Lambda_\phi(\mathfrak{m})$. Recall that we have defined an action $*$ of the ideals of A on the set of all pairs (ϕ, λ) by $\mathfrak{a} * (\phi, \lambda) = (\mathfrak{a} * \phi, \phi_\mathfrak{a}(\lambda))$. We now define a narrow ray class group $\mathrm{Cl}^+_\mathfrak{m}(A)$ with respect to the function sgn:

$$\mathrm{Cl}^+_\mathfrak{m}(A) = I_\mathfrak{m}(A)/P^+_\mathfrak{m}(A) \tag{4.13}$$

where, $I_\mathfrak{m}(A)$ is, as before, the group of fractional ideals of A relatively prime to $\mathfrak{m}$, and $P^+_\mathfrak{m}(A)$ is the group of principal fractional ideals of the form (a) where $a \equiv 1 \pmod{\mathfrak{m}}$ and $\mathrm{sgn}(a) = 1$.

Theorem 4.3.4. *The set $X_\mathfrak{m}$ has the structure of a principal homogeneous space for $\mathrm{Cl}^+_\mathfrak{m}(A)$ under the action induced by $*$.*

Proof. We first show that for any integral ideal $\mathfrak{a}$ of A relatively prime to $\mathfrak{m}$ and any pair $(\phi, \lambda) \in X_\mathfrak{m}$, we have $\mathfrak{a} * (\phi, \lambda) = (\mathfrak{a} * \phi, \phi_\mathfrak{a}(\lambda)) \in X_\mathfrak{m}$ as well. We already know that $\mathfrak{a} * \phi$ is sgn-normalized, and we've shown previously that $\phi_\mathfrak{a}(\lambda)$ is also a generator of $\Lambda_\phi(\mathfrak{a})$. We conclude that indeed $\mathfrak{a} * (\phi, \lambda) \in X_\mathfrak{m}$.

Now, we prove that if the integral ideal $\mathfrak{a}$ represents the trivial ideal class in $\mathrm{Cl}^+_\mathfrak{m}(A)$, then the action of $\mathfrak{a}$ on $X_\mathfrak{m}$ is trivial. Suppose that $\mathfrak{a}$ belongs to the trivial ideal class of $\mathrm{Cl}^+_\mathfrak{m}(A)$, that is, $\mathfrak{a} = (a)$ is generated by a positive element $a \in A$ that is congruent to 1 mod $\mathfrak{m}$. Let (ϕ, λ) be an arbitrary element of $X_\mathfrak{m}$. Because a is positive and ϕ is sgn-normalized, $\mu_\phi(a) = 1$, and it follows that $\phi_\mathfrak{a} = \phi_a$ and $\mathfrak{a} * \phi = \phi$. Finally, because $\Lambda_\phi(\mathfrak{a})$ is isomorphic to $A/\mathfrak{m}$ under the A-module structure induced by ϕ, and a is 1 mod $\mathfrak{m}$, $\phi_\mathfrak{a}$ acts trivially on $\Lambda_\phi(\mathfrak{a})$. Hence $\phi_\mathfrak{a}(\lambda) = \phi_a(\lambda) = \lambda$. We conclude that $\mathfrak{a} * (\phi, \lambda) = (\mathfrak{a} * \phi, \phi_\mathfrak{a}(\lambda)) = (\phi, \lambda)$ as desired.

Hence the action of the ideals of A on the set of pairs (ϕ, λ) descends to an action of $\mathrm{Cl}^+_{\mathfrak{m}}(A)$ on $X_{\mathfrak{m}}$. We now show that this action is free, and we will conclude that $X_{\mathfrak{m}}$ is a principal homogeneous space for $\mathrm{Cl}^+_{\mathfrak{m}}(A)$ by counting elements.

To show that the action is free: suppose there exists an ideal $\mathfrak{a}$ of $\mathrm{Cl}^+_{\mathfrak{m}}(A)$ such that for some $(\phi, \lambda) \in X_{\mathfrak{m}}$, $\mathfrak{a} * (\phi, \lambda) = (\phi, \lambda)$. We must show that the ideal class $[\mathfrak{a}]$ in $\mathrm{Cl}^+_{\mathfrak{m}}(A)$ is the identity. From our conditions, we have $\mathfrak{a} * \phi = \phi$ and $\phi_{\mathfrak{a}}(\lambda) = \lambda$. Because $\mathfrak{a} * \phi$ is equal to ϕ, we also have the weaker statement that $\mathfrak{a} * \phi$ is isomorphic to ϕ, which, by Proposition 4.2.11 implies that $\mathfrak{a}$ is a principal ideal. Write $\mathfrak{a} = (a)$ for some $a \in A$. By Lemma 4.3.1 $\phi_{\mathfrak{a}}(\lambda) = \mu_\phi(a)^{-1}\phi_a(\lambda)\mu_\phi(a)$. Then $\phi = \mathfrak{a} * \phi = \mu_\phi(a)^{-1} \cdot \phi \cdot \mu_\phi(a)$. By comparing coefficients, we see that this is only possible if $\mu_\phi(a)$ lies in the subgroup $\mathbb{F}_q^\times$ of $k_{\mathfrak{p}}^\times$: because ϕ is sgn-normalized, $\mathrm{sgn}(a)$ must also lie in $\mathbb{F}_q^\times$. By multiplying by the appropriate element of $\mathbb{F}_q^\times$, we may now assume that $\mathrm{sgn}\, a = 1$, so also $\mu_\phi(a) = 1$. It then follows that $\phi_{\mathfrak{a}} = \mu_\phi(a)^{-1}\phi_a = \phi_a$. By our original condition that $\phi_{\mathfrak{a}}(\lambda) = \lambda$, it follows that $\phi_a(\lambda) = \lambda = \phi_1(\lambda)$, and since $\Lambda_\phi(\mathfrak{m})$ is isomorphic to $A/\mathfrak{m}$ as an $\mathfrak{a}$-module, this implies that $a \equiv 1 \pmod{\mathfrak{m}}$.

Finally, we show that $X_{\mathfrak{m}}$ and $\mathrm{Cl}^+_{\mathfrak{m}}(A)$ have the same number of elements. We know by Corollary 4.2.11 that the set of isomorphism classes of Drinfeld modules over $\mathbf{C}_\infty$ is a principal homogeneous space for $\mathrm{Cl}(A)$, so the number of such isomorphism classes equals $\#(\mathrm{Cl}(A))$. Also, any isomorphism class contains $\frac{q^{\deg_{\mathfrak{p}}}-1}{q-1}$ sgn-normalized Drinfeld modules by Proposition 4.3.2. Finally, the set of $\mathfrak{m}$ torsion points of any sgn-normalized Drinfeld module is an A-module isomorphic to $A/\mathfrak{m}$, and so the number of its generators equals $\#((A/\mathfrak{m})^\times)$. Multiplying, we find that the number of sgn-normalized Drinfeld modules is equal to

$$\#(\mathrm{Cl}(A)) \cdot \frac{q^{\deg_{\mathfrak{p}}} - 1}{q-1} \cdot \#((A/\mathfrak{m})^\times) \tag{4.14}$$

To count the size of $\mathrm{Cl}^+_{\mathfrak{m}}(A)$, we recall that $\mathrm{Cl}^+_{\mathfrak{m}}(A) = I_{\mathfrak{m}}(A)/P^+_{\mathfrak{m}}(A)$. On the other hand, the class group $\mathrm{Cl}(A)$ is defined as ideals modulo principal ideals, so $\mathrm{Cl}^+(A) = I(A)/P(A) \cong I_{\mathfrak{m}}(A)/(P(A) \cap I_{\mathfrak{m}}(A))$. Comparing, we see that $\#(\mathrm{Cl}^+_{\mathfrak{m}}(A))/\#(\mathrm{Cl}(A)) = [P(A) \cap I_{\mathfrak{m}}(A) : P_{\mathfrak{m}}(A)]$, which is the size of the quotient of the group of principal ideals by the group of principal ideals generated by positive elements congruent to 1 mod $\mathfrak{m}$. A simple counting argument in group theory shows that this index equals $\frac{q^{\deg_{\mathfrak{p}}}-1}{q-1} \cdot \#((A/\mathfrak{m})^\times)$. Hence $\#(X_{\mathfrak{m}}) = \#(\mathrm{Cl}^+_{\mathfrak{m}}(A))$, and it follows that the two groups have the same number of elements. □

4.4 Explicit class field theory

Now, let $\phi \in X$ be a fixed Hayes-module for sgn. Let y be any nonconstant element of the ring A. Let H^+_A be the field extension of F generated by the coefficients of ϕ_y. Although we will not show it, it is the case that

Proposition 4.4.1. *The field extension H^+_A is independent of our choice of element y.*

This means in particular that ϕ is in fact defined as a Drinfeld-module over H_A^+, and so all twisted polynomials of the form ϕ_a or $\phi_{\mathfrak{a}}$ reside in the ring $H_A^+\{\tau\}$. Furthermore, we show that

Proposition 4.4.2. *The field extension H_A^+ is independent of our choice of Hayes-module ϕ.*

Proof. By Theorem 4.3.4, any other Hayes-module ψ is of the form $\psi = \mathfrak{a} * \phi$ for some fractional ideal $\mathfrak{a}$ of A. The construction of the module $\mathfrak{a} * \phi$ can be carried out entirely in the field H_A^+, so the coefficients of ψ_y live in the field H_A^+ generated by the coefficients of ϕ_y. Conversely, using $\phi = \mathfrak{a}^{-1} * \psi$, we see that the coefficients of ϕ_y also live in the field generated by the coefficients of ψ_y, and so the two fields are the same. $\square$

We also show that

Proposition 4.4.3. *The field H_A^+ is a separable extension of F.*

Proof. We must show that for a Hayes-module ϕ over $\mathbf{C}_{\mathfrak{p}}$, the coefficients of ϕ lie in a separable extension of F. Because the completion $\mathbf{F}_{\mathfrak{p}}$ of F at $\mathfrak{p}$ is separable, it will suffice to show that these coefficients lie in a separable extension of $\mathbf{F}_{\mathfrak{p}}$.

