Joost Michielsen

L-functions of the projective line

Master Thesis, defended on December 9, 2010

Thesis advisor: prof.dr. H.W. Lenstra

Mathematisch Instituut, Universiteit Leiden

Contents

CHAPTER 1

Introduction

1. Arithmetic in $k[X]$

Just as in $\mathbf{Z}$, there are several problems in $k[X]$ with k a finite field that are much easier to formulate than to prove. One of them is the following theorem.

Theorem 1.1.1. *Let k be a field with q elements, let $f \in k[X]_{\neq 0}$ and let $n \in \mathbf{Z}_{>0}$. Then $(k[X]/fk[X])^*$ is generated by the set of residue classes of the monic irreducible polynomials of degree n coprime to f if $n \geq 2\log_q(\deg f + 4)$.*

A proof of this theorem will be given in Chapter 4 of this thesis.

Theorem 1.1.1 has an analogue in $\mathbf{Z}$. Let $n \in \mathbf{Z}_{>0}$ and assume the extended Riemann hypothesis (see the next section). Then $(\mathbf{Z}/n\mathbf{Z})^*$ is generated by the set of residue classes of the numbers coprime to n that are smaller than $2(\log n)^2$. A proof of this theorem can be found in [**1**].

Another theorem to be proved in this thesis has a well known analogue in $\mathbf{Z}$. Dirichlet's theorem on primes in arithmetic progressions states that for all $a, b \in \mathbf{Z}_{>0}$ such that $(a, b) = 1$ the set of primes p such that $p \equiv a \mod b$ is infinite. A stronger statement tells that if $\pi_{a,b}(x)$ is the number of primes p smaller than x such that $p \equiv a \mod b$, then

$$\lim_{x\to\infty} \frac{\pi_{a,b}(x)\log x}{x} = \frac{1}{\phi(b)}$$

where $\phi(b) = \#(\mathbf{Z}/b\mathbf{Z})^*$. This is called the prime number theorem on arithmetic progressions, see [**3**], Theorem 4, p. 315.

If we replace $\mathbf{Z}_{>0}$ by the set of monic polynomials in $k[X]$ with k a finite field there is no 'exact' analogue for Dirichlet's theorem since there is no clear ordering on $k[X]$ like there is on $\mathbf{Z}_{>0}$. So in this case we look, for all $a, f \in k[X]_{\neq 0}$ such that $(a, f) = 1$, at the set of all monic irreducible polynomials $g \in k[X]$ of degree n such that $g \equiv a \mod f$. In fact we can even do more. The set we are going to estimate is the following.

Definition 1.1.2. Let $a, f \in k[X]_{\neq 0}$ be such that $(a, f) = 1$, let $b = (b_1, \ldots, b_{c-1})$ be an element of k^{c-1} for $c \in \mathbf{Z}_{>0}$. Then we define $S_n(a, f, b, c)$ be the set of monic irreducible polynomials g of degree n such that $g \equiv a \mod f$ and g has coefficient b_i at X^{n-i} for $0 < i < c$.

Now the analogue of Dirichlet's theorem on primes in arithmetic progressions is as follows.

Theorem 1.1.3. *Let $a, f \in k[X]_{\neq 0}$ be such that $(a, f) = 1$, let b be an element of k^{c-1} for $c \in \mathbf{Z}_{>0}$ and let $n \in \mathbf{Z}_{>0}$. Then*

$$\left| \#S_n(a, f, b, c) - \frac{q^{n-c+1}}{n\Phi(f)} \right| \leq \frac{\max\{\frac{q}{q-1}, \deg f + c - \frac{q-2}{q-1}\} q^{n/2}}{n}.$$

where $\Phi(f) = \#(k[X]/fk[X])^*$.

The only 'ugly' thing about this theorem is the maximum taken on the right side on the equation, but this is only relevant if $\deg f = 0$ and $c = 1$. The similarity with the $\mathbf{Z}$-case is obvious from the following two corollaries.

Corollary 1.1.4. *We have*

$$\lim_{n \to \infty} \#S_n(a, f, b, c) = \infty$$

and

$$\lim_{n \to \infty} \frac{\#S_n(a, f, b, c)}{\#S_n(1, 1, (), 1)} = \frac{1}{\Phi(f) q^{c-1}}.$$

A proof of the special case of Corollary 1.1.4 where $c = 1$ can also be found in [**4**]. In [**4**] one can also find a version of the special case of Theorem 1.1.3 where $c = 1$. The author did not bother to calculate explicit bounds like in Theorem 1.1.3 though. As far as I know, nobody has ever done this, nor has anybody ever considered the cases where $c > 1$.

The main ingredient of the proof of these theorems is the fact that the absolute value of each zero of each L-function of the projective line over k (see Definition 2.1.7 in the next chapter) is either 1 or $\frac{1}{\sqrt{q}}$. The complete theorem is formulated in Theorem 2.1.10. A sketch of the proof can be found in [**5**]. The sketch given in [**5**] is very brief and its only reference, namely Appendix V of [**9**], is not easy to read. So it seemed a nice task to work through the proof of this theorem and write down a detailed proof.

2. Riemann hypotheses

The proof of Theorem 2.1.10 is a consequence of the so called "Riemann hypothesis for function fields". In this section I will give a sketch of various Riemann hypotheses and how they are related.

One of the main open problems in mathematics is the Riemann hypothesis. This hypothesis states properties about a certain complex valued function $\zeta(s)$, the so called zeta function. It is defined as follows. One can show that the function $\sum_{n=1}^{\infty} n^{-s}$ is analytic on the set $\{s \in \mathbf{C} : \operatorname{Re} s > 1\}$. Then it can be shown that this function has a unique analytic continuation to $\mathbf{C} \setminus \{1\}$, in this way we obtain $\zeta(s)$. The Riemann hypothesis states that all zeros of ζ in the region $\{s \in \mathbf{C} : 0 < \operatorname{Re} s < 1\}$ satisfy $\operatorname{Re} s = \frac{1}{2}$.

One of the generalizations of the Riemann hypothesis, called the extended Riemann hypothesis, is the following. Let χ be a character of $\mathbf{Z}$, that is a map $\chi : \mathbf{Z}_{>0} \to \mathbf{C}$ for which there exists $n \in \mathbf{Z}_{>0}$ and a group homomorphism $\chi' : (\mathbf{Z}/n\mathbf{Z})^* \to \mathbf{C}^*$ with the property that $\chi(a) = \chi'(a \mod n)$ for all $a \in \mathbf{Z}_{>0}$ with $\gcd(a, n) = 1$ and $\chi_1(a) = 0$ for all $a \in \mathbf{Z}_{>0}$ with $\gcd(a, n) \neq 1$. Now one can show that $\sum_{n=1}^{\infty} \chi(n) n^{-s}$ is analytic on the set $\{s \in \mathbf{C} : \operatorname{Re} s > 1\}$ and can be uniquely continued to an analytic function on $\mathbf{C} \setminus \{1\}$. This function is often denoted by $L(s, \chi)$. The extended Riemann hypothesis states that all zeros of $L(s, \chi)$ in the region $\{s \in \mathbf{C} : 0 < \operatorname{Re} s < 1\}$ satisfy $\operatorname{Re} s = \frac{1}{2}$. The statement of the extended Riemann hypothesis implies the Riemann hypothesis since we can take χ to be the map that sends all elements of $\mathbf{Z}_{\geq 0}$ to 1.

Another generalization of the Riemann hypothesis, called the generalized Riemann hypothesis, is as follows. Let K be a number field and let $\mathcal{I}$ be the set of nonzero ideals of $\mathcal{O}_K$, the ring of integers of K. Let $N_{K/\mathbf{Q}} : \mathcal{I} \to \mathbf{Z}_{>0}$ be the norm function of the ideals. Then it can be shown that $\sum_{I \in \mathcal{I}} (N_{K/\mathbf{Q}}(I))^{-s}$ is analytic on the set $\{s \in \mathbf{C} : \operatorname{Re} s > 1\}$ and can be uniquely continued to an analytic function on $\mathbf{C} \setminus \{1\}$. This function is often denoted by $\zeta_K(s)$. The generalized Riemann hypothesis states that all zeros of $\zeta_K(s)$ in the region $\{s \in \mathbf{C} : 0 < \operatorname{Re} s < 1\}$ satisfy $\operatorname{Re} s = \frac{1}{2}$. The statement of the generalized Riemann hypothesis implies the extended Riemann hypothesis, but not trivially. In fact the proof of this is similar to what is done in chapter 3 of this thesis, in the number field case it is just a little bit more complicated since one needs to worry about convergence.

All these conjectures have analogues in $k[X]$ where k is a field with q elements. In this case the zeta-functions are always functions in q^{-s}. So it is convenient to do the substitution $q^{-s} = T$. The statement of the zeros having real part $\frac{1}{2}$ then changes into the zeros having absolute value $\frac{1}{\sqrt{q}}$. The analogue of the extended Riemann hypothesis is the main theorem of this thesis. In section 1 of chapter 2 we give an explicit version. The classical Riemann hypothesis should then be the case were the character is trivial. In the case of the classical Riemann hypothesis the analogue is not too interesting though. It merely states that all the zeros of the rational function $\frac{1}{(1-T)(1-qT)} \in \mathbf{C}(T)$ have absolute value $\frac{1}{\sqrt{q}}$, which is obvious since this function does not have any zeros. Why this is analogous to the classical Riemann hypothesis follows from the generalized version.

The analogue of the generalized Riemann hypothesis is the theorem people usually mean when they speak of the Riemann hypothesis for function fields (which is no hypothesis at all, since it was proved by Weil in 1948). A proper definition in terms of ideles is given in Chapter 2. Chapter 3 is devoted to proving why the Riemann hypothesis for function fields implies our main theorem by means of class field theory.

CHAPTER 2

L-functions

1. L-functions of the projective line

Just as we can define Dirichlet characters on $\mathbf{Z}_{>0}$, we can define characters on the set of monic polynomials of $k[X]$ (denoted by $k[X]_{\mathrm{monic}}$) where k is a finite field. For convenience we generalize this definition a bit.

Definition 2.1.1. Let k be a finite field. Let $\chi_1 : k[X] \to \mathbf{C}$ be a map for which there exists a nonzero polynomial $f \in k[X]_{\mathrm{monic}}$ and a group homomorphism $\chi_1' : (k[X]/fk[X])^* \to \mathbf{C}^*$ with the property that $\chi_1(h) = \chi_1'(h \mod f)$ for all $h \in k[X]$ with $\gcd(h, f) = 1$ and $\chi_1(h) = 0$ for all $h \in k[X]$ with $\gcd(h, f) \neq 1$. Let $\chi_\infty : 1 + X^{-1}k[[X^{-1}]] \to \mathbf{C}^*$ be a group homomorphism such that there is $c \in \mathbf{Z}_{>0}$ with $1 + X^{-c}k[[X^{-1}]] \subset \ker \chi_\infty$. A *character* of $k[X]$ is a map $\chi : k[X]_{\mathrm{monic}} \to \mathbf{C}$ defined by $\chi(h) = \chi_1(h)\chi_\infty(X^{-\deg h}h)$.

Lemma 2.1.2. *Let χ be a character of $k[X]$. Then the pair (χ_1, χ_∞) is uniquely determined by χ.*

Proof. Let $\chi = (\chi_1, \chi_\infty)$ and let $f \in k[X]_{\mathrm{monic}}$ and $c \in \mathbf{Z}_{>0}$ be as in Definition 2.1.1. Let $\psi = (\psi_1, \psi_\infty)$ with corresponding monic polynomial g. Now suppose $\chi = \psi$ and take $h \in k[X]_{\mathrm{monic}}$ arbitrary. Then there exists $d \in \mathbf{Z}_{>0}$ such that $1 + X^{-d}k[[X^{-1}]] \subset \ker \chi_\infty$ and $1 + X^{-d}k[[X^{-1}]] \subset \ker \psi_\infty$. Moreover, there is $j \in k[X]$ such that

$$X^{-\deg(h+jfg)}(h + jgf) \in 1 + X^{-d}k[[X^{-1}]].$$

Hence we have

$$\chi_\infty(X^{-\deg(h+jfg)}(h + jgf)) = \psi_\infty(X^{-\deg(h+jfg)}(h + jgf)) = 1.$$

So we have $\chi(h+jgf) = \chi_1(h+jfg) = \chi_1(h)$ and $\psi(h+jgf) = \psi_1(h+jfg) = \psi_1(h)$. Since we assumed that $\chi = \psi$ this shows that $\chi_1 = \psi_1$. Then it immediately follows that $\chi_\infty = \psi_\infty$, hence (χ_1, χ_∞) is uniquely determined by χ. □

It follows immediately that for any character χ and for any $h_1, h_2 \in k[X]$ we have $\chi(h_1h_2) = \chi(h_1)\chi(h_2)$. Now we will give some more useful definitions.

Definition 2.1.3. Let $\chi = (\chi_1, \chi_\infty)$ be a character. If $\operatorname{im} \chi \subset \{0, 1\}$ we call χ *principal*. With a monic polynomial f that comes from χ_1 and a $c \in \mathbf{Z}_{>0}$ that comes from χ_∞ we define a pair (f, c) to be a *modulus* of χ. We denote the set of characters with modulus (f, c) by $\mathcal{X}(f, c)$.

Note that $\mathcal{X}(f, c)$ is a group by pointwise multiplication. Next we are going to define the notion of a primitive character. The following lemma is useful.

