Riemann-Roch Theory for Function Fields

Andrei Jorza

March 15, 2005

1 Motivation

Let K be a global field (i.e., K is a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_q(x)$).

Definition 1.1. The ζ-function is

$$\zeta_K(s) = \sum_I \frac{1}{\mathbf{N}I^s},$$

where I runs through all the ideals of $\mathcal{O}_K$.

Proposition 1.2. *We have*

$$\zeta_K(s) = \prod_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}_K} \frac{1}{1-\mathbf{N}\mathfrak{p}^{-s}}.$$

Proof. There are sensible convergence issues here, but we will not worry about these. Since $\mathcal{O}_K$ is a Dedekind domain, with unique factorization, every ideal $I = \mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_k^{n_k}$ so

$$\zeta_K(s) = \sum(\mathbf{N}\mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_k^{n_k})^{-s} = \prod_{\mathfrak{p}_i}\sum_{n_i=0}^{\infty}(\mathbf{N}\mathfrak{p}_i)^{-n_i s} = \prod_{\mathfrak{p}_i}\frac{1}{1-\mathbf{N}\mathfrak{p}_i^{-s}}.$$

□

The $\zeta_K(s)$ clearly converges for $\mathrm{Re}\, s > 1$ and moreover it has an analytic continuation to $\mathbb{C}\setminus\{1\}$.

Theorem 1.3 (Dirichlet's Class Number Formula). *If K is a number field then the residue of ζ_K at 1 is*

$$vol(\mathbb{A}_K^\times/K^\times) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{w_K\sqrt{|D_K|}}.$$

This can be rewritten as

$$\zeta_K^{r_1+r_2-1}(0) = -\frac{h_K R_K}{w_K},$$

which looks exactly like the Birch And Swinnerton-Dyer conjecture since the rank of $\mathbb{G}_m(\mathcal{O}_K)$ *is* $r_1 + r_2 - 1$.

One way to prove this is to relate ζ_K to ζ-functions associated to characters $\mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$ and then use harmonic analysis. We will not prove this theorem here but we'll see more of this analogy later when we study elliptic curves.

2 Riemann-Roch on Function Fields

2.1 Divisors on Adèles

We would like to obtain similar formulas for function fields.

Let K be a finite extension of $\mathbb{F}_q(x)$. Recall the topological rings $K^\times \hookrightarrow \mathbb{A}_K^1 \hookrightarrow \mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K$. For each finite place v of K (all places are finite!) recall that we have $K_v, \mathcal{O}_v, \wp_v, k_v/\mathbb{F}_q, q_v = q^{d_v}$.

Definition 2.1. $\mathrm{Div}(K)$ is the free abelian group generated by the (finite) places v of K, i.e. $\mathrm{Div}(K) = \bigoplus_v v\mathbb{Z}$. The map $\mathrm{Div}(K) \to \mathbb{Z}$ given by $\deg : \sum n_v v \mapsto \sum n_v d_v$ is a homomorphism with kernel $\mathrm{Div}^0(K)$.

There is an obvious map $\mathbb{A}_K^\times \to \mathrm{Div}(K)$ given by $\mathrm{div} : \mathfrak{a} = (a_v) \mapsto \sum v(a_v)v$, a homomorphism. Then we clearly have $|\mathfrak{a}|_{\mathbb{A}} = q^{-\deg \mathfrak{a}}$ so this gives

Lemma 2.2. *The map* div *is a surjection from* $\mathbb{A}_K^1$ *to* $\mathrm{Div}^0(K)$ *with kernel* $\prod \mathcal{O}_v^\times$.

Let $P(K) = \mathrm{div}(K^\times)$ be the principal divisors. Then write $\mathrm{Pic}(K) = \mathrm{Div}(K), \mathrm{Pic}^0(K) = \mathrm{Div}^0(K)/P(K)$.

Proposition 2.3. *There is an isomorphism* $Cl(K) \cong \mathrm{Pic}^0(K)$ *which proves that* $Cl(K)$ *is finite.*

Proof. There is an isomorphism between the group of fractional ideals and $\mathbb{A}_K^1$. Moreover, the group $\mathbb{A}_K^1/K^\times$ is compact and $\prod \mathcal{O}_v^\times$ is open so $\mathrm{Pic}^0(K) \cong \mathbb{A}_K^1/K^\times \prod \mathcal{O}_v^\times$ is finite. □