By Theorem 4.2.4, there is some lattice Γ in $\mathbf{C}_{\mathfrak{p}}$ such that $\phi = \phi^{\Gamma}$. Furthermore, we can write Γ as $\xi\mathfrak{a}$ for some $\xi \in \mathbf{C}_{\mathfrak{p}}$ and some $\mathfrak{a} \subset A$. It follows that $\phi = \phi^{\Gamma} = \phi^{\xi\mathfrak{a}} = \xi\phi^{\mathfrak{a}}\xi^{-1}$. We observe that $\phi^{\mathfrak{a}}$ was constructed by purely analytic means, and so the coefficients of $\phi^{\mathfrak{a}}$ live in $\mathbf{C}_{\mathfrak{p}}$. Now, for any $y \in A$, the leading coefficient $\mu_\phi(y)$ is given by

$$\mu_\phi(y) = \xi\xi^{-q^{\deg_{\mathfrak{p}} y}}\mu_{\phi^{\mathfrak{a}}}(y) = \xi^{1-q^{\deg_{\mathfrak{p}} y}}\mu_{\phi^{\mathfrak{a}}}(y).$$

By sgn-normalization of ϕ, $\mu_\phi(y)$ is an element of $k_{\mathfrak{p}} \subset \mathbf{F}_{\mathfrak{p}}$. Hence the element ξ satisfies the polynomial equation $\xi^{q^{\deg_{\mathfrak{p}} y}-1} = \mu\phi^{\mathfrak{a}}(y)/\mu_\phi(y)$ with coefficients in $\mathbf{F}_{\mathfrak{p}}$. This equation is separable since $q^{\deg_{\mathfrak{p}} y}-1$ is relatively prime to the characteristic of the field, so the extension $\mathbf{K}_{\mathfrak{p}}(x)/\mathbf{K}$ is separable. $\square$

We now use the division values to build another extension on top of H_A^+. Fix an ideal $\mathfrak{m}$ of A.

Proposition 4.4.4. *Let ϕ be a Hayes-module and let $\lambda \in \Lambda_\phi(\mathfrak{m})$ be a division value of ϕ. Then the extension $L = H_A^+(\lambda)$ is independent of the choice of λ (although it does depend on $\mathfrak{m}$).*

Proof. Suppose that we made a second choice of Hayes-module ϕ' and division value $\lambda' \in \Lambda_{\phi'}(\mathfrak{m})$. Then, by transitivity of the action of $\mathrm{Cl}_{\mathfrak{m}}^+(A)$ on $X_{\mathfrak{m}}$, there exists some ideal $\mathfrak{a}$ of A such that $\mathfrak{a} * (\phi, \lambda) = (\phi', \lambda')$. This means that $\lambda' = \phi_{\mathfrak{a}}(\lambda)$. Now, we know that $\phi_{\mathfrak{a}}$ has coefficients in the field H_A^+, so it follows that $\lambda' = \phi_{\mathfrak{a}}(\lambda) \in H_A(\lambda)$. The same argument in reverse gives $\lambda \in H_A(\lambda')$, so $H_A(\lambda) = H_A(\lambda')$, and the extension $L = H_A^+(\lambda)$ is independent of the choice of λ. $\square$

Proposition 4.4.5. *The extension $H_A^+(\lambda)/F$ is separable.*

Proof. By Proposition 4.4.3, it suffices to show that the extension $H_A^+(\lambda)/H_A^+$ is separable. This extension is generated by the roots of the polynomial $\phi_{\mathfrak{m}}(x)$ for any Hayes-module ϕ. We have seen previously that the polynomial $\phi_{\mathfrak{m}}(x)$ has distinct roots, so it is separable. Hence the extension $H_A^+(\lambda)/F$ is separable as well. □

We now note that for any Galois extension K of F, the Galois group $\mathrm{Gal}(K/F)$ has a natural action on $K\{\tau\}$ by acting on the coefficients, and this action respects the algebra structure on $K\{\tau\}$. This action in turn induces an action of $\mathrm{Gal}(K/F)$ on the set of Hayes-modules over K. That is, if ϕ is a rank-one Drinfeld module that is defined over K, the Drinfeld module $\sigma\phi$ obtained by composing the homomorphism $\phi : A \to K\{\tau\}$ with the map $K\{\tau\} \to K\{\tau\}$ induced by $\sigma \in \mathrm{Gal}(K/F)$ is also a rank-one Drinfeld module over K. We have shown that the field H_A^+ generated by the coefficients of any given rank-one Drinfeld module over K contains the coefficients of all rank-one Drinfeld modules, and it follows that the separable extension H_A^+/F is in fact Galois.

Now suppose that $\sigma \in H_A^+(\lambda)/F$. Applying σ gives us a map of A-modules $\sigma : \Lambda_\phi(A) \to \Lambda_{\sigma\phi}(A)$ which is an isomorphism. We obtain an action of σ on $X_{\mathfrak{m}}$ given by $\sigma(\phi, \lambda) = (\sigma\phi, \lambda^\sigma)$.

We now wish to understand the Galois group $\mathrm{Gal}(L/F) = \mathrm{Gal}(H_A^+(\lambda)/F)$. We know that this Galois group acts on the set $X_{\mathfrak{m}}$. Furthermore, this action is free because the field $L = H_A^+(\lambda)$ is generated over F by the coefficients of any given Hayes-module ϕ along with a division value λ (note that, in particular, this implies that $\mathrm{Gal}(L/F)$ is finite). On the other hand, the narrow ray class group $\mathrm{Cl}_{\mathfrak{m}}^+(A)$ also acts on X. We would ultimately like to identify the two groups $\mathrm{Gal}(L/F)$ and $\mathrm{Cl}_{\mathfrak{m}}^+(A)$ with each other. The first step is to show that these two actions commute.

Lemma 4.4.6. *For all $\sigma \in \mathrm{Gal}(L/F)$ and all $\mathfrak{a} \in \mathrm{Cl}^+(A)$, the identity*

$$\sigma(\mathfrak{a} * (\phi, \lambda)) = \mathfrak{a} * (\sigma(\phi, \lambda)) \tag{4.15}$$

holds for all pairs $(\phi, \lambda) \in X_{\mathfrak{m}}$.

Proof. We have two things to show: first, that $\sigma(\mathfrak{a} * \phi) = \mathfrak{a} * \sigma(\phi)$, and secondly, that $(\phi_{\mathfrak{a}}(\lambda))^\sigma = \phi_{\sigma\mathfrak{a}}(\lambda^\sigma)$.

For the first, we must show that for any $b \in A$, we have $(\sigma\phi)_{\mathfrak{a}}(\sigma\phi)_b = ((\mathfrak{a} * \sigma\phi))_b(\sigma\phi)_{\mathfrak{a}}$. By the definition of $\mathfrak{a} * \phi$, we know already that $\phi_{\mathfrak{a}}\phi_b = (\mathfrak{a} * \phi)_b\phi_{\mathfrak{a}}$. Applying σ to both sides yields the desired result.

Likewise, we see that $\sigma(\phi_{\mathfrak{a}}(\lambda)) = (\phi_{\mathfrak{a}}(\lambda))^\sigma = \phi_{\sigma\mathfrak{a}}(\lambda^\sigma)$. □

Hence the action of $\mathrm{Gal}(L/F)$ preserves the structure of $X_{\mathfrak{m}}$ as a principal homogeneous space for $\mathrm{Cl}^+(A)$. It follows from basic facts about principal homogeneous spaces that:

Corollary 4.4.7. *For any $\sigma \in \mathrm{Gal}(L/F)$, there is a unique $\mathfrak{a} = \mathfrak{a}_\sigma \in \mathrm{Cl}_{\mathfrak{m}}^+(A)$ such that $\sigma(\phi, \lambda) = \mathfrak{a} * (\phi, \lambda)$ for all $\phi \in X_{\mathfrak{m}}$. The correspondence $\sigma \mapsto \mathfrak{a}_\sigma$ identifies $\mathrm{Gal}(L/F)$ with a subgroup of $\mathrm{Cl}_{\mathfrak{m}}^+(A)$.*

We now come to the punchline. We have shown that L is a finite extension of F with Galois group $\mathrm{Gal}(L/F)$ contained in $\mathrm{Cl}^+(A)$. We can use class field theory as we have done before to construct a Galois extension of F with Galois group equal to $\mathrm{Cl}^+(A)$. In fact, this extension is exactly the $L_{\mathfrak{mp}}$ defined by the construction (3.22), with Galois group equal to

$$\mathrm{Gal}(L_{\mathfrak{p}m}/F) = \mathbb{A}_F^\times/(F^\times \prod_{v|\mathfrak{m}} \mathbf{U}_{v,\mathfrak{m}} \prod_{v\nmid\mathfrak{mp}} \boldsymbol{\mathcal{O}}_v^\times \times \ker \mathrm{sgn}_\mathfrak{p}) \tag{4.16}$$

and which is a narrow ray class field for A. (We have used here the fact that $\ker \mathrm{sgn}_\mathfrak{p} = U_{\mathfrak{p},1} \cdot \varpi^\mathbb{Z}$.)

As we would hope, these two fields are equal, although we will not prove it here. (The proof, which can be found in [5], involves the reduction theory of Drinfeld modules.) Even better, the correspondence $\mathrm{Gal}(L/F) \to \mathrm{Cl}_\mathfrak{m}^+(A)$ is exactly inverse to the Artin map $\mathrm{Cl}_\mathfrak{m}^+(A) \to \mathrm{Gal}(L_{\mathfrak{mp}}/F)$! We summarize these results in the following theorem, whose proof can be found in Section 7.5 of [5].

Theorem 4.4.8. *The class field* $\mathrm{Gal}(L_{\mathfrak{mp}}/F)$ *defined by* (3.22) *is equal to the field* $H_A^+(\lambda)$ *generated by the coefficients and* $\mathfrak{m}$*-division values of the rank-one Drinfeld modules for* A*. The Artin map* $\sigma : \mathrm{Cl}_\mathfrak{m}^+(A) \to \mathrm{Gal}(L_{\mathfrak{mp}}/F)$ *is given explicitly as follows: for* $\mathfrak{a} \in \mathrm{Cl}_\mathfrak{m}^+(A)$*, the associated Artin element* $\sigma_\mathfrak{a}$ *is the unique element of* $\mathrm{Gal}(L_{\mathfrak{mp}}/F)$ *such that for any* $(\phi, \lambda) \in X_\mathfrak{m}$*,*

$$\sigma_\mathfrak{a}(\phi, \lambda) = \mathfrak{a} * (\phi, \lambda). \tag{4.17}$$

In particular,

$$\lambda^{\sigma_\mathfrak{a}} = \phi_\mathfrak{a}(\lambda). \tag{4.18}$$

Comparing (2.3) and (4.16), we see that the maximal subfield of $L_{\mathfrak{pm}}$ that is unramified at $\mathfrak{p}$ is the ray class field $K_\mathfrak{m}$.