Lemma 2.1.4. *Let $f \in k[X]_{\mathrm{monic}}$ and let $c \in \mathbf{Z}_{>0}$. Write $f = \prod_i p_i^{n_i}$ with all p_i monic irreducible such that $p_i \neq p_j$ if $i \neq j$ and all $n_i > 0$. Then for any character*

$\chi = (\chi_1, \chi_\infty)$ with modulus (f, c) there are characters $(\chi_{p_i^{n_i}}, 1) \in \mathcal{X}(p_i^{n_i}, 1)$ such that $\chi = (\prod_i \chi_{p_i^{n_i}}, \chi_\infty)$. We have an isomorphism

$$\begin{aligned} \mathcal{X}(f,c) &\xrightarrow{\sim} \prod_i \mathcal{X}(p_i^{n_i},1) \times \mathcal{X}(1,c) \\ \chi &\longmapsto ((\chi_{p_i^{n_i}})_i, \chi_\infty) \end{aligned}$$

Proof. Use the Chinese remainder theorem and Lemma 2.1.2. □

Let $f \in k[X]_{\text{monic}}$. Let $f = \prod_i p_i^{n_i}$ with all p_i monic irreducible such that $p_i \neq p_j$ if $i \neq j$ and all $n_i > 0$ be the prime factorization of f. Then for each p_i and m_i such that $0 \leq m_i \leq n_i$ we have an injective map

$$\mathrm{Hom}((k[X]/p_i^{m_i} \cdot k[X])^*, \mathbf{C}^*) \longrightarrow \mathrm{Hom}((k[X]/p_i^{n_i} \cdot k[X])^*, \mathbf{C}^*),$$

so we have an injective map (which is an inclusion if $m_i > 0$)

$$\pi_{p_i,m_i,n_i} : \mathcal{X}(p_i^{m_i}, 1) \longrightarrow \mathcal{X}(p_i^{n_i}, 1).$$

Let $c \in \mathbf{Z}_{>0}$. Then for each d such that $1 \leq d \leq c$ we have an injective map

$$\begin{gathered} \mathrm{Hom}((1 + X^{-1}k[[X^{-1}]])/(1 + X^{-d}k[[X^{-1}]]), \mathbf{C}^*) \longrightarrow \\ \mathrm{Hom}((1 + X^{-1}k[[X^{-1}]])/(1 + X^{-c}k[[X^{-1}]]), \mathbf{C}^*), \end{gathered}$$

so we get an inclusion

$$\mathcal{X}(1, d) \longrightarrow \mathcal{X}(1, c).$$

Definition 2.1.5. Let $\chi = (\chi_1, \chi_\infty)$ be a character with modulus (f, c). Let $f = \prod_i p_i^{n_i}$ with all p_i monic irreducible be the prime factorization of f. Write χ_1 like $\prod_i \chi_{p_i^{n_i}}$ like in Lemma 2.1.4. Let π_{p_i,m_i,n_i} be as above. We say that a character $\psi = (\psi_1, \psi_\infty)$ *induces* χ if the following two conditions are met.

- There are $m_i \in \mathbf{Z}_{\geq 0}$ and maps $(\chi_{p_i^{m_i}}, 1) \in \mathcal{X}(p_i^{m_i}, 1)$ such that $\psi_1 = \prod_i \chi_{p_i^{m_i}}$ and for all i we have $\pi_{p_i,m_i,n_i}(\chi_{p_i^{m_i}}, 1) = (\chi_{p_i^{n_i}}, 1)$.
- We have $\psi_\infty = \chi_\infty$.

We call χ *primitive* if χ is only induced by itself. Let g be the polynomial $\prod_i p_i^{k_i}$ where each $k_i \in \mathbf{Z}_{\geq 0}$ is the smallest number such that there exists $(\chi_{p_i^{k_i}}, 1) \in \mathcal{X}(p_i^{k_i}, 1)$ with $\pi_{p_i,k_i,n_i}(\chi_{p_i^{k_i}}, 1) = (\chi_{p_i^{n_i}}, 1)$. Let $d \in \mathbf{Z}_{>0}$ be the smallest number such that $(1, \chi_\infty) \in \mathcal{X}(1, d)$. We define the *conductor* of χ to be the pair (g, δ) where $\delta = d$ if $\chi_1|_{k^*}$ or χ_∞ is nontrivial and $\delta = 0$ otherwise.

Proposition 2.1.6. *Each character χ with modulus (f, c) is induced by a unique primitive character ψ with modulus the conductor of χ. For each $h \in k[X]$ with $(h, f) = 1$ we have $\chi(h) = \psi(h)$.*

Proof. Obvious from the construction. □

To these characters we can associate L-functions.

Definition 2.1.7. The L-function $L(T, \chi)$ associated to a character χ of $k[X]$ is defined by the formal power series

$$L(T, \chi) = \sum_h \chi(h) T^{\deg h} \in \mathbf{C}[[T]]$$

where the sum is taken over the monic polynomials h in $k[X]$.

Each L-function satisfies an Euler product.

Proposition 2.1.8. *We have*

$$L(T,\chi) = \prod_h \frac{1}{1-\chi(h)T^{\deg h}}$$

where the product is taken over the monic irreducible polynomials h in $k[X]$.

Proof. Standard. □

Proposition 2.1.9. *Let ψ be the primitive character with conductor (g,δ) that induces χ. Then we have*

$$L(T,\chi) = L(T,\psi)\cdot \prod_{h\in k[X]} (1-\psi(h)T^{\deg h})$$

where h ranges over all monic irreducible factors h of f that do not divide g.

Proof. Compare the factors of $L(T,\chi)$ and $L(T,\psi)$ in the Euler product. □

The following theorem is the main theorem of the thesis.

Theorem 2.1.10. *Let $\chi = (\chi_1,\chi_\infty)$ be a character on $k[X]$ with modulus (f,c), where k has q elements. Let (g,δ) be the conductor of χ. Then:*

i. *If χ is principal, then*

$$L(T,\chi) = \frac{1}{1-qT}\cdot\prod_h (1-T^{\deg h})$$

where h ranges over all monic irreducible factors of f.

ii. *If χ is not principal then there are $\alpha_1,\dots,\alpha_m\in\mathbf{C}$, where $m=\deg g-2+\delta$, such that $|\alpha_i|=\sqrt{q}$ for $1\le i\le m$ and such that*

$$L(T,\chi) = \prod_{i=1}^m (1-\alpha_i T)\cdot(1-T)^{\max\{0,1-\delta\}}\cdot\prod_h (1-\chi(h)T^{\deg h})$$

where h ranges over all monic irreducible factors of f that do not divide g.

The first part of the theorem is very easy. If $\chi=(\chi_1,1)$ is principal with modulus (f,c) then χ is induced by the primitive character $\psi=(1,1)$ which has conductor $(1,0)$. We see that

$$L(T,\psi) = \sum_h T^{\deg h} = \sum_{n=1}^\infty (qT)^n = \frac{1}{1-qT}$$

where h ranges over the monic polynomials of $k[X]$, since there are exactly q^d monic polynomials of degree d. Now we use Proposition 2.1.9 to see

$$L(T,\chi) = L(T,\psi)\cdot\prod_h (1-\psi(h)T^{\deg h}) = \frac{1}{1-qT}\prod_h (1-T^{\deg h})$$

where h ranges over the monic irreducible factors of f. This proves the first part of Theorem 2.1.10.

The second part of Theorem 2.1.10 is significantly more difficult. The proof will be given at the end of Chapter 3.

Now we will calculate a couple of examples to give evidence for this theorem.

Example 2.1.11. Let $k = \mathbf{F}_2$. Let $\chi = (\chi_1, \chi_\infty)$ be a character with modulus $f = X^3+X+1$ where $\chi_1 : k[X] \to \mathbf{C}$ maps X to ζ_7, where ζ_7 is a primitive seventh root of unity and χ_∞ is the trivial map. We are going to calculate $L(T,\chi)$. First we note that $L(T,\chi)$ will be a polynomial of degree at most 2 by 2.1.10 ($\deg g = 3$ and $\delta = 0$), so we only need to calculate $\chi(g)$ where g is a polynomial of degree 0, 1, or 2. We have

$$L(T,\chi) = \sum_{h \in k[X]_{\text{monic}}} \chi(h) T^{\deg h} = 1 + s_1 T + s_2 T^2.$$

So we need to calculate s_1 and s_2. Let α a zero of f. We see that $\alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1, \alpha^7 = 1$, in this way we have expressed all polynomials of degree less than 3 in terms of powers of α. So we see that $\chi_1(X) = \zeta_7, \chi_1(X+1) = \zeta_7^3$, so $s_1 = \zeta_7 + \zeta_7^3$. We have $\chi_1(X^2) = \zeta_7^2, \chi_1(X^2+1) = \zeta_7^6, \chi_1(X^2+X) = \zeta_7^4, \chi_1(X^2+X+1) = \zeta_7^5$, so $s_2 = \zeta_7^2 + \zeta_7^6 + \zeta_7^4 + \zeta_7^5$. Hence we have

$$L(T,\chi) = 1 + (\zeta_7 + \zeta_7^3)T + (\zeta_7^2 + \zeta_7^6 + \zeta_7^4 + \zeta_7^5)T^2.$$

We immediately see that 1 is a zero of $L(T,\chi)$, since $\sum_{i=1}^6 \zeta_7^i = -1$. Now we can find the other zero by dividing out $1-T$. We see:

$$L(t,\chi) = (1-T)(1-(\zeta_7^2 + \zeta_7^6 + \zeta_7^4 + \zeta_7^5)T).$$

We see that $\zeta_7^2 + \zeta_7^6 + \zeta_7^4 + \zeta_7^5 = -(1+\zeta_7+\zeta_7^3)$. Since we only want to determine an absolute value, it is sufficient to calculate $|1+\zeta_7+\zeta_7^3|^2$. We have

$$|1+\zeta_7+\zeta_7^3|^2 = (1+\zeta_7+\zeta_7^3)\overline{(1+\zeta_7+\zeta_7^3)} = (1+\zeta_7+\zeta_7^3)(1+\zeta_7^6+\zeta_7^4) = 2 + \sum_{i=0}^{6} \zeta_7^i = 2.$$

This shows that $|1+\zeta_7+\zeta_7^3| = \sqrt{2}$, hence the theorem has been confirmed.

Example 2.1.12. Let $k = \mathbf{F}_3 = \{0,1,-1\}$. Let $\chi = (\chi_1, \chi_\infty)$ be a character with modulus $f = X$ such that χ_1 is the map that sends -1 to -1 and 1 to 1 and χ_∞ is the map that sends $1+X^{-1}$ to ζ_3, where ζ_3 is a primitive third root of unity, and maps $1+X^{-2}k[[X^{-1}]]$ to 1. We see that $g=1$ and $\delta = 2$. By Theorem 2.1.10 we know that $L(T,\chi)$ has degree 1. So we see that

$$L(T,\chi) = 1 + (\zeta_3 - \zeta_3^2)T.$$

Since $\zeta_3 - \zeta_3^2 = \sqrt{-3}$ we have $|\zeta_3 - \zeta_3^2| = \sqrt{3}$, which again confirms the theorem.

2. Ideles

First we recall some important definitions and theorems about valuations.

Definition 2.2.1. Let K be a field. A *valuation ring* of K is a subring $\mathcal{O} \subsetneq K$ such that for all $x \in K^*$ one has $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. If in addition $K^*/\mathcal{O}^* \cong \mathbf{Z}$ we call $\mathcal{O}$ a *discrete valuation ring.* A *place* $\mathfrak{p}$ of K is a maximal ideal of a valuation ring $\mathcal{O} \subset K$.

Theorem 2.2.2. *Any valuation ring is a local ring. If a valuation ring is discrete its place is a principal ideal.*

PROOF. Let $\mathcal{O}$ be a valuation ring. Then it is easy to check that $\mathcal{O} \setminus \mathcal{O}^*$ is an ideal of $\mathcal{O}$, so $\mathcal{O}$ is a local ring. If $K^*/\mathcal{O}^* \cong \mathbf{Z}$, take $x \in K^*$ that is mapped to 1. If $x \in \mathcal{O}$, then x generates the ideal $\mathcal{O} \setminus \mathcal{O}^*$, otherwise x^{-1} generates $\mathcal{O} \setminus \mathcal{O}^*$. □

Definition 2.2.3. If $\mathfrak{p}$ is a place of K, then its valuation ring is denoted by $\mathcal{O}_\mathfrak{p}$.

Theorem 2.2.4. *Let K be a finite extension of $k(X)$, where k is a finite field, let $\mathfrak{p}$ be a place of K and let $\mathcal{O}_\mathfrak{p}$ be its valuation ring. Then $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring. We have a group homomorphism*

$$\begin{array}{rrl} |\cdot|_\mathfrak{p}: & K \longrightarrow & \mathbf{R} \\ & x \longmapsto & \left\{ \begin{array}{cr} (\#\mathcal{O}_\mathfrak{p}/x\mathcal{O}_\mathfrak{p})^{-1} & \text{if } x \in \mathcal{O} \setminus \{0\} \\ \#\mathcal{O}_\mathfrak{p}/x^{-1}\mathcal{O}_\mathfrak{p} & \text{if } x \in K^* \setminus \mathcal{O} \\ 0 & \text{if } x = 0 \end{array} \right. \end{array}$$

such that $(x, y) \mapsto |x - y|_\mathfrak{p}$ defines a metric on K.

PROOF. See [**8**], Theorem I.1.6, p. 3 and Note 2, p. 4. □

Note that in this case k is contained in any valuation ring of K, since if $x \in k^*$ then x^{-1} is a power of x, because k is finite. This justifies the following definition.

Definition 2.2.5. The *degree* of a place $\mathfrak{p} \subset K$, denoted by $\deg \mathfrak{p}$, is the degree of the extension $k \to \mathcal{O}/\mathfrak{p}$. We define the function $\mathrm{ord}_\mathfrak{p} : K^* \to \mathbf{Z}$ to be $\mathrm{ord}_\mathfrak{p}(x) = -\log_{\#(O_\mathfrak{p}/\mathfrak{p})}(|x|_\mathfrak{p})$. By $K_\mathfrak{p}$ we denote the completion of K with respect to $|\cdot|_\mathfrak{p}$.

Theorem 2.2.6. *Let K be a finite extension of $k(X)$, where k is a finite field. Then $K_\mathfrak{p}$ is a topological field which is complete with respect to $|\cdot|_\mathfrak{p}$. Let t be an element that generates $\mathfrak{p}$ and let $R_\mathfrak{p}$ be a set of representatives of $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ in $\mathcal{O}_\mathfrak{p}$ containing 0. Then every element in $K_\mathfrak{p}^*$ has a unique representation $\sum_{i=n}^\infty a_i t^i$ where $n \in \mathbf{Z}$ and $a_i \in R_\mathfrak{p}$ with $a_n \neq 0$.*

PROOF. See [**8**], Theorem IV.2.6, p. 143. □

Definition 2.2.7. We make the unit group $K_\mathfrak{p}^*$ into a topological group by giving it the induced topology of $K_\mathfrak{p}$. The subset of $K_\mathfrak{p}$ given by $\{x \in K_\mathfrak{p} : |x|_\mathfrak{p} \leq 1\}$ is a subring, which we denote by $A_\mathfrak{p}$.