2.2 Invertible sheaves associated with divisors

Definition 2.4. For $\mathfrak{a} = \sum a_v v \in \mathrm{Div}(K)$ let $U(\mathfrak{a}) = \{b = (b_v) \in \mathbb{A}_K^\times | |b_v|_v \leq q_v^{-a_v}\} = \prod \{b \in K_v^\times | |b|_v \leq q_v^{-a_v}\}$ which is compact by Tychonov since each factor is compact. Let $\mathcal{L}(\mathfrak{a}) = (U(\mathfrak{a}) \cap K^\times) \cup \{0\}$. This is compact in $K^\times$ which is discrete, so $\mathcal{L}(\mathfrak{a})$ is a finite $K \cap \prod \mathcal{O}_v$ module. Since $K \cap \prod K_v = \mathbb{F}_q$ we get $|\mathcal{L}(\mathfrak{a})| = q^{\ell(\mathfrak{a})}$ where $\ell(\mathfrak{a}) = \dim_{\mathbb{F}_q} \mathcal{L}(\mathfrak{a})$.

Lemma 2.5. *If* $\deg \mathfrak{a} < 0$ *then* $\mathcal{L}(\mathfrak{a}) = 0$. *If* $\deg \mathfrak{a} = 0$ *but* $\mathfrak{a} \neq 0$ *in* $\mathrm{Pic}(K)$ *then* $\mathcal{L}(\mathfrak{a}) = 0$.

Proof. $\mathcal{L}(\mathfrak{a})$ consists of elements $x \in K^\times$ such that $|x|_{\mathbb{A}} = q^{-\deg \mathfrak{a}} > 1$ which cannot be unless $\mathfrak{a} = 0$.

If $\deg \mathfrak{a} = 0$ then the above proof shows that the only possible nonzero element in $\mathcal{L}(\mathfrak{a})$ must be $x \in K^\times$ such that $x_v = -a_v$ which means that $\mathfrak{a} = \mathrm{div} x = 0$ in $\mathrm{Pic}(K)$ contradicting the hypothesis. □

Lemma 2.6. *Prove that* $\mathcal{L}(\mathfrak{a})$ *can be identified with divisors* $\mathfrak{b} \in \mathrm{Div}(K)$ *such that* $\mathfrak{b} \geq 0$ *and* $\mathfrak{b} = \mathfrak{a} \in \mathrm{Pic}(K)$.

Proof. $\mathcal{L}(\mathfrak{a}) = K \cap \{\mathfrak{b} \in \mathbb{A}_K | v(\mathfrak{b}_v) + v(a_v) \geq 0\}$. So the divisor $\mathfrak{b} + \mathfrak{a}$ is nonnegative and is clearly linearly equivalent to $\mathfrak{a}$ since $\mathfrak{b} \in K$. □

Remark 2.7. We have $\ell(0) = 1$ which corresponds to the fact that $\mathcal{L}(0) = K^\times \cap \prod \mathcal{O}_v = \mathbb{F}_q$.

Lemma 2.8. *If* I *is an ideal of* $\mathcal{O}_K$ *then* $\mathbf{N}I = q^{\deg(\mathrm{div} \circ ideal(I))}$, *where* $ideal : I = \prod \mathfrak{p}_v^{n_v} \mapsto (\pi_v^{n_v})$ *for uniformizers* $\pi_v \in K_v$.

Proof. Assume that $I = \prod \mathfrak{p}_v^{n_v}$ then $\mathrm{div} \circ \mathrm{ideal} I = \sum n_v v$ while $\mathbf{N}I = q^{\sum n_v d_v} = q^{\deg(\mathrm{div} \circ \mathrm{ideal}(I))}$. □

2.3 The canonical divisor

Let $\chi : \mathbb{A}_K/K \to \mathbb{C}^\times$ be a nontrivial character, which corresponds to a collection of local characters $\chi_v : K_v \to \mathbb{C}^\times$ that are trivial on $\mathcal{O}_v$ for almost all v. Let $\mathrm{ord}(\chi_v)$ be the smallest integer n_v such that χ_v is trivial on $\wp_v^{n_v}$. Then $\mathrm{ord}(\chi) = \sum \mathrm{ord}(\chi_v) v \in \mathrm{Div}(K)$.

Proposition 2.9. *Let* χ' *be another nontrivial character of* $\mathbb{A}_K/K$. *Then* $\mathrm{ord}(\chi) = \mathrm{ord}(\chi')$ *in* $\mathrm{Pic}(K)$.

