L-functions, elliptic curves and the parity conjecture

Benjamin Wagener
Université Pierre et Marie Curie
Paris VI

June 15, 2008

Ce texte est un mémoire de Master de Mathématiques effectué à l'Université Paris 6, Pierre et Marie Curie, pendant l'année scolaire 2007-2008. Ce travail est composé essentiellement de deux parties. Premièrement, je présente le contexte général des fonctions L. Ensuite, après avoir fait quelques rappels sur les courbes elliptiques, je présente un article ([14]) de Tim et Vladimir Dokchitser. J'ai choisi de réaliser ce travail en anglais principalement car je pense que c'est un bon exercice dans le contexte de la recherche actuelle.

Presentation

This work has been done in the context of a training course at the Master "Algèbre et Géométrie" of the University Paris 6, *Pierre et Marie Curie*, during the year 2007-2008. The primary goal of this course is to prepare students to do research in Mathematics by giving them research articles to study. I was directed by the Professor Marc Hindry of Paris 7 University who gave me the article [14] of Tim and Vladimir Dokchitser about a special case of the parity conjecture.

The parity conjecture says that the sign of the functional equation of the L-function of an elliptic curve E over a number field K is equal to $(-1)^{\text{rank } E(K)}$, the group of rational points of E, $E(K)$, been a finitely generated abelian group by the Mordell-Weil theorem. This conjecture is a consequence of the Birch and Swinnerton-Dyer conjecture.

L-function of algebraic varieties are not simple objects and the related theory remains conjectural. That's why I wanted to have some insight into the theoretical framework that underpins this subject. This is what I did in the first part of this work. As such, beginning with classical zeta functions, I motivate the introduction of L-functions of algebraic varieties and their related objects such as $l-$adic representations, $\epsilon-$factors and root numbers. I think that it is a good way to place the article of Tim and Vladimir Dokchitser in its conceptual context. This part is more general that what is needed to [14], however it is only with these ideas in mind that one may fully understand it in my opinion.

The second part of this text is devoted to elliptic curves and the article [14]. First I deal with elliptic curves, I presented what is necessary to understand the text, Weierstrass equations, reduction of elliptic curves, L-functions... The next chapter deals with the article itself. I didn't want to reproduce the article, so I had proofs of facts that could appear not obvious at a first reading. Also I motivated the way the articled is hanged together: $p-$Selmer ranks, root numbers, parity conjecture with a 2-isogeny.

I am grateful to the Professor Marc Hindry who has permitted me to do this work and for his willingness teaching the courses on elliptic curves and on abelian varieties during this academic year.

Benjamin Wagener

Contents

Part I

"L" Generalities

Preliminary remark: *This chapter is a general presentation of L-functions. For this reason there are only few proofs but I tried to add references in the text.*

The history of zeta and L-functions goes back to Euler ,at least, with the Riemann zeta function defined, for $\Re(s) > 1$, by

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}.$$

The zeta function has two properties which are verified by similar functions. First of all, it has an Euler product:

$$\zeta(s) = \prod_{p \,\text{prime}} \frac{1}{1 - p^{-s}}, \quad \text{for } \Re(s) > 1.$$

Secondly, it has an analytic continuation to the whole complex plane with a simple pole at $s = 1$. Furthermore if we define (almost the Mellin transform of ζ) :

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

then ξ satisfies the following functional equation:

$$\xi(s) = \xi(1 - s).$$

These properties link the zeta function with the properties of the set of prime numbers, the crucial conjecture being the still unproved Riemann hypothesis.

There are many generalizations of this, the first to have appeared are known as Dirichlet L-functions, they were generalized to number field and the proof of the corresponding relation was given by Hecke and then the correct conceptual point of view was given by Tate in his Ph.D thesis. This together with a point of view developed by Artin is the origin of the modern standpoint of the subject. The generalization of this to algebraic geometry is still conjectural even if Grothendieck and Deligne, among others, have made the ground work for it.

In this part we are going to present some essential concept of the theory of L-functions, our principal goal being to motivate the notion of L-function associated to elliptic curves and the related concepts.

This part is essentially descriptive.

Chapter 1

Dirichlet L-functions

Series of the form:

$$\sum_{n\geq 1} \frac{a_n}{n^s} \quad (a_n, s \in \mathbb{C})$$

are called Dirichlet series. Dirichlet used these series in the special case where $a_n = \chi(n)$ for χ a modular character to prove a conjecture of Gauss that there are infinitely many primes in any sequence of the form $an+b(n = 1, 2, \ldots)$ when a and b are relatively prime integers.

More precisely, a Dirichlet (modular) character modulo m is defined in the following way:

Definition 1.0.1 *Dirichlet characters*

Let m be a positive integer, a Dirichlet character χ modulo m is a group homomorphism from $(\mathbb{Z}/m\mathbb{Z})^*$ to the multiplicative group $\mathbb{C}^*$. In other terms it is an element of the dual group $\widehat{(\mathbb{Z}/m\mathbb{Z})^*}$. As $(\mathbb{Z}/m\mathbb{Z})^*$ is a finite group, χ takes its values in the group of roots of unity modulo $\phi(m)$ (ϕ is the Euler totient function). If χ is a Dirichlet character modulo m we define by extension $\chi : \mathbb{Z} \to \mathbb{C}^*$ by

$$\chi(n) := \begin{cases} \chi(n \bmod [m]) \text{ if } & \gcd(m,n) = 1 \\ 0 \quad \text{otherwise} & \end{cases}$$

A Dirichlet character modulo m is called primitive if it is not induced from any character to a modulus n with $n \leq m$. If χ is primitive modulo m we call m the conductor of χ and denote it by f_χ.

The inverse of χ is the character $\overline{\chi}$ which is the complex conjugate map of χ : $\overline{\chi}(a) = \overline{\chi(a)}$, $a \in \mathbb{Z}$

Let $m \geq 1$ and χ a Dirichlet character modulo m, we define the Dirichlet L-serie relative to m and χ as :

$$L(s, \chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}$$

Due to the multiplicative property of Dirichlet characters we have the following proposition ([45]):

Proposition 1.0.1 *If $\chi \neq 1$, $L(s,\chi)$ is convergent in the right half plane $\Re(s) > 0$ and absolutely convergent in the right half plane $\Re(s) > 1$. Moreover it has the following Euler product expansion :*

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}} \quad , \Re(s) > 1,$$

where the product is taken over every prime number.

Dirichlet used this to prove that if $\gcd(a,m) = 1$:

$$\sum_{\substack{p \\ p \equiv a \bmod[m]}} \frac{1}{p^s} \sim_{s\to 1} \frac{1}{\phi(m)} \log \frac{1}{s-1},$$

proving in a non trivial manner that there are infinitely primes p such that $p \equiv a \bmod[m]$.

Dirichlet L-functions admit a meromorphic continuation to the whole complex plane, furthermore if $\chi = 1$ it has a unique pole of order 1 and residue 1 at $s = 1$ and if $\chi \neq 1$ it is holomorphic everywhere.

Dirichlet L-functions also satisfy a functional equation which is given in the following theorem (see [22] for a proof).

Theorem 1.0.1 *Let χ be a Dirichlet character with conductor f, we define the Gauss sum of χ by:*

$$r(\chi) = \sum_{a=1}^{f} \chi(a) e^{\frac{2\pi i a}{f}}$$

and define the modified L-function of χ by

$$\Lambda(s,\chi) = \left(\frac{f}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s,\chi),$$

where $\delta = 0$ if $\chi(-1) = 1$ and $\delta = 1$ if $\chi(-1) = -1$ and Γ is the usual gamma function. Then

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

$W(\chi)$ being given by :

$$W(\chi) = \frac{r(\chi)}{\sqrt{f} i^{\delta}}, \qquad |W(\chi)| = 1,\ i = \sqrt{-1}$$

The behavior or value of an L-function near $s = 1$ is important in number theory. In the special case of a Dirichlet L-series it is :

Proposition 1.0.2 *If $\chi = 1$ then*

$$\lim_{s \to 1} L(s, 1) = 1.$$

If $\chi \neq 1$

$$L(1, \chi) = -\frac{r(\chi)}{f} \sum_{\substack{1 \leq a \leq f \\ \gcd(a, f) = 1}} \overline{\chi}(a) log(1 - e^{-2ai\pi/f})$$

, where f and $r(\chi)$ are defined in the previous theorem.

The following is a special case which is very important from a historical point of view ([4]).

Proposition 1.0.3 *Let K be a quadratic imaginary field, χ the quadratic character attached to it, such that $\chi(-1) = -1$, f the conductor of χ and d_K the discriminant of K. Let h be the class number of K and ω be the number of roots of unity in K. Then*

$$L(1, \chi) = \frac{2\pi h}{\omega \sqrt{|d_K|}}.$$

From this it can be inferred that

$$h = -\frac{\omega}{2|d_K|} \sum_{m=1}^{f} \chi(m) m \qquad \textit{(Dirichlet's class number formula)}$$

The next step was to generalize this to number fields in general.

Chapter 2

Dedekind zeta functions and Hecke's L-functions

2.1 The Dedekind zeta function

With the development of algebraic number theory, it was natural (and needed) to generalize these notions to arbitrary number fields. Instead of $\mathbb{Q}$ we consider a number field K and instead of $\mathbb{Z}$, we consider the ring $\mathcal{O}_K$ of integers of K. We denote by J_K the group of fractional ideals, P_K the group of principal ideals and $\mathrm{Pic}(K) = J_K/P_K$ the ideal class group.

If $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal the quotient group $\mathcal{O}_K/\mathfrak{a}$ is finite and we define the norm of $\mathfrak{a}$ as the index $\mathfrak{N}(\mathfrak{a}) = \mathrm{Card}(\mathcal{O}_K/\mathfrak{a})$. Then the Dedekind zeta function of the number field K is defined by :

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \in \mathfrak{I}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} \qquad \text{for } \Re(s) > 1.$$

The reason why ζ_K has the same half plane of convergence as ζ is that there are at most $[K : \mathbb{Q}]$ ideals in $\mathcal{O}_K$ of given norm. It what follows, we denote $n := [K : \mathbb{Q}]$.

Furthermore, the Dedekind zeta function has an Euler product over every prime ideals, a functional equation, and a meromorphic continuation to the entire complex plane.

$$\zeta_K(s) = \sum_{\mathfrak{p}} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}} \qquad \text{for } \Re(s) > 1$$

If d_K is the absolute discriminant of K and if r_1 and r_2 are the number of real and complex places of K respectively, then the function

$$\xi_K(s) = \left(\frac{\sqrt{|d_K|}}{2^{r_1} \pi^{n/2}} \right)^s \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta_K(s)$$

satisfies

$$\xi_K(s) = \xi_K(1-s).$$

The factors $\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)$ and $(2\pi)^{1-s}\Gamma(s)$ $(r_1+2r_2=n)$ are interpreted as the missing factors at real and complex infinite places respectively.

The functional equation was proved by Hecke using a generalization of what has been done about the Riemann zeta function.

Following [29], let us present some steps of the proof.

The first step is to transform the definition of the Dedekind zeta function into something computable. For this, for each ideal class $\mathfrak{R} \in \mathrm{Pic}(K)$ we choose an ideal $\mathfrak{a}_{\mathfrak{R}} \in \mathfrak{R}^{-1}$. Then the map $\mathfrak{R} \ni \mathfrak{b} \mapsto \mathfrak{a}_{\mathfrak{R}}\mathfrak{b} = (\xi) \subset \mathfrak{a}_{\mathfrak{R}}$ defines a bijection between ideal in $\mathfrak{R}$ and elements of $\mathfrak{a}_{\mathfrak{R}}$ modulo units. We call $C(\mathfrak{a}_{\mathfrak{R}})$ a set of representatives of elements in $\mathfrak{a}_{\mathfrak{R}}$ under the equivalence relation for which two elements of $\mathfrak{a}_{\mathfrak{R}}$ are equivalent if they differ by a unit.