Chapter 5

Application to the Gross-Stark conjecture

5.1 Hayes's construction of a Stark unit

We construct a Stark element $u_{K_\mathfrak{m},\eta}(\mathfrak{b}) \in K_\mathfrak{m}$ for each ideal class $[\mathfrak{b}]$ in $\mathrm{Cl}_\mathfrak{m}(A)$. Ultimately, the unit $u_{K_\mathfrak{m},\eta}(1)$ corresponding to the ideal class of the identity will turn out to satisfy the properties needed of the conjectural Stark unit $u_{K_\mathfrak{m},\eta}$, and the other elements $u_{K_\mathfrak{m},\eta}(\mathfrak{b})$ will be related by $u_{K_\mathfrak{m},\eta}(\mathfrak{b}) = u_{K_\mathfrak{m},\eta}(1)^{\sigma_\mathfrak{b}}$. Let $\mathfrak{b}$ be an ideal of A; the construction below will turn out to depend only upon the class of $\mathfrak{b}$ in $\mathrm{Cl}_\mathfrak{m}(A)$.

By Proposition 4.3.2, we can choose $\xi = \xi_{\mathfrak{b}^{-1}\mathfrak{m}} \in \mathbf{C}_\mathfrak{p}$ such that the Drinfeld module $\phi = \phi^{\xi\mathfrak{b}^{-1}\mathfrak{m}}$ associated to the exponential function $\xi \cdot e_{\mathfrak{b}^{-1}\mathfrak{m}}(\xi^{-1}t) = e_{\xi\mathfrak{b}^{-1}\mathfrak{m}}$ is sgn-normalized. Define

$$\lambda(\mathfrak{b}) = \xi \cdot e_{\mathfrak{b}^{-1}\mathfrak{m}}(1) \tag{5.1}$$

and

$$u_{K_\mathfrak{m},\eta}(\mathfrak{b}) = \lambda(\mathfrak{b})^{\sigma_\eta - N\eta}. \tag{5.2}$$

We note that our choice of ξ is only unique up to multiplication by roots of unity, and so $\lambda(\mathfrak{b})$ is only defined up to roots of unity. The unit $u_{K_\mathfrak{m},\eta}(\mathfrak{b})$ is however well-defined because $\sigma_\eta - N\eta$ annihilates roots of unity.

By construction, the value $\lambda(\mathfrak{b})$ is an $\mathfrak{m}$-torsion value of ϕ, and it follows by Theorem 4.4.8 that $\lambda(\mathfrak{b}) \in L_{\mathfrak{p}\mathfrak{m}}$. We now show that $u_{K_\mathfrak{m},\eta}(\mathfrak{b})$ is an element of $K_\mathfrak{m}$. Since $\mathrm{Gal}(K_\mathfrak{m}/F) \cong \mathrm{Cl}_\mathfrak{m}(A) = I_\mathfrak{m}(A)/P_\mathfrak{m}(A)$, it suffices to show that for any ideal $\mathfrak{a} = (a)$ generated by an element a that is congruent to 1 mod $\mathfrak{f}$, the Artin element $\sigma_\mathfrak{a}$ fixes $u_{K_\mathfrak{m},\eta}$ (note that a need not be totally positive; if a is totally positive, then $\sigma_\mathfrak{a}$ fixes all of $L_{\mathfrak{p}\mathfrak{m}}$). We first describe the action of such an Artin element $\sigma_\mathfrak{a} \in \mathrm{Gal}(L_{\mathfrak{p}\mathfrak{m}}/K)$ on the element $\lambda(\mathfrak{b}) \in \mathrm{Gal}(L_{\mathfrak{p}\mathfrak{m}})$.

Lemma 5.1.1. *For all $\mathfrak{a}$ in the set $P_\mathfrak{m}(\mathfrak{a})$ of principal ideals generated by elements congruent to 1 mod $\mathfrak{m}$, the Artin element $\sigma_\mathfrak{a}$ acts on $\lambda(\mathfrak{b})$ by $\sigma_\mathfrak{a}(\lambda(\mathfrak{b})) = \zeta\lambda(\mathfrak{b})$ for some root of unity $\zeta \in \mu_{\mathbf{K}_\mathfrak{p}}$.*

Proof. Write $\mathfrak{a} = (a)$, where $a \equiv 1 \pmod{\mathfrak{m}}$. By Lemma 4.4.8, we have

$$\sigma_{\mathfrak{a}}(\lambda(\mathfrak{b})) = \phi_{\mathfrak{a}}(\lambda(\mathfrak{b})) = \mu_\phi(a)^{-1}\phi_a(\lambda(\mathfrak{b})).$$

Since $a \equiv 1 \pmod{\mathfrak{m}}$, we have $\phi_a(\lambda(\mathfrak{b})) = \lambda(\mathfrak{b})$, and $\mu_\phi(a)$ is a unit in $\mathbf{K}_{\mathfrak{p}}$ because ϕ is sgn-normalized. □

Corollary 5.1.2. *The unit $u_{K_{\mathfrak{m}},\eta}$ lies in $K_{\mathfrak{m}}$.*

Proof. Combining Lemma 5.1.1 with the fact that $\sigma_\eta - N\eta$ annihilates roots of unity, we see that $u_{K_{\mathfrak{m}},\eta}(\mathfrak{b}) = \lambda(\mathfrak{b})^{\sigma_\eta - N\eta}$ is fixed by the image of $I_{\mathfrak{m}}(\mathfrak{a})$ under the Artin map. The result follows. □

5.2 Proof of Hayes's construction

We first make explicit the action of the Artin map on $u_{K_{\mathfrak{m}}}(\mathfrak{b})$.

Proposition 5.2.1. *For any fractional ideal $\mathfrak{a}$ of A relatively prime to $\mathfrak{m}$, the element $\sigma_{\mathfrak{a}} \in \mathrm{Gal}(K_{\mathfrak{m}}/F)$ acts on $u_{K_{\mathfrak{m}}}(\mathfrak{b})$ by $u_{K_{\mathfrak{m}}}(\mathfrak{b})^{\sigma_{\mathfrak{a}}} = u_{K_{\mathfrak{m}}}(\mathfrak{a}\mathfrak{b})$.*

Proof. By Lemma 4.2.9, the Drinfeld module $\mathfrak{a} * \phi^{\xi\mathfrak{b}^{-1}\mathfrak{m}}$ is the Drinfeld module of the lattice $D\phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}} \cdot \mathfrak{a}^{-1}\xi\mathfrak{b}^{-1}\mathfrak{m}$. If we write

$$\xi' = D\phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}} \cdot \xi,$$

we obtain

$$\mathfrak{a} * \phi^{\xi\mathfrak{b}^{-1}\mathfrak{m}} = \phi^{\xi'\cdot\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{m}}.$$

Because the $*$ action of ideals maps sgn-normalized Drinfeld modules to other sgn-normalized Drinfeld modules, the Drinfeld module $\phi^{\xi'\cdot\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{m}}$ is sgn-normalized. This means that we can let ξ' play the role of $\xi_{\mathfrak{a}\mathfrak{b}}$ in our construction of $u_{K_{\mathfrak{m}}(\mathfrak{a}\mathfrak{b})}$. Doing this, we obtain

$$\lambda(\mathfrak{a}\mathfrak{b}) = \xi' e_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{m}}(1).$$

Now, by definition of $\phi^{\xi\mathfrak{b}^{-1}\mathfrak{m}}$, the entire function $\phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}}(e_{\xi\mathfrak{b}^{-1}\mathfrak{m}}(z)) = \phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}}(\xi e_{\mathfrak{b}^{-1}\mathfrak{m}}(\xi^{-1}z))$ has zeroes at exactly the points of $\xi\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{m}$. It follows by change of variables that

$$\phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}}(\xi e_{\mathfrak{b}^{-1}\mathfrak{m}}(z)) \tag{5.3}$$

has zeroes at exactly the points of $\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{m}$. The same is true of the entire function

$$\xi' e_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{m}}(z), \tag{5.4}$$

hence the two functions agree up to a constant multiple. Also, looking at the coefficients of z, we see that

$$D(\phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}}(\xi e_{\mathfrak{b}^{-1}\mathfrak{m}}(z))) = D(\phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}}) \cdot \xi = \xi'$$

by definition of ξ', and also

$$D(\xi' e_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{m}}(z)) = \xi'.$$

By Lemma 4.1.11 we conclude that the two entire functions in (5.3) and (5.4) are identical. Setting $z = 1$, we obtain

$$\phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}}(\xi e_{\mathfrak{b}^{-1}\mathfrak{m}}(z)) = \xi' e_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{m}}(1). \tag{5.5}$$

The left hand side is

$$\phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}}(\xi e_{\mathfrak{b}^{-1}\mathfrak{m}}(z)) = \phi_{\mathfrak{a}}^{\xi\mathfrak{b}^{-1}\mathfrak{m}}(\lambda(\mathfrak{b})) = \sigma_{\mathfrak{a}}(\lambda(\mathfrak{b}))$$

by Theorem 4.4.8, while the right hand side is $\lambda(\mathfrak{ab})$.

Hence $\sigma_{\mathfrak{a}}(\lambda(\mathfrak{b})) = \lambda(\mathfrak{ab})$. We now apply $N\eta - \sigma_\eta$ and obtain the desired result. □

We are now ready to show that $u_{K_{\mathfrak{m}},\eta}(1)$ is a shifted Stark unit.