Proof. Characters are defined up to scalar action so for each v there exists a $b_v \in K_v^\times$ such that $\chi'_v(x) = \chi_v(b_v x)$ which means that $\chi'(x) = \chi(bx)$ where $b = (b_v)_v \in \mathbb{A}_K$. But χ and χ' are trivial on K by definition so $\chi(b) = 1$ which implies that $\mathrm{ord}(\chi') = \mathrm{ord}(\chi(b)) = \mathrm{ord}(\chi) + \mathrm{div}(b) = \mathrm{ord}(\chi)$ since $b \in K$. □

Definition 2.10. There exists a unique divisor $\mathfrak{c} = \mathrm{ord}(\chi)$ for some χ nontrivial character of $\mathbb{A}_K/K$. This is called the canonical divisor and $\ell(\mathfrak{c}) = g$ is called the genus of K. (For number fields there are analogous notions genus of K coming from Arakelov geometry.)

2.4 Topological duality

For a topological group G we define the topological dual $\widehat{G} = \mathrm{Hom}_{\text{continuous}}(G, \mathbb{C}^\times)$. Fix χ a nontrivial character of $\mathbb{A}_K/K$ for which $\mathfrak{c} = \mathrm{ord}(\chi)$. The map $a \mapsto \chi(a-)$ identifies $\mathbb{A}_K$ to its topological dual.

Lemma 2.11. *If $H \subset G$ is an open topological subgroup and $H^\perp = \{f \in \widehat{G} | f(H) = 1\}$ then $\widehat{G/H} \cong H^\perp$. Moreover, G is compact if $\hat{G}$ is discrete and G is discrete if $\hat{G}$ is compact. Via topological duals the exact sequence*

$$1 \to H \to G \to G/H \to 1$$

becomes

$$1 \to H^\perp \to \hat{G} \to \hat{H} \to 1.$$

If G/H is compact and H is discrete in G then the measure on G is the composite of the discrete measure on H and the Haar measure on G/H.

Remark 2.12. This shows that $\widehat{\mathbb{A}_K/K} = K$ is discrete.

Lemma 2.13. *For $\mathfrak{a} \in \mathrm{Div}(K)$ we write $U = U(\mathfrak{a})$ and $U'(\mathfrak{c} - \mathfrak{a})$. Then $\mathbb{A}_K/(K+U)$ is the topological dual of $K \cap U'$.*

Proof. It is enough to show that $(K+U)^\perp \cong K \cap U'$. First, $(K+U)^\perp \subset K^\perp = K$. Now under the indentification $\mathbb{A}_K \cong \widehat{\mathbb{A}_K}$ the set $(K+U)^\perp$ consists of $x \in \mathbb{A}_K$ such that $\chi(x(K+U)) = 1$. This happens if and only if $\chi(x(k+b)) = 1$ for all $k \in K$ and b such that $|b|_v \le q_v^{-a_v}$. Therefore we want $\chi_v(x_v(k_v + b_v)) = 1$ which happens for all $x_v(k_v + b_v) \in \wp_v^{\mathrm{ord}(\chi_v)}$. This happens when $x_v \in \wp_v^{\mathrm{ord}(\chi_v)+a_v}$ so $x \in U'$. Therefore, $(K+U)^\perp = K \cap U'$. □

2.5 Riemann-Roch

Lemma 2.14. *Let μ be a Haar measure on $\mathbb{A}_K$ induced from the discrete measure on K and the normalized Haar measure on $\mathbb{A}_K/K$. Then $\mu(U) = q^{-\deg \mathfrak{a}} = q^{\ell(\mathfrak{a})}\mu((K+U)/U)$. Moreover, $\mu(\mathbb{A}_K/K) = q^{\ell(\mathfrak{c}-\mathfrak{a})}\mu((K+U)/U)$.*

Proof. We have an exact sequence $1 \to K \to \mathbb{A}_K \to \mathbb{A}_K/K \to 1$ in which we have an exact sequence $1 \to K \cap U \to U \to (K+U)/K \to 1$. Therefore $\mu(U) = q^{\ell(\mathfrak{a})}\mu((K+U)/U)$ since $\mu(K \cap U) = \mu(\mathcal{L}(\mathfrak{a}))$. The fact that $\mu(U) = q^{-\deg \mathfrak{a}}$ is immediate from definition.