Example 2.2.8. Consider the case $K = k(X)$. Then the valuation rings of K are the rings $\{\frac{a}{b} \in k(X) : \mathrm{ord}_f(a) \geq \mathrm{ord}_f(b)\}$ where $f \in k[X]$ is an irreducible polynomial, of which a place corresponds to the maximal ideal generated by f, and the ring $\{\frac{a}{b} \in k(X) : \deg a \leq \deg b\}$, of which the place is the maximal ideal generated by X^{-1} (which is also called the place at infinity, denoted by ∞). If $\mathfrak{f}$ is the place corresponding to an irreducible polynomial $f \in k[X]$ and R_f is a set of representatives of $k[X]/fk[X]$ in $k[X]$, then $K_\mathfrak{f} = \{\sum_{i=-n}^\infty a_i f^i : n \in \mathbf{Z}, a_i \in R_f\}$ and $A_\mathfrak{f} = \{\sum_{i=0}^\infty a_i f^i : a_i \in R_f\}$. In the case of the place ∞ we have $k(X)_\infty = k((X^{-1}))$ and $A_\infty = k[[X^{-1}]]$.

Definition 2.2.9. Let K be a finite field extension of $k(X)$, where k is a finite field. The *adele ring* of K, denoted by $\mathbf{A}_K$, is defined by

$$\prod_\mathfrak{p}{}' K_\mathfrak{p} = \{(x_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} K_\mathfrak{p} : x_\mathfrak{p} \in A_\mathfrak{p} \text{ for all but finitely many } \mathfrak{p}\}.$$

We put a topology on $\mathbf{A}_K$ by taking the sets $\prod_{\mathfrak{p} \in P} O_\mathfrak{p} \times \prod_{\mathfrak{p} \notin P} A_\mathfrak{p}$ as a base for the open subsets where P is a finite set of places of K and $O_\mathfrak{p}$ is an open subset of $K_\mathfrak{p}$

for all $\mathfrak{p} \in P$. This makes $\mathbf{A}_K$ into a topological ring. Now $\mathbf{A}_K^*$ can be described as follows:

$$\mathbf{A}_K^* = \prod_{\mathfrak{p}}{}' K_{\mathfrak{p}}^* = \{(x_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} K_{\mathfrak{p}}^* : x_{\mathfrak{p}} \in A_{\mathfrak{p}}^* \text{ for all but finitely many } \mathfrak{p}\}.$$

The topology on $\mathbf{A}_K^*$ is obtained by a classical trick: we give $\mathbf{A}_K \times \mathbf{A}_K$ the product topology and we consider the embedding $\mathbf{A}_K^* \subset \mathbf{A}_K \times \mathbf{A}_K$ given by $x \mapsto (x, x^{-1})$. Then we give the image of $\mathbf{A}_K^*$ the relative topology from $\mathbf{A}_K \times \mathbf{A}_K$, which makes it into a topological group. We call $\mathbf{A}_K^*$ the *idele group* of K.

Proposition 2.2.10. *The topology on $\mathbf{A}_K^*$ is generated by the open subsets $\prod_{\mathfrak{p} \in P} O_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin P} A_{\mathfrak{p}}^*$ where P is a finite set of places of K and $O_{\mathfrak{p}}$ is an open subset of $K_{\mathfrak{p}}^*$ for each $\mathfrak{p} \in P$.*

Proof. Denote by $\mathcal{S}$ the topology mentioned in the second part of Definition 2.2.9 and denote by $\mathcal{T}$ the topology mentioned in the proposition. Take a set of the form $\prod_{\mathfrak{p} \in P} O_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin P} A_{\mathfrak{p}}^* \in \mathcal{T}$ where P is a finite set of places of K and $O_{\mathfrak{p}}$ is an open subset of $K_{\mathfrak{p}}^*$. Note that for all places $\mathfrak{p}$ the set $O_{\mathfrak{p}}$ is open in $K_{\mathfrak{p}}^*$ if and only if $O_{\mathfrak{p}}$ is an open subset of $K_{\mathfrak{p}}$. Also, the map $x \mapsto x^{-1}$ is continuous on $K_{\mathfrak{p}}$ and hence on $\mathbf{A}_K^*$ with topology $\mathcal{T}$. This shows that the map $\mathcal{T} \to \mathcal{S}$ given by $X \mapsto (\{(x, x^{-1}) : x \in X\})$ is a bijection, which we wanted to prove. □

Proposition 2.2.11. *For any $x \in K^*$ the element $(x)_{\mathfrak{p}}$ is an element of $\prod_{\mathfrak{p}} A_{\mathfrak{p}}^*$.*

Proof. It is sufficient to show that any element $x \in K^*$ is only contained in finitely many places of K. In the case that $K = k(X)$, use example 2.2.8. For the general case, see [**8**], Corollary I.3.4, p. 14. □

So the diagonal embedding $K \to \mathbf{A}_K$ makes $\mathbf{A}_K$ into a K-algebra.

Definition 2.2.12. We define $\mathbf{A}_{K,1}^*$ to be $\{(x_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbf{A}_K^* : \sum_{\mathfrak{p}} (\deg \mathfrak{p}) \operatorname{ord}_{\mathfrak{p}} x_{\mathfrak{p}} = 0\}$.

Proposition 2.2.13. *The map $\mathbf{A}_K^* \to \mathbf{Z}$ given by $(x_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \sum_{\mathfrak{p}} (\deg \mathfrak{p}) \operatorname{ord}_{\mathfrak{p}} x_{\mathfrak{p}}$ is a continuous group homomorphism with kernel $\mathbf{A}_{K,1}^*$.*

Proof. By definition of $\mathbf{A}_K^*$ the map is well defined. To show continuity it suffices to show that $\mathbf{A}_{K,1}^*$ is open in $\mathbf{A}_K^*$. Clearly $\mathbf{A}_{K,1}^*$ contains $\prod_{\mathfrak{p}} A_{\mathfrak{p}}^*$, which is open in $\mathbf{A}_K^*$. Since $\mathbf{A}_{K,1}^* = \bigcup_{x \in \mathbf{A}_{K,1}^*} x \prod_{\mathfrak{p}} A_{\mathfrak{p}}^*$ it follows that $\mathbf{A}_{K,1}^*$ is also open in $\mathbf{A}_K^*$. □

Remark 2.2.14. One might ask whether the map from Proposition 2.2.13 is surjective. If we choose an algebraic closure $\bar{K}$ of K and let $\bar{k}$ be the algebraic closure of k in $\bar{K}$, then the map has image $n\mathbf{Z}$ where $n = [K \cap \bar{k} : k]$. So the map is surjective if and only if $K \cap \bar{k} = k$. See [**8**], Corollary V.1.11, p. 164.

Definition 2.2.15. The diagonal embedding $K^* \to \mathbf{A}_K^*$ gives rise to a topological group $\mathbf{A}_K^*/K^*$, the *idele class group* of K, which we denote by C_K. The idele class group gets the quotient topology from $\mathbf{A}_K^*$.

The following theorem is called Artin's product formula.

Theorem 2.2.16. *Let $x \in K^*$. Then $\sum_{\mathfrak{p}} (\deg \mathfrak{p}) \operatorname{ord}_{\mathfrak{p}} x_{\mathfrak{p}} = 0$.*

Proof. In the case that $K = k(X)$, use Example 2.2.8. For the general case, see [**8**], Theorem V.I.I, p. 158 (this is also investigated in the next chapter). □

Now the following definition is justified.

Definition 2.2.17. We define $C_{K,1}$ to be to be $\mathbf{A}_{K,1}/K^*$.

Note that $C_{K,1}$ is open in C_K.

Theorem 2.2.18. *The map $\mathbf{A}_K^* \to \mathbf{Z}$ given by $(x_\mathfrak{p})_\mathfrak{p} \mapsto \sum_\mathfrak{p} (\deg \mathfrak{p}) \operatorname{ord}_\mathfrak{p} x_\mathfrak{p}$ and the induced map $C_K \to \mathbf{Z}$ give rise to exact sequences*

$$1 \longrightarrow \mathbf{A}_{K,1}^* \longrightarrow \mathbf{A}_K^* \longrightarrow \mathbf{Z}$$

and

$$1 \longrightarrow C_{K,1} \longrightarrow C_K \longrightarrow \mathbf{Z}.$$

We have $\mathbf{A}_K^* \cong \mathbf{A}_{K,1}^* \times \mathbf{Z}$ and $C_K \cong C_{K,1} \times \mathbf{Z}$ as topological groups.

Proof. Since the map $\mathbf{A}_K^* \to \mathbf{Z}$ is a non-trivial homomorphism there is $n > 0$ such that we have short exact sequences

$$1 \longrightarrow \mathbf{A}_{K,1}^* \longrightarrow \mathbf{A}_K^* \longrightarrow n\mathbf{Z} \longrightarrow 0$$

and

$$1 \longrightarrow C_{K,1} \longrightarrow C_K \longrightarrow n\mathbf{Z} \longrightarrow 0.$$

Any short exact sequence of abelian groups with $\mathbf{Z}$ on the third position splits. Since $\mathbf{Z}$ has the discrete topology any section is continuous. Hence both sequences also split as sequences of topological abelian groups. □

Generally there are no canonical sections.

3. L-functions of an idele class group

Definition 2.3.1. Let G be a topological group. A *character* on G is a continuous group homomorphism $\omega : G \to \mathbf{C}^*$, where $\mathbf{C}^*$ gets the usual topology. The characters of G form a group which we denote by $\mathcal{X}(G)$.

So a character on $\mathbf{A}_K^*$ is a continuous group homomorphism $\omega : \mathbf{A}_K^* \to \mathbf{C}^*$. The following theorem is completely obvious but nevertheless important.

Theorem 2.3.2. *Let G be a topological group, let N be a normal subgroup of G and let $i : G \to G/N$ be the natural map that induces the quotient topology on G/N. Then the map $\mathcal{X}(G/N) \to \mathcal{X}(G)$ which maps ω to $\omega \circ i$ is injective with image the characters of G that are trivial on N.*

Proof. Obvious. □

So there is an isomorphism between the group of characters of $\mathbf{A}_K^*$ that are trivial on K^* and the group of characters of C_K.

The following lemma enables us to define a conductor of a character of an idele group.

Lemma 2.3.3. *Let G be a topological group and let $\{N_i\}_i$ be a set of open subgroups of G such that for any open neighbourhood V of $1 \in G$ there is i such that $N_i \subset V$. Let $\omega : G \to \mathbf{C}^*$ be a character of G. Then there is j such that $N_j \subset \ker \omega$. If G is compact, then ω has finite image.*

PROOF. Let V be the open neighbourhood of $1 \in \mathbf{C}^*$ given by $\{x \in \mathbf{C} : 0 < \operatorname{Re} x < 2\}$. Then the only subgroup of $\mathbf{C}^*$ contained in S is $\{1\}$. Since there is i such that $N_i \subset \omega^{-1}S$ and $\omega(N_i)$ is a group it follows that $N_i \subset \omega^{-1}\{1\}$, hence $N_i \subset \ker\omega$. If G is compact, then any open subgroup has finite index in G, so N_i has finite index in G. Hence $\ker\omega$ also has finite index in G, so the image of ω is finite. □

Corollary 2.3.4. *Let K be a finite extension of $k(X)$ where k is a finite field, let $\mathfrak{p}$ be a place of K and let $\omega : K_\mathfrak{p}^* \to \mathbf{C}^*$ be a character. Then there is $n \in \mathbf{Z}_{>0}$ such that $1 + \mathfrak{p}^n \subset \ker\omega$.*

PROOF. Note that $\{1+\mathfrak{p}^n\}_{n\in\mathbf{Z}_{>0}}$ is a local base for neighbourhoods of $1 \in K_\mathfrak{p}^*$ and apply Lemma 2.3.3. □

This justifies the following definition.

Definition 2.3.5. Let $\omega : \mathbf{A}_K^* \to \mathbf{C}^*$ be a character and let $\mathcal{P}$ be the set of places of K. Let $\mathfrak{p} \in \mathcal{P}$ and let $\omega_\mathfrak{p} : K_\mathfrak{p}^* \to \mathbf{C}^*$ be the map $\omega \circ \pi_\mathfrak{p}$ with $\pi_\mathfrak{p} : K_\mathfrak{p}^* \to \mathbf{A}_K^*$ the embedding on the $K_\mathfrak{p}^*$-axis. We define a function $r : \mathcal{P} \to \mathbf{Z}_{\geq 0}$ where $r(\mathfrak{p}) = 0$ if $A_\mathfrak{p}^* \subset \ker\omega_\mathfrak{p}$ and $r(\mathfrak{p}) = \min\{n \in \mathbf{Z}_{>0} : 1 + \mathfrak{p}^n \subset \ker\omega_\mathfrak{p}\}$ otherwise. If $r(\mathfrak{p}) > 0$, we say that ω *ramifies* at $\mathfrak{p}$. We define the *conductor* of ω to be the formal sum $\sum_{\mathfrak{p}\in\mathcal{P}} r(\mathfrak{p}) \cdot \mathfrak{p}$.

Lemma 2.3.6. *Let $\omega : \mathbf{A}_K^* \to \mathbf{C}^*$ be a character and let $\mathcal{P}$ be the set of places of K. Then there are only finitely many $\mathfrak{p} \in \mathcal{P}$ where ω ramifies.*

PROOF. By Proposition 2.2.10 we see that any open set of $\mathbf{A}_K^*$ contains a set of the form $\prod_{\mathfrak{p}\in P} 1 \times \prod_{\mathfrak{p}\notin P} A_\mathfrak{p}^*$ where P is a finite set of places of K. Assuming that $\prod_{\mathfrak{p}\in P} O_\mathfrak{p} \times \prod_{\mathfrak{p}\notin P} A_\mathfrak{p}^*$ is contained in the kernel of ω we see that ω can only ramify at the places in P, so only at finitely many places. □

In geometric terms this implies that the conductor of ω is an element of $\operatorname{Div}(K)$.

Corollary 2.3.7. *Let $\omega : \mathbf{A}_K^* \to \mathbf{C}^*$ be a character. Then $\omega(x) = \prod_\mathfrak{p} \omega_\mathfrak{p}(x_\mathfrak{p})$ and $\omega_\mathfrak{p}(x_\mathfrak{p}) = 1$ for all but finitely many places $\mathfrak{p}$.*

We need one more lemma.

Lemma 2.3.8. *For each $N \in \mathbf{Z}_{>0}$ the set $\{\mathfrak{p} \in \mathcal{P} : \deg\mathfrak{p} \leq N\}$ is finite.*

PROOF. In the case that $K = k(X)$, use Example 2.2.8. For the general case, see [**8**], Theorem I.4.11, p. 18. □

Now we are ready to define L-functions for the idele class group.