Proposition 5.2.2. *The unit $u_{K_{\mathfrak{m}},\eta}(1)$ corresponding to the ideal $1 = (1) = 1 \cdot A$ of A is a unit at all primes of $K_{\mathfrak{m}}$ not dividing $\mathfrak{p}$, and $u_{K_{\mathfrak{m}},\eta}(A) \equiv 1$ mod all primes in $K_{\mathfrak{m}}$ dividing η.*

Proof. For the first part, we first show that $\lambda(1)$ is a unit at primes not dividing $\mathfrak{p}$ or $\mathfrak{m}$. Because $\lambda(1) = \xi e_{\mathfrak{b}^{-1}\mathfrak{m}}(1)$ is an $\mathfrak{m}$-division point of the Drinfeld module $\phi = \phi^{\xi\mathfrak{b}^{-1}\mathfrak{m}}$ associated to $\xi\mathfrak{b}^{-1}\mathfrak{m}$, $\lambda(\mathfrak{b})$ is a root of the polynomial $\phi_{\mathfrak{m}}(x)$. By definition, $\phi_{\mathfrak{m}}(x)$ is monic and has constant term 0, and by Proposition 4.3.3, the coefficients of $\phi_{\mathfrak{m}}(x)$ belong to the integral closure of A in H_A^+. It follows that λ divides the coefficient of t in $\phi_{\mathfrak{m}}(t)$, and this coefficient is the same as the constant coefficient $D\phi_{\mathfrak{m}}$ of the twisted polynomial $\phi_{\mathfrak{m}} \in K\{\tau\}$. By finiteness of the ideal class group, there exists an integer j such that $\mathfrak{m}^j = (m)$ is principal. Then $\phi_{\mathfrak{m}}$ divides $\phi_{(m)} = \mu_\phi(m)\phi_m$. Because ϕ is sgn-normalized, the leading coefficient $\mu_\phi(m)$ is a unit of A, and looking at constant coefficients, we conclude that $D\phi_{\mathfrak{m}}$ divides $D\phi_m$, which is m by definition.

Hence λ divides $D\phi_{\mathfrak{m}}$, which divides m: by definition, the primes dividing m are exactly the primes dividing $\mathfrak{m}$, so λ is a unit at all other primes of A.

We now do the remaining case of primes $\mathfrak{q}$ dividing $\mathfrak{m}$. Let $\mathfrak{q}'$ be a prime dividing $\mathfrak{m}$ other than $\mathfrak{q}$ (we know there must be another one by the assumption that S contains at least two primes other than $\mathfrak{p}$). Also let $\mathfrak{m}' = \mathfrak{m}/\mathfrak{q}'$, so $\mathfrak{m} = \mathfrak{m}'\mathfrak{q}'$, and $\phi_m = \phi_{\mathfrak{q}'}\phi_{\mathfrak{m}'}$. Hence $\phi_{\mathfrak{m}'}(\lambda)$ is a root of $\phi_{\mathfrak{q}'}$, and by the previous argument, $\phi_{\mathfrak{m}'}(\lambda)$ is a unit at primes not dividing $\mathfrak{q}'$, in particular, is a unit at $\mathfrak{q}$. Because λ divides $\phi_{m'}(\lambda(\mathfrak{b})$, the element $\lambda(\mathfrak{b})$ is also a unit at $\mathfrak{q}$, as desired.

It follows that $\lambda(\mathfrak{b})^{\sigma_\eta}$ is also a unit at all primes not dividing $\mathfrak{p}$, and thus that the same is true of $u_{K_{\mathfrak{m}}}(1)_{\mathfrak{P},\eta} = \lambda(1)^{\sigma_\eta - N\eta}$.

The second part is simpler: by definition of the Frobenius element, $\sigma_\eta(\lambda(1)) \equiv \lambda(1)^{N\eta}$ modulo every prime dividing η. We have shown that $\lambda(1)$ is a unit at η, so we may divide through by $\lambda(1)^{N\eta}$ to conclude that u is 1 mod every prime dividing η. □

The above proposition shows that $u_{K_{\mathfrak{m}}}(1)$ satisfies the first and third conditions in Proposition 3.2.3 for a shifted Stark unit. We now verify the most important part of Stark's conjecture, the second condition. First we derive a convenient explicit formula for $u_{K_{\mathfrak{m}}}(\mathfrak{b})$. We use the following notation: for an integral ideal $\mathfrak{a}$ of A, let $\Sigma_N(\mathfrak{a})$ be the set of all elements $z \in \mathfrak{a}^{-1}\mathfrak{f} + 1$ (equivalently, $z \in \mathfrak{a}^{-1}$ and $z \equiv 1 \pmod{\mathfrak{f}}$) such that z is relatively prime to R and $\deg_{\mathfrak{p}} z \leq N$.

Lemma 5.2.3. *For any ideal $\mathfrak{b}$, we have*

$$u_{K_{\mathfrak{m}}}(\mathfrak{b}) = \lim_{N\to\infty} \frac{\prod_{z\in\Sigma_N(\mathfrak{b}\eta)} z}{\prod_{z\in\Sigma_N(\mathfrak{b})} z^{N\eta}} \tag{5.6}$$

Proof. By Theorem 4.4.8, we can write $u_{K_{\mathfrak{m}}}(\mathfrak{b})$ as

$$u_{K_{\mathfrak{m}}}(\mathfrak{b}) = \lambda(\mathfrak{b})^{\sigma_\eta - N\eta} = \frac{\phi_\eta(\lambda(\mathfrak{b}))}{\lambda(\mathfrak{b})^{N\eta}}. \tag{5.7}$$

Now, the roots of ϕ_η are the η-division values of ϕ, which are of the form $\xi e_{\mathfrak{m}\mathfrak{b}^{-1}}(a)$ for $a \in \mathfrak{m}\eta^{-1}\mathfrak{b}^{-1}/\mathfrak{m}\mathfrak{b}^{-1}$, hence

$$\phi_\eta(\lambda(\mathfrak{b})) = \prod_{a\in\mathfrak{m}\eta^{-1}\mathfrak{b}^{-1}/\mathfrak{m}\mathfrak{b}^{-1}} (\lambda - \xi e_{\mathfrak{m}\mathfrak{b}^{-1}}(a)).$$

We can now substitute $\lambda(\mathfrak{b}) = \xi e_{\mathfrak{m}\mathfrak{b}^{-1}}(1)$ into (5.7) Let $\mathcal{S}$ be a complete set of coset representatives for $\mathfrak{m}\eta^{-1}\mathfrak{b}^{-1}/\mathfrak{m}\mathfrak{b}^{-1}$. After substituting in, we cancel the ξ factors and apply additivity of $e_{\mathfrak{m}\mathfrak{b}}^{-1}$ to rewrite $u_{K_{\mathfrak{m}}}(\mathfrak{b})$ as

$$\begin{aligned} u_{K_{\mathfrak{m}}}(\mathfrak{b}) = \lambda(\mathfrak{b})^{\sigma_\eta - N\eta} &= \frac{\prod_{a\in\mathfrak{m}\eta^{-1}\mathfrak{b}^{-1}/\mathfrak{m}\mathfrak{b}^{-1}} (\xi e_{\mathfrak{m}\mathfrak{b}^{-1}}(1) - \xi e_{\mathfrak{m}\mathfrak{b}^{-1}}(a))}{\xi(e_{\mathfrak{m}\mathfrak{b}^{-1}}(1))^{N\eta}} \\ &= \frac{\displaystyle\prod_{a\in\mathfrak{m}\eta^{-1}\mathfrak{b}^{-1}/\mathfrak{m}\mathfrak{b}^{-1}} (e_{\mathfrak{m}\mathfrak{b}^{-1}}(1-a))}{e_{\mathfrak{m}\mathfrak{b}^{-1}}(1)^{N\eta}} \\ &= \prod_{x\in\mathfrak{m}\mathfrak{b}^{-1}} \prod_{a\in\mathcal{S}} \frac{1-\frac{1-a}{x}}{1-\frac{1}{x}} \\ &= \prod_{x\in\mathfrak{m}\mathfrak{b}^{-1}} \prod_{a\in\mathcal{S}} \frac{1+a-x}{1-x} \\ &= \lim_{N\to\infty} \prod_{\substack{x\in\mathfrak{m}\mathfrak{b}^{-1} \\ \deg_{\mathfrak{p}} x\le N}} \prod_{a\in\mathcal{S}} \frac{1+a+x}{1+x}, \end{aligned} \tag{5.8}$$

where in the last step we have replaced x by $-x$ in our sum. We now break up our product into its numerator and denominator. As x runs through $\mathfrak{m}\mathfrak{b}^{-1}$ and a runs through a complete set of coset representatives for $\mathfrak{m}\eta^{-1}\mathfrak{b}^{-1}/\mathfrak{m}\mathfrak{b}^{-1}$, $a+x$ runs through $\mathfrak{m}\eta^{-1}\mathfrak{b}^{-1}$. Also, because the set of elements of degree $\le N$ is closed under addition, x and $a+x$ each have degree $\le N$ if and only if x has degree $\le N$, provided that N is larger than the largest degree of any element $a \in S$. In the denominator, every value of x appears $|\mathcal{S}| = N\eta$ times, so it can be written as an $N\eta$th power. Hence we can break up our limit for $u_{K_{\mathfrak{m}}}(\mathfrak{b})$ and rewrite it by making the substitution $z = 1 + a + x$ on top and $z = 1 + x$ on bottom:

$$u_{K_\mathfrak{m}}(\mathfrak{b}) = \lim_{N\to\infty} \frac{\displaystyle\prod_{\substack{a+x \in \mathfrak{m}\eta^{-1}\mathfrak{b}^{-1} \\ \deg_\mathfrak{p} x \le N}} (1+a+x)}{\displaystyle\prod_{\substack{x \in \mathfrak{m}\mathfrak{b}^{-1} \\ \deg_\mathfrak{p} x \le N}} (1+x)^{N\eta}}$$

$$= \lim_{N\to\infty} \frac{\displaystyle\prod_{\substack{z \equiv 1 \pmod{\mathfrak{m}\eta^{-1}\mathfrak{b}^{-1}} \\ \deg_\mathfrak{p} z \le N}} z}{\displaystyle\prod_{\substack{z \equiv 1 \pmod{\mathfrak{m}\mathfrak{b}^{-1}} \\ \deg_\mathfrak{p} z \le N}} z^{N\eta}} \tag{5.9}$$

$$= \lim_{N\to\infty} \frac{\displaystyle\prod_{z \in \Sigma_N(\eta\mathfrak{b})} z}{\displaystyle\prod_{z \in \Sigma_N(\mathfrak{b})} z^{N\eta}},$$

as desired. ☐

Lemma 5.2.4. *The $\mathfrak{p}$-adic absolute value of $u_{K_\mathfrak{m}}(\mathfrak{b})$ satisfies*

$$\log |u_{K_\mathfrak{m}}(\mathfrak{b})|_\mathfrak{p} = -\zeta'_{S,\eta}(K/F, \sigma_\mathfrak{b}, 0). \tag{5.10}$$

Proof. By Lemma 5.2.3, Equation (5.10) is equivalent to

$$(d_\mathfrak{p} \log q) v_\mathfrak{p}(u_{K_\mathfrak{m}}(\mathfrak{b})) = \zeta'_{S,\eta}(K_\mathfrak{m}/F, \sigma_\mathfrak{b}, 0). \tag{5.11}$$