The last equality follows from the exact sequence $1 \to (K+U)/K \to \mathbb{A}_K/K \to (\mathbb{A}_K/K)/((K+U)/K) = \mathbb{A}_K/(K+U) \to 1$ because $\mu(K \cap U') = q^{\ell(\mathfrak{c}-\mathfrak{a})}$. □

Theorem 2.15 (Riemann-Roch). *For each $\mathfrak{a} \in \mathrm{Div}(K)$ we have*

$$\ell(\mathfrak{a}) = \ell(\mathfrak{c} - \mathfrak{a}) + \deg \mathfrak{a} - g + 1.$$

Proof. From Lemma 2.14 we have

$$\begin{aligned}\mu(\mathbb{A}_K/K) &= q^{\ell(\mathfrak{c}-\mathfrak{a})}\mu((K+U)/U) = q^{\ell(\mathfrak{c}-\mathfrak{a})}q^{-\deg\mathfrak{a}}/q^{\ell(\mathfrak{a})} \\ &= q^{\ell(\mathfrak{c}-\mathfrak{a})-\deg\mathfrak{a}-\ell(\mathfrak{a})}\end{aligned}$$

The theorem follows if say $q^{g-1} = \mu(\mathbb{A}_K/K)$. □

Proposition 2.16. *We have* $\deg\mathfrak{c} = 2g-2$ *and* $g = \ell(\mathfrak{c})$.

Proof. Add $\ell(\mathfrak{a}) = \ell(\mathfrak{c}-\mathfrak{a}) + \deg\mathfrak{a} - g + 1$ and $\ell(\mathfrak{c}-\mathfrak{a}) = \ell(a) + \deg(\mathfrak{c}-\mathfrak{a}) - g + 1$ and get $\deg\mathfrak{c} = 2g-2$. So if $\mathfrak{a} = 0$ in the formula we get $\ell(0) = \ell(\mathfrak{c})+0-g+1$ so $\ell(\mathfrak{c}) = g-1+1 = g$. □

Proposition 2.17. *If* $\deg\mathfrak{a} > 2g-2$ *then* $\ell(\mathfrak{a}) = \deg\mathfrak{a} - g + 1$.

Proof. Then $\deg(\mathfrak{c}-\mathfrak{a}) < 0$ so by Lemma 2.5 we have $\ell(\mathfrak{c}-\mathfrak{a}) = 0$. □

3 Class number formula for function fields

Let's get back to our analogy between the case of number and function fields. Let K be a finite extension of $\mathbb{F}_q(x)$. Recall that $\zeta_K(s) = \sum_I(\mathbf{N}I)^{-s}$ and we have a homomorphism $\mathrm{div}: I \to \mathrm{Div}(K)$ that takes integral ideals to nonnegative divisors.

Lemma 3.1. *There exists* $u \in \mathrm{Div}(K)$ *such that* $\deg u = 1$.

Proof. If $u = \sum n_v v$ then $\deg u = \sum n_v d_v$ so it is enough to prove that the d_v have no common factor. I am not going to prove this, but you can think about what happens if $K = \mathbb{F}_q(x)$ (the analogous case of $K = \mathbb{Q}$ for number fields) and generalize. (See Weil, Basic Number Theory, pp 126 if impatient.) □

Lemma 3.2. *We have*

$$\begin{aligned}\zeta_K(s) &= \sum_{\mathfrak{a}\in\mathrm{Div}_{\geq 0}(K)} q^{\deg\mathfrak{a}} = \sum_{k=0}^{\infty}\sum_{\deg\mathfrak{a}=k,\mathfrak{a}\geq 0} q^{-ks} \\ &= \sum_{\mathfrak{a}_i\in\mathrm{Pic}^0(K)}\sum_{k=0}^{\infty}\sum_{\mathfrak{a}\geq 0,\mathfrak{a}=\mathfrak{a}_i+ku} q^{-ks} \\ &= (q-1)^{-1}\sum_{\mathfrak{a}_i\in\mathrm{Pic}^0(K)}\sum_{k=0}^{\infty} q^{\ell(\mathfrak{a}_i+ku)-ks} - \sum_{\mathfrak{a}_i\in\mathrm{Pic}^0(K)} 1/(1-q^{-s})\end{aligned}$$

Proof. The first equality follows from Lemma 2.8. From Lemma 2.6 we get that the number of $\mathfrak{a} \geq 0$ such that $\mathfrak{a} = \mathfrak{a}_i + ku$ is equal to $(q^{\ell(\mathfrak{a}_i+ku)} - 1)/(q-1)$ (the 0 divisor corresponds to no ideal and any ideal defines a divisor up to a unit of $\mathbb{F}_q^\times$) so the last equality follows. (Here I used that $\mathfrak{a} - ku \in \mathrm{Pic}^0(K)$ must equal one of the $\mathfrak{a}_i$-s, up to scalars, which do not count.) □

Lemma 3.3. *We have* $\sum_{k=0}^{\infty} q^{\ell(\mathfrak{a}_i+ku)-ks} = \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)-ks} + q^{g-s(2g-1)}/(1-q^{1-s})$.