Definition 2.3.9. Let K be a finite extension of $k(X)$ with k a finite field, let $\omega = \prod_\mathfrak{p} \omega_\mathfrak{p}$ be a character of C_K and let $\mathcal{P}_\omega$ be the set of places of K where ω does not ramify. Define a function $\lambda_\omega : \mathcal{P}_\omega \to \mathbf{C}^*$ given by $\lambda_\omega(\mathfrak{p}) = \omega_\mathfrak{p}(x)$ with x a prime element in $K_\mathfrak{p}$. Then we define the L-function $L(T,\omega)$ to be

$$L(T,\omega) = \prod_{\mathfrak{p}\in\mathcal{P}_\omega} \frac{1}{1-\lambda_\omega(\mathfrak{p})T^{\deg\mathfrak{p}}} \in \mathbf{C}[[T]].$$

The special case $\omega = 1$ gives rise to the function $L(T,1)$, which is the well known zeta-function of K. Now we can state the famous Riemann Hypothesis for function fields.

Theorem 2.3.10. *Let K be a finite extension of $k(X)$ with k a finite field with q elements. Choose an algebraic closure $\bar{K}$ of K and let $\bar{k}$ the algebraic closure of k in $\bar{K}$. Let $n = [K \cap \bar{k} : k]$ and let 1 be the trivial character of C_K. Then $L(T, 1)$, which is also denoted by $Z_K(T)$, can be written as*

$$Z_K(T) = \frac{P(T)}{(1 - T^n)(1 - (qT)^n)}$$

with $P \in 1 + T\mathbf{Z}[T]$ and the zeros α of P satisfy $|\alpha| = \frac{1}{\sqrt{q}}$.

Proof. See [**2**], Theorem 12.2.1, p. 64 and Corollary 14.3.1, p. 77 for the case $n = 1$. For general n, use [**4**], Proposition 8.18, p. 111. □

Example 2.3.11. If $K = k(X)$, then it is easy to show that

$$Z_K(T) = \frac{1}{(1 - T)(1 - qT)}$$

and hence $P = 1$.

From now on we will restrict to the case $K = k(X)$ with k a finite field. In this case, a lot more can be said. A brief summary of the following can be found in Appendix V of [**9**].

Definition 2.3.12. Let $k(X)$ be the field of rational functions over a finite field k. Denote by $\mathfrak{f}$ the place of $k(X)$ corresponding to a monic irreducible polynomial f and denote by ∞ the place $X^{-1}k[X^{-1}]_{(X^{-1})}$. By $\widehat{k[X]}$ we denote the ring $\prod_{\mathfrak{f}} A_{\mathfrak{f}}$.

In the remainder of this section we will stick to the notation above. We will also be using the diagonal embedding $k(X) \to \mathbf{A}_{k(X)}$ without comment.

Theorem 2.3.13. *The map*

$$\begin{array}{rcl} s : \mathbf{A}^*_{k(X)} & \longrightarrow & k(X)^* \\ ((x_{\mathfrak{f}})_{\mathfrak{f}}, x_\infty) & \longmapsto & c_\infty \cdot \prod_{\mathfrak{f}} f^{\operatorname{ord}_{\mathfrak{f}} x_f}, \end{array}$$

where c_∞ is the leading coefficient of x_∞, is a homomorphism of topological groups that is the identity on $k(X)^*$. The kernel of s is the subgroup

$$\widehat{k[X]}^* \times \left(\langle X \rangle \cdot (1 + X^{-1}k[[X^{-1}]])\right).$$

Furthermore, the exact sequence

$$1 \longrightarrow k(X)^* \longrightarrow \mathbf{A}^*_{k(X)} \longrightarrow C_{k(X)} \longrightarrow 1$$

splits and the map

$$\begin{array}{rcl} u : C_{k(X)} & \longrightarrow & \widehat{k[X]}^* \times \left(\langle X \rangle \cdot (1 + X^{-1}k[[X^{-1}]])\right) \\ x & \longmapsto & x \cdot \dfrac{1}{s(x)} \end{array}$$

is an isomorphism of topological groups.

Finally the restriction of u to $C_{k(X),1}$ gives rise to an isomorphism of topological groups between $C_{k(X),1}$ and $\widehat{k[X]}^* \times \left(1 + X^{-1}k[[X^{-1}]]\right)$.

Proof. First we are going to determine the kernel of s. Exactly the elements $((x_\mathfrak{f})_\mathfrak{f}, x_\infty) \in \mathbf{A}^*_{k(X)}$ such that $\operatorname{ord}_\mathfrak{f} x_\mathfrak{f} = 0$ for all finite places $\mathfrak{f}$ and such that the leading coefficient of x_∞ is equal to 1 are mapped to 1. So this is $\widehat{k[X]}^* \times \big(\langle X\rangle \cdot (1 + X^{-1}k[[X^{-1}]])\big)$. It is clear that s is a group homomorphism. To show that s is continuous it suffices to show that $s^{-1}(1)$ is open in $\mathbf{A}^*_{k(X)}$. This is the kernel of s, which we already determined as $\widehat{k[X]}^* \times \big(\langle X\rangle \cdot (1 + X^{-1}K[[X^{-1}]])\big)$, which is open in $\mathbf{A}^*_{k(X)}$. Now consider the exact sequence

$$1 \longrightarrow k(X)^* \longrightarrow \mathbf{A}^*_{k(X)} \longrightarrow C_{k(X)} \longrightarrow 1.$$

The map s is a retraction of the sequence since s is the identity on $k(X)^*$. Naturally we have a section $u : x \mapsto x \cdot \frac{1}{s(x)}$. The maps are visualized in the following diagram:

$$\begin{tikzcd}
1 \arrow[r] & k(X)^* \arrow[r] & \mathbf{A}^*_{k(X)} \arrow[r] \arrow[l, bend right, "s"'] & C_{k(X)} \arrow[r] \arrow[l, bend right, "u"'] & 1.
\end{tikzcd}$$

It is clear that the image of u is equal to $\widehat{k[X]}^* \times \big(\langle X\rangle \cdot (1 + X^{-1}k[[X^{-1}]])\big)$. Also, u is injective since it is a section. Hence u induces an isomorphism of groups between $C_{k(X)}$ and $\widehat{k[X]}^* \times \big(\langle X\rangle \cdot (1 + X^{-1}k[[X^{-1}]])\big)$. Also, u is clearly a continuous map since it is a composition of continuous maps. Hence we have shown that $C_{k(X)}$ and $\widehat{k[X]}^* \times \big(\langle X\rangle \cdot (1 + X^{-1}k[[X^{-1}]])\big)$ are isomorphic as topological groups.

We have $u(C_{k(X),1}) = \widehat{k[X]}^* \times (1 + X^{-1}k[[X^{-1}]])$, since $\operatorname{im} u = \ker s$. □

Definition 2.3.14. Let $g \in k[X]_{\neq 0}$. Then we define V_g to be the group $(1 + g\widehat{k[X]}) \cap \widehat{k[X]}^*$.

Lemma 2.3.15. *For any $g \in k[X]_{\neq 0}$ we have a natural group isomorphism*

$$\widehat{k[X]}^*/V_g \quad \xrightarrow{\sim} \quad (\widehat{k[X]}/g\widehat{k[X]})^*$$

and a natural ring isomorphism

$$\widehat{k[X]}/g\widehat{k[X]} \quad \xrightarrow{\sim} \quad k[X]/gk[X].$$

Proof. Use the fact that for any $v \in \widehat{k[X]}$ there is a $h \in k[X]$ uniquely determined modulo g such that $v \in h + g\widehat{k[X]}$. □

So for each $g \in k[X]_{\neq 0}$ we have a natural isomorphism $\widehat{k[X]}^*/V_g \xrightarrow{\sim} (k[X]/gk[X])^*$.

Lemma 2.3.16. *All elements of $\mathcal{X}\left(\widehat{k[X]}^* \times \big(1 + X^{-1}k[[X^{-1}]]\big)\right)$ have finite image.*

Proof. It is sufficient to show that all characters of $\widehat{k[X]}^*$ have finite image, since we already proved that all characters of $1 + X^{-1}k[[X^{-1}]]$ have finite image in Theorem 2.1.2. We are going to apply Lemma 2.3.3. We already know that for all $A^*_\mathfrak{f}$ we can take $\{N_i\}_i = \{1 + \mathfrak{f}^n A_\mathfrak{f}\}_{n \in \mathbf{Z}_{>0}}$. Hence for $\widehat{k[X]}^*$ we can take $\{N_i\}_i = \{V_g\}_{g \in k[X]_{\neq 0}}$. Note that $\widehat{k[X]}^*$ is compact by Tychonoff's theorem. Hence the conditions of 2.3.3 are satisfied and it follows that any character of $\widehat{k[X]}^*$ has finite image. □

So Lemmas 2.3.15 and 2.3.16 show that for any character ω on $\widehat{k[X]}^*$ there is $g \in k[X]_{\neq 0}$ such that $V_g \subset \ker \omega$ and ω can be viewed as a character on $(k[X]/gk[X])^*$.

Definition 2.3.17. Let $h \in k[X]_{\neq 0}$. Then we define $h^\circ \in \prod_{\mathfrak{f}} A_{\mathfrak{f}}^*$ to be the element $(x_{\mathfrak{f}})_{\mathfrak{f}}$ where $x_{\mathfrak{f}} = h$ if $h \notin \mathfrak{f}$ and $x_{\mathfrak{f}} = 1$ if $h \in \mathfrak{f}$.

Theorem 2.3.18. *Write any character of $C_{k(X),1}$ as $(\omega_1, \omega_\infty)$ where ω_1 is a character of $\widehat{k[X]}^*$ and ω_∞ is a character of $1 + X^{-1}k[[X^{-1}]]$. Let $\mathcal{X}_{\text{primitive}}$ be the set of primitive characters of $k[X]$. Define χ_1 as the map on $k[X]$ which comes from the induced map $\bar{\omega}_1 : \widehat{k[X]}^*/V_g \to \mathbf{C}^*$ where g is the monic polynomial of minimal degree such that $V_g \subset \ker \omega_1$. Then the map*

$$\begin{aligned} \pi : \mathcal{X}(C_{k(X),1}) &\longrightarrow \mathcal{X}_{\text{primitive}} \\ (\omega_1, \omega_\infty) &\longmapsto (\chi_1, \omega_\infty) \end{aligned}$$

is bijective and for all h such that $(h, g) = 1$ we have $\omega_1(h^\circ) = \chi_1(h)$, where h° is as in Definition 2.3.17.

Proof. By Lemma 2.3.16 we know there is $g \in k[X]$ such that $V_g \subset \ker \omega_1$, and there is a unique monic g of minimal degree having this property. The obtained (χ_1, ω_∞) is primitive because g is chosen of minimal degree. This shows that π is well defined. Now it is straightforward to show that π is bijective. For any character (χ_1, χ_∞) we can make χ_1 into a character ω_1 on $\widehat{k[X]}^*$ by 2.3.15, in this way the map that maps (χ_1, χ_∞) to (ω_1, χ_∞) is the inverse of π. The last part of the theorem follows immediately since $h^\circ \in h + g\widehat{k[X]}$. □

Remark 2.3.19. Clearly we have skipped the $\langle X \rangle$-part of $\langle X \rangle \cdot (1 + X^{-1}k[[X^{-1}]])$, we restrict to characters of $C_{k(X),1}$. The reason is that the additional characters we get make the typography uglier and are of no use in this thesis. We could have made Theorem 2.3.18 work for the complete group by extending the definition of a character of $k[X]$. Instead of a pair (χ_1, χ_∞) we would get a triple $(\chi_1, \chi_\infty, \chi_{\mathbf{Z}})$ where $\chi_{\mathbf{Z}}(f)$ is defined to be $x^{\deg f}$ for some fixed $x \in \mathbf{C}^*$.

Now let us recall some important maps. Let $\omega : C_{k(X)} \to \mathbf{C}^*$ be a character and let $\mathfrak{p}$ be a place of $k(X)$. Then $r_\omega(\mathfrak{p}) = 0$ if $A_{\mathfrak{p}}^* \subset \ker \omega$ and $r_\omega(\mathfrak{p}) = \min\{n \in \mathbf{Z}_{>0} : 1 + \mathfrak{p}^n \subset \ker \omega\}$ otherwise where $1 + \mathfrak{p}^n$ is embedded in C_K on the $K_{\mathfrak{p}}^*$-axis. If ω does not ramify at $\mathfrak{p}$ (so $r_\omega(\mathfrak{p}) = 0$), then $\lambda_\omega(\mathfrak{p}) = \omega(x)$ where x is a generator of $\mathfrak{p}$, embedded in C_K on the $K_{\mathfrak{p}}^*$-axis.

Theorem 2.3.20. *Let $\omega = (\omega_1, \omega_\infty) : C_{k(X)} \to \mathbf{C}^*$ be a character that is trivial on $\langle X \rangle$ in $\langle X \rangle(1 + X^{-1}k[[X^{-1}]])$. Let π be the isomorphism of Lemma 2.3.18 and let (g, δ) be the conductor of $\pi(\omega)$ (ω can be viewed as a character of $C_{k(X),1}$ since it is trivial on $\langle X \rangle$ in $\langle X \rangle(1 + X^{-1}k[[X^{-1}]])$). Then for any finite place $\mathfrak{f}$ of $k(X)$ with monic generator f we have $r_\omega(\mathfrak{f}) = \operatorname{ord}_f g$. We have $\delta = r_\omega(\infty)$. Also, if ω does not ramify at $\mathfrak{f}$ we have $\lambda_\omega(\mathfrak{f}) = \pi(\omega)(f^{-1})$. If ω does not ramify at ∞ we have $\lambda_\omega(\infty) = 1$.*

Proof. First we deduce from Theorem 2.3.18 that g is the monic polynomial of minimal degree such that $V_g \subset \ker \omega_1$. Now we look at what happens to the place at infinity. Let $x = \sum_{i=-\infty}^{n} c_i X^i$ with all $c_i \in k$ and $c_n \neq 0$ be an element of

A_∞^*, viewed as an element of $C_{k(X)}$ by embedding on the $k(X)_\infty^*$-axis. We have

$$\omega(x) = \omega(\frac{1}{c_n} \cdot x) = \omega_1(\frac{1}{c_n}) \cdot \omega_\infty(\frac{1}{c_n} \cdot x).$$

Hence ω does not ramify at ∞ (so $r(\infty) = 0$) if and only if ω_1 is trivial on k^* and ω_∞ is trivial. Otherwise $r_\omega(\infty)$ is the smallest $n \in \mathbf{Z}_{>0}$ such that $(1 + X^{-n}k[[X^{-1}]]) \subset \ker \omega_\infty$. This shows that $r_\omega(\infty) = \delta$. If ω does not ramify at ∞ we indeed have $\lambda_\omega(\infty) = \omega(1, \dots, X^{-1}) = \omega_\infty(X^{-1}) = 1$.