Then

$$\zeta_K(s) = \sum_{0\neq I\in\mathfrak{I}} \frac{1}{\mathfrak{N}(I)^s} = \sum_{\mathfrak{R}\in\mathrm{Pic}(K)} \sum_{\mathfrak{b}\in\mathfrak{R}} \frac{1}{\mathfrak{N}(\mathfrak{b})^s}$$

$$= \sum_{\mathfrak{R}\in\mathrm{Pic}(K)} \sum_{\xi\in C(\mathfrak{a}_{\mathfrak{R}})} \frac{1}{\left(\mathfrak{N}(\mathfrak{a}_{\mathfrak{R}}^{-1}(\xi))\right)^s} \quad .$$

$$= \sum_{\mathfrak{R}\in\mathrm{Pic}(K)} \mathfrak{N}(\mathfrak{a}_{\mathfrak{R}})^s \sum_{\xi\in C(\mathfrak{a}_{\mathfrak{R}})} \frac{1}{N_{K/\mathbb{Q}}(\xi)^s}$$

Now we sum norms of algebraic numbers. We denote by σ_ν the canonical embeddings of K at infinite places ordered so that $\sigma_1, \ldots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$ and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+1}, \ldots, \overline{\sigma}_{r_1+r_2} : K \hookrightarrow \mathbb{C}$ and for $\xi \in K$ and $i = 0, \ldots, n$ we put $\xi_{\sigma_i} = \sigma_i(\xi)$.

The next step is to use the following formula:

$$\frac{\Gamma(s/2)}{a^s} = \int_0^\infty \exp(-a^2 y) y^{s/2} \frac{dy}{y} \quad , a > 0$$

which gives for $1 \leq i \leq r_1 + r_2$:

$$\left(\frac{\pi^{-1/2} d_K^{1/2} \mathfrak{N}(\mathfrak{a}_{\mathfrak{R}})^{1/n}}{N_{\sigma_i}}\right)^{sN_{\sigma_i}} \frac{\Gamma(sN_{\sigma_i}/2)}{|\xi_{\sigma_i}|^{sN_{\sigma_i}}} = \int_0^\infty \exp(-\pi d_{\mathfrak{a}}^{-1/n} N_{\sigma_i} |\xi_{\sigma_i}|^2 y) y^{sN_{\sigma_i}} \frac{dy}{y},$$

where we put $d_{\mathfrak{a}} = \mathfrak{N}(\mathfrak{a}_{\mathfrak{R}})^2 d_K$ (the absolute value of the discriminant of $\mathfrak{a}_{\mathfrak{R}}$) and $N_{\sigma_i} = 1$ or 2 provided that σ_i is a real or a complex embedding respectively.

In order to perform the product we have to introduce some notations which is due to the fact that there is a difference between real and complex embeddings. The product will give an integral over $r_1 + r_2$ copies of $\mathbb{R}^{+*}$. For $y = (y_i) \in \prod_{i=1}^{r_1+r_2} \mathbb{R}^{+*}$ we define $N(y) = y_1 y_2 \cdots y_{r_1} y_{r_1+1}^2 \cdots y_{r_1+r_2}^2$ and we define the measure $\frac{dy}{y}$ on $\prod_1^{r_1+r_2} \mathbb{R}^{+*}$ as the product measure of the Haar measures $\frac{dt}{t}$ on $\mathbb{R}^{+*}$ (for details see the paragraph on higher-dimensional gamma functions in the next section). Then

$$(2^{-r_2} d_K^{1/2} \pi^{-n/2})^s \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} \frac{\mathfrak{N}(\mathfrak{a}_{\mathfrak{R}})^s}{N_{K/\mathbb{Q}}(\xi)^s}$$

$$= \int_0^\infty \cdots \int_0^\infty \exp(-\pi d_{\mathfrak{a}}^{-1/n} \sum_{1\leq i\leq r_1+r_2} |\xi_{\sigma_i}|^2 y_i) N(y)^{s/2} \frac{dy}{y}$$

The final step is to sum over ξ and to transform the expression into something which involves theta functions as for the Riemann zeta function.

For this purpose, we define theta function in the following way: we choose $\mathfrak{c} = \{c_i | 1 \leq i \leq r_1 + r_2\}$ a list of n strictly positive real numbers enumerated such that $c_{r_1+i} = c_{r_1+r_2+i}$ for $1 \leq i \leq r_2$ and we define for a fractional ideal $\mathfrak{a}$ of K:

$$\Theta(\mathfrak{c}, \mathfrak{a}) = \sum_{\xi \in \mathfrak{a}} \exp\left(-\pi d_{\mathfrak{a}}^{-1/n} \sum_{1 \leq i \leq r_1+r_2} c_i |\xi_{\sigma_i}|^2 \right)$$

where $d_{\mathfrak{a}} = N\mathfrak{a}^2 d_K$ is the absolute discriminant of $\mathfrak{a}$.

Hecke proved that the following functional equation holds:

$$\Theta(\mathfrak{c}, \mathfrak{a}) = \frac{1}{\sqrt{\prod_{1 \leq i \leq r_1+r_2} c_i}} \Theta(\mathfrak{c}^{-1}, \mathfrak{a}'),$$

where $\mathfrak{c}^{-1} = \{c_i^{-1} | 1 \leq i \leq r_1 + r_2\}$ and $\mathfrak{a}'$ is the ideal dual to $\mathfrak{a}$ with respect to the bilinear form given by the trace of K over $\mathbb{Q}$, $\mathfrak{a}'$ is also given by $\mathfrak{a}' = (\mathfrak{d}\mathfrak{a})^{-1}$, where $\mathfrak{d}$ is the different of K over $\mathbb{Q}$.

With some manipulations (see [29] or [37]), it can be shown that the function $\Xi(s, \mathfrak{R})$ defined by:

$$\Xi(s, \mathfrak{R}) = (2^{-r_2} d_K^{1/2} \pi^{-n/2})^s \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} \mathfrak{N}(\mathfrak{a}_{\mathfrak{R}})^s \sum_{\xi \in C(\mathfrak{a}_{\mathfrak{R}})} \frac{1}{N_{K/\mathbb{Q}}(\xi)^s},$$

satisfies the following equation:

$$\Xi(s, \mathfrak{R}) = \int_1^\infty \int_E \frac{1}{\omega} \left(\Theta(t^{1/n}\mathfrak{c}, \mathfrak{a}) - 1 \right) d\mathfrak{c}\, t^{s/2} \frac{dt}{t} - \frac{2\mu(E)}{s\omega}$$

$$\ldots + \int_1^\infty \int_E \frac{1}{\omega} \left(\Theta(t^{1/n}\mathfrak{c}, \mathfrak{a}') - 1 \right) d\mathfrak{c}\, t^{(1-s)/2} \frac{dt}{t} - \frac{2\mu(E)}{(1-s)\omega}$$

Here $\mathfrak{R}' = (\mathfrak{d}\mathfrak{R})^{-1}$ is the dual to $\mathfrak{R}$ with respect to the trace and ω is the number of roots of unity in K. The terms $t^{1/N}\mathfrak{c}$ come from the fact that we can write $(y_{\sigma_i}) \in \prod_i \mathbb{R}$ as $t^{1/N}\mathfrak{c}$ with $\prod_i y_{\sigma_i} = t$ and $\prod_i c_i = 1$. Moreover, E is an adequate fundamental domain and $\mu(E)$ is the measure of E with respect to $d\mathfrak{c}$.

This show that $\Xi(s, \mathfrak{R}) = \Xi(1 - s, \mathfrak{R}')$ and summing over $\mathfrak{R}$ the functional equation for $\zeta_K(s)$ follows.

Furthermore, the value of $\mu(E)$ can be computed as something depending on the regulator $\mathrm{Reg}(K)$ of the field and the residue of $\zeta_K(s)$ in the simple pole $s = 1$ follows:

$$\mathrm{res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{Reg}(K)}{d_K^{1/2}\omega}$$

As we can see, the proof is quite complicated and we could expect it to be even more if we consider the equivalent for number fields of Dirichlet characters, this was done by Hecke in 1920 and conceptually improved later by Tate.

2.2 Hecke Grössenchrakters

We keep the notations of the previous section for K, $n = [K : \mathbb{Q}]$, $\mathcal{O}_K$, J_K (ideal group), $Cl(K)$ (ideal class group)...

We could consider generalizations of Dirichlet characters on J_K. We would consider an integral ideal $\mathfrak{m} \in J_K$, the group $J_K^{\mathfrak{m}}$ of fractional ideal relatively primes to $\mathfrak{m}$ and the subgroup $P_+^{\mathfrak{m}}$ of all those principal ideals $(x), x \in K^*$ for which x is totally positive and $x - 1 \in \mathfrak{m}$. Then a Dirichlet character modulo $\mathfrak{m}$ (also called a periodic character) is a character on $J_K^{\mathfrak{m}}/P_+^{\mathfrak{m}}$.

Actually, Hecke considered more general characters in such a way that a functional equation still exists.We want to define characters on $\mathcal{O}_K$ modulo an integral ideal $\mathfrak{m} \in J_K$. So we define a group homomorphism $\chi_{\mathfrak{m}} : (J_K/\mathfrak{m})^* \to \mathbb{C}^*$. Equivalently, we consider a character on $\mathcal{O}_K$ which is trivial on $\mathfrak{m}$.

The problem is that we would like to extend it to a character on J_K ? We may try to define it on principal ideals at least by defining it on generators. However there is no reason for such a function to be trivial on units.

Hecke succeeded in doing this but the properties of the characters are not simple ; he called the corresponding characters Grössencharakters.

Definition 2.2.1 *Grössencharakters*
Let $\mathfrak{m}$ be an integral ideal of the number field K and let $J_L^{\mathfrak{m}}$ be the group of all ideals of K which are relatively prime to $\mathfrak{m}$.
A Grössencharakter mod $\mathfrak{m}$ is a group homomorphism

$$\chi : J_K^{\mathfrak{m}} \to S^1 = \{z \in \mathbb{C} || z| = 1\},$$

for which exists a pair of characters:

$$\chi_f : (\mathcal{O}_K/\mathfrak{m})^* \to S^1, \qquad \chi_\infty : \mathbb{R}^* \to S^1,$$

such that

$$\chi((a)) = \chi_f(a)\chi_\infty(a)$$

for every algebraic integer $a \in \mathcal{O}_K$ relatively prime to $\mathfrak{m}$.
A Grössencharakter χ mod $\mathfrak{m}$ is a called primitive if it is not the restriction of a Grössencharakter χ' mod $\mathfrak{m}'$ for any proper divisor $\mathfrak{m}'$ of $\mathfrak{m}$. It can be shown (see [37] CR. VIII prop 6.2) that it is equivalent to say that χ_f factors through $(\mathcal{O}_K/\mathfrak{m}')^*$. The conductor of a Grössencharakter χ is the smallest divisor $\mathfrak{f}$ of $\mathfrak{m}$ such that χ is the restriction of a Grössencharakter mod $\mathfrak{f}$

The characters χ_f and χ_∞ are uniquely determined by the Grössencharakter χ. Characters of the ideal class groups are determined by Grössencharakters in the following way(e.g [37] CR. VIII 6.10):

Proposition 2.2.1 *The characters of the ideal class $Cl(K)$,i.e the group homomorphisms $\chi : J_K \to S^1$ which are trivial on principal ideals, are precisely the Grössencharakter χ mod 1 satisfying $\chi_\infty = 1$*

To χ or χ_f we can associate a Gauss sum:

Definition 2.2.2 *Gauss Sums*
Let χ_f be a character of $(\mathcal{O}_K/\mathfrak{m})^*$, let $\mathfrak{d}$ be the different of $K/\mathbb{Q}$ and $y \in \mathfrak{m}^{-1}\mathfrak{d}^{-1}$. Then we might associate a Gauss sum of χ_f as be

$$\tau_{\mathfrak{m}}(\chi_f, y) = \sum_{\substack{x \ mod\, \mathfrak{m} \\ gcd(x,\mathfrak{m})=1}} \chi_f(x) e^{2\pi\imath Tr(xy)}$$

We define naturally L-functions with Grössencharakters χ as

$$L_K(s,\chi) = \sum_{0 \neq \mathfrak{a} \in \mathfrak{I}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}}.$$

Hecke generalized theta functions to arbitrary number fields and along the same lines as in the proof of the functional equations (e.g. [37]) of Dedekind zeta functions he proved the functional equations for L-functions with Grössencharakters.

First of all he defined partial L-functions. For a ideal class $\mathfrak{R}$ de Pie(K) we define:

$$L(\mathfrak{R}, \chi, s) = \sum_{\substack{\mathfrak{a} \in \mathfrak{R} \\ \mathfrak{a}\ \text{integral}}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}$$

To obtain the functional equation theta functions over number fields can be used, I refer to [37] for a general presentation. There is something else which is needed: higher-dimensional Gamma functions which play the role of factors at infinity.