Proof. Recall that for $k > 2g-2$ we have $\ell(\mathfrak{a}_i + ku) = \deg(\mathfrak{a}_i + ku) - g + 1 = k - g + 1$ so $\sum_{k=0}^{\infty} q^{\ell(\mathfrak{a}_i+ku)-ks} = \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)-ks} + \sum_{k>2g-2} q^{k(1-s)-g+1}$ which is equal to $\sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)-ks} + \sum_{k>2g-2} q^{(k-2g+1)(1-s)+g-s(2g-1)} = \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)-ks} + q^{g-s(2g-1))}/(1-q^{1-s})$. □

Proposition 3.4. *There exists a polynomial P of degree $2g$ such that*

$$\zeta_K(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

Proof. By Lemma 3.3 and the fact that $q^{s-s(2g-1)}/(1-q^{1-s})$ and $-1/(1-q^{-s})$ have the above property, it is enough to show that for each i the sum $\sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)-ks}$ has the required property.

But $(1-q^{-s})(1-q^{1-s}) \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)-ks}$ has degree $2g$ in q^{-s} since only the term corresponding to $k = 2g-2$ counts. The conclusion then follows. □

The really interesting facts that are analogous to the analytic class number formula in the case of number fields occur when we apply the Riemann-Roch theory.

Theorem 3.5 (Class number formula). *We have $P(z) = q^g z^{2g} P(1/qz)$.*

Proof. Clearly we can get rid of the $(q-1)^{-1}$ factor for the first part of the problem. Define $P_i(q^{-s}) = (1-q^{-s})(1-q^{1-s}) \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)-ks} + (1-q^{-s})q^{g-s(2g-1)} - (1-q^{1-s})$ so $P_i(z) = (1-z)(1-qz) \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)} z^k + (1-z)q^g z^{2g-1} - (1-qz)$.

We need to show that $\sum_i P_i(z) = q^g z^{2g}(\sum_i P_i(1/qz))$. This is equivalent to $\sum_i((1-z)(1-qz) \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)} z^k + (1-z)q^g z^{2g-1} - (1-qz)) = \sum_i (q^g z^{2g}((1-1/qz)(1-1/z) \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)} q^{-k} z^{-k} + (1-1/qz)q^{-(g-1)} z^{-(2g-1)}) + (1-z)q^g z^{2g-1})$

But the RHS is equal to

$$\sum_i ((1-z)(1-qz) \sum_{k=0}^{2g-2} q^{\ell(a_i+ku)-k+g-1} z^{2g-2-k} + (qz-1) + (1-z)q^g z^{2g-1}).$$

But the Riemann-Roch formula gives that $\ell(a_i + ku) - k + g - 1 = \ell(\mathfrak{c} - \mathfrak{a}_i + ku)$. But $\mathfrak{c} = \mathfrak{a}_1 + (2g-2)u$ for our choice of $\mathfrak{a}_1$.

So we need to show that $\sum_i((1-z)(1-qz) \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_i+ku)} z^k + (1-z)q^g z^{2(g-1)} + (qz-1)) = \sum_i((1-z)(1-qz) \sum_{k=0}^{2g-2} q^{\ell(\mathfrak{a}_1-\mathfrak{a}_i+(2g-2-k)u)} z^{2g-2-k} + (qz-1) + (1-z)q^g z^{2(g-1)})$ which is obvious. □

Proposition 3.6. *We have $P(0) = 1$ and $P(1) = h_K$.*

Proof. We have $P(z) = (q-1)^{-1} \sum_{\mathfrak{a}_i \in \mathrm{Pic}^0(K)} P_i(z)$. Since $P_i(1) = q - 1$ we have $P(1) = (q-1)^{-1} h_K (q-1) = h_K$.

Also note that $\lim_\infty \zeta_K(-s) = 1$ by definition. So $P(0) = 1$. ☐

Proposition 3.7 (Class number formula). *The residue at 0 of ζ_K is*

$$Res_0 \zeta_K(s) = \frac{h_K}{(1-q)\log q}.$$

Proof. The residue at 0 is

$$\lim_{s \to 0} \frac{P(q^{-s})}{1 - q^{1-s}} \frac{s}{1 - q^{-s}} = \frac{h_K}{1-q} \frac{1}{\log q}.$$

☐