Now let $\mathfrak{f}$ be a place with monic generator f. View $A_\mathfrak{f}^*$ as a subset of $C_{k(X)}$ by embedding on the $k(X)_\mathfrak{f}^*$-axis. Determining whether ω ramifies at $\mathfrak{f}$ is equivalent to determining whether $\omega_1(x) = 1$ for all $x \in \widehat{k[X]}^*$. We will make use of Theorem 2.3.18. We know that g is the monic polynomial of minimal degree such that $V_g \subset \ker \omega_1$. If f does not divide g then $gA_\mathfrak{f} = A_\mathfrak{f}$, hence ω does not ramify at $\mathfrak{f}$. If f does divide g, then $gA_\mathfrak{f} = f^m A_\mathfrak{f}$ for some $m > 0$. Since g is of minimal degree it follows that $r_\omega(\mathfrak{f}) = m$. This shows that $r_\omega(\mathfrak{f})$ is equal to the number of factors of f in g. Since ω_∞ maps $\langle X \rangle$ to 1 we have $\omega_\infty(f^{-1}) = \omega_\infty(X^{\deg f} f^{-1})$. So if ω does not ramify at $\mathfrak{f}$, we have

$$\lambda_\omega(\mathfrak{f}) = \omega(1, \dots, f, \dots, 1) = \omega((1, \dots, f, \dots, 1) \cdot f^{-1}) = \omega_1((f^\circ)^{-1})\omega_\infty(X^{\deg f} f^{-1})$$

where f° is as in Definition 2.3.17. Finally by the last part of Theorem 2.3.18 we have

$$\omega_1((f^\circ)^{-1})\omega_\infty(X^{\deg f} f^{-1}) = \pi(\omega)(f^{-1}),$$

exactly what we wanted to prove. □

The theorem yields the following corollary, which relates the L-functions.

Corollary 2.3.21. *Let χ be a primitive character of $k[X]$ and let ω be the character of $C_{k(X),1}$ such that $\pi(\omega) = \chi^{-1}$. Extend ω to a character of $C_{k(X)}$ by $\omega(X) = 1$. Let (g, δ) be the conductor of χ and let $\mathfrak{g}$ be the conductor of ω. Then* $\deg g + \delta = \deg \mathfrak{g}$ *and*

$$L(T, \chi) = L(T, \omega)(1 - T)^{\max\{0, 1-\delta\}}.$$

Proof. Note that the conductors of χ^{-1} and χ are the same. The rest follows immediately from Theorem 2.3.20. □

CHAPTER 3

Class field theory

1. Some algebraic number theory

Definition 3.1.1. Let K be a finite extension of $k(X)$ with k a finite field, let L be a finite extension of K and let $\mathfrak{p}$ be a place of K with valuation ring $\mathcal{O}_{\mathfrak{p}}$. If $\mathfrak{q}$ is a place of L, we say that $\mathfrak{q}$ *lies above* $\mathfrak{p}$, denoted by $\mathfrak{q} \mid \mathfrak{p}$ if $\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{q}} \cap K$. If $\mathfrak{q}$ lies above $\mathfrak{p}$ we define $f(\mathfrak{q} \mid \mathfrak{p})$ to be the dimension of $\mathcal{O}_{\mathfrak{q}}/\mathfrak{q}$ as $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$-vector space and we define $e(\mathfrak{q} \mid \mathfrak{p})$ to be the number such that $\mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})} = \mathfrak{p}\mathcal{O}_{\mathfrak{q}}$. We define $r(\mathfrak{p})$ to be the number of places lying above $\mathfrak{p}$. Often we just use the letters f, e and r if it is clear which extension is meant.

Theorem 3.1.2. *Let K be a finite extension of $k(X)$ with k a finite field, let L be a finite extension of K and let $\mathfrak{p}$ be a place of K. Then $\sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q} \mid \mathfrak{p})e(\mathfrak{q} \mid \mathfrak{p}) = [L : K]$.*

The proof of this theorem in the case that L is separable over K can be found in [**7**]. We will give a sketch here. In the following lemma, let $\mathfrak{q}$ be a place lying above $\mathfrak{p}$.

Lemma 3.1.3. *We have $f(\mathfrak{q} \mid \mathfrak{p})e(\mathfrak{q} \mid \mathfrak{p}) = [L_{\mathfrak{q}} : K_{\mathfrak{p}}]$.*

Proof. See [**7**], Theorem 3.7, p. 26. □

Lemma 3.1.4. *The canonical map $K_{\mathfrak{p}} \otimes_K L \to \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$ is an isomorphism of $K_{\mathfrak{p}}$-algebras.*

Proof. See [**7**], Theorem 3.8, p. 26 for the special case where L is separable over K; see [**4**], Proposition 7.2, p. 81 for the general case. □

Now we can easily prove 3.1.2. As a $K_{\mathfrak{q}}$-vector space $K_{\mathfrak{p}} \otimes_K L$ is isomorphic to $K_{\mathfrak{p}}^{[L:K]}$ and each $L_{\mathfrak{q}}$ is as a $K_{\mathfrak{p}}$-vector space isomorphic to $K_{\mathfrak{q}}^{[L_{\mathfrak{q}}:K_{\mathfrak{p}}]}$. Now 3.1.3 proves 3.1.2.

The following theorem is known as the weak approximation theorem.

Theorem 3.1.5. *Let K be a finite extension of $k(X)$ with k a finite field and let S be a finite set of distinct places of K. Let T be a subset of S. Then there exists $x \in L$ such that $|x|_{\mathfrak{p}} > 1$ if $\mathfrak{p} \in T$ and $|x|_{\mathfrak{p}} < 1$ if $\mathfrak{p} \in S \setminus T$.*

Proof. See [**8**], Theorem I.1.3, p. 11.

□

2. Galois extensions

Theorem 3.2.1. *Let K be a finite extension of $k(X)$ with k a finite field, let L/K be a finite Galois extension with Galois group G and let $\mathfrak{p}$ be a place of K. Then G acts transitively on the set of places of L lying above $\mathfrak{p}$.*

Proof. First note that G indeed acts on the set of places of L lying above $\mathfrak{p}$, since if $\mathfrak{q}$ is a place lying over $\mathfrak{p}$ then $\sigma\mathcal{O}_{\mathfrak{q}}$ is clearly also a discrete valuation ring with maximal ideal $\sigma\mathfrak{q}$. Moreover we have $\sigma\mathfrak{q} \cap K = \mathfrak{p}$ since σ is the identity on K. Now suppose that there are places $\mathfrak{q}_1$ and $\mathfrak{q}_2$ lying above $\mathfrak{p}$ such that $G\mathfrak{q}_1 \cap G\mathfrak{q}_2 = \varnothing$. By 3.1.5 there is $x \in L$ such that $|x|_{\mathfrak{q}} > 1$ if $\mathfrak{q} \in G\mathfrak{q}_1$ and $|x|_{\mathfrak{q}} < 1$ if $\mathfrak{q} \in G\mathfrak{q}_2$. Note that $N_{L/K}x$ is an element of K (in the next section we will get back to the definition of the norm), so $|N_{L/K}x|_{\mathfrak{q}_1} = |N_{L/K}x|_{\mathfrak{q}_2}$. Now on one hand we have

$$|N_{L/K}x|_{\mathfrak{q}_1} = \left|\prod_{\sigma\in G} \sigma(x)\right|_{\mathfrak{q}_1} = \prod_{\sigma\in G} |x|_{\sigma^{-1}(\mathfrak{q}_1)} > 1$$

and on the other hand we have

$$|N_{L/K}x|_{\mathfrak{q}_2} = \left|\prod_{\sigma\in G} \sigma(x)\right|_{\mathfrak{q}_2} = \prod_{\sigma\in G} |x|_{\sigma^{-1}(\mathfrak{q}_2)} < 1$$

which is a contradiction. □

This theorem yields us the following important corollary.

Corollary 3.2.2. *Let K be a finite extension of $k(X)$ with k a finite field, let L/K be a finite Galois extension and let $\mathfrak{p}$ be a place of K. Let $\mathfrak{q}$ be any place of L lying above $\mathfrak{p}$. Then $f(\mathfrak{q} \mid \mathfrak{p})$ and $e(\mathfrak{q} \mid \mathfrak{p})$ do not depend on the choice of $\mathfrak{q}$ and $[L : K] = rf(\mathfrak{q} \mid \mathfrak{p})e(\mathfrak{q} \mid \mathfrak{p})$.*

Proof. This is an immediate consequence of Theorem 3.1.2, since for any $\mathfrak{q}, \mathfrak{q}'$ lying above $\mathfrak{p}$ there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}'$ and as a consequence $\sigma(\mathcal{O}_{\mathfrak{q}}) = \mathcal{O}_{\mathfrak{q}'}$. □

So if L/K is a Galois extension, the variables f and e do not depend on the chosen extension of a place.

Definition 3.2.3. Let K be a finite extension of $k(X)$ with k a finite field, let L/K be a finite Galois extension with Galois group G, let $\mathfrak{q}$ be a place of L. We define the *decomposition group* of $\mathfrak{q}$ in G, denoted by $G_{\mathfrak{q}}$, to be the subgroup of G given by $\{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}$. Note that we have a natural map

$$G_{\mathfrak{q}} \to \mathrm{Gal}((\mathcal{O}_{\mathfrak{q}}/\mathfrak{q})/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}))$$

We define the kernel of this map to be the *inertia group* of $\mathfrak{q}$, denoted by $I_{\mathfrak{q}}$.

Note that $I_{\mathfrak{q}}$ is a normal subgroup of $G_{\mathfrak{q}}$.

Theorem 3.2.4. *Let K be a finite extension of $k(X)$ with k a finite field, let L/K be a finite Galois extension with Galois group G, let $\mathfrak{p}$ be a place of K and let $\mathfrak{q}$ be a place of L lying above $\mathfrak{p}$. Then the order of $G_{\mathfrak{q}}$ is equal to fe. Also, $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is a finite Galois extension. If $G = \mathrm{Gal}(L/K)$, then there is a natural isomorphism from $G_{\mathfrak{q}}$ to $\mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$, where $G_{\mathfrak{q}}$ is the subgroup of G given by $\{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}$.*

Proof. By theorem 3.2.1 we know that $G\mathfrak{q}$ consists of r places. Also there is a well known bijection $G\mathfrak{q} \leftrightarrow G/G_{\mathfrak{q}}$, which shows that $r = \#(G/G_{\mathfrak{q}})$. Hence we have $\#G_{\mathfrak{q}} = fe$. Clearly every element of $G_{\mathfrak{q}}$ can be extended to an automorphism of $L_{\mathfrak{q}}$ being the identity on $K_{\mathfrak{p}}$. By Lemma 3.1.3 we know that $[L_{\mathfrak{q}} : K_{\mathfrak{p}}] = fe$. Since $\#\,\mathrm{Aut}_{K_{\mathfrak{p}}} L_{\mathfrak{q}} \leq [L_{\mathfrak{q}} : K_{\mathfrak{p}}]$ with equality if and only if $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is Galois, we have proved that the natural embedding of $G_{\mathfrak{q}}$ in $\mathrm{Aut}_{K_{\mathfrak{p}}} L_{\mathfrak{q}}$ is an isomorphism, and that $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is Galois. □

Now we are going to determine the order of $I_{\mathfrak{q}}$.

Theorem 3.2.5. *Let K be a finite extension of $k(X)$ with k a finite field, let L/K be a finite Galois extension with Galois group G, let $\mathfrak{q}$ be a place of L, let $G_{\mathfrak{q}}$ be the decomposition group of $\mathfrak{q}$ and let $I_{\mathfrak{q}}$ be the inertia group of $\mathfrak{q}$. Then we have a short exact sequence*

$$1 \longrightarrow I_{\mathfrak{q}} \longrightarrow G_{\mathfrak{q}} \longrightarrow \mathrm{Gal}((\mathcal{O}_{\mathfrak{q}}/\mathfrak{q})/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})) \longrightarrow 1$$

Proof. Apply the map in 3.2.4 and use [**7**], p. 39. □

Corollary 3.2.6. *The order of $I_{\mathfrak{q}}$ is equal to e.*

Proof. We know that the order of $G_{\mathfrak{q}}$ is fe by 3.2.4. By definition we have $[\mathcal{O}_{\mathfrak{q}}/\mathfrak{q} : \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}] = f$, so this is also the order of the Galois group. Hence by 3.2.5 the order of $I_{\mathfrak{q}}$ is equal to $\frac{fe}{f}$, thus equal to e. □

Definition 3.2.7. The coset of $G_{\mathfrak{q}}/I_{\mathfrak{q}}$ that is mapped to the Frobenius map of $\mathrm{Gal}((\mathcal{O}_{\mathfrak{q}}/\mathfrak{q})/(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}))$ is denoted by $(\mathfrak{q}, L/K)$, which we call the *Frobenius symbol.*

In the case that L/K is unramified at $\mathfrak{q}$ it is clear that $(\mathfrak{q}, L/K)$ is a generator of $G_{\mathfrak{q}}$.

3. Norms

We recall an important definition.

Definition 3.3.1. Let K be a field and let L be a finite extension of K. Then for any $a \in L$ we have a map $f_a : L \to L$ given by $x \mapsto ax$. We define

$$N_{L/K}a = \det_K(f_a),$$

which is an element of K. For any subgroup $U \subset L^*$ we define

$$N_{L/K}U = \{N_{L/K}x : x \in U\},$$

which is a subgroup of K^*.

Note that $N_{L/K}L^* \subset K^*$, but it is generally not easy to determine which subgroup this is. The following theorem is well known.