We first work on the zeta function side and differentiate term-by-term to obtain the derivative:

$$\zeta'_{S,\eta}(K_\mathfrak{m}/F, \sigma_\mathfrak{b}, s) = -\sum_{\substack{(\mathfrak{a},R)=1 \\ \sigma_\mathfrak{a} = \sigma_{\mathfrak{b}\eta}}} \log(N\mathfrak{a}) N\mathfrak{a}^{-s} - N\eta^{1-s} \sum_{\substack{(\mathfrak{a},R)=1 \\ \sigma_\mathfrak{a} = \sigma_\mathfrak{b}}} \log(N\mathfrak{a}\eta) N\mathfrak{a}^{-s}. \tag{5.12}$$

In the first sum, we have $\sigma_\mathfrak{a} = \sigma_\mathfrak{b}\eta$ exactly when $\mathfrak{a} = z\mathfrak{b}\eta$ for some $z \in (\mathfrak{b}\eta)^{-1}$ that is 1 (mod m), by definition of $\mathrm{Cl}_\mathfrak{m}(A)$. Since the ring A has no units other than constants, such a z will be unique, and we can change variables to z in the first sum. Likewise, we can do a similar change of variables in the second sum:

$$\begin{aligned}\zeta'_{S,\eta}(K_{\mathfrak{m}}/F,\sigma_{\mathfrak{b}},s) = N(\mathfrak{b}\eta)^{-s}\Bigg(&- \sum_{\substack{z\in\mathfrak{b}^{-1}\eta^{-1}\\ z\equiv 1 \pmod m}} (\log Nz + \log N\mathfrak{b}\eta)Nz^{-s} \\ &+ N\eta - \sum_{\substack{z\in\mathfrak{b}^{-1}\\ z\equiv 1 \pmod m}} (\log Nz + \log N\mathfrak{b}\eta)Nz^{-s}\Bigg) \\ = d_{\mathfrak{p}}\log q\Bigg(&\sum_{\substack{z\in\mathfrak{b}^{-1}\eta^{-1}\\ z\equiv 1 \pmod m}} v_{\mathfrak{p}}(z)q^{-d_{\mathfrak{p}}v_{\mathfrak{p}}(z)s} - N\eta \sum_{\substack{z\in\mathfrak{b}^{-1}\\ z\equiv 1 \pmod m}} v_{\mathfrak{p}}(z)q^{-d_{\mathfrak{p}}v_{\mathfrak{p}}(z)s}\Bigg) \\ &+ \log(N\mathfrak{b}\eta)\Bigg(\sum_{\substack{z\in\mathfrak{b}^{-1}\eta^{-1}\\ z\equiv 1 \pmod m}} Nz^{-s} - N\eta \sum_{\substack{z\in\mathfrak{b}^{-1}\\ z\equiv 1 \pmod m}} Nz^{-s}\Bigg).\end{aligned} \tag{5.13}$$

Now, the last term in parentheses is exactly $\zeta_{S,\eta}(K_{\mathfrak{m}}/F,\sigma_{\mathfrak{b}},s)$. The first term, however, is a finite Dirichlet series by Corollary 3.6.3, so we can cut off the sum at some point, and only consider the terms with $v_{\mathfrak{p}}(z)\le N$, for N taken to be sufficiently large. The sums become sums over $\Sigma_N(\mathfrak{b}\eta)$ and $\Sigma_N(\mathfrak{b})$. We conclude that

$$\begin{aligned}\zeta'_{S,\eta}(K_{\mathfrak{m}}/F,\sigma_{\mathfrak{b}},s) = N(\mathfrak{b}\eta)^{-s}d_{\mathfrak{p}}\log q\left(\sum_{z\in\Sigma_N(\mathfrak{b}\eta)} v_{\mathfrak{p}}(z)q^{-d_{\mathfrak{p}}v_{\mathfrak{p}}(z)s} - N\eta\sum_{z\in\Sigma_N(\mathfrak{b})} v_{\mathfrak{p}}(z)q^{-d_{\mathfrak{p}}v_{\mathfrak{p}}(z)s}\right) \\ + \log(N\mathfrak{b}\eta)\zeta_{S,\eta}(K_{\mathfrak{m}}/F,\sigma_{\mathfrak{b}},0)\end{aligned}$$

for sufficiently large N. Now, let $s=0$: by (3.2), the second term vanishes, and we are left with

$$d_{\mathfrak{p}}\log q\left(\sum_{z\in\Sigma_N(\mathfrak{b}\eta)} v_{\mathfrak{p}}(z) - N\eta\sum_{z\in\Sigma_N(\mathfrak{b})} v_{\mathfrak{p}}(z)\right) = (d_{\mathfrak{p}}\log q)v_{\mathfrak{p}}\left(\frac{\prod_{z\in\Sigma_N(\mathfrak{b})} z}{\prod_{z\in\Sigma_N(\mathfrak{b}\eta)} z^N\eta}\right)$$

for all sufficiently large N. Now, letting $N\to\infty$, we find that

$$\zeta'_{S,\eta}(K_{\mathfrak{m}}/F,\sigma_{\mathfrak{b}},s) = (d_{\mathfrak{p}}\log q)u_{K_{\mathfrak{m}}}(\mathfrak{b}),$$

as desired. ∎

We conclude that

Theorem 5.2.5 (Hayes). *The element $u_{K_{\mathfrak{m}},\eta}(1)\in K_{\mathfrak{m}}$ is a Stark unit $u_{K_{\mathfrak{m}},\eta}$ for the extension $K_{\mathfrak{m}}/F$.*

Proof. We showed in Proposition 5.2.2 than $u_{K_{\mathfrak{m}},\eta}(1)$ satisfies the first and third conditions for a shifted Stark unit. We now establish the second one. By surjectivity of the Artin map, any $\sigma \in \mathrm{Gal}(K_{\mathfrak{m}}/F)$ can be written as $\sigma = \sigma_{\mathfrak{b}}$ for some $\mathfrak{b} \in \mathrm{Cl}_{\mathfrak{m}}(A)$. By Lemma 5.2.1, $u_{K,\eta}(1)^{\sigma_{\mathfrak{b}}} = u_{K,\eta}(\mathfrak{b})$, and the desired result follows from Lemma 5.2.4. $\square$

Finally, we show that our shifted Stark unit $u_{K_{\mathfrak{m}}}(1)$ does in fact agree with Gross's conjecture.

Proposition 5.2.6. *The Stark unit $u_{K_{\mathfrak{m}}}(1)$ satisfies Gross's conjecture 3.3.1, equivalently, we have:*

$$u_{K_{\mathfrak{m}}}(\mathfrak{b}) = \prod_{x \in (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^m\mathcal{O}_{\mathfrak{p}})^\times} x^{\zeta_{S,\eta}(L_{\mathfrak{m}\mathfrak{p}^m}/F, \sigma_{\mathfrak{b}} \operatorname{rec}(x)^{-1}, 0)} \text{ in } \mathbf{K}_{\mathfrak{p}}^\times/\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}} \tag{5.14}$$

Proof. By Proposition 5.2.3, it suffices to show that

$$\lim_{N\to\infty} \frac{\prod_{z\in\Sigma_N(\mathfrak{b}\eta)} z}{(\prod_{z\in\Sigma_N(\mathfrak{b})} z)^{N\eta}} = \prod_{x \in (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^m\mathcal{O}_{\mathfrak{p}})^\times} x^{\zeta_{S,\eta}(L_{\mathfrak{m}\mathfrak{p}^m}/F, \sigma_{\mathfrak{b}} \operatorname{rec}(x)^{-1}, 0)} \text{ in } \mathbf{K}_{\mathfrak{p}}^\times/\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}}. \tag{5.15}$$

We know that the the limit on the left hand side exists, and the quotient $\mathbf{K}_{\mathfrak{p}}^\times/\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}}$ is discrete, so we have

$$\lim_{N\to\infty} \frac{\prod_{z\in\Sigma_N(\mathfrak{b}\eta)} z}{(\prod_{z\in\Sigma_N(\mathfrak{b})} z)^{N\eta}} = \frac{\prod_{z\in\Sigma_N(\mathfrak{b}\eta)} z}{(\prod_{z\in\Sigma_N(\mathfrak{b})} z)^{N\eta}} \text{ in } \mathbf{K}_{\mathfrak{p}}^\times/\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}}. \tag{5.16}$$

for sufficiently large N. We now break up this finite product according to the class of z in the quotient $\mathbf{K}_{\mathfrak{p}}^\times/\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}}$ to obtain:

$$\prod_{[x]\in\mathbf{K}_{\mathfrak{p}}^\times/\mathbf{U}_{\mathfrak{p},m}\cdot\varpi^{\mathbb{Z}}} \frac{\prod_{z\in\Sigma_N(\mathfrak{b}\eta)\cap[x]} z}{\left(\prod_{z\in\Sigma_N(\mathfrak{b})\cap[x]} z\right)^{N\eta}} = \prod_{[x]\in\mathbf{K}_{\mathfrak{p}}^\times/\mathbf{U}_{\mathfrak{p},m}\cdot\varpi^{\mathbb{Z}}} \frac{\prod_{z\in\Sigma_N(\mathfrak{b}\eta)\cap[x]} x}{\left(\prod_{z\in\Sigma_N(\mathfrak{b})\cap[x]} x\right)^{N\eta}} \tag{5.17}$$

in $\mathbf{K}_{\mathfrak{p}}^\times/\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}}$. We now claim that for any $[x] \in \mathbf{K}_{\mathfrak{p}}^\times/\mathbf{U}_{\mathfrak{p},m} \cdot \varpi^{\mathbb{Z}}$, we have

$$\frac{\prod_{z\in\Sigma_N(\mathfrak{b}\eta)\cap[x]} x}{\left(\prod_{z\in\Sigma_N(\mathfrak{b})\cap[x]} x\right)^{N\eta}} = x^{\zeta_{S,\eta}(L_{\mathfrak{m}\mathfrak{p}^m}/F, \sigma_{\mathfrak{b}} \operatorname{rec}(x)^{-1}, 0)}. \tag{5.18}$$

Indeed, we can use the same techniques as in Corollary 3.6.3 to show the Dirichlet series for $\zeta_{S,\eta}(L_{\mathfrak{m}\mathfrak{p}^m}/F, \sigma_{\mathfrak{b}} \operatorname{rec}(x)^{-1}, s)$ is finite. After truncating and setting $s = 0$, we obtain

$$\zeta_{S,\eta}(L_{\mathfrak{m}\mathfrak{p}^m}/F, \sigma_{\mathfrak{b}} \operatorname{rec}(x)^{-1}, 0) = \#\Sigma_N(\mathfrak{b}\eta) \cap [x] - \#N\eta\Sigma_N(\mathfrak{b}) \cap [x].$$

The desired results follow. $\square$

5.3 Dasgupta's conjecture in function fields

Recall that for some e, we have that $\mathfrak{p}^e$ is a principal ideal (π) of $\mathcal{O}$, where π is totally positive and congruent to 1 mod $\mathfrak{f}$. We have defined $\mathbf{O} = \boldsymbol{\mathcal{O}}_{\mathfrak{p}} - \pi\boldsymbol{\mathcal{O}}_{\mathfrak{p}}$. If $\mathfrak{p}$ is a principal ideal in $\mathcal{O}$ generated by a totally positive element congruent to 1 mod $\mathfrak{f}$, then $\mathbf{O}$ is the same as $\boldsymbol{\mathcal{O}}_{\mathfrak{p}}^{\times}$.