Higher-dimensional Γ-Function and characters on local fields In [37] a general presentation of Γ- functions is made which associate to any Gal$(\mathbb{C}/\mathbb{R})$-set, X, a complex function Γ_X. We only present the case of interest for us which is when $X = \mathrm{Hom}(K, \mathbb{C})$. So we define $X = \mathrm{Hom}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+1}}, \ldots, \overline{\sigma_{r_1+r_2}}\}$ where σ_i is real for $1 \leq i \leq r_1$ and complex otherwise. The fact that two conjugate complex embeddings define the same place whereas there are only one embedding in each conjugacy class has some consequences. Actually we can't deal them on the same footing.

For this reason we consider the space

$$\mathbf{C} = \prod_{\sigma \in X} \mathbb{C}$$

and we define homomorphisms N : $\mathbf{C} \to \mathbb{C}$ and Tr : $\mathbf{C} \to \mathbb{C}$ by

$$N(z) = \prod_{\sigma \in X} z_\sigma \quad Tr(z) = \sum_{\sigma \in X} z_\sigma.$$

We define the conjugation on $\mathbf{C}$ of an element $z = (z_\sigma)$ by $(\overline{z})_\sigma = \overline{z}_{\overline{\sigma}}$ and we define an involution * by $z^*_\sigma = z_{\overline{\sigma}}$. The space of interest is then:

$$\mathbf{R}^{+*} = \{z = (z_\sigma) \in \mathbf{C} | z = \overline{z},\ z = z^* \text{ and } \forall\, \sigma,\ z_\sigma > 0\}.$$

Actually

$$\mathbf{R}^{+*} = \prod_{\mathfrak{p}} \mathbb{R}^{+*}_{\mathfrak{p}},$$

where $\mathfrak{p} = \{\sigma, \overline{\sigma}\}$ is a conjugacy class of embeddings (a prime or a place) and $\mathbb{R}^{+*}_{\mathfrak{p}}$ is defined by

$$\mathbb{R}^{+*}_{\mathfrak{p}} = \begin{cases} \mathbb{R}^{+*} \text{ if } \mathfrak{p} \text{ is real} \\ \Delta(\mathbb{R}^{+*} \times \mathbb{R}^{+*}) = \{(x,x) | x \in \mathbb{R}^{+*}\} \text{ if } \mathfrak{p} \text{ is complex} \end{cases}.$$

There is a natural isomorphism $\mathbb{R}^{+*}_{\mathfrak{p}} \cong \mathbb{R}^{+*}$ which sends x to x if $\mathfrak{p}$ is real and (x,x) to x^2 if $\mathfrak{p}$ is complex. Thus we obtain

$$\mathbf{R}^{+*} \tilde{\longrightarrow} \prod_{\mathfrak{p}} \mathbb{R}^{+*}.$$

Via this isomorphism we transport the product of the Haar measures $\frac{dt}{t}$ of the right-hand side to a Haar measure $\frac{dy}{y}$ on $\mathbf{R}^{+*}$.

Definition 2.2.3 *Higher-dimensional $\Gamma-$functions*
With the preceding notations, for $s = (s_\sigma) \in \boldsymbol{C}$ such that $\Re(s_\sigma) > 0$ we define the $\Gamma-$function for $X = Hom(K, \mathbb{C})$ by

$$\Gamma_X(s) = \int_{\boldsymbol{R}^{+*}} N(e^{-y} y^s) \frac{dy}{y}.$$

The convergence reduce to the convergence of ordinary gamma functions. Then we define the L-function of X (here K) by

$$L_X(s) = N(\pi^{-s/2}) \Gamma_X(s/2)$$

The following lemma ([37]) is important for the purpose of the functional equation of L-functions with Grössencharakters.

Lemma 2.2.1 *If $\chi : J_K^{\mathfrak{m}} \to S^1$ is a Grössencharakter with associated characters χ_f and χ_∞, there exist unique $p \in \prod_\sigma \mathbb{Z}$ and*
$q \in \{z \in \boldsymbol{C} | z = \overline{z} \text{ and } z = z^*\}$ such that

$$\chi_\infty(x) = N\left(x^p |x|^{-p+\imath q}\right)$$

where x^p stands for $\prod_\sigma (\sigma x)^{p_\sigma}$ and same thing for $|x|^{-p+\imath q}$.

For such p and q, χ is called of type (p,q) and $p - \imath q$ is called its exponent. For χ of type (p,q) we define

$$L_\infty(\chi, s) = L_X(s\mathbf{1} + p - \imath q)$$

We are now ready to state the theorem of Hecke.

Theorem 2.2.1 *Functional equation of L-functions with Grössencharakters (1920) Let K be a number field with $n = [K : \mathbb{Q}]$ and $\mathfrak{d}$ the different of K. Let χ be a primitive Grössencharackter of conductor $\mathfrak{f}$, then the function:*

$$\Lambda(\mathfrak{R}, \chi, s) = (|d_K|\mathfrak{N}(\mathfrak{m}))^{s/2} L_\infty(\chi, s) L(\mathfrak{R}, \chi, s), \qquad \Re(s) \geq 1.$$

has a meromorphic continuation to the complex plane $\mathbb{C}$ and satisfies the functional equation:

$$\Lambda(\mathfrak{R}, \chi, s)) = W(\chi)\Lambda(\mathfrak{R}', \overline{\chi}, 1 - s)$$

where $\mathfrak{R}'$ is the ideal class defined by $\mathfrak{R} \cdot \mathfrak{R}' = [\mathfrak{m}\mathfrak{d}]$ and the constant factor is given by

$$W(\chi) = \left(\imath^{Tr(\overline{p})} N\left((\mathfrak{m}\mathfrak{d}|md|)^{\overline{p}}\right)\right)^{-1} \frac{\tau(\chi_f)}{\sqrt{\mathfrak{N}(\mathfrak{m})}}$$

Where m and d are such that $(m) = \mathfrak{m}$ and $(d) = \mathfrak{d}$.

Furthermore $|W(\chi)| = 1$ and $\Lambda(\mathfrak{R}, \chi, s)$ is holomorphic except for poles of order at most one at $s = Tr(-p+iq)/n$ and $s = 1+tr(p+iq)/n$ and holomorphic everywhere in the cases $\mathfrak{m} \neq 1$ or $p \neq 0$

The proof goes along the same lines as for the Dedekind zeta function and needs the use of general theta functions.

Corollary 2.2.1 *With the notations of the previous proposition, then the completed Hecke L-function*

$$\Lambda(\chi, s) = (|d_K|\mathfrak{N}(\mathfrak{a}))^{s/2} L_\infty(\chi, s) L(\chi, s) = \sum_{\mathfrak{R}} \Lambda(\mathfrak{R}, \chi, s)$$

admits a holomorphic continuation to

$$\mathbb{C} \setminus \{Tr(-p + \imath q)/n, 1 + tr(p + \imath q)/n\}$$

and satisfies the functional equation

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

Furthermore it is holomorphic on $\mathbb{C}$ if $\mathfrak{m} \neq 1$ or $p \neq 0$

Chapter 3

From classical to contemporary number theory

There is a natural generalization of this in more modern terms. It was conceived by Hecke and concretized by Iwasawa and principally by Tate in his thesis [54]. The principal idea is to consider idèles groups instead of ideals and characters on idèle class group. It turns out that, correctly set, it overlaps the previous theory and offers the good theoretical framework. The result being a more involved theoretical point of view while technicalities are in some sense simpler. The work of Tate has opened a new area of mathematics which is the basis of the current treatment of the subject.

Independently, Artin considered L-functions associated to Galois representations and Weil built a framework that include Artin L-functions and Hecke L-functions as special cases.

3.1 Tate's Thesis

Tate thesis [54], *Fourier analysis in number fields and Hecke's zeta function* has been a major breakthrough in the theory.

3.1.1 From ideals to idèles

For a general presentation of restricted products, idèles and adèles see [29] or [44]. Here we show that we can define characters on idèles, called Hecke characters, and their associated Hecke L-functions which generalize L-functions with Gössencharakters. This is the basis for an idelic treatment of the subject which was dealt with by Tate. First of all, remind the definition of the idèle group of K. It is the restricted direct product of the multiplicative groups K_ν^* of the

completions of K with respect to the local unit groups $\mathcal{O}_\nu^\times$:

$$\mathbb{I}_K = \left\{ (x_\nu) \in \prod_\nu K_\nu^* | x_\nu \in \mathcal{O}_\nu^\times \text{ for all but finitely many places } \nu \text{ of } K \right\}.$$

There is a natural algebraic embedding

$$\begin{array}{ccc} K^* & \hookrightarrow & \mathbb{I}_K \\ x & \mapsto & (x, x, x, \ldots) \end{array}.$$

We define the idèle class group to be the quotient $\mathbb{I}_K / K^*$ with respect to this embedding. Then we can define the characters of interest:

Definition 3.1.1 *An idèle class quasi-character is a continuous homomorphism from $\mathbb{I}_K$ to $\mathbb{C}^*$ that is trivial on the image of K^* in $\mathbb{I}_K$ under the preceding diagonal embedding.*

A Hecke character, χ is a continuous homomorphism $\chi : \mathbb{I}_K \to S^1$ such that $\chi(K^*) = 1$ (under the canonical embedding).

Before presenting Tate's thesis, I want to build the bridge between Grössencharakters and Hecke characters. It is only with this that we see that Tate's work generalizes and enriches what was done by Hecke. For this purpose, let us remind the basis of local fields theory. The most general definition of a local field is given in the book of Weil [57], it is a non-discrete locally compact topological field. On the additive group of a local field there is a Haar measure μ that defines a discrete valuation. For this reason a local field is sometimes defines as a field which is complete with respect to a discrete valuation and with (finite) perfect residue field or as a completion of a global field.

Let K be a number field and $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$ an integral ideal of K which is prime to ∞ ($n_\mathfrak{p} = 0$ if $\mathfrak{p} | \infty$). Remind that for every prime $\mathfrak{p}$ there is a basis of neighborhoods of 1 in the multiplicative group $K_\mathfrak{p}^*$ given by

$$\mathcal{O}_\mathfrak{p}^\times = U_\mathfrak{p}^{(0)} \supseteq U_\mathfrak{p}^{(1)} \supseteq U_\mathfrak{p}^{(2)} \supseteq \cdots$$

where $U_\mathfrak{p}^{(n)} = 1 + \pi_\mathfrak{p}^n \mathcal{O}_\mathfrak{p}$ for $\pi_\mathfrak{p}$ a uniformizing parameter of the local ring $\mathcal{O}_\mathfrak{p}$. Then we define

$$\bar{\mathbb{I}}_K^\mathfrak{m} = \mathbb{I}_f^\mathfrak{m} \times \mathbb{I}_\infty \quad \text{for} \quad \mathbb{I}_f^\mathfrak{m} = \prod_{\mathfrak{p} \nmid \infty} U_\mathfrak{p}^{(n_\mathfrak{p})}, \text{ and } \mathbb{I}_\infty = (K \otimes_\mathbb{Q} \mathbb{R})^* = \prod_{\mathfrak{p} | \infty} K_\mathfrak{p}^*$$

Definition 3.1.2 *Module of definition of a Hecke character.*
With the preceding notations, $\mathfrak{m}$ is called a module of definition of the Hecke character χ if

$$\chi(\mathbb{I}_K^\mathfrak{m}) = 1$$

Now we can build the correspondence between Hecke characters with module of definition $\mathfrak{m}$ and Grössencharkters (mod $\mathfrak{m}$). Recall that we noted $J_K^\mathfrak{m}$ the group of ideals relatively prime to $\mathfrak{m}$. We define $C(\mathfrak{m})$ by

$$C(\mathfrak{m}) = \mathbb{I}_K / \mathbb{I}_f^\mathfrak{m} K^*.$$

For every prime $\mathfrak{p} \nmid \infty$ we choose a prime element $\pi_\mathfrak{p}$ (i.e a uniformizing parameter of $\mathcal{O}_\mathfrak{p}$) of $K_\mathfrak{p}$. Then we define a homomorphism

$$\begin{array}{ccc} J_K^\mathfrak{m} & \longrightarrow & C(\mathfrak{m}) \\ \mathfrak{p} \nmid \mathfrak{m} & \longmapsto & (\ldots, 1, 1, \pi_\mathfrak{p}, 1, 1 \ldots) \end{array} .$$

It doesn't depend of the choice of $\pi_\mathfrak{p}$ since the idèles $(\ldots, 1, 1, u_\mathfrak{p}, 1, 1 \ldots)$, $u_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^*$, for $\mathfrak{p} \nmid \mathfrak{m}$, lie in $\mathbb{I}_f^\mathfrak{m}$. Then the composition

$$J_K^\mathfrak{m} \to C(\mathfrak{m}) \to S^1$$

define a 1-1 correspondence between Hecke characters modulo $\mathfrak{m}$ and Grössencharackters modulo $\mathfrak{m}$. For an explanation of these facts see [37], this idelic interpretation is due to Chevalley in [8].