Theorem 3.3.2. *Let K be a field, let L be a finite extension of K and let $\bar{L}$ be an algebraic closure of L. Let K^{sep} be the separable closure of K in L and let $i = [L : K^{\mathrm{sep}}]$ be the inseparability degree of L/K. Then for any $x \in K$ we have*

$$N_{L/K}x = \prod_{\sigma \in \mathrm{Hom}_K(L, \bar{L})} \sigma(x)^i.$$

Proof. See [**6**] for example. □

Theorem 3.3.3. *Let K be a finite extension of $k(X)$ with k a finite field, let L/K be a finite extension and let $\mathfrak{p}$ be a place of K. Then*

$$N_{L/K}x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}x.$$

Proof. We make use of lemma 3.1.4 which says that the canonical map $K_{\mathfrak{p}} \otimes_K L \to \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$ is an isomorphism. Since any K-basis for L is a $K_{\mathfrak{p}}$-basis for $K_{\mathfrak{p}} \otimes_K L$, we see that $N_{L/K}x = N_{K_{\mathfrak{p}} \otimes_K L/K_{\mathfrak{p}}}x$, and by 3.1.4 we have $N_{K_{\mathfrak{p}} \otimes_K L/K_{\mathfrak{p}}}x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}x$, which is what we wanted to prove. □

Lemma 3.3.4. *Let $x \in K_{\mathfrak{p}}$. Then $|x|_{\mathfrak{q}} = |x|_{\mathfrak{p}}^{[L_{\mathfrak{q}}:K_{\mathfrak{p}}]}$.*

Proof. First suppose $x \in \mathcal{O}_{\mathfrak{p}} \setminus \{0\}$. Then $x \in \mathcal{O}_{\mathfrak{q}}$. We have

$$|x|_{\mathfrak{q}} = \#(\mathcal{O}_{\mathfrak{q}}/x\mathcal{O}_{\mathfrak{q}})^{-1} = \#(\mathcal{O}_{\mathfrak{q}}/\mathfrak{q})^{-\operatorname{ord}_{\mathfrak{q}} x} = (\#(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})^{f})^{-\operatorname{ord}_{\mathfrak{q}} x} =$$

$$(\#(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})^{f})^{-e\operatorname{ord}_{\mathfrak{p}} x} = (\#(\mathcal{O}_{\mathfrak{p}}/x\mathcal{O}_{\mathfrak{p}})^{-1})^{fe} = |x|_{\mathfrak{p}}^{[L_{\mathfrak{q}}:K_{\mathfrak{p}}]}.$$

Now suppose $x \in K_{\mathfrak{p}} \setminus \mathcal{O}_{\mathfrak{p}}$. Then $x^{-1} \in \mathcal{O}_{\mathfrak{q}}$. Since we have $|x^{-1}|_{\mathfrak{q}} = |x|_{\mathfrak{q}}^{-1}$, we can just use the argument above. Finally if $x = 0$ the lemma is obvious, hence the lemma has been proved. □

Lemma 3.3.5. *Let $x \in L_{\mathfrak{q}}$. Then $|N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}x|_{\mathfrak{p}} = |x|_{\mathfrak{q}}$.*

Proof. We know by Theorem 3.3.2 that $N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}x = \prod_{\sigma \in \operatorname{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}, \bar{L_{\mathfrak{q}}})} \sigma(x)^i$ where i is the inseparability degree of $L_{\mathfrak{q}}/K_{\mathfrak{p}}$. Let M be a splitting field of $L_{\mathfrak{q}}$ over $K_{\mathfrak{p}}$. Then we can corestrict any element in $\operatorname{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}, \bar{L_{\mathfrak{q}}})$ to an element of $\operatorname{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}, M)$. Moreover, M is also a local field with a unique place $\mathfrak{r}$ that lies above $\mathfrak{p}$ and $\mathfrak{q}$. So we have

$$|N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}x|_{\mathfrak{p}} = \left| \prod_{\sigma \in \operatorname{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}, \bar{L_{\mathfrak{q}}})} \sigma(x)^i \right|_{\mathfrak{p}} = \left| \prod_{\sigma \in \operatorname{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}, M)} \sigma(x) \right|_{\mathfrak{r}}^{\frac{i}{[M:K_{\mathfrak{p}}]}},$$

using Lemma 3.3.4 (for any element $x \in K_{\mathfrak{p}}$ we have $|x|_{\mathfrak{p}}^{[M:K_{\mathfrak{p}}]} = |x|_{\mathfrak{r}}$ so also $|x|_{\mathfrak{p}} = |x|_{\mathfrak{r}}^{\frac{1}{[M:K_{\mathfrak{p}}]}}$). Since $\mathfrak{r}$ is fixed under the action of $\operatorname{Gal}(M/K_{\mathfrak{p}})$ we have

$$\left| \prod_{\sigma \in \operatorname{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}, M)} \sigma(x) \right|_{\mathfrak{r}}^{\frac{i}{[M:K_{\mathfrak{p}}]}} = \prod_{\sigma \in \operatorname{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}, M)} |x|_{\sigma^{-1}(\mathfrak{r})}^{\frac{i}{[M:K_{\mathfrak{p}}]}} = |x|_{\mathfrak{r}}^{\frac{[L_{\mathfrak{q}}:K_{\mathfrak{p}}]}{[M:K_{\mathfrak{p}}]}} = |x|_{\mathfrak{q}},$$

again making use of Lemma 3.3.4. This proves the lemma. □

Corollary 3.3.6. *We have $x \in A_{\mathfrak{q}}$ if and only if $N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}x \in A_{\mathfrak{p}}$.*

Theorem 3.3.2 and Corollary 3.3.6 justify the following definition.

Definition 3.3.7. Let K be a finite extension of $k(X)$ with k a finite field, let L/K be a finite extension and let $x \in \mathbf{A}_L$. Then we define

$$N_{L/K}(x) = \left(\prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(x_{\mathfrak{q}}) \right)_{\mathfrak{p}},$$

which is an element of $\mathbf{A}_K$, and for any subgroup $U \subset \mathbf{A}_L^*$ we define

$$N_{L/K}(U) = \{N_{L/K}x : x \in U\},$$

which is a subgroup of $\mathbf{A}_K^*$. In the same manner we can define for any subgroup $U \subset C_L$ the subgroup $N_{L/K}(U)$ of C_K.

By Theorem 3.3.3 we see that the map $N_{L/K}|_L$ is just the regular norm. We also see that for any place $\mathfrak{q}$ of L lying above a place $\mathfrak{p}$ of K the map $N_{L/K}|_{L_{\mathfrak{q}}}$ on the $L_{\mathfrak{q}}$-axis is the regular norm $N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}$.

4. The main theorem

Now we have all the ingredients to formulate the heavy theorem which we will need.

Theorem 3.4.1. *Let K be a finite extension of $k(X)$ with k a finite field. Let G_K^{ab} be the Galois group of the maximal abelian extension of K, which is a topological group ([**6**]). Then there is a continuous injective homomorphism*

$$\mathfrak{a} : C_K \to G_K^{\mathrm{ab}}$$

such that for each finite extension L of K that is contained in K^{ab} we have an induced isomorphism

$$\bar{\mathfrak{a}} : C_K / N_{L/K} C_L \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

and for each place $\mathfrak{p}$ of K the map $\bar{\mathfrak{a}}$ restricts to isomorphisms

$$K_{\mathfrak{p}}^* \cdot N_{L/K} C_L / N_{L/K} C_L \xrightarrow{\sim} G_{\mathfrak{p}}$$

and

$$A_{\mathfrak{p}}^* \cdot N_{L/K} C_L / N_{L/K} C_L \xrightarrow{\sim} I_{\mathfrak{p}}.$$

Moreover, for each open subgroup H of C_K of finite index there is precisely one subfield L of K^{ab}, finite over K, such that $N_{L/K} C_L = H$.

Proof. See [**9**], Theorem 6, p. 275, Corollary 2, p. 277 and Corollary 2, p. 279. □

Definition 3.4.2. If L and H are as in the last part of Theorem 3.4.1, we say that L is the *class field* to H.

Now we can state the most important ingredient of the proof of Theorem 2.1.10. The proof is similar to the proof of the number field case, see [**3**], Theorem 1, p. 230.

Theorem 3.4.3. *Let K be a finite extension of $k(X)$ with k a finite field and let L be a finite abelian extension of K. Let H be $N_{L/K} C_L$ and let $\mathcal{X}(C_K/H)$ be the group of characters of C_K/H. Then*

$$\prod_{\omega \in \mathcal{X}(C_K/H)} L(T, \omega) = Z_L(T).$$

Proof. Since the extension is abelian, it is Galois in particular. So by 3.2.2 for any place $\mathfrak{p}$ of K we have $[L : K] = fer = f(\mathfrak{q} \mid \mathfrak{p}) e(\mathfrak{q} \mid \mathfrak{p}) r$ where r is the number of places lying above $\mathfrak{p}$. Hence we can write $\mathfrak{p} L = (\mathfrak{q}_1 \ldots \mathfrak{q}_r)^e$ where for each place $\mathfrak{q}_i$ we have $\deg \mathfrak{q}_i = \deg \mathfrak{p}^f$. So we have

$$Z_L(T) = \prod_{\mathfrak{q}} \frac{1}{1 - T^{\deg \mathfrak{q}}} = \prod_{\mathfrak{p}} \prod_{\mathfrak{q} | \mathfrak{p}} \frac{1}{1 - T^{f \deg \mathfrak{p}}}$$

where $\mathfrak{p}$ runs over all places of K and $\mathfrak{q}$ runs over all places of L. We know that $L(T, \omega) = \prod_{\mathfrak{p}} \frac{1}{1 - \lambda_\omega(\mathfrak{p}) T^{\deg \mathfrak{p}}}$ for all $\omega \in \mathcal{X}(C_K/H)$, where the product is taken over all places of K where ω does not ramify. So it is sufficient to prove the theorem at each factor $\mathfrak{p}$. Denote by $\mathcal{X}(C_K/H, \mathfrak{p}) \subset \mathcal{X}(C_K/H)$ the subgroup of characters that do not ramify at $\mathfrak{p}$. Then it suffices to prove that

$$(1 - W^f)^r = \prod_{\omega \in \mathcal{X}(C_K/H, \mathfrak{p})} (1 - \lambda_\omega(\mathfrak{p}) W).$$

where $W = T^{\deg \mathfrak{p}}$.

We have $K_\mathfrak{p}^* H/H \cong G_\mathfrak{p}$ and $A_\mathfrak{p}^* H/H \cong I_\mathfrak{p}$ by Theorem 3.2.4 and Theorem 3.4.1. We have $\# K_\mathfrak{p}^* H/A_\mathfrak{p}^* H = \# G_\mathfrak{p}/I_\mathfrak{p} = f$ by Corollary 3.2.6 and Theorem 3.4.1. Moreover, by Theorem 3.2.5 it follows that $G_\mathfrak{p}/I_\mathfrak{p}$ and hence $K_\mathfrak{p}^* H/A_\mathfrak{p}^* H$ is cyclic. Let it be generated by an element $\bar{\pi} \in K_\mathfrak{p}^* H/A_\mathfrak{p}^* H$, which we choose such that π generates $\mathfrak{p}$. Then the character ψ of $K_\mathfrak{p}^* H/A_\mathfrak{p}^* H$ that maps π to ζ_f generates $\mathcal{X}(K_\mathfrak{p}^* H/A_\mathfrak{p}^* H)$. Since all the characters in $\mathcal{X}(K_\mathfrak{p}^* H/A_\mathfrak{p}^* H)$ are determined by the image of $\bar{\pi}$, it follows that the elements of $\mathcal{X}(K_\mathfrak{p}^* H/A_\mathfrak{p}^* H)$ are the characters that send $\bar{\pi}$ to ζ_f^i, with $0 \leq i \leq f-1$.

Note that we have a surjective homomorphism $\mathcal{X}(C_K/H) \to \mathcal{X}(A_\mathfrak{p}^* H/H)$ given by restriction. The kernel of this homomorphism is $\mathcal{X}(C_K/H, \mathfrak{p})$, the subgroup of characters that do not ramify at $\mathfrak{p}$. We also have a surjective homomorphism $\mathcal{X}(C_K/H) \to \mathcal{X}(K_\mathfrak{p}^* H/H)$ given by restriction. Hence we have a surjective homomorphism $\mathcal{X}(C_K/H, \mathfrak{p}) \to \mathcal{X}(K_\mathfrak{p}^* H/A_\mathfrak{p}^* H)$, where each fiber has r elements. So we have

$$\prod_{\omega \in \mathcal{X}(C_K/H,\mathfrak{p})} (1 - \lambda_\omega(\mathfrak{p}) W) = \prod_{\omega \in \mathcal{X}(K_\mathfrak{p}^* H/A_\mathfrak{p}^* H)} (1 - \omega(\bar{\pi}) W)^r =$$

$$\prod_{i=0}^{f} (1 - \zeta_f^i W)^r = (1 - W^f)^r.$$

This is what we wanted to prove. □

5. The proof of Theorem 2.1.10

Now we are almost ready to prove Theorem 2.1.10. We mention one more result without proof.

Theorem 3.5.1. *Let K be a finite extension of $k(X)$ with k a finite field and let ω be a character of C_K that is non-trivial on $C_{K,1}$. Then $L(T,\omega) \in \mathbf{C}[T]$. If $K = k(X)$ then the degree of $L(T,\omega)$ is equal to $\deg \mathfrak{f} - 2$, where $\mathfrak{f}$ is the conductor of ω.*

Proof. See [**9**], Theorem 6, p. 134. □

Theorem 3.5.2. *Let K be a finite extension of $k(X)$ with k a finite field with q elements and let ω be a character of C_K that is non-trivial on $C_{K,1}$ and trivial on the $\langle X \rangle$-part of C_K (as in Theorem 2.3.13). Then all zeroes α of $L(T,\omega)$ satisfy $|\alpha| = \frac{1}{\sqrt{q}}$.*

Proof. Let H be the kernel of ω, then H is open and of finite index. So by the last statement of Theorem 3.4.1 there is a finite abelian extension L/K such that L is the class field to H. By Theorem 3.4.3 we know that

$$\prod_{\psi \in \mathcal{X}(C_K/H)} L(T,\psi) = Z_L(T)$$

and by Theorem 2.3.10 it follows that all zeroes α of $\prod_{\psi \in X_H} L(T,\psi)$ satisfy $|\alpha| = \frac{1}{\sqrt{q}}$ and all poles β of $\prod_{\psi \in \mathcal{X}(C_K/H)} L(T,\psi)$ satisfy $|\beta| = 1$ or $|\beta| = \frac{1}{q}$. By Theorem 3.5.1 we know that all $L(T,\psi)$ except $L(T,1)$ are polynomials in $\mathbf{C}[T]$. Moreover, Theorem 2.3.10 again tells us that $L(T,1) = Z_K(T)$ is a rational function of which all poles β satisfy $|\beta| = 1$ or $|\beta| = \frac{1}{q}$. Combining all this, it follows that all zeroes α of all the factors $L(T, \omega)$ satisfy $|\alpha| = \frac{1}{\sqrt{q}}$, which proves the theorem. □

Now let $\chi = (\chi_1, \chi_\infty)$ be a character of $k(X)$ with modulus f, where k has q elements. Let ψ_1 be the map that induces χ_1 such that $\psi = (\chi_1, \chi_\infty)$ is primitive and let g be the conductor of χ. As in Proposition 2.1.9 can we write

$$L(T, \chi) = L(T, \psi) \cdot \prod_h (1 - \psi(h) T^{\deg h})$$

where ψ is the primitive character inducing χ and h ranges over the monic irreducible factors of f. By Corollary 2.3.21 we know there is a character ω of $C_{k(X)}$ with conductor $\mathfrak{g}$ and $r(\infty) = \delta$ such that

$$L(T, \psi) = L(T, \omega)(1 - T)^{\max\{0, 1-\delta\}}$$

and $\deg \mathfrak{g} = \deg g + \delta$. Assume ψ is not principal, then ω is not trivial on $C_{k(X),1}$. Then by Theorem 3.5.1 we know that $L(T, \psi)$ is a polynomial of degree $\deg \mathfrak{g} - 2 = \deg g - 2 + \delta$ and by Theorem 3.5.2 we know that all zeroes of α of $L(T, \psi)$ satisfy $|\alpha| = \frac{1}{\sqrt{q}}$. Hence substituting in the formula of Proposition 2.1.9 we see that there are $\alpha_1, \ldots, \alpha_m \in \mathbf{C}$, where $m = \deg g - 2 + \delta$, such that $|\alpha_i| = \sqrt{q}$ for $1 \leq i \leq m$ and such that

$$L(T, \chi) = \prod_{i=1}^{m} (1 - \alpha_i T) \cdot (1 - T)^{\max\{0, 1-\delta\}} \cdot \prod_h (1 - \psi(h) T^{\deg h})$$

where h ranges over all monic irreducible factors of f. This completes the proof of Theorem 2.1.10.