Definition. Define

$$u_H(\mathfrak{b}) = \epsilon(\mathfrak{b}, \mathcal{D}, \pi)\pi^{\zeta_{R,\eta}(H_{\mathfrak{f}}/F,\sigma_{\mathfrak{b}},0)} \times\!\!\!\!\!\!\int_{\mathbf{O}} x \, d\mu(x) \in F_{\mathfrak{p}}^{\times} := H_{\mathfrak{P}}{}^{\times}, \tag{5.19}$$

where $\epsilon(\mathfrak{b}, \mathcal{D}, \pi)$ is given by

$$\epsilon(\mathfrak{b}, \mathcal{D}, \pi) := \prod_{\epsilon \in E_{\mathfrak{f}}} \epsilon^{\nu(\mathfrak{b}, \epsilon\mathcal{D} \cap \pi^{-1}\mathcal{D}, \mathcal{O}_{\mathfrak{p}})}. \tag{5.20}$$

As things stand, our unit $u_H(\mathfrak{b})$ appears to depend upon our choice of Shintani domain $\mathcal{D}$ and of our generator π for $\mathfrak{p}^e$. In fact, it does not, by the same argument used to prove Proposition 3.19 of [3].

Recall from Section 3.6 that we have defined $B(x, r)$ as the $\mathfrak{p}$-adic open ball $x + \mathfrak{p}^r\boldsymbol{\mathcal{O}}_{\mathfrak{p}}$ in $\boldsymbol{\mathcal{O}}_{\mathfrak{p}}$. Also, let $S_N(\mathfrak{b})$ be the set of totally positive $\alpha \in \mathfrak{b}^{-1}\mathfrak{f} + 1$ that are in $\mathbf{O}$, and such that $\iota(\alpha) \in \mathcal{D}$ and $\deg_\infty \alpha \le N$. In the notation of Section 3.6, the set $S_N(\mathfrak{b})$ is the disjoint union $\bigcup_{M \le N} A_N(\mathfrak{b})$

Let T be a set of elements of $F^{\times}$ whose images under ι are coset representatives for the finite group $\iota(F^{\times}) \cap Q/\iota(E_{\mathfrak{p}}(\mathfrak{f}))$. We additionally require that the elements of T lie in the ring A and are all 1 mod $\mathfrak{f}$, which we can do by strong approximation (equivalently, the Chinese remainder theorem) because an element $x \in F^{\times}$ is totally positive with $v_{\infty_i}(x) = v$ if and only if $x \equiv \pi_{\infty_i}^{v} \pmod{\pi_{\infty_i}^{v+1}}$.

This means that any $\alpha \in F^{\times}$ can be written uniquely as $x_\alpha y \beta$, where $x_\alpha \in T$, $y \in E_{\mathfrak{p}}(\mathfrak{f})$ and $\beta \in \ker \iota$. Because $E_{\mathfrak{p}}(\mathfrak{f})$ is generated by π along with the set $E_{\mathfrak{f}} = \{\epsilon \in \mathcal{O}^{\times} \mid \epsilon \equiv 1 \pmod{\mathfrak{f}}\}$, we see that any $\alpha \in F^{\times}$ can be written uniquely as

$$\alpha = x_\alpha \cdot \pi^{d_\alpha} \cdot \epsilon_\alpha \cdot \beta, \tag{5.21}$$

where $\epsilon_\alpha \in E_{\mathfrak{f}}$. We will use the above equation (5.21) as a definition of x_α, d_α, ϵ_α for any $\alpha \in F^{\times}$. We also define an equivalence relation $\sim$ on $F^{\times}$ by $\alpha \sim \beta$ if and only if $x_\alpha = x_\beta$, or, equivalently, if $\alpha \equiv \beta \pmod{E_{\mathfrak{p}}(\mathfrak{f}) \cdot \ker \iota}$.

From this point on, we assume that the absolute value $|\pi|_{\infty_i}$ is the same for all infinite places ∞_i. Because our Shintani domain is the union of simplicial cones, it follows that $\pi\mathcal{D} = \mathcal{D}$, so the domain $\mathcal{D}$ is preserved under multiplication by powers of π. Since $\mathcal{D}$ is a fundamental domain for the multiplicative action of $E_{\mathfrak{f}}$, we can choose our set T such that $\iota(x) \in \mathcal{D}$ for all $x \in T$.

Lemma 5.3.1. *For every α satisfying $\iota(\alpha) \in \mathcal{D}$, the associated unit ϵ_α is 1.*

Proof. First apply ι to both sides of (5.21):

$$\iota(\alpha) = \iota(x_\alpha \cdot \pi^{d_\alpha} \cdot \epsilon_\alpha \cdot \beta) = \iota(x \cdot \pi^{d_\alpha}) \cdot \iota(\epsilon_\alpha).$$

We know that $\iota(x) \in \mathcal{D}$, and by our assumption about π, it follows that $\iota(x \cdot \pi^{d_\alpha}) \in \mathcal{D}$ as well. On the other hand, we also know that $\iota(\alpha) \in \mathcal{D}$. But $\mathcal{D}$ is a fundamental domain for the group $E_\mathfrak{f}$, so $\iota(\alpha)$ and $\iota(x_\alpha \cdot \pi^{d_\alpha})$ can only both be in $\mathcal{D}$ if they are equal. This implies that $\iota(\epsilon_\alpha) = 1$, hence ϵ_α is a unit at all places and is congruent to 1 mod $\mathfrak{f}$, hence must be 1. $\square$

Hence we can rewrite (5.21) without the ϵ term; for any $\alpha \in \iota^{-1}(\mathcal{D})$, there are uniquely determined $x_\alpha \in T$, $\beta \in \ker \iota$, and $d_\alpha \in \mathbb{Z}$ such that

$$\alpha = x_\alpha \cdot \pi^{d_\alpha} \cdot \beta. \tag{5.22}$$

The assumption that $\pi\mathcal{D} = \mathcal{D}$ was crucial to the above result – if we relax that assumption, all our formulas will have additional ϵ terms. These terms are the source of the ϵ correction factor in Theorem 3.7.2.

Recall that we have defined a degree function $\deg_\infty$ with respect to the places on $F^\times$ by

$$\deg_\infty(\alpha) = \log_q N(\alpha\mathcal{O}) = \sum_i d_{\infty_i} v_{\infty_i}(\alpha). \tag{5.23}$$

Note that $\deg_\infty(\beta) = 0$ for $\beta \in \ker \iota$ because $v_{\infty_i}(\beta) = 0$ for each i.

We observe the following convenient fact:

Lemma 5.3.2. *For $\alpha \in F^\times$, the difference $d_\alpha - \frac{\deg_\infty(\alpha)}{\deg_\infty(\pi)}$ depends only on the equivalence class of α under $\sim$.*

Proof. We apply the map $\deg_\infty$ to both sides of (5.22). Since $\deg_\infty(\beta) = 0$, we obtain:

$$\deg_\infty(\alpha) = \deg_\infty(x) + d_\alpha \deg_\infty(\pi). \tag{5.24}$$

Dividing through by $\deg_\infty(\pi)$ and rearranging, we see that $d_\alpha - \frac{\deg_\infty(\alpha)}{\deg_\infty(\pi)}$ depends only on x, which in turn depends only on the equivalence class of α, as desired. $\square$

Lemma 5.3.3. *The following equality holds:*

$$u_H(\mathfrak{b}) = \lim_{N\to\infty} \frac{\prod_{\alpha \in S_N(\mathfrak{b}\eta)} \alpha\pi^{-d_\alpha}}{(\prod_{\alpha \in S_N(\mathfrak{b})} \alpha\pi^{-d_\alpha})^{N\eta}}$$

Proof. We pick a $\mathfrak{p}$-adic uniformizer $\varpi \in \boldsymbol{\mathcal{O}}_\mathfrak{p}$. Our choice of ϖ does not matter, as it will only be used in intermediate calculations to make certain products converge. We have $\varpi\boldsymbol{\mathcal{O}}_\mathfrak{p} = \mathfrak{p}\boldsymbol{\mathcal{O}}_\mathfrak{p}$. Then we can write our domain of integration as $\mathbf{O} = \boldsymbol{\mathcal{O}}_\mathfrak{p} - \pi\boldsymbol{\mathcal{O}}_p = \boldsymbol{\mathcal{O}}_\mathfrak{p} - (\varpi)^e\boldsymbol{\mathcal{O}}_p = \bigcup_{i=0}^{e-1} \varpi^i \boldsymbol{\mathcal{O}}_p^\times$. In other words, any element of $\mathbf{O}$ can be written uniquely as $\varpi^i x$ for i with $0 \le i \le e-1$ and $x \in \boldsymbol{\mathcal{O}}_p^\times$.