Tate's thesis

Tate's thesis itself [54] is a good account of the theory, there is also the more recent book [44] which is very pedagogical.

Let K be a number field and consider its completion $K_\mathfrak{p}$ at a prime $\mathfrak{p}$, $\mathbb{F}_q$ the residue field and a corresponding uniformizing parameter $\pi_\mathfrak{p}$ if $\mathfrak{p}$ is non-archimedean. Then $K_\mathfrak{p}$ is a local field with absolute value $|\cdot|_\mathfrak{p}$. The additive group possesses a Haar measure $\mu_\mathfrak{p}$ normalized so that $\mu(\mathcal{O}_\mathfrak{p}) = 1$. We then have an associated Haar measure $\mu_\mathfrak{p}^\times$ on the multiplicative group $K_\mathfrak{p}^*$ normalized so that $\mu_\mathfrak{p}^\times(\mathcal{O}_\mathfrak{p}^*) = 1$ given by

$$d\mu_\mathfrak{p}^\times(x) = \begin{cases} (1 - \mathfrak{N}\mathfrak{p}^{-1})^{-1} \frac{d\mu_\mathfrak{p}(x)}{|x|_\mathfrak{p}} & \text{if} \quad \mathfrak{p} \nmid \infty \\ \frac{d\mu_\mathfrak{p}(x)}{|x|_\mathfrak{p}} & \text{if} \quad \mathfrak{p} \mid \infty \end{cases} .$$

Generally, $K_\mathfrak{p}^* = U_\mathfrak{p} \times \mathcal{G}_\mathfrak{p}$ where $U_\mathfrak{p}$ is the subgroup of elements of unit absolute values and $\mathcal{G}_\mathfrak{p} = \{y \in \mathbb{R}^{+*} \mid \exists x \in K_\mathfrak{p}^*, y = |x|_\mathfrak{p}\}$ is the valuation group.

Characters of $\mathcal{G}_\mathfrak{p}$ are of the form $t \mapsto t^s$ for some $s \in \mathbb{C}$, whereas group homomorphisms (quasi-characters) $U_\mathfrak{p} \to \mathbb{C}^*$ take their values in S^1. Hence we have:

Lemma 3.1.1 *With the preceding decomposition, a quasi-character of $K_\mathfrak{p}^*$, i.e a group homomorphism $\chi : K_\mathfrak{p}^* \to \mathbb{C}^*$ can be written*

$$\chi = \omega |\ |_\mathfrak{p}^s$$

where ω is a character of $U_\mathfrak{p}$ (with values in S^1) and s is a complex number. The number s is not uniquely determined by this decomposition but its real part $\sigma = \Re(s)$ is. σ is called the real part or exponent of χ and noted $\sigma = \Re(\chi)$.

Definition 3.1.3 *A (quasi-)character χ on a local field F is said to be unramified if its restriction to the local units U_F is trivial, $\chi | U_F = 1$*

The basis of Tate's thesis rest on the following simple computation which allow to transform the L-functions defined as a sum as an integral.

Let $\mathfrak{p} \nmid \infty$ and $\xi_{\mathfrak{p}} : K_{\mathfrak{p}}^* \to \mathbb{C}$ an unramified quasi-character. We have the following decompositions

$$K_{\mathfrak{p}}^* = \bigcup_{n\in\mathbb{Z}} \pi_{\mathfrak{p}}^n \mathcal{O}_{\mathfrak{p}}^\times \qquad \mathcal{O}_{\mathfrak{p}} \setminus \{0\} = \bigcup_{n\geq 0} \pi_{\mathfrak{p}}^n \mathcal{O}_{\mathfrak{p}}^\times.$$

Then

$$\int_{\pi_{\mathfrak{p}}^n \mathcal{O}_{\mathfrak{p}}^\times} \xi_{\mathfrak{p}}(x) d\mu_{\mathfrak{p}}^\times(x) = \xi_{\mathfrak{p}}(\pi_{\mathfrak{p}}^n) \left(\int_{\mathcal{O}_{\mathfrak{p}}^\times} \chi_{\mathfrak{p}}(\epsilon) d\mu_{\mathfrak{p}}^\times(\epsilon) \right) = \xi_{\mathfrak{p}}(\pi_{\mathfrak{p}})^n,$$

the first equality being due to the property of the Haar measure. This gives

$$\int_{\mathcal{O}_{\mathfrak{p}}\setminus\{0\}} \xi_{\mathfrak{p}}(x) d\mu_{\mathfrak{p}}^\times(x) = \sum_{n\geq 0} \int_{\pi_{\mathfrak{p}}^n \mathcal{O}_{\mathfrak{p}}^\times} \xi_{\mathfrak{p}}(x) d\mu_{\mathfrak{p}}^\times(x) = (1 - \xi_{\mathfrak{p}}(\pi_{\mathfrak{p}}))^{-1}.$$

Now, let ψ be a Hecke character corresponding to the Grössencharkter χ by the preceding correspondence. Then by the properties of the restricted direct products ψ decomposes into a product $\psi(x) = \prod_{\mathfrak{p}} \psi_{\mathfrak{p}}(x_{\mathfrak{p}})$ for $x = (x_{\mathfrak{p}}) \in \mathbb{I}_K$ such that $\psi_{\mathfrak{p}} : K_{\mathfrak{p}}^* \to \mathbb{C}^*$ is a quasi-character, unramified for almost all $\mathfrak{p}$, $\psi_{\mathfrak{p}}$. Then if $\xi_{\mathfrak{p}} = \psi_{\mathfrak{p}} |\ |^s$ which is also a quasi-character, $\xi_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = \chi(\mathfrak{p})\mathfrak{N}\mathfrak{p}^{-s}$. So, in this case, we find the Euler factor of the L-functions with Grössencharakters.

With this in mind we would like to define the L-functions associated to quasi-characters of the idèle class group, called Hecke L-functions. If χ is such a quasi-character, we may define $L(\chi) = \prod_{\mathfrak{p}} L(\chi_{\mathfrak{p}})$, where for a quasi-character $\xi_{\mathfrak{p}} : K_{\mathfrak{p}}^* \to \mathbb{C}$ at a finite place we define the local L-factor ,$L(\xi_{\mathfrak{p}}) = (1-\xi_{\mathfrak{p}}(\pi_{\mathfrak{p}}))^{-1}$ if $\xi_{\mathfrak{p}}$ is unramified and 1 otherwise. It remains to define the factors at infinity.

There are defined as follow. If $K_{\mathfrak{p}} = \mathbb{C}$, $U_{\mathfrak{p}} = S^1$ and $\xi_{\mathfrak{p}}$ takes the form

$$\chi_{s,n} : re^{\imath\theta} \mapsto r^s e^{\imath n\theta}, \text{ for some } s \in \mathbb{C},\ n \in \mathbb{Z}$$

and we define the local factor

$$L(\chi_{s,n}) = (2\pi)^{-(s+\frac{|n|}{2}}\Gamma(s + \frac{|n|}{2}).$$

If $K_{\mathfrak{p}}$ is non-archimedean, χ is a quasi-character of $K_{\mathfrak{p}}^*$ and $\pi_{\mathfrak{p}}$ is a uniformizing parameter of $\mathcal{O}_{\mathfrak{p}}$ we put:

$$L(\chi) = \begin{cases} 1 & \text{If } \chi \text{ is ramified} \\ \frac{1}{1-\chi(\pi)} & \text{If } \chi \text{ is unramified} \end{cases}$$

If $K_{\mathfrak{p}} = \mathbb{R}$, $U_{\mathfrak{p}} = \{-1, 1\}$ and $\xi_{\mathfrak{p}}$ is of the form $\mu|\cdot|^s$ where μ is either the trivial character or the character $\mathrm{sgn} : x \mapsto x/|x|$. We define the corresponding local L-factors are defined by

$$L(\mu|\cdot|^s) = \begin{cases} \pi^{-s/2}\Gamma(s/2) & \text{if } \mu = 1 \\ \pi^{-(s+1)/2}\Gamma(\frac{s+1}{2}) & \text{if } \mu = \mathrm{sgn} \end{cases}$$

Definition 3.1.4 *Let ψ be an idèle class quasi-character, it can be written*

$$\psi = \prod_{\mathfrak{p}} \psi_{\mathfrak{p}}.$$

We define

$$L(\psi) = \prod_{\mathfrak{p}} L(\psi_{\mathfrak{p}})$$

where the local factors $L(\chi_{\mathfrak{p}})$ are define according to what precedes. With this definition, we further define the Hecke L-function corresponding to χ as

$$L(s, \psi) = L(\psi |\cdot|^s)$$

Actually, Tate defined more general class of function called zeta integrals and used Fourier analysis to deduce the analytic continuation and functional equation for them.

As before, we consider a Hecke character (mod $\mathfrak{m}$), $\psi : J_K/K^* \to S^1$ associated to a Grössencharakter $\chi : \mathbb{I}_K \to S^1$ (mod $\mathfrak{m}$).

If $\mathfrak{p}$ is a finite place (prime) $c : K_{\mathfrak{p}}^* \to \mathbb{C}$ is a quasi-character and $f \in L^1(K_{\mathfrak{p}})$ is such that $fc \in L^1(K_{\mathfrak{p}}^\times)$ for $\Re(c) > 0$, we define the local zeta integral by

$$\zeta_{\mathfrak{p}}(f, c) = \int_{K_{\mathfrak{p}}} f(x)c(x)d\mu_{\mathfrak{p}}^\times(x).$$

The motivation for this definition is that if $f = \delta_{\mathcal{O}_{\mathfrak{p}} \setminus \{0\}}$ is the characteristic function of $\mathcal{O}_{\mathfrak{p}} \setminus \{0\}$ then

$$\zeta_{\mathfrak{p}}(f, \psi_{\mathfrak{p}} |\cdot|^s) = \frac{1}{1 - \chi(\mathfrak{p})\mathfrak{N}\mathfrak{p}^{-s}}.$$

For archimedean places we find that the corresponding local zeta integral equals the local factors we computed previously (e.g. [7]).

We can work it out globally. For this purpose we consider a function $f(x) = \prod_{\mathfrak{p}} f_{\mathfrak{p}}(x_{\mathfrak{p}})$ on the additive group of adèles $\mathbb{A}_K$ such that $f_{\mathfrak{p}} \in L^1(K_{\mathfrak{p}}^*)$ and $f_{\mathfrak{p}} = \delta_{\mathcal{O}_{\mathfrak{p}} \setminus \{0\}}$ for non-archimedean places prime to $\mathfrak{m}$, i.e for $\mathfrak{p} \nmid \mathfrak{m}$ and $\mathfrak{p} \nmid \infty$. We define $S(\mathfrak{m}) := \{\mathfrak{q} : \mathfrak{q} \nmid \mathfrak{m} \text{ and } \mathfrak{q} \nmid \infty\}$. Then

$$\zeta(f, \psi |\cdot|^s) = L(s, \chi) \prod_{\mathfrak{p} \in S(\mathfrak{m})} \zeta_{\mathfrak{p}}(f_{\mathfrak{p}}, \psi_{\mathfrak{p}} |\cdot|^s).$$

Actually, the product term in the last equation correspond exactly to the missing factors for the functional equation of the L-functions with Grössencharakters. The key theoretical tool of Tate's thesis is Fourier theory on adèle group $\mathbb{A}_K$ that we present next.

3.1.2 Some Fourier theory

Let K be a number field, $\mathbb{A}_K$ its adèle group and if $\mathfrak{p}$ is a prime of K, let $K_\mathfrak{p}$ the corresponding local field.

The following lemma is simple but important.

Lemma 3.1.2 *([7] p. 308)*
Let k be a local field, k^+ its additive group. If $a \mapsto \chi(a)$ is a non-trivial character of k^+. The correspondence $\eta \leftrightarrow (a \mapsto \chi(\eta a))$ is both a topological and an algebraic isomorphism between, k^+ and its character group.

Now, we define a particular character of $\mathbb{A}_K/K$ by specifying a particular character on each completion $K_\mathfrak{p}$.