CHAPTER 4

Applications

1. The main tools

Definition 4.1.1. Let k be a finite field and let $f \in k[X]_{\neq 0}$. Then we define $\Phi(f) = \#(k[X]/fk[X])^*$.

Theorem 4.1.2. *Let k be a finite field with q elements and let $f \in k[X]_{\neq 0}$. Then the group $\mathcal{X}(f,c)$ has order $\Phi(f) \cdot q^{c-1}$.*

Proof. By Lemma 2.1.2 we see that the number of elements of $\mathcal{X}(f,c)$ is equal to $\#\operatorname{Hom}((k[X]/fk[X])^*, \mathbf{C}^*) \cdot \#\operatorname{Hom}(1+X^{-1}k[[X^{-1}]]/1+X^{-c}k[[X^{-1}]], \mathbf{C}^*)$. It is well known that for each finite abelian group A we have $\#\operatorname{Hom}(A, \mathbf{C}^*) = \#A$, so it follows that the number of characters with modulus (f,c) is indeed equal to $\Phi(f) \cdot q^{c-1}$. □

The following theorem is a well known orthogonality relation.

Theorem 4.1.3. *Let k be a finite field and let $f \in k[X]_{\neq 0}$, let $c \in \mathbf{Z}_{>0}$, let $a \in k[X]$ and $g \in k[X]_{\text{monic}}$ be such that $(a,f) = (g,f) = 1$, let $b = (b_1, \ldots, b_{c-1}) \in k^{c-1}$ and let $b' = 1 + \sum_{i=1}^{c-1} b_i X^{-i} \mod X^{-c}k[X^{-1}]$. Then*

$$\sum_{\chi \in \mathcal{X}(f,c)} \chi(g)\overline{\chi_1(a)\chi_\infty(b')} = \Phi(f)q^{c-1}\delta(g,a,b')$$

where we have $\delta(g,a,b') = 1$ if $g \equiv a \mod f$ and $\frac{g}{X^{\deg g}} \equiv b' \mod X^{-c}k[X^{-1}]$ and $\delta(g,a,b') = 0$ otherwise.

Proof. First suppose that $g \equiv a \mod f$ and $\frac{g}{X^{\deg g}} \equiv b' \mod X^{-c}k[X^{-1}]$. Then

$$\sum_{\chi \in \mathcal{X}(f,c)} \chi(g)\overline{\chi_1(a)\chi_\infty(b')} = \sum_{\chi \in \mathcal{X}(f,c)} 1 = \#\mathcal{X}(f,c).$$

by Theorem 4.1.2.

Now suppose that $g \not\equiv a \mod f$ or $\frac{g}{X^{\deg g}} \not\equiv b' \mod X^{-c}k[X^{-1}]$. Then there is $\psi \in \mathcal{X}(f,c)$ such that $\psi_1(a)\psi_\infty(b') \neq \psi(g)$. We have

$$\psi(g)\overline{\psi_1(a)\psi_\infty(b')} \sum_{\chi \in \mathcal{X}(f,c)} \chi(g)\overline{\chi_1(a)\chi_\infty(b')} =$$

$$\sum_{\chi \in \mathcal{X}(f,c)} \psi(g)\chi(g)\overline{\psi_1(a)\chi_1(a)\psi_\infty(b')\chi_\infty(b')} = \sum_{\chi' \in \mathcal{X}(f,c)} \chi'(g)\overline{\chi'_1(a)\chi'_\infty(b')}.$$

Hence, since $\psi(g)\overline{\psi_1(a)\psi_\infty(b')} \neq 1$, it follows that $\sum_{\chi \in \mathcal{X}(f,c)} \chi(g)\overline{\chi_1(a)\chi_\infty(b')} = 0$. □

Definition 4.1.4. We define $A_{n,f} = \sum_j \deg j$ where j ranges over all monic irreducible factors of f such that $\deg j \mid n$. We define $B_{n,f} = \sum_j \deg j$ where j ranges over all monic irreducible polynomials that do not divide f such that $\deg j \mid n$ and $\deg j < n$.

The next theorem is a generalization of what is done in [**4**], pp. 44-45.

Theorem 4.1.5. *Let k be a finite field with q elements, let χ be a character of $k[X]$ with modulus (f, c) and conductor (g, δ) and let $L(T, \chi)$ be the L-function of χ. Then we have*

$$T\frac{d\log}{dT}L(T,\chi) = \sum_{n=1}^{\infty} a_n T^n$$

where all a_n are complex numbers such that $a_n = q^n - A_{n,f}$ if χ is principal and $|a_n| \leq (\deg g + \delta - 2)q^{n/2} + \max\{0, 1-\delta\} + A_{n,f} - A_{n,g}$ if χ is not principal.

Proof. In both cases we use Theorem 2.1.10. In the case that χ is principal we have

$$T\frac{d\log}{dT}L(T,\chi) = T\frac{d\log}{dT}\left(\frac{1}{1-qT}\cdot\prod_h(1-T^{\deg h})\right)$$

where h ranges over all monic irreducible factors of f. Using geometric expansions we see that

$$T\frac{d\log}{dT}\left(\frac{1}{1-qT}\cdot\prod_h(1-T^{\deg h})\right) = \sum_{n=1}^{\infty} q^n T^n - \sum_h\left(\sum_{n=1}^{\infty}(\deg h)T^{n\deg h}\right).$$

So the coefficient of $T\frac{d\log}{dT}L(T,\chi)$ at T^n is equal to $q^n - \sum_h \deg h$ where h ranges over all monic irreducible factors of f such that $\deg h \mid n$. This proves the first case of the theorem.

In the case that χ is non-trivial we have

$$T\frac{d\log}{dT}L(T,\chi) =$$

$$T\frac{d\log}{dT}\left(\prod_{i=1}^{\deg g - 2 + \delta}(1-\alpha_i T)\cdot(1-T)^{\max\{0,1-\delta\}}\cdot\prod_h(1-\psi(h)T^{\deg h})\right)$$

where h ranges over all monic irreducible factors of f that do not divide g and ψ is the primitive character that induces χ. Again making use of geometric expansions we see that

$$T\frac{d\log}{dT}L(T,\chi) =$$

$$-\sum_{i=1}^{\deg g-2+\delta}\sum_{n=1}^{\infty}(\alpha_i T)^n - \max\{0,1-\delta\}\sum_{n=1}^{\infty}T^n - \sum_h\sum_{n=1}^{\infty}(\deg h)\psi(h)^n T^{n\deg h}.$$

So the coefficient of $T\frac{d\log}{dT}L(T,\chi)$ at T^n is equal to $-\sum_{i=1}^{\deg g-2+\delta}\alpha_i^n - \max\{0, 1-\delta\} - \sum_h(\deg h)\psi(h)^{\frac{n}{\deg h}}$ where h ranges over all monic irreducible factors of f that do not divide g such that $\deg h \mid n$. By the triangle inequality this proves the second part of the theorem. □

Theorem 4.1.6. *Let k be a finite field with q elements and let χ be a character of $k[X]$ with modulus (f, c) and conductor (g, δ). Let I_n be the set of monic irreducible polynomials of degree n with $n > 0$. Then*

$$\sum_{h \in I_n} \chi(h) = \frac{q^n - A_{n,f} - B_{n,f}}{n}$$

if χ is principal and

$$\left| \sum_{h \in I_n} \chi(h) \right| \leq \frac{(\deg g + \delta - 2)q^{n/2} + \max\{0, 1-\delta\} + A_{n,f} - A_{n,g} + B_{n,f}}{n}$$

otherwise. Furthermore, we have $A_{n,f} \leq \deg f$ and $A_{n,f} - A_{n,g} \leq \deg f - \deg g$ and we have $B_{n,f} \leq \frac{q^{\frac{n}{2}+1}-1}{q-1}$.

Proof. The trick is to calculate $T\frac{d\log}{dT}L(T,\chi)$ in a different way, namely via Proposition 2.1.8. We have

$$T\frac{d\log}{dT}L(T,\chi) = T\frac{d\log}{dT}\left(\prod_{h \in k[X]} \frac{1}{1-\chi(h)T^{\deg h}}\right)$$

where the product is taken over the monic irreducible polynomials h in $k[X]$. The standard calculation using geometric series shows that the coefficient of $T\frac{d\log}{dT}L(T,\chi)$ at T^n is equal to $\sum_h (\deg h)\chi(h)^{\frac{n}{\deg h}}$ where the sum is taken over all monic irreducible h such that $\deg h \mid n$. First suppose that χ is principal. Then we know by Theorem 4.1.5 that the coefficient of $T\frac{d\log}{dT}L(T,\chi)$ at T^n is equal to $q^n - A_{n,f}$. So we have an equality

$$\sum_h (\deg h)\chi(h) = q^n - A_{n,f}$$

where the sum is taken over all monic irreducible h such that $\deg h \mid n$. Hence we see that

$$\sum_{h \in I_n} n\chi(h) = q^n - A_{n,f} - \sum_j (\deg j)\chi(j)$$

where the latter sum is taken over all monic irreducible j such that $\deg j \mid n$ and $\deg j < n$. This proves the first part of the theorem.

In the case that χ is nontrivial, Theorem 4.1.5 shows that that the coefficient of $T\frac{d\log}{dT}L(T,\chi)$ at T^n is at most $(\deg g + \delta - 2)q^{n/2} + \max\{0, 1-\delta\} + A_{n,f} - A_{n,g}$. So we have

$$\left| \sum_h (\deg h)\chi(h)^{\frac{n}{\deg h}} \right| \leq$$

$$(\deg g + \delta - 2)q^{n/2} + \max\{0, 1-\delta\} + A_{n,f} - A_{n,g}$$

where the sum is taken over all monic irreducible h such that $\deg h \mid n$. In this case we have

$$\left| \sum_{h \in I_n} n\chi(h) \right| \leq (\deg g + \delta - 2)q^{n/2} + \max\{0, 1-\delta\} + A_{n,f} - A_{n,g} + \left| \sum_j (\deg j)\chi(j)^{\frac{n}{\deg j}} \right|$$

where the latter sum is taken over all monic irreducible j such that $\deg j \mid n$ and $\deg j < n$. Now using the triangle inequality on $\left|\sum_j (\deg j)\chi(j)^{\frac{n}{\deg j}}\right|$, the second part of the theorem has been proved.

For the third part, note that the sum of the degrees of the factors of f is equal to $\deg f$, so $A_{n,f}$ cannot be bigger than $\deg f$. More precisely, we have $A_{n,f} = \deg f - \sum_h (n_h - 1)\deg h$ where h ranges over the irreducible h such that $\deg h \mid f$ and $\deg h \mid n$, and where n_h is the number of factors of h in f. This way we immediately see that $A_{n,g} \geq \deg g - \sum_h (n_h - 1)\deg h$ and hence $A_{n,f} - A_{n,g} \leq \deg f - \deg g$. The first part also shows that the number of irreducible polynomials of degree n is at most $\frac{q^n}{n}$ (take $f = 1$ and χ principal). So using geometric expansions we have $B_{f,n} \leq \frac{q^{\frac{n}{2}+1}-1}{q-1}$. □

We also have the following slightly weaker bound which is more suitable for the applications.

Corollary 4.1.7. *For all $n > 0$ we have*

$$\left|\sum_{h\in I_n} \chi(h)\right| \leq \frac{(\deg f + c - 2)q^{n/2} + B_{n,f}}{n}.$$

Proof. We have

$$(\deg g + \delta - 2)q^{n/2} + \max\{0, 1-\delta\} + A_{n,f} - A_{n,g} + B_{n,f} \leq$$
$$(\deg g + c - 2)q^{n/2} + A_{n,f} - A_{n,g} + B_{n,f}$$

since $c \geq 1$ per definition. Moreover,

$$(\deg g + c - 2)q^{n/2} + A_{n,f} - A_{n,g} + B_{n,f} \leq (\deg g + c - 2)q^{n/2} + \deg f - \deg g + B_{n,f}.$$

by the last part of Theorem 4.1.6. Since $\deg f - \deg g \leq q^{n/2}(\deg f - \deg g)$ we have

$$(\deg g + c - 2)q^{n/2} + \deg f - \deg g + B_{n,f} \leq (\deg f + c - 2)q^{n/2} + B_{n,f},$$

which proves the corollary. □

Remark 4.1.8. In the next two sections we will mostly be using Corollary 4.1.7 since usually the conductor (g, δ) in Theorem 4.1.6 is not known. In special cases where g or δ is known one might achieve stronger bounds by using Theorem 4.1.6 though.

2. Multiplicative groups

Theorem 4.2.1. *Let k be a finite field with q elements and let $f \in k[X]$ such that $f \neq 0$. Let $A_{n,f}$ and $B_{n,f}$ as in Definition 4.1.4. Then for any n such that $q^n > (\deg f - 1)q^{n/2} + A_{n,f} + 2B_{n,f}$ the set of monic irreducible polynomials in $k[X]$ of degree n that are coprime to f generates $(k[X]/fk[X])^*$.*

Proof. Let $n \in \mathbf{Z}_{>0}$ and suppose the group generated by J_n (the set of monic irreducible polynomials of degree n that are coprime to f) in $(k[X]/fk[X])^*$ is not equal to $(k[X]/fk[X])^*$. Then there is a maximal subgroup M such that $J_n \subset M \subsetneq (k[X]/fk[X])^*$. There is a nontrivial homomorphism $\chi_1 : (k[X]/fk[X])^* \to \mathbf{C}^*$ such that $M = \ker \chi_1$.