We first convert our multiplicative integral to a limit.

$$\times\!\!\!\!\!\!\int_{\mathbf{O}} x\, d\mu_{\mathfrak{b}} = \lim_{r\to\infty} \prod_{i=0}^{e-1} \prod_{x\in(\mathcal{O}/\mathfrak{p}^r)^\times} (\varpi^i x)^{\mu_{\mathfrak{b}}(B(\varpi^i x, i+r))}. \tag{5.25}$$

Now, by Lemma 3.6.2 the product can be rewritten as

$$\prod_{i=0}^{e-1} \prod_{x\in(\mathcal{O}/\mathfrak{p}^r)^\times} (\varpi^i x)^{\mu_{\mathfrak{b}}(B(\varpi^i x, i+r))} = \prod_{i=0}^{e-1} \prod_{x\in(\mathcal{O}/\mathfrak{p}^r)^\times} (\varpi^i x)^{\#(S_N(\mathfrak{b}\eta)\cap B(\varpi^i x, i+r)) - N\eta\cdot\#(S_N(\mathfrak{b})\cap B(\varpi^i x, i+r))}. \tag{5.26}$$

for any $N > N(r)$. Observe that the exponent of ϖ in this product is

$$C_N = \sum_{i=0}^{e-1} i \cdot \left(\#(S_N(\mathfrak{b}\eta)\cap \varpi^i \boldsymbol{\mathcal{O}}_{\mathfrak{p}}^\times) - N\eta \cdot \#(S_N(\mathfrak{b})\cap \varpi^i \boldsymbol{\mathcal{O}}_{\mathfrak{p}}^\times)\right).$$

Each of these terms is a difference of shifted partial zeta values, so the sequence $\{C_N\}$ eventually becomes constant by Corollary 3.6.3. Let C be that constant value, so that $C_N = C$ for N sufficiently large. We can now set the ϖ factors aside for the moment while handling our limits. This means that all our remaining factors are $\mathfrak{p}$-adic units.

For any $\alpha \in B(\varpi^i x, i+r)$, $\varpi^{-i}\alpha$ is a $\mathfrak{p}$-adic unit, and is congruent to x mod $\mathfrak{p}^r$. We can use this to deduce the following congruence

$$\begin{aligned}
\prod_{i=0}^{e-1} \prod_{x\in(\mathcal{O}/\mathfrak{p}^r)^\times} x^{\#(S_N(\mathfrak{b})\cap B(\varpi^i x, i+r))} &= \prod_{i=0}^{e-1} \prod_{x\in(\mathcal{O}/\mathfrak{p}^r)^\times} \prod_{\alpha\in(S_N(\mathfrak{b})\cap B(\varpi^i x, i+r))} x \\
&\equiv \prod_{i=0}^{e-1} \prod_{x\in(\mathcal{O}/\mathfrak{p}^r)^\times} \prod_{\alpha\in(S_N(\mathfrak{b})\cap B(\varpi^i x, i+r))} \varpi^{-i}\alpha \\
&= \prod_{i=0}^{e-1} \prod_{\alpha\in S_N(\mathfrak{b})\cap\varpi^i\boldsymbol{\mathcal{O}}_p^\times} \varpi^{-i}\alpha \pmod{\mathfrak{p}^r}
\end{aligned} \tag{5.27}$$

since every $\alpha \in S_N(\mathfrak{b})\cap\varpi^i\boldsymbol{\mathcal{O}}_{\mathfrak{p}}^\times$ belongs to exactly one of the congruence classes $B(\varpi^i x, i+r)$.

We now use (5.27) twice in the expression of (5.26), noting that all the ϖ factors cancel out to obtain

$$\prod_{i=0}^{e-1} \prod_{x\in(\mathcal{O}/\mathfrak{p}^r)} (\varpi x)^{\mu_{\mathfrak{b}}(B(\varpi^i x, i+r))} \equiv \frac{\prod_{\alpha\in S_N(\mathfrak{b}\eta)}\alpha}{\left(\prod_{\alpha\in S_N(\mathfrak{b})}\alpha\right)^{N\eta}} \pmod{\mathfrak{p}^{r+C}}. \tag{5.28}$$

Since this is true for all $N \geq N(r)$, it follows also that

$$\prod_{x\in(\mathcal{O}/\mathfrak{p}^r)} x^{\mu_{\mathfrak{b}}(B(x,r))} \equiv \lim_{N\to\infty} \frac{\prod_{\alpha\in S_N(\mathfrak{b}\eta)}\alpha}{\left(\prod_{\alpha\in S_N(\mathfrak{b})}\alpha\right)^{N\eta}} \pmod{\mathfrak{p}^{r+C}}. \tag{5.29}$$

This is true for all r, so we in fact have an equality:

$$\lim_{r\to\infty} \prod_{x\in(\mathcal{O}/\mathfrak{p}^r)} x^{\mu_{\mathfrak{b}}(B(x,r))} = \frac{\prod_{\alpha\in S_N(\mathfrak{b}\eta)} \alpha}{\left(\prod_{\alpha\in S_N(\mathfrak{b})} \alpha\right)^{N\eta}}. \tag{5.30}$$

Now we rewrite the $\pi^{\zeta_{R,\eta}(H_{\mathfrak{f}}/F,\sigma_{\mathfrak{b}},0)}$ term as a limit. We first write out the nonshifted zeta value $\zeta_{R,\eta}(H_{\mathfrak{f}}/F,\sigma_{\mathfrak{b}},0)$ as a sum over ideals of $\mathcal{O}$. Because any ideal $\mathfrak{a}$ such that $\mathfrak{a}\sim\mathfrak{b}$ belongs to the same ideal class as $\mathfrak{b}$, we can then apply the change of variables $\mathfrak{a}=\alpha\mathfrak{b}$, where α is well-defined modulo units:

$$\zeta_R(H_{\mathfrak{f}}/F,\sigma_{\mathfrak{b}},s) = \sum_{\substack{\mathfrak{a}\subset\mathcal{O}\\ (\mathfrak{a},R)=0\\ \sigma_{\mathfrak{a}}=\sigma_{\mathfrak{b}}\text{ on }H_{\mathfrak{f}}}} \frac{1}{N\mathfrak{a}^s} = \frac{1}{N\mathfrak{b}^s}\sum_{\substack{\alpha\in\mathfrak{b}^{-1}/E_{\mathfrak{f}}^{\times}\\ \alpha\gg0\\ \alpha\equiv1 \pmod{\mathfrak{f}}}} \frac{1}{N\alpha^s}. \tag{5.31}$$

Now, any equivalence class in $\mathfrak{b}^{-1}/E_{\mathfrak{f}}^{\times}$ can be represented by an element of the form $\alpha\pi^m$ where $\alpha\in\mathfrak{b}^{-1}\cap\mathbf{O}$ and m is a non-negative integer. Additionally, α is well-defined modulo $E_{\mathfrak{f}}^{\times}$, so we can specify α uniquely by taking the unique choice of α with $\iota(\alpha)\in\mathcal{D}$. This allows us to rewrite (5.31) by applying the formula for the sum of a geometric series, as follows:

$$\zeta_R(H_{\mathfrak{f}}/F,\sigma_{\mathfrak{b}},s) = \frac{1}{1-N\pi^s}\sum_{\substack{\alpha\in\mathfrak{b}^{-1}\cap\mathbf{O}\cap\mathcal{D}\\ \alpha\gg0\\ \alpha\equiv1 \pmod{\mathfrak{f}}}} \frac{1}{N\alpha^s}. \tag{5.32}$$

We now reintroduce the shifting to get a formula for $\zeta_{R,\eta}$:

$$\zeta_{R,\eta}(H_{\mathfrak{f}}/F,\sigma_{\mathfrak{b}},s) = \frac{1}{1-N\pi^s}\left(\sum_{\substack{\alpha\in\mathfrak{b}^{-1}\eta^{-1}\cap\mathbf{O}\cap\mathcal{D}\\ \alpha\gg0\\ \alpha\equiv1 \pmod{\mathfrak{f}}}} \frac{1}{N\alpha^s} - N\eta^{1-s}\cdot\sum_{\substack{\alpha\in\mathfrak{b}^{-1}\cap\mathbf{O}\cap\mathcal{D}\\ \alpha\gg0\\ \alpha\equiv1 \pmod{\mathfrak{f}}}} \frac{1}{N\alpha^s}\right). \tag{5.33}$$

By the argument of Lemma 3.6.3, this is a finite Dirichlet series in s, and for large enough N it is the same as

$$\frac{1}{N\mathfrak{b}^s}\frac{1}{1-N\pi^s}\left(\sum_{\alpha\in S_N(\mathfrak{b}\eta)}\frac{1}{N\alpha^s} - N\eta^{1-s}\cdot\sum_{\alpha\in S_N(\mathfrak{b})}\frac{1}{N\alpha^s}\right) \tag{5.34}$$

We wish to evaluate (5.34) at $s=0$ to obtain $\zeta_{R,\eta}(H_{\mathfrak{f}}/F,\sigma\mathfrak{b},s)$. Since the denominator $1-N\pi^s$ is 0 at $s=0$, we apply L'Hôpital's rule. The $\frac{1}{N\mathfrak{b}^s}$ doesn't make a difference, as it is 1 at $s=0$. Also $\frac{d}{ds}(1-N\pi^s)|_{s=0} = (-\log(N\pi)(N\pi)^s)|_{s=0} = -e\deg_\infty(\pi)$. We differentiate the expression in parentheses term-by-term using the fact that $N\alpha = q^{\deg_\infty(\alpha)}$, and evaluating at $s=0$:

$$-\sum_{\alpha\in S_N(\mathfrak{b}\eta)}\log(N\alpha)+N\eta\cdot\sum_{\alpha\in S_N(\mathfrak{b})}\log(N\alpha) = \sum_{\alpha\in S_N(\mathfrak{b}\eta)}\deg_\infty(\alpha)\log q - N\eta\cdot\sum_{\alpha\in S_N(\mathfrak{b})}\deg_\infty(\alpha)\log q. \tag{5.35}$$

We can now apply L'Hôpital to get:

$$\zeta_{R,\eta}(H_{\mathfrak{f}}/F, \sigma\mathfrak{b}, s) = \sum_{\alpha \in S_N(\mathfrak{b}\eta)} \frac{\deg_\infty(\alpha)}{\deg_\infty(\pi)} - N\eta \cdot \sum_{\alpha \in S_N(\mathfrak{b})} \frac{\deg_\infty(\alpha)}{\deg_\infty(\pi)}. \tag{5.36}$$

By Lemma 5.3.2, $\frac{\deg_\infty(\alpha)}{\deg_\infty(\pi)} - d_\alpha$ depends only on the equivalence class of α with respect to $\sim$. Additionally, we claim that, for a given equivalence class $[\beta]$, we have

$$\#\{\alpha \in S_N(\beta\eta) \mid \alpha \sim \beta\} - N\eta \cdot \#\{\alpha \in S_N(\beta\eta) \mid \alpha \sim \beta\} = 0.$$

for all sufficiently large N. First, by the argument of Propositon 3.6.3, this sum is finite, and is equal to the value of the series

$$\sum_{N=0}^{\infty} \left(\#\{\alpha \in A_N(\beta\eta) \mid \alpha \sim \beta\} q^{-Ns} - N\eta \cdot \#\{\alpha \in A_N(\beta\eta) \mid \alpha \sim \beta\} q^{-Ns}\right)$$

at $s = 0$. However, one can show that this series is equal to $\zeta_S(K_{\mathfrak{m}}, \sigma_x, 0)$, which is 0 by Equation 3.2.