Definition 3.1.5 *Let $\mathfrak{p}$ a prime of $\mathcal{O}_K$ that we identify with a place of K and let $K_\mathfrak{p}$ be the corresponding completion. We define:*

$$\lambda_\mathfrak{p}(x_\mathfrak{p}) = \begin{cases} \exp(-2\pi\imath x_\mathfrak{p}) & \text{if} \quad K_\mathfrak{p} \cong \mathbb{R}, \\ \exp(-2\pi\imath\Re(x_\mathfrak{p})) & \text{if} \quad K_\mathfrak{p} \cong \mathbb{C} \\ \exp(-2\pi\imath(Tr_{K_\mathfrak{p}/\mathbb{Q}_p}x_\mathfrak{p})) & \text{if} \quad [K_\mathfrak{p} : \mathbb{Q}_p] < \infty. \end{cases}$$

and a global character

$$\begin{array}{rcl} \lambda : \mathbb{A}_K/K & \to & \mathbb{C}^* \\ x & \mapsto & \prod_\mathfrak{p} \lambda_\mathfrak{p}(x_\mathfrak{p}). \end{array}$$

$\lambda_\mathfrak{p}$ defines an isomorphism $K_\mathfrak{p} \cong \widehat{K}_\mathfrak{p}$ (the character group) by the preceding lemma and we have similarly an isomorphism $\mathbb{A}_K \cong \widehat{\mathbb{A}_K}$ defined by $x \mapsto (y \mapsto \lambda(yx))$.

If $\mathfrak{p}$ is non-archimedean, the local different $\mathfrak{d}_\mathfrak{p} \subset \mathcal{O}_\mathfrak{p}$ is defined by:

$$\mathfrak{d}_\mathfrak{p}^{-1} = \{x \in K_\mathfrak{p} | \lambda_\mathfrak{p}(xy) \in \mathbb{Z}, \forall y \in \mathcal{O}_\mathfrak{p}\}.$$

One has $\mathfrak{d}_\mathfrak{p} = \mathfrak{d}_K\mathcal{O}_\mathfrak{p}$ and $\mathfrak{N}\mathfrak{d}_K = |d_K|$ (the absolute discriminant of K).

We then define normalized measures on the completion of K.

Definition 3.1.6 *(Self-dual measures)*
Let K be a number field and $\mathfrak{p}$ a place of K. We define the measure

$$\tilde{\mu}_\mathfrak{p} = \begin{cases} \mathfrak{N}(\mathfrak{d}_\mathfrak{p})^{-1/2}\mu_\mathfrak{p} & \text{if} \quad \mathfrak{p} \quad \text{is non-archimedean} \\ \text{Lebesque measure} \quad dx & \text{if} \quad K_\mathfrak{p} \cong \mathbb{R} \\ 2dxdy & \text{for} \quad z = x + iy \in K_\mathfrak{p} \cong \mathbb{C}. \end{cases}$$

The measure $\tilde{\mu}$ on $\mathbb{A}_K$ is then (well) defined by $\tilde{\mu} = \prod_\mathfrak{p} \tilde{\mu}_\mathfrak{p}$ and is a Tamagawa measure, in the sense that $\tilde{\mu}(\mathbb{A}_K/K) = 1$.

We are ready to define Fourier transforms:

Definition 3.1.7 *Let $f \in L^1(\mathbb{A}_K)$ and $f_\mathfrak{p} \in L^1(K_\mathfrak{p})$, the spaces L^1 being defined by the self-dual measures. Their Fourier transform are*

$$\hat{f}_\mathfrak{p}(x) = \int_{K_\mathfrak{p}} f_\mathfrak{p}(y)\lambda_\mathfrak{p}(x_\mathfrak{p}y)d\tilde{\mu}_\mathfrak{p}(y), \quad \hat{f}(x) = \int_{\mathbb{A}_K} f(y)\lambda(xy)d\tilde{\mu}(y).$$

The following inversion formula holds

$$\hat{\hat{f}}(-x) = f(x), \quad \hat{\hat{f}}_\mathfrak{p}(-x_\mathfrak{p}) = f(x_\mathfrak{p}).$$

One of the great feature of Tate's thesis is to replace the complex computations of Hecke by quite simple Fourier analysis. In this process, the use of generalized theta series is replaced by a Poisson summation formula.

Proposition 3.1.1 *(Poisson summation formula)*
Let f be a continuous function on $\mathbb{A}_K$ such that both $|f|$ and $|\hat{f}|$ are summable over $K \subset \mathbb{A}_K$ and the series $\sum_{\alpha\in K} f(x+\alpha)$ converges uniformly on every compact subset of $\mathbb{A}_K$. Then

$$\sum_{\alpha\in K} f(\alpha) = \sum_{\alpha\in K} \hat{f}(\alpha).$$

Theorem 3.1.1 *Let ψ a Hecke quasi-character and let f a function which satisfies the hypothesis of the Poisson summation formula and such that for all $\sigma > 0$, $|f(x)|\|x\|^\sigma$ is integrable over the group of idèles $\mathfrak{J}_K$. Then for $\Re(\psi|\cdot|^s) > 1$ the following integral*

$$\zeta(f, \psi|\cdot|^s) = \int_{\mathfrak{J}_K} f(x)\psi(x)|x|^s d\mu^\times(x)$$

is well defined.

$\zeta(f, \psi|\cdot|^s)$ admits an analytic continuation to the entire complex plane and satisfies the following functional equation

$$\zeta(f, \psi|\cdot|^s) = \zeta(\hat{f}, \psi^{-1}|\cdot|^{1-s}).$$

As one can see the result of Tate is much more general than the result of Hecke without been much more complex but theoretically more evolved and certainly very elegant.

3.2 Artin L-functions

Artin around 1920 constructed a family of functions associated to a representation of Galois groups $\mathrm{Gal}(L/K)$ of extensions of number fields L/K. Tate's thesis and Artin L-functions are the origins of the current treatment of the subject of L-functions, an open field with many far reaching conjectures.

In the particular case of Dirichlet L-functions, the correspondence takes the following form. Let χ be a modular character modulo m for m an integer and

let $G_m = \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ be the Galois group of the cyclotomic field $\mathbb{Q}(\mu_m)$ generated by m-th roots of unity. There is a classical isomorphism

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^* & \widetilde{\rightarrow} & G_m \\ \text{for } p \bmod [m] & \mapsto & (\phi_p : \zeta \mapsto \zeta^p) \end{array},$$

where we take only the prime number p, prime to m.ϕ_p being the Frobenius automorphism. Thus we can interpret χ as a character of G_m, i.e a one-dimensional representation of G_m. Then $L(s,\chi)$ rewrites

$$L(\chi, s) = \prod_{p \nmid m} \frac{1}{1 - \chi(\phi_p)p^{-1}}.$$

Artin extended these notion to arbitrary complex representation of the Galois group $G := \mathrm{Gal}(L/K)$ of an extension L/K. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and $\mathcal{P}$ a prime ideal of $\mathcal{O}_L$ above $\mathfrak{p}$. We know by classical algebraic number theory that G acts transitively on prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Thus we can define $\mathcal{D}_\mathcal{P} = \{\tau \in G | \tau\mathcal{P} = \mathcal{P}\}$, called the decomposition group of $\mathcal{P}$ and $I_\mathcal{P} = \{\tau \in G | \tau(x) \equiv x \bmod \mathcal{P},\ \forall x \in \mathcal{O}_L\}$, called the inertia group of $\mathcal{P}$.

Let $L_{(\mathcal{P})}$ and $K_{(\mathfrak{p})}$ denote the residue fields $\mathcal{O}_L/\mathcal{P}$ and $\mathcal{O}_K/\mathfrak{p}$. There is ([37] Ch. I (9.4)) a surjective homomorphism $\mathcal{D}_\mathcal{P} \rightarrow \mathrm{Gal}(L_{(\mathcal{P})}/K_{(\mathfrak{p})})$ with kernel $I_\mathcal{P}$, hence an isomorphism $D_\mathcal{P}/I_\mathcal{P} \cong \mathrm{Gal}(L_{(\mathcal{P})}/K_{(\mathfrak{p})})$. As $L_{(\mathcal{P})}/K_{(\mathfrak{p})}$ is an extension of finite fields, $D_\mathcal{P}/I_\mathcal{P}$ is cyclic with a generator, ϕ_p, called naturally the Frobenius automorphism and which is characterized by

$$\forall x \in \mathcal{O}_E,\ \phi_\mathcal{P}(x) \equiv x^{\mathfrak{N}(\mathfrak{p})} \bmod \mathcal{P}.$$

The action of the Galois group on primes above $\mathfrak{p}$ being transitive, if $\mathcal{P}_1$ and $\mathcal{P}_2$ are above $\mathfrak{p}$ there is an element of G which sends $\mathcal{P}_1$ to $\mathcal{P}_2$, $\mathcal{D}_{\mathcal{P}_1}$ to $\mathcal{D}_{\mathcal{P}_2}$ and $\mathcal{I}_{\mathcal{P}_1}$ to $\mathcal{I}_{\mathcal{P}_2}$. This implies that if $\rho : G \rightarrow \mathrm{Aut}_\mathbb{C}(V)$ is a representation:

$$\det(1 - \rho(\phi_{\mathcal{P}_1})\mathfrak{N}\mathfrak{p}^{-s} | V^{I_{\mathcal{P}_1}}) = \det(1 - \rho(\phi_{\mathcal{P}_2})\mathfrak{N}\mathfrak{p}^{-s} | V^{I_{\mathcal{P}_2}}),$$

where $V^{I_\mathcal{P}}$ is the invariant subspace of V according to the action of $I_\mathcal{P}$. Furthermore two equivalent representations ρ and ρ' define the same factor $\det(1 - \rho(\phi_\mathcal{P})\mathfrak{N}\mathfrak{p}^{-s}|V^{I_\mathcal{P}})$ whereas two representations are equivalent if and only if they have the same character, so this factor depends only on χ.

Then, the following function is well defined.

Definition 3.2.1 *Artin L-functions*
Let L/K be a Galois extension of number fields with Galois group G and for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathcal{P}$ an arbitrary prime ideal of $\mathcal{O}_L$ above $\mathfrak{p}$. Let $I_\mathcal{P}$ be the inertia group of $\mathcal{P}$ and (ρ, V) a complex representation of G of character χ, the Artin L-function attached to (ρ, V) and G is

$$L(s, \rho, L/K) = \prod_\mathfrak{p} \det(1 - \rho(\phi_\mathcal{P})\mathfrak{N}\mathfrak{p}^{-s} | V^{I_\mathcal{P}}).$$

The series is convergent for $\Re(s) > 1$.

3.2.1 Some usual facts about representations

In this section a representation mean a complex representation. A representation (ρ, V) of a finite group G in a complex vector space V is a group homomorphism $\rho : G \to GL_{\mathbb{C}}(V)$, equivalently it is a complex vector space with an action of G, i.e a G-module. When no ambiguity occurs we will denote the representation (ρ, V) by ρ or even by V.

The degree of a representation V is the dimension of V. Two representations (ρ, V) and (ρ', V') are called equivalent if V and V' are isomorphic as G-modules, i.e. if there is an isomorphism $T : V \to V'$ compatible with the operation of G:

$$\forall g \in G, \forall v \in V, \rho'(g)T(v) = T(\rho(g)v).$$

The character χ of (ρ, V) is the map $\chi : G \to \mathbb{C}$ defined by $\chi(g) = \text{Trace}(\rho(g))$. $\chi(1)$ is equal to the degree of ρ, i.e. to the dimension of V. Furthermore, χ is obviously, a class function, that is to say that χ is constant on each conjugacy class of G.

The character of the direct sum of two representations is the sum of their characters and the character of the tensor product of two representation is the product of their characters.

A representation is called irreducible if V doesn't admit any G-invariant subspace other than V itself, a character is called irreducible if it comes from an irreducible representation. Every representation V factors into a direct sum $V = n_1V_1 \oplus n_2V_2 \oplus \cdots \oplus n_rV_r$. Actually the multiplicities n_i can be computed using characters. We define an hermitian inner product on the set of all class functions by

$$< \chi, \chi' >= \frac{1}{\text{Card}(G)} \sum_{g \in G} \chi(g)\bar{(}\chi'(g)).$$

Then $n_i =< \chi, \chi_i >$ where χ_i is the character of the irreducible representation V_i. Thus, a representation is determined by its character.

There are two usual representations of a finite group G. The *trivial representation*, $\rho : G \to GL(V)$ where $dimV = 1$ and $\rho \equiv 1$ which we denoted by $\mathbf{1}_G$. The *regular representation* of G, denoted $\mathbf{R}_G$, is given by the G-module $V = \mathbb{C}[G] = \{\sum_{g \in G} x_g g | x_g \in \mathbb{C}\}$ on which G acts by multiplication.

If H is a subgroup of G, there is a natural (in fact universal) way of associating to a representation ρ of H, a representation of G called the induced representation. Let (ρ, V) be a representation H the induced representation $(\text{Ind}(\rho), \text{Ind}_H^G(V)$ is defined by the induced G-module

$$\text{Ind}_H^G(V) = \{f : G \to V | \forall h \in H, f(hx) = hf(x)\}$$

on which $g \in G$ acts by $(gf)(x) = f(gx)$. If χ is the character of ρ the induced character $Ind_G^H(\chi)$ of $Ind(\rho)$ is:

$$Ind_G^H(\chi)(g) = \sum_{\tau \in G/H} \chi(\tau g \tau^{-1}),$$

where τ varies over a system of representatives on the right of G/H and we put $\chi(\tau g \tau^{-1}) = 0$ if $\tau g \tau^{-1}$ doesn't belong to H.

3.2.2 Basic properties of Artin L-functions

Actually the Artin L-function $L(s, \rho, L/K)$ doesn't depend essentially on ρ but on its equivalence class so we may write $L(s, \chi, L/K)$ for $L(s, \rho, L/K)$ where χ is the character of ρ.

The following theorems, due to Artin, can be found in [7] and [37], see also [39].

Theorem 3.2.1 *Let G be the Galois group of a Galois extension L/K of number fields. Let H and N be subgroups of G with N normal. Let χ and χ' be characters of G. Let ψ be a character of H and let $Ind_G^H(\chi)$ the induced character on G. Let $\overline{\eta}$ be a character of G/N and let η the pull back of $\overline{\eta}$ to G. Then*

1. $L(s, \chi_1 \oplus \chi_2, L/K) = L(s, \chi_1, L/K)L(s, \chi_2, L/K)$
2. $L(s, \psi, L/L^H) = L(s, Ind_G^H(\psi), L/K)$
3. $L(s, \overline{\eta}, L^N/K) = L(s, \eta, L/K)$

A first link with zeta functions is made in the following theorem:

Theorem 3.2.2 *Let G be the Galois group of a Galois extension L/K of number fields. Let $\mathbf{1}_G$ and $\mathbf{R}_G$ be the trivial character and the regular character respectively.*

1. $L(s, \mathbf{1}_G, L/K) = \zeta_K(s)$
2. $L(s, \mathbf{R}_G, L/K) = \zeta_L(s)$
3. $\zeta_L(s) = \prod_{\chi \in \hat{G}} L(s, \chi, L/K)^{\chi(1)}$

3.2.3 Artin vs Hecke

In this section we begin by recalling local class field theory in order to define the norm residue symbol that will be used in the second part of this text. Next we recall global class field theory. This is motivated by the definition of Weil groups (see below) which involves reciprocity and by its use in the article [14] that we want to study. Finally we make the link between Artin L-functions and Hecke L-functions following [37].

Some local class field theory

Class field theory describe abelian Galois extension. This section as two purpose : stating Artin reciprocity and defining the local norm residue symbol, also called the local Artin symbol. First of all we state the *existence theorem* of local class field theory.

Theorem 3.2.3 *(Existence theorem, [37] ch. V) Let K be a local field. The map*

$$L \to \mathcal{N}_L := N_{L/K}L^*$$

, where $N_{L/K}$ is the usual norm, gives a one to one correspondence between the finite abelian extension of K and the open subgroup of finite index in K^*. Furthermore

- $L_1 \subseteq L_2 \Leftrightarrow \mathcal{N}_{L_1} \subseteq \mathcal{N}_{L_2}$
- $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$
- $\mathcal{N}_{L_1 \cup L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$

Theorem 3.2.4 *(Local reciprocity law) For every finite Galois extension L/K of local fields we have an isomorphism, called Artin reciprocity map,*

$$r_{L/K} : Gal(L/K)^{ab} \tilde{\to} K^*/N_{L/K}L^*,$$

where $Gal(L/K)^{ab}$ is the abelianization of $Gal(L/K)$ define as its quotient by the commutator group.

We are ready to define the *local norm residue symbol*

Definition 3.2.2 *The local norm residue symbol is defined by inverting the local reciprocity map, it gives*

$$(\, , L/K) : K^* \to Gal(L/K)^{ab}$$

which as kernel $N_{L/K}L^*$.

Some global class field theory

We denote by C_K the idèle class group $\mathfrak{J}_K/K$ of a number field K. For global fields, the existence theorem takes the form

Theorem 3.2.5 *(Existence Theorem)*
There is a 1:1 correspondence between finite abelian extensions L/K and closed subgroups of finite index of C_K given by

$$L \mapsto \mathcal{N}_L = N_{L/K}C_L,$$

where $N_{L/K}$ is the usual norm. Moreover

1. $L_1 \subseteq L_2 \Leftrightarrow \mathcal{N}_1 \supseteq \mathcal{N}_2$
2. $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$
3. $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$

The field L/K corresponding to a subgroup $\mathcal{N}_L$ of C_K is called the class field of $\mathcal{N}_L$ and satisfies

$$Gal(L/K) \cong C_K/\mathcal{N}$$

Theorem 3.2.6 *(Global reciprocity law) For every Galois extension L/K of finite algebraic number fields we have a canonical isomorphism*

$$r_{L/K} : Gal(L/K)^{ab} \tilde{\to} C_K/N_{L/K}C_L.$$

We define the global norm residue symbol by way of this isomorphism

Definition 3.2.3 *We define the global norm residue symbol $(\ ,L/K)$ as the inverse of $r_{L/K}$, it gives*

$$(\ ,L/K) : C_K \to Gal(L/K)^{ab}$$

with kernel $N_{L/K}C_L$.

The link between local and global norm residue symbol is contained in the following proposition.

Proposition 3.2.1 *(Local-global relationship, product formula, [37] ch. VI) If L/K is an abelian extension, $\mathfrak{p}$ is a place of K and $L_\mathfrak{p}$ a completion of L above $\mathfrak{p}$, then*

- *The following diagram is commutative*

$$\begin{array}{ccc} K_\mathfrak{p}^* & \xrightarrow{(\ ,L_\mathfrak{p}/K_\mathfrak{p})} & Gal(L_\mathfrak{p}/K_\mathfrak{p}) \\ \downarrow & & \downarrow \\ C_K & \xrightarrow{(\ ,L/K)} & Gal(L/K) \end{array}$$

  . Where the left arrow is the canonical embedding.

- *(Product formula) For $a \in K^*$*

$$\prod_\mathfrak{p} (a, L_\mathfrak{p}/K_\mathfrak{p}) = 1.$$

  and, more generally, for $\alpha = (\alpha_\mathfrak{p}) \in \mathbb{I}_K$,

$$(\alpha, L/K) = \prod_\mathfrak{p} (\alpha_\mathfrak{p}, L_\mathfrak{p}/K_\mathfrak{p}).$$

Artin symbol and Artin L-functions

If n is an integer, we defined in (1.3.1) the higher unit groups $U^{(n)} = 1 + \pi_{\mathfrak{p}}^n \mathcal{O}_{\mathfrak{p}}$ of the completion $K_{\mathfrak{p}}$ of a number field K.

Definition 3.2.4 *(congruence group, ray class group)*
We define a finite cycle as a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{n_{\mathfrak{p}}}, \quad n_{\mathfrak{p}} \geq 0.$$

The congruence subgroup modulo $\mathfrak{m}$ *is defined by*

$$I_K^{\mathfrak{m}} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$$

and the ray class group modulo $\mathfrak{m}$ *is* $Cl_K := C_K / C_K^{\mathfrak{m}}$ *where*

$$C_K^{\mathfrak{m}} = I_K^{\mathfrak{m}} K^* / K^*.$$

Definition 3.2.5 *(ray class fields)*
The class field associated to $C_K^{\mathfrak{m}}$ *by the existence theorem is denoted* $K^{\mathfrak{m}}/K$ *and called the ray class field modulo* $\mathfrak{m}$.

The Galois group of a ray class field is canonically isomorphic to the ray class group modulo $\mathfrak{m}$, i.e $Gal(K^{\mathfrak{m}}/K) \cong C_K/C_K^{\mathfrak{m}}$ and every abelian extension L/K is contained in a ray class field. This motivates the following definition.

Definition 3.2.6 *Let* L/K *be a finite abelian extension and let* $\mathcal{N}_L = N_{L/K} C_L$. *The conductor* $\mathfrak{f}$ *of* L/K *is the greatest common divisor of all finite cycles* $\mathfrak{m}$ *such that* $L \subseteq K^{\mathfrak{m}}$.

To an extension L/K and primes $\mathfrak{p}$ (resp. $\mathcal{P}$) of K and L respectively, we associated a Frobenius automorphism $\phi_{\mathcal{P}}$. We define

$$\left[\frac{L/K}{\mathfrak{p}}\right] = \phi_{\mathcal{P}}.$$

We are going to extend this definition.

Let $\mathfrak{m}$ be a finite cycle of K such that L lies in the ray class field modulo $\mathfrak{m}$, then each $\mathfrak{p} \nmid \mathfrak{m}$ is unramified in L because there is an equivalence between being ramified in L and dividing the conductor of L/K. We then define a group homomorphism, called the Artin symbol:

$$\left[\frac{L/K}{\ }\right] : J_K^{\mathfrak{m}} \to Gal(L/K)$$

from the group of all ideals of K relatively prime to $\mathfrak{m}$ by putting :

$$\left[\frac{L/K}{\mathfrak{a}}\right] = \prod_{\mathfrak{p}} \left[\frac{L/K}{\mathfrak{p}}\right]^{\nu_{\mathfrak{p}}},$$

for an ideal $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$.

Proposition 3.2.2 *[37]*
Let $\mathfrak{m}$ be a finite cycle of K. We define $P_K^{\mathfrak{m}}$ as the group of principal ideal (a) of K such that $a \equiv 1 \mod \mathfrak{m}$ and a is totally positive.

The Artin symbol $\left[\frac{L/K}{\mathfrak{a}}\right]$ only depends on the class $\mathfrak{a} \bmod P_K^{\mathfrak{m}}$ and define an isomorphism

$$\left[\frac{L/K}{\ }\right] : J_K^{\mathfrak{m}}/H^{\mathfrak{m}} \tilde{\to} Gal(L/K),$$

where $H^{\mathfrak{m}} = (N_{L/K} J_L^{\mathfrak{m}}) P_K^{\mathfrak{m}}$.

Hence, let K/L be an abelian extension and $\mathfrak{f}$ be the conductor of L/K. The Artin symbol $\left[\frac{L/K}{\mathfrak{a}}\right]$ gives a surjective homomorphism

$$\begin{array}{rcl} J^{\mathfrak{f}}/P^{\mathfrak{f}} & \to & Gal(K/L) \\ \mathfrak{a} \bmod P^{\mathfrak{m}} & \mapsto & \left[\frac{L/K}{\mathfrak{a}}\right]. \end{array}$$

Let χ be an irreducible character of the abelian group $\mathrm{Gal}(L/K)$, composing it with the Artin symbol we get a character of the ray class group $J^{\mathfrak{f}}/P^{\mathfrak{f}}$ which induced a character on $J^{\mathfrak{f}}$ that we denote $\widetilde{\chi}$. It appears that $\widetilde{\chi}$ is a Grössencharakter modulo $\mathfrak{f}$ of type $(p, 0)$.

Finally, a link between Hecke L-functions with Grössencharakters and Artin L-functions is given in the following theorem ([37]):

Theorem 3.2.7 *Let L/K be an abelian extension, let $\mathfrak{f}$ be the conductor of L/K and $\chi \neq \mathbf{1}$ be an irreducible character of $Gal(L/K)$ and $\widetilde{\chi}$ the associated Grössencharaker modulo $\mathfrak{f}$.*

Then the Artin L-function for the character χ and the Hecke L-function for the Grössencharakter $\widetilde{\chi}$ are related by

$$L(s, \chi, L/K) = L(\widetilde{\chi}, s) \prod_{\mathfrak{p} \in S} \frac{1}{1 - \chi(\phi_{\mathcal{P}}) \mathfrak{N}^{-s}},$$

where $S = \{\mathfrak{p} \mid \mathfrak{f} | \chi(I_{\mathcal{P}}) = 1\}$.

3.2.4 The functional equation

Let χ be an irreducible character of $Gal(L/K)$ we define the Artin conductor of χ as the ideal $\mathfrak{f}(\chi)$ given by:

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

with

$$n_{\mathfrak{p}}(\chi) = \sum_{i \geq 0} \frac{\mathrm{Card}(G_i)}{\mathrm{Card}(G_0)} \mathrm{codim}_V(V^{G_i}),$$

where G_i is the i-th ramification group of L:

$$G_i = \{\sigma \in Gal(L/K) | \forall a \in \mathcal{O}_L, v_L(\sigma a - a) \geq s+1\}$$
$$v_L \text{ a normalized discret valuation of } L$$

.

It is a theorem of Artin that $n_{\mathfrak{p}}(\chi)$ is a rational integer.

If we want to obtain a functional equation for Artin L-function we need to complete the L-function

$$L(s, \chi, L/K) = \prod_{\mathfrak{p} \nmid \infty} \frac{1}{\det(1 - \rho(\phi_{\mathcal{P}})\mathfrak{N}(\mathfrak{p})^{-s} | V^{I_{\mathcal{P}}})},$$

with factor at ∞.

For every infinite place $\mathfrak{p}$ of K we put:

$$L_{\mathfrak{p}}(s, \chi, L/K) = \begin{cases} \Gamma_{\mathbb{C}}(s)^{\chi(1)} & \text{if } \mathfrak{p} \text{ is complex} \\ \Gamma_{\mathbb{R}}(s)^{n^+}\Gamma_{\mathbb{R}}(s+1)^{n^-} & \text{if } \mathfrak{p} \text{ is real} \end{cases}$$

where $n^+ = \frac{\chi(1)+\chi(\phi_{\mathcal{P}})}{2}$, $n^- = \frac{\chi(1)-\chi(\phi_{\mathcal{P}})}{2}$, $\phi_{\mathcal{P}}$ is the Frobenius automorphism introduced previously and the $\Gamma-$factors are defined by

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2), \quad \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s).$$

Definition 3.2.7 *(Completed Artin L-function)*
The completed Artin L-function for a character χ of $Gal(L/K)$ is defined to be

$$\Lambda(L/K) = A(\chi)L_{\infty}(s, \chi, L/K)L(s, \chi, L/K),$$

where

$$A(\chi) = |d_K|^{\chi(1)}\mathfrak{N}(f(\chi)), \quad \textit{and} \quad L_{\infty}(s, \chi, L/K) = \prod_{\mathfrak{p} | \infty} L_{\mathfrak{p}}(s, \chi, L/K).$$

Proposition 3.2.3 *([37]) If χ is a character of degree 1 of $Gal(L/K)$ and $\widetilde{\chi}$ is its associated Grössencharakter then the completed Artin L-function and the completed Hecke L-function coincide:*

$$\Lambda(s, \chi, L/K) = \Lambda(s, \widetilde{\chi})$$

This proposition together with a theorem of Brauer according which any character decomposes into a sum of characters induced by characters of degree 1 on subgroups of $Gal(L/K)$ permits to prove ([37]) the functional equation for Artin L-function provided that we know the functional equation of Hecke L-functions with Grössencharakters.

Theorem 3.2.8 *(Functional equation of Artin L-functions)*
The Artin L-function $\Lambda(s, \chi, L/K)$ admits a meromorphic continuation to $\mathbb{C}$ and satisfies the functional equation

$$\Lambda(s, \chi, L/K) = W(\chi)\Lambda(1 - s, \overline{\chi}, L/K)$$

with $W(\chi) \in \mathbb{C}$ (called the root number) of absolute value 1.

3.3 "Weil" L-functions

Let us call Weil L-functions functions associated to representations of some groups, called Weil groups, related to Galois groups. These L-functions include as special cases the L-functions of Hecke and the L-functions of Artin. We begin by presenting Weil groups. A good synthetic reference for what follows is [55], [54] and [58] are also good references. Remark that the term "Weil L-function" is not used in the literature, one prefers to use the general term of Artin L-functions as does Langlands in [30] or simply L-functions.

3.3.1 Generalities

Every field K is equipped with a distinguish Galois extension, the separable closure $\overline{K}/K$, its Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ is called the *absolute Galois group* of K. This group is often of infinite degree but it collects all information about the Galois finite extension of K. Hence, it is an important object of study. However the main theorem of Galois theory needs to be adapted, it is false for infinite extension, even in simple cases as $K = \mathbb{F}_p$.

There are two main ingredients to overcome this difficulty. First of all for any Galois extension (finite or infinite) $\mathrm{Gal}(\mathcal{L}/K)$ carries a natural topology called the *Krull topology*, secondly even if $\mathcal{L}/K$ is infinite $\mathrm{Gal}(\mathcal{L}/K)$ it is a profinite group, that is to say that $\mathrm{Gal}(\mathcal{L}/K)$ is the projective limit of finite groups, each given the discrete topology.

The Krull topology is defined as follows: for every $\sigma \in \mathrm{Gal}(\mathcal{L}/K)$ and for L/K ranging over the finite subextensions of $\mathcal{L}/K$ we take the cosets $\sigma\mathrm{Gal}(\mathcal{L}/L))$ as a basis of neighborhoods of σ. As a consequence the Krull topology is compact Hausdorff.

The main theorem of Galois theory is restated in this context by:

Theorem 3.3.1 *(Main theorem of Galois theory)*
Let $\mathcal{L}/K$ be any Galois extension. Then there is a 1:1 correspondence between the subextensions L/K of $\mathcal{L}/K$ and the closed subgroups of $Gal(\mathcal{L}/K)$ such that the open subgroups of $Gal(\mathcal{L}/K)$ are given by the finite subextensions of $\mathcal{L}/K$. This correspondence is given by

$$L \mapsto Gal(\mathcal{L}/L).$$

If $\mathcal{L}/K$ is a Galois extension, the Galois group $Gal(\mathcal{L}/K)$ with the Krull topology is the projective limit of the Galois groups $Gal(L_f/K)$ of the finite Galois extensions L_f/K which are contained in $\mathcal{L}/K$.

Let us remind that we denoted $C_K = \mathbb{I}_K/K$ the idèle class group of a number field K. We then state the global reciprocity law of class field theory that we will need later.

If G is a topological group we denote by $G^{ab} = G/\overline{[G,G]}$ the maximal abelian Hausdorff quotient of G, where $\overline{[G,G]}$ is the closure of the commutator subgroup of G.

Theorem 3.3.2 *(Artin reciprocity law)*
For every Galois extension L/K of finite algebraic number fields we have a canonical isomorphism

$$r_{L/K} : Gal(L/K)^{ab} \xrightarrow{\sim} C_K/N_{L/K}C_L.$$

The inverse map of $r_{L/K}$ yields a surjective homomorphism

$$(\quad, L/K) : C_K \longrightarrow Gal(L/K)^{ab},$$

called the global norm residue symbol.

If H is a subgroup of finite index of a topological group there is a *transfer* homomorphism (cf. [47] VII.3 propositions 7-8)

$$t : G^{ab} \longrightarrow H^{ab},$$

defined as follows: if $s : H \setminus G \to G$ is any section, then for $g \in G$,

$$t(g\overline{[G,G]}) = \prod_{x \in\ H\setminus G} h_{g,x} \mod \overline{[H,H]},$$

where $h_{g,x} \in H$ is defined by $s(x)g = h_{g,x}s(xg)$.

3.3.2 Weil Groups, according to Tate in [55]

Here, K will denote a local or a global field and $\overline{K}$ its separable closure. By E we will mean a finite extension of K in $\overline{K}/K$, and G_E will denote the Galois group $Gal(\overline{K}/E)$.

Definition 3.3.1 *A Weil group for $(\overline{K}/K)$ is a triple $(W_K, \phi, \{r_E\})$ where*

- *W_K is a topological group.*
- *ϕ is a continuous homomorphism $\phi : W_K \to G_K$ with dense image.*
  We define $W_E := \phi^{-1}(G_E)$ for each finite extension E of K in $\overline{K}$.
- *For each E, r_E is an isomorphism of topological groups $r_E : C_E \xrightarrow{\sim} W_E^{ab}$ where*

$$C_E = \begin{cases} \textit{The multiplicative group} \quad E^* \quad \textit{in the local case} \\ \textit{The idèle class group} \quad \mathbb{A}_E^*/E^* \quad \textit{in the global case.} \end{cases}$$

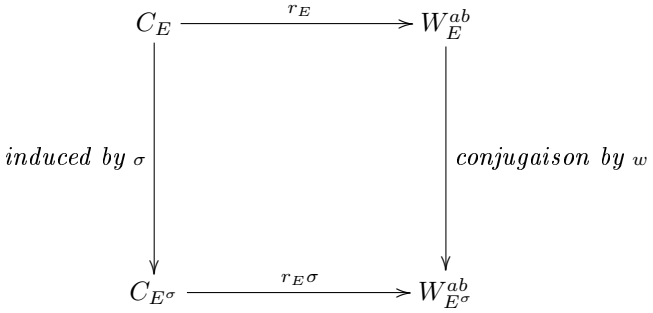
This triplet is subject to the conditions $(W1)$ to $(W4)$ below.

- *(W1)*
  For each E, the composed map

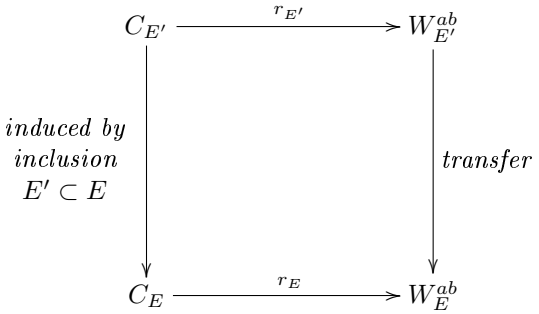
$$C_E \xrightarrow{r_E} W_E^{ab} \xrightarrow{\textit{induced by } \phi} G_E^{ab}$$

is the reciprocity law of class field theory (Theorem 1.3.8).

- *(W2)*
  Let $w \in W_K$ and $\sigma = \phi(w) \in G_K$. For each E the following diagram is commutative



- *(W3)*
  For $E' \subset E$ the following diagram is commutative

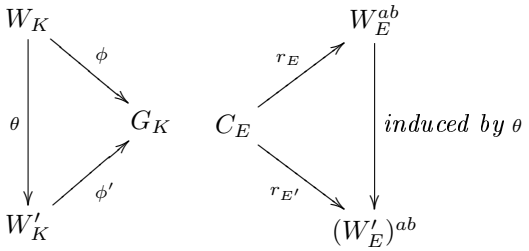


- *(W4)*
  If $W_{E/K}$ denotes W_K/W_E^c where $W_E^c = \overline{[W_E : W_E]}$, the following map is an isomorphism of topological groups

$$W_K \longrightarrow proj\ lim_E\{W_{E/K}\}.$$

Proposition 3.3.1 *(Properties of Weil groups [54])*

1. *Weil groups exist and are unique up to isomorphism: If W_K and W'_K are two Weil groups for $\overline{K}/K$, there exists an isomorphism $\theta : W_K \tilde{\to} W'_K$ such that the following diagrams are commutative*



2.

$$W_K/W_E \xrightarrow{\cong \text{ induced by } \phi} G_F/G_E$$

3. *If $(W_K, \phi, \{r_E\})$ is a Weil group for $\overline{K}/K$ and if E is a finite Galois subextension, $(W_E, \phi|W_E, r_{E'})$ is a Weil group for $\overline{K}/E$.*

4. *If W_K is a Weil group, then for $F \subset E' \subset E$ the following diagram is commutative*

$$\begin{array}{ccc} C_E & \xrightarrow{r_E} & W_E^{ab} \\ \Big\downarrow{\scriptstyle norm\ N_{E'/E}} & & \Big\downarrow{\scriptstyle induced\ by\ W_E \subset W_{E'}} \\ C_{E'} & \xrightarrow{r'_E} & W_{E'}^{ab} \end{array}$$

So the construction of Weil groups is functorial and satisfies a local-global relationship given by

Proposition 3.3.2 *(prop. 1.6 of [55], local-global relationship) Let K be a global field, ν a place of K and K_ν the corresponding completion. Let $\overline{K}$(resp. $\overline{K_\nu}$) the separable closure of F(resp. K_ν and W_K(resp. W_{K_ν}) the corresponding Weil group.*

Let $i_\nu : \overline{K} \to \overline{K_\nu}$ be an F-homomorphism. For each finite extension E of K in $\overline{K}$, let $E_\nu = i(E)K_\nu$ the induced completion of E. There is a continuous homomorphism $\theta_\nu : W_{K_\nu} \to W_K$ such that the following diagrams are commutative.

$$\begin{array}{ccc} W_{K_\nu} & \longrightarrow & G_{K_\nu} \\ \Big\downarrow{\scriptstyle \theta_\nu} & & \Big\downarrow{\scriptstyle induced\ by\ i_\nu} \\ W_K & \longrightarrow & G_K \end{array} \qquad \begin{array}{ccc} E_\nu^* & \xrightarrow{\sim} & W_{K_\nu}^{ab} \\ \Big\downarrow{\scriptstyle n_\nu} & & \Big\downarrow{\scriptstyle induced\ by\ i_\nu} \\ C_E & \xrightarrow{\sim} & W_E^{ab} \end{array}$$

where n_ν maps $a \in E_\nu^*$ to the class of the idèle whose ν-component is a and whose other components are 1

3.3.3 Special cases

Here we discuss the particular cases when K is a local field, a global function field or a global number field.

- if k is a finite field with q elements, the Weil group W_k is the subgroup of $Gal(\overline{k}/k)$ generated by (topological generator) the Frobenius endomorphism $\phi : x \mapsto x^q$ in $\overline{k}$. So $W_k \cong \mathbb{Z}$. We make W_k into a topological group by giving it the discrete topology.

  Definition 3.3.2 *(Geometric Frobenius)*
  If $\phi \in W_k$ is the Frobenius endomorphism, we define the geometric Frobenius as $F = \phi^{-1} \in W_k$.

- K local non-archimedean
  For each E we consider, k_E the residue field and $q_E = \mathrm{Card}(k_E)$. We put $\overline{k} = \bigcup_E k_E$. W_K is the dense subgroup of G_K consisting of the elements $\sigma \in G_K$ which induce on $\overline{k}$ the map $x \to x^{q_K^n}$ for some $n \in \mathbb{Z}$. The inertia group I_K is then contained in W_K and the topology of W_K is such that I_F gets the profinite topology induced from G_K and is open in W_K. ϕ is the inclusion and r_E is the reciprocity law.

  There is an exact sequence

  $$1 \longrightarrow I_K \longrightarrow W_K \xrightarrow{\pi} W_k \longrightarrow 1 \ ,$$

  and

  $$W_K = \bigcup_{n \in \mathbb{Z}} \Phi^n I_K,$$

  for any $\Phi \in \mathrm{Gal}(\overline{K}/K)$ such that $\pi(\Phi) = F$, where F is a geometric Frobenius.

- K local archimedean
  If $K \cong \mathbb{C}$ we take $W_K = K^*$, ϕ trivial and r_K the identity.
  If $K \cong \mathbb{R}$ we take $W_K = \overline{K}^* \cup j\overline{K}^*$ with the relations $j^2 = -1$ and $jcj^{-1} = \overline{c}$ for c the non trivial element of G_K. ϕ maps $\overline{K}^*$ to 1 and $j\overline{K}^*$ to c. $r_{\overline{K}}$ is the identity and r_K is characterized by

  $$r_K(-1) = j\overline{[W_K : W_K]}$$
  $$r_K(x) = \sqrt{x}[W_K : W_K], \quad \text{for } x > 0$$

- K a global function field
  The construction is similar to that of a local non-archimedean field with the constant field in place of residue field and geometric Galois group $Gal(\overline{K}/K\overline{k})$ in place of inertia group.

- K a global number field
  There is no simple known construction in this case, only a cohomological construction due to Weil in [58]

3.3.4 L-functions and ϵ-factors

Here we bring together the idea of Hecke, Tate, Artin and others to build a theory of L-functions associated to representations of Weil groups.

Local case

Let K be a local field, $\mathcal{O}_K$ its integer ring, π a uniformizing parameter, k its residue field, p the characteristic of k, q its the cardinal and I the inertia group of $\overline{K}/K$. We have $q = p^d$ where $d = [k : \mathbb{F}_p]$. Moreover, let $\overline{K}$ be a separable closure of K, $\overline{\mathcal{O}}_K$ the integral closure of $\mathcal{O}_K$ in $\overline{\mathcal{O}}_K$ and $\overline{k}$ the corresponding residue field which is a separable closure of k.

On note $\omega_s : x \mapsto \|x\|^s$ the (quasi-character) group homomorphism $K^* \to \mathbb{C}$, where $\|x\| = q^{-v(x)}$ is the normalized absolute value corresponding to the valuation v.

If χ is a quasi-character $\chi : K^* \to \mathbb{R}^*$ we define the L-factor $L(\chi)$ by (1.3.1 p. 20).

Proposition 3.3.3 *(Tate)*
Let K be a local field, ψ an additive character of K, dx an additive Haar measure on K, $\chi : K^* \to \mathbb{C}^*$ a quasi-character and f a smooth function with compact support on K.

We defined the Fourier transform of f by

$$\hat{f}(y) := \int_K f(x)\psi(xy)dx.$$

There exists a constant $\epsilon(\chi, \psi, dx) \in \mathbb{C}^*$ independent of f which satisfies Tate's local functional equation:

$$\frac{\int_{K^*} \hat{f}(x)\omega_1\chi^{-1}(x)d^*x}{L(\omega_1\chi^{-1})} = \epsilon(\chi, \psi, dx)\frac{\int_{K^*} f(x)\chi(x)d^*x}{L(\chi)}.$$

Corollary 3.3.1 *(Basic properties of ϵ-factors)*

1. $\forall\, r > 0, \quad \epsilon(\chi, \psi, rdx) = r\epsilon(\chi, \psi, dx)$
2. $\forall\, a \in K^*, \quad \epsilon(\chi, \psi(ax), dx) = \chi(a)\|a\|^{-1}\epsilon(\chi, \psi, dx)$

The construction of L-functions associated to representations of Weil groups needs the notion of virtual representations to be fully understood. It would be too long to present it here, I send the reader back to the article of Deligne [9] which is a complete exposition of the subject. I present only what is necessary for understanding the subject.

Artin showed that there is a L-functions of representations of Weil groups of local fields which is additive on exact sequences and such that $L(V) = L(\chi)$ for a representation V of degree 1 associated to the quasi-character χ. As L is additive, it can be defined by giving its values on irreducible representations.

K $\cong \mathbb{C}$ In this case $W_K = K^*$ is abelian and the only irreducible characters of V are quasi-characters for which L as been defined previously.

K $\cong \mathbb{R}$ In this case the only irreducible representations V of degree different from 1 are of the form $V = \mathrm{Ind}_{\overline{F}}^{F}\chi$ for χ a quasi-character of $\overline{F}^* = W_{\overline{F}}$. We then define $L(V) = L(\chi)$.

K non-archimedean With I the inertia group and F the geometric Frobenius we put

$$L(V) = det(1 - \phi|V^I)^{-1}$$

The following proposition is proved in [9]

Proposition 3.3.4 *1. For each exact sequence $0 \to V' \to V \to V''$ of representations of $W(\overline{K}/K)$:*

$$L(V) = L(V')L(V'')$$

2. Let E be a finite subextension of $\overline{K}/K$ and V_E a complex representation of $W(\overline{K}/E)$. Let V_K be the induced representation of V_L on $W(\overline{K}/K)$ then

$$L(V_K) = L(V_L).$$

The following theorem, firstly due to Langlands [30] has been proved an other way by Deligne and can be found in [9].

Theorem 3.3.3 *(Existence and uniqueness of local constants)*
There exists a unique function ϵ associated to a $(K, \overline{K}, \psi, dx, V, \rho)$ composed of a local field K, an algebraic closure $\overline{K}$, an additive character ψ on K, an additive Haar measure dx, a complex finite dimensional vector space V and a representation $\rho : W(\overline{K}/K) \to GL(V)$, such that

1. *For each exact sequence of representations $V' \longrightarrow V \longrightarrow V''$*

$$\epsilon(V, \psi, dx) = \epsilon(V', \psi, dx)\epsilon(V'', \psi, dx)$$

2.

$$\forall\, a > 0, \quad \epsilon(V, \psi, adx) = a^{dim(V)}\epsilon(V, \psi, dx)$$

3. *If E is a finite separable subextension of $\overline{K}/K$ and V_K is a representation of $W(\overline{K}/K)$ induced by a representation V_L of $W(\overline{K}/L)$*

$$\epsilon(V_K, \psi) = \epsilon(V_L, \psi \circ Tr_{L/K})$$

4. *If $dim(V) = 1$, ρ corresponding to a quasi-character χ, we have*

$$\epsilon(V, \psi, dx) = \epsilon(\chi, \psi, dx)$$

I finish this section with some properties of ϵ-factors that will be needed later in this text.

Definition 3.3.3 *Let K be a non-archimedean local field, $\mathcal{O}_K$ its integer ring, π a uniformizing parameter. In accordance with the preceding notation we define the numbers $n(\psi)$ and $a(V)$ as:*

$n(\psi)$ is the largest integer n such that $\psi(\pi^{-n}\mathcal{O}_K) = 1$.

$a(\chi)$ is the exponent of the conductor of χ. It equals 0 if χ is unramified and is the smallest integer m such that χ is trivial on $U^{(m)} = 1 + \pi^n\mathcal{O}_K$ if χ is ramified.

Proposition 3.3.5 *(Properties of ϵ-factors)*
We keep the notations in use.

- $$\forall\, a > 0, \quad \epsilon(V, \psi(a\cdot), dx) = (det(V))(a)\|a\|^{-dim(V)}\epsilon(V, \psi, dx)$$
- $$\epsilon(V \otimes \omega_s, \psi, dx) = (f(V))^{-s}\delta(\psi)^{-s\, dim(V)}\epsilon(V, \psi, dx),$$

  where $\delta(\psi) = q^{n(\psi)}$ in the non-archimedean case and 1 in the archimedean case, $f(V)$ the absolute norm of the Artin conductor of V which is defined additively from the Artin conductors of characters (cf. paragraph "Artin vs Hecke" in 1.3.1). $f(V) = q^{a(V)}$ in the non-archimedean cases and 1 in others.

- *If K is non archimedean and W unramified (inertia invariant)*
$$\epsilon(V \otimes W, \psi, dx) = \epsilon(V, \psi, dx)^{dim(W)}\, det(W)(\pi^{a(V)+n(\psi)dim(V)})$$

Global case Let K be a global field, for any place $\mathfrak{p}$ let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$. Let $\mathbb{A}_K$ be the adèle group of K , dx a Tamagawa measure on $\mathbb{A}_K$ (i.e. $dx(\mathbb{A}_K/K) = 1$ and define the norm $\|\quad\|$ on $\mathbb{A}_K$ by $d(ax) = \|a\|dx$. Moreover define the quasi-character $\omega_s : \mathbb{A}_K^* \to \mathbb{C}$ by $\omega_s(a) = \|a\|^s$.

Let ψ be an additive character on $\mathbb{A}_K$ and denote its local component at a place $\mathfrak{p}$ by $\psi_\mathfrak{p}$. Similarly let χ be a quasi-character on $\mathbb{A}_K^* = \mathbb{I}_K$ and denote its local components by $\chi_\mathfrak{p}$.

We define the global L-function and global factor of χ and ψ by

$$L(\chi) = \prod_\mathfrak{p} L(\chi_\mathfrak{p}), \text{ and} \qquad \epsilon(\chi) = \prod_\mathfrak{p} \epsilon(\chi_\mathfrak{p}, \psi_\mathfrak{p}, dx_\mathfrak{p}).$$

Definition 3.3.4 *With the previous notation we define $L(s, V)$ and $\epsilon(s, V)$ by*

$$L(s, V) = L(V \otimes \omega_s), \text{ and} \quad \epsilon(V, s) = \epsilon(\chi, \omega_s \otimes \psi, dx).$$

The central theorem of this theory is then

Theorem 3.3.4 *(Functional equation)*
The previous products converge for s in some right half plane and define a function $L(V, s)$ which is meromorphic in the whole s-plane and satisfies the functional equation

$$L(V, s) = \epsilon(V, s)L(V^*, 1 - s),$$

where V^* is the contragredient representation.

Actually, for "classical" Artin L-function, the ϵ-factors can be computed because they come from Hecke L-functions with Grössencharakters for which they are known. For Weil L-functions these factors come from