We know by 4.1.6 that

$$\#J_n = \frac{q^n - A_{n,f} - B_{n,f}}{n}.$$

Since J_n is contained in $\ker \chi_1$ and χ_1 is nontrivial, we can also bound J_n in another way. Clearly, we can extend χ_1 to a character χ with modulus $(f, 1)$. We have

$$\#J_n = \sum_{h \in J_n} 1 = \sum_{h \in J_n} \chi(h) = \sum_{h \in I_n} \chi(h)$$

using that $\chi(h) = 1$ for all $h \in J_n$ and $\chi(h) = 0$ if $(h, f) \neq 1$. Now we can apply Corollary 4.1.7, which tells us that

$$\left| \sum_{h \in I_n} \chi(h) \right| \leq \frac{(\deg f + c - 2) q^{n/2} + B_{n,f}}{n},$$

so we have

$$\#J_n \leq \frac{(\deg f - 1) q^{n/2} + B_{n,f}}{n}$$

since $c = 1$. Hence for any n such that

$$\frac{q^n - A_{n,f} - B_{n,f}}{n} > \frac{(\deg f - 1) q^{n/2} + B_{n,f}}{n}$$

we have a contradiction. It follows immediately that for any n such that

$$q^n > (\deg f - 1) q^{n/2} + A_{n,f} + 2B_{n,f}$$

J_n cannot be contained in any maximal subgroup M of $(k[X]/fk[X])^*$. So in this case the elements of J_n generate $(k[X]/fk[X])^*$, which is what we wanted to prove. □

Theorem 4.2.1 yields us some interesting corollaries.

Corollary 4.2.2. *Let k be a field with q elements and let $f \in k[X]$ be irreducible of degree greater than 1. Then $(k[X]/f \cdot k[X])^*$ is generated by the set of residue classes of the monic linear polynomials if* $\deg f < q^{1/2} + 1$.

Proof. Theorem 4.2.1 tells that the monic linear polynomials will generate $(k[X]/fk[X])^*$ if $q > (\deg f - 1) q^{1/2} + A_{1,f} + 2B_{1,f}$. Since f is irreducible of degree greater than 1 we have $A_{1,f} = B_{1,f} = 0$. So just getting $\deg f$ to the left of the equation proves the corollary. □

The following corollary is Theorem 1.1.1 from the introduction.

Corollary 4.2.3. *Let k be a field with q elements, let $f \in k[X]_{\neq 0}$ and let $n \in \mathbf{Z}_{>0}$. Then $(k[X]/fk[X])^*$ is generated by the set of residue classes of the monic irreducible polynomials of degree n coprime to f if $n \geq 2\log_q(\deg f + 4)$.*

Proof. Suppose

$$n \geq 2 \log_q(\deg f + 4),$$

then

$$q^{n/2} \geq \deg f + 4.$$

So then it follows that

$$q^n - (\deg f + 3) q^{n/2} - \deg f = q^{n/2}(q^{n/2} - \deg f - 3) - \deg f \geq$$
$$(\deg f + 4)(\deg f + 4 - \deg f - 3) - \deg f = 4 > 0.$$

So we have

$$q^n > (\deg f + 3)q^{n/2} + \deg f.$$

Further rewriting shows

$$q^n > (\deg f - 1)q^{n/2} + \deg f + 4q^{n/2}.$$

Note that we have $\frac{q^{n/2+1}-1}{q-1} < 2q^{\frac{n}{2}}$, so

$$q^n > (\deg f - 1)q^{n/2} + \deg f + 2\frac{q^{n/2+1}-1}{q-1}.$$

Now we use the fact that

$$A_{n,f} + 2B_{n,f} \leq \deg f + 2\frac{q^{n/2+1}-1}{q-1}$$

(this is the last part of Theorem 4.1.6). Hence it follows that

$$q^n > (\deg f - 1)q^{n/2} + A_{n,f} + 2B_{n,f}.$$

Now Theorem 4.2.1 proves the corollary. □

3. Primes in arithmetic progressions

In this section we are going to prove a function field-version of Dirichlet's theorem on primes in arithmetic progressions. We recall the definition and the theorem already stated in the introduction.

Definition 4.3.1. Let $a, f \in k[X]_{\neq 0}$ such that $(a, f) = 1$, let $b = (b_1, \ldots, b_{c-1})$ be an element of k^{c-1} for $c \in \mathbf{Z}_{>0}$ and let $n \in \mathbf{Z}_{>0}$. Then we define $S_n(a, f, b, c)$ be the set of monic irreducible polynomials g of degree n such that $g \equiv a \mod f$ and $\frac{g}{X^n} \equiv 1 + \sum_{i=1}^{c-1} b_i X^{-i} \mod X^{-c}k[X^{-1}]$.

Theorem 4.3.2. *Let $a, f \in k[X]_{\neq 0}$ such that $(a, f) = 1$, let b be an element of k^{c-1} for $c \in \mathbf{Z}_{>0}$ and let $n \in \mathbf{Z}_{>0}$. Then*

$$\left| \#S_n(a, f, b, c) - \frac{q^{n-c+1}}{n\Phi(f)} \right| \leq \frac{\max\{\frac{q}{q-1}, \deg f + c - \frac{q-2}{q-1}\} \cdot q^{n/2}}{n}.$$

Proof. We make use of the orthogonality relation in Theorem 4.1.3. Let $\mathcal{X}(f, c)$ be the group of characters with modulus (f, c). Let $b' = 1 + \sum_{i=1}^{c-1} b_i X^{-i}$. Then the orthogonality relation tells us that

$$\sum_{\chi \in \mathcal{X}(f,c)} \chi(g)\overline{\chi_1(a)\chi_\infty(b')} = \Phi(f)q^{c-1}$$

if $g \equiv a \mod f$ and $\frac{g}{X^{\deg g}} \equiv b' \mod X^{-c}k[X^{-1}]$, and

$$\sum_{\chi \in \mathcal{X}(f,c)} \chi(g)\overline{\chi_1(a)\chi_\infty(b')} = 0$$

otherwise. So this shows that

$$\sum_{g} \sum_{\chi \in \mathcal{X}(f,c)} \chi(g)\overline{\chi_1(a)\chi_\infty(b')} = \#S_n(a, f, b, c)\Phi(f)q^{c-1}$$

where the first sum is taken over all monic irreducible polynomials g of degree n. Rewriting shows that

$$\#S_n(a,f,b,c) = \frac{1}{\Phi(f)q^{c-1}} \sum_{\chi \in \mathcal{X}(f,c)} \sum_g \chi(g)\overline{\chi_1(a)\chi_\infty(b')}$$

where the second sum is taken over all monic irreducible polynomials g of degree n. If $\chi = \chi_0$, the principal character, then we have by Theorem 4.1.6

$$\sum_g \chi(g)\overline{\chi_1(a)} = \frac{q^n - A_{n,f} - B_{n,f}}{n}.$$

We take $\frac{q^n}{n}$ to the left in the equation, hence we have

$$\#S_n(a,f,b,c) - \frac{q^n}{n\Phi(f)q^{c-1}} =$$

$$\frac{1}{\Phi(f)q^{c-1}} \left(\sum_{\chi \in \mathcal{X}(f,c)\setminus\{\chi_0\}} \sum_g \chi(g)\overline{\chi_1(a)\chi_\infty(b')} - \frac{A_{n,f} - B_{n,f}}{n} \right)$$

so in particular

$$\left| \#S_n(a,f,b,c) - \frac{q^n}{n\Phi(f)q^{c-1}} \right| =$$

$$\left| \frac{1}{\Phi(f)q^{c-1}} \left(\sum_{\chi \in \mathcal{X}(f,c)\setminus\{\chi_0\}} \sum_g \chi(g)\overline{\chi_1(a)\chi_\infty(b')} - \frac{A_{n,f} - B_{n,f}}{n} \right) \right|.$$

The left side of the equation is already as in the theorem. We need to estimate the right side, this comes down to estimating

$$\left| \sum_{\chi \in \mathcal{X}(f,c)\setminus\{\chi_0\}} \sum_g \chi(g)\overline{\chi_1(a)\chi_\infty(b')} - \frac{A_{n,f} + B_{n,f}}{n} \right|.$$

Now we apply Corollary 4.1.7. First, applying a triangle inequality, we have

$$\left| \sum_{\chi \in \mathcal{X}(f,c)\setminus\{\chi_0\}} \sum_g \chi(g)\overline{\chi_1(a)\chi_\infty(b')} - \frac{A_{n,f} + B_{n,f}}{n} \right|$$

$$\leq \sum_{\chi \in \mathcal{X}(f,c)\setminus\{\chi_0\}} \left| \sum_g \chi(g) \right| + \frac{A_{n,f} + B_{n,f}}{n}.$$

For all non-trivial characters we have

$$\left| \sum_g \chi(g) \right| \leq \frac{(\deg f + c - 2)q^{n/2} + B_{n,f}}{n}.$$

Note that there are $\Phi(f)q^{c-1} - 1$ characters that are non-trivial, so we get

$$\left| \#S_n(a,f,b,c) - \frac{q^{n-c+1}}{n\Phi(f)} \right| \leq$$

$$\frac{(\Phi(f)q^{c-1} - 1)(\deg f + c - 2)q^{n/2} + \Phi(f)q^{c-1}B_{n,f} + A_{n,f}}{n\Phi(f)q^{c-1}}.$$

We would like to estimate $(\Phi(f)q^{c-1}-1)(\deg f+c-2)q^{n/2}+A_{n,f}$ by $\Phi(f)q^{c-1}(\deg f+c-2)q^{n/2}$. Then by the facts that $B_{n,f} \leq \frac{q^{n/2+1}-1}{q-1}$ and $\frac{q^{\frac{n}{2}+1}-1}{q-1} < \frac{q}{q-1} \cdot q^{n/2}$ the main theorem follows.

We have

$$(\Phi(f)q^{c-1}-1)(\deg f+c-2)q^{n/2}+A_{n,f} \leq \Phi(f)q^{c-1}(\deg f+c-2)q^{n/2}$$

if and only if

$$A_{n,f} \leq (\deg f+c-2)q^{n/2}.$$

We know that $A_{n,f} \leq \deg f$. So the inequality is always satisfied if $c > 1$. Now assume $c = 1$. Then we would like to know in which cases we have

$$A_{n,f} \leq (\deg f-1)q^{n/2}.$$

If $\deg f > 3$ this is always the case since $4 < 3\sqrt{2} \leq 3q^{n/2}$. In the case that $\deg f = 2$ or $\deg f = 3$ the inequality is satisfied if $n > 1$. So it is clear which exceptions we need to treat.

First suppose $\deg f = 0$ and $c = 1$. Then, since $\Phi(f) = 1$, we have

$$\frac{(\Phi(f)q^{c-1}-1)(\deg f+c-2)q^{n/2}+\Phi(f)q^{c-1}B_{n,f}+A_{n,f}}{n\Phi(f)q^{c-1}} =$$

$$\frac{B_{n,f}}{n} < \frac{\frac{q}{q-1}\cdot q^{n/2}}{n}$$

which is correct.

Now suppose $\deg f = 1$ and $c = 1$. Then, since $\Phi(f) = q-1$, we have

$$\frac{(\Phi(f)q^{c-1}-1)(\deg f+c-2)q^{n/2}+\Phi(f)q^{c-1}B_{n,f}+A_{n,f}}{n\Phi(f)q^{c-1}} =$$

$$\frac{(q-1)B_{n,f}+1}{n(q-1)} \leq \frac{q^{n/2+1}-1+1}{n(q-1)} = \frac{\frac{q}{q-1}\cdot q^{n/2}}{n}$$

which is again correct.

Now suppose $\deg f > 1$, $c = 1$ and $n = 1$. Then $\#S_n(a,f,b,c) = 0$ or $\#S_n(a,f,b,c) = 1$. Also, $\frac{q^{n-c+1}}{n\Phi(f)} = \frac{q}{\Phi(f)} < 1$. So

$$\left|\#S_1(a,f,b,c) - \frac{q^{n-c+1}}{n\Phi(f)}\right| = \left|\#S_1(a,f,b,c) - \frac{q}{\Phi(f)}\right| < 1,$$

confirming the theorem.

□

Finally we calculate a lower bound on n such that $\#S_n(a,f,b,c) > 0$.

Corollary 4.3.3. *If $n > 2(c+\deg f+\log_q(\deg f+c-\frac{q-2}{q-1}))$ we have $\#S_n(a,f,b,c) > 0$.*

Proof. Assume

$$n > 2(c + \deg f + \log_q(\deg f + c - \frac{q-2}{q-1})).$$

Then we also have

$$n/2 - c - \deg f > \log_q(\deg f + c - \frac{q-2}{q-1})$$

and

$$q^{n/2-c-\deg f} > \deg f + c - \frac{q-2}{q-1}.$$

Since $q^{\deg f} > \Phi(f)$ we have

$$\frac{q^{n/2-c}}{\Phi(f)} > \deg f + c - \frac{q-2}{q-1}.$$

Multiplying by $\frac{q^{n/2}}{n}$, we finally get

$$\frac{q^{n-c}}{n\Phi(f)} > \frac{(\deg f + c - \frac{q-2}{q-1})q^{n/2}}{n},$$

implying that $\#S_n(a, f, b, c) > 0$ if $\frac{q}{q-1} \leq \deg f + c - \frac{q-2}{q-1}$. This is the case if $\deg f + c \geq 2$, so the only exception we have to consider is $\deg f = 0$ and $c = 1$. Since we know $\#S_n(1, 1, (), 1) > 0$ for all $n \geq 1$, the corollary has been proved.

□

Bibliography

[1] E. Bach: *Explicit Bounds for Primality testing and Related Problems*, Mathematics of Computation 55, pp. 355-380, 1990

[2] B. Edixhoven, L. Taelman: *Mastermath Algebraic Geometry*, www.math.leidenuniv.nl/∼astolk/ag/ag-notes.pdf (notes written by M. Kosters), 2009

[3] S. Lang: *Algebraic Number Theory*, Springer-Verlag, 1986

[4] M. Rosen: *Number theory in function fields*, Springer, 2002

[5] V. Shoup: *Searching for Primitive Roots in Finite Fields*, Mathematics of Computation 58, pp. 369-380, 1992

[6] P. Stevenhagen: *Algebra 3*, http://websites.math.leidenuniv.nl/algebra/, 2008

[7] P. Stevenhagen: *Local Fields*, http://websites.math.leidenuniv.nl/algebra/, 2002

[8] H. Stichtenoth: *Algebraic function fields and codes*, Springer-Verlag, 1993

[9] A. Weil: *Basic Number theory*, Third edition, Springer-Verlag, 1974