This implies that we can change all the $\frac{\deg_\infty(\alpha)}{\deg_\infty(\pi)}$ terms to d_α without affecting the sum. We now take the limit as $N \to \infty$.

$$\zeta_{R,\eta}(H_{\mathfrak{f}}/F, \sigma\mathfrak{b}, s) = \lim_{N\to\infty} \left(\sum_{\alpha \in S_N(\mathfrak{b}\eta)} d_\alpha - N\eta \cdot \sum_{\alpha \in S_N(\mathfrak{b})} d_\alpha \right). \tag{5.37}$$

Exponentiating, we obtain

$$\pi^{\zeta_{R,\eta}(H_{\mathfrak{f}}/F,\sigma\mathfrak{b},s)} = \pi^{\lim_{N\to\infty}\left(\sum_{\alpha\in S_N(\mathfrak{b}\eta)} d_\alpha - N\eta\cdot\sum_{\alpha\in S_N(\mathfrak{b})} d_\alpha\right)} \tag{5.38}$$

Multiplying equations (5.30) and (5.37) yields the desired result.

□

We now justify the change of variables that we will use to convert each term of the product in Lemma 5.3.3 into a product of the form found in Proposition 5.2.3.

Lemma 5.3.4. *For all $x \in T$, and any ideal $\mathfrak{b}$ of $\mathcal{O}$ relatively prime to $\mathfrak{p}m\infty$, there is a one-to-one correspondence between the subset set $\{\alpha \in S_N(\mathfrak{b})$ of elements α such that $x_\alpha = x$ (x_α is defined as in* (5.22)*), and the set $\Sigma_N(x\mathfrak{b})$. This correspondence sends the element α of $S_N(\mathfrak{b})$ to the element $\beta = \alpha x^{-1}\pi^{-d_\alpha}$ of $\Sigma_N(\mathfrak{b})$, where d_α is defined as in* (5.22)*.*

Proof. If we make the change of variables $\beta = \alpha x^{-1}\pi^{-d_\alpha}$, as in equation (5.21), we know that $\beta \in \ker\iota$, which means that β is a unit at all places at infinity, and that β is totally positive. Since we already know that $\alpha \in \mathfrak{b}^{-1}\eta^{-1}\mathcal{O}$, the fact that $\beta = \alpha\pi^{-d_\alpha}x^{-1}$ is a unit at all places at infinity implies that β actually lies in in $x^{-1}\eta^{-1}\mathfrak{b}^{-1}A$, where A is the ring of elements that are integral away from $\mathfrak{p}$. Since β is a unit at all infinite places, the statement that β is totally positive just means that β is 1 mod each infinite place ∞_i, i.e. β is 1 mod $\infty = \infty_1 \cdots \infty_n$. Also, $\beta \equiv 1 \pmod{\mathfrak{f}}$, because all other terms in the product are 1 mod $\mathfrak{f}$, so in fact $\beta \equiv 1 \pmod{\mathfrak{m}}$, where $\mathfrak{m} = \mathfrak{f}\infty$.

We now exhibit the inverse map. For any $\beta \in \Sigma_N(x\mathfrak{b})$, there is a unique d_β such that $\beta\pi^{d_\beta} \in \mathbf{O}$. Since multiplying by a power of π only adds poles at infinity and removes the pole at p, and multiplying by units in $E_{\mathfrak{f}}$ only adds and removes poles at infinity, it follows that $\beta\pi^{d_\beta}\epsilon_\beta$ belongs to the ideal $x^{-1}\eta^{-1}\mathfrak{b}^{-1}$ of $\mathcal{O}$. Make the change of variables $\alpha = x\beta\pi^{d_\beta}$: then $\alpha \in \eta^{-1}\mathfrak{b}^{-1}$. Running the arguments of the previous paragraph in reverse shows that α is 1 mod $\mathfrak{f}$ and $\alpha \sim x$. Furthermore $\iota(\alpha) = \iota(x\beta\pi^{d_\beta}) = \iota(x\pi^{d_\beta})$ lies in $\mathcal{D}$ because $x \in \mathcal{D}$ and $\pi^{d\beta}\mathcal{D} = \mathcal{D}$. Finally, this map is an inverse to the map of the previous paragraph because π^{d_β} is uniquely determined by β. Hence we have our desired bijection.

□

Lemma 5.3.5. *For $x \in T$, we have*

$$u_{K_{\mathfrak{m}}}(x\mathfrak{b}) = \lim_{N\to\infty} \frac{\prod_{\substack{\alpha\in S_N(\mathfrak{b}\eta)\\ \alpha\sim x}} \alpha\pi^{-d_\alpha}\epsilon_\alpha^{-1}}{(\prod_{\substack{\alpha\in S_N(\mathfrak{b})\\ \alpha\sim x}} \alpha\pi^{-d_\alpha}\epsilon_\alpha^{-1})^{N\eta}}$$

Proof. We use the change of variables in Lemma 5.3.4 to change the right hand side from a product over $\alpha \in S_N(\mathfrak{b}\eta)$ to a product over $\beta \in \Sigma_N(\mathfrak{b}\eta A)$. By definition of β, $\alpha\pi^{-d\alpha}\epsilon_\alpha^{-1} = x\beta$, so

$$\lim_{N\to\infty} \frac{\prod_{\substack{\alpha\in S_N(\mathfrak{b}\eta)\\ \alpha\sim x}} \alpha\pi^{-d_\alpha}\epsilon_\alpha^{-1}}{(\prod_{\substack{\alpha\in S_N(\mathfrak{b})\\ \alpha\sim x}} \alpha\pi^{-d_\alpha}\epsilon_\alpha^{-1})^{N\eta}} = \lim_{N\to\infty} \frac{\prod_{\beta\in\Sigma_N(\mathfrak{b}\eta A)} x\beta}{(\prod_{\beta\in\Sigma_N(\mathfrak{b}A)} x\beta)^{N\eta}}. \tag{5.39}$$

The exponent of x here can be seen to equal $\zeta_S(K_{\mathfrak{m}}, \sigma_x, 0)$, which is zero by (3.2), so we are left with exactly the formula for $u_{K_{\mathfrak{m}}}(x\mathfrak{b})$ given in Lemma 5.2.3.

□

Proposition 5.3.6. *The element $u_H(\mathfrak{b})$ can be written in terms of our previously constructed Stark units as follows:*

$$u_H(\mathfrak{b}) = \prod_{x\in T} u_{K_{\mathfrak{m}}}(x\mathfrak{b}).$$

Proof. This follows by taking the product of Lemma 5.3.5 over all $x \in T$ and applying Lemma 5.3.3. □

We are now in a position to prove our function field analogue of Dasgupta's refinement of Gross's conjecture.

Proof of Theorem 3.7.1. We recall that the elements of T were chosen so that their images under ι would be a complete set of coset representatives for the quotient group $(\iota(F^\times) \cap Q)/\iota(E_{\mathfrak{p}}(\mathfrak{f}))$, which is canonically isomorphic to $\mathrm{Gal}(K_{\mathfrak{m}}/H)$. We now apply Theorem 4.4.8

to the formula of Theorem 5.3.6, and obtain

$$
\begin{aligned}
u_H(\mathfrak{b}) = \prod_{x\in T} u_{K_\mathfrak{m}}(x\mathfrak{b}) &= \prod_{x\in T} u_{K_\mathfrak{m}}(\mathfrak{b})^{\sigma_x} \\
&= \prod_{\sigma\in \mathrm{Gal}(K_\mathfrak{m}/H)} u_{K_\mathfrak{m}}(\mathfrak{b})^{\sigma} = N_{K_\mathfrak{m}/H}(u^{\sigma}_{K_\mathfrak{m}(\mathfrak{b})}).
\end{aligned}
\tag{5.40}
$$

$\square$

Since $u_{K_\mathfrak{m}}(1)$ is a shifted Stark unit for $K_\mathfrak{m}$, it follows from Proposition 3.2.4 that $u_H(1) = N_{K_\mathfrak{m}/H}(u^{\sigma}_{K_\mathfrak{m}(\mathfrak{b})})$ is a shifted Stark unit for H, as desired.

Bibliography

[1] Jörg Bewersdorff. *Galois theory for beginners*, volume 35 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2006. A historical perspective, Translated from the second German (2004) edition by David Kramer.

[2] Henri Darmon and Samit Dasgupta. Elliptic units for real quadratic fields. *Ann. of Math. (2)*, 163(1):301–346, 2006.

[3] Samit Dasgupta. Shintani zeta-functions and Gross-Stark units for totally real fields. *Duke Math J., to appear.*

[4] Pierre Deligne and Kenneth A. Ribet. Values of abelian L-functions at negative integers over totally real fields. *Invent. Math.*, 59(3):227–286, 1980.

[5] David Goss. *Basic structures of function field arithmetic.* Springer-Verlag, Berlin, 1996.

[6] Benedict H. Gross. On the values of abelian L-functions at $s = 0$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 35(1):177–197, 1988.

[7] Helmut Hasse. History of class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 266–279. Thompson, Washington, D.C., 1967.

[8] David R. Hayes. Stickelberger elements in function fields. *Compositio Math.*, 55(2):209–239, 1985.

[9] David R. Hayes. The refined $\mathfrak{p}$-adic abelian Stark conjecture in function fields. *Invent. Math.*, 94(3):505–527, 1988.

[10] David R. Hayes. A brief introduction to Drinfel′d modules. In *The arithmetic of function fields (Columbus, OH, 1991)*, volume 2 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 1–32. de Gruyter, Berlin, 1992.

[11] Takuro Shintani. On evaluation of zeta functions of totally real algebraic number fields at non-positive integers. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 23(2):393–417, 1976.

[12] Kaloyan Slavov. Gross-Stark units for totally real number fields. *Senior thesis, Harvard University*, 2007.

[13] John Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, volume 47 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Lecture notes edited by Dominique Bernardi and Norbert Schappacher.

[14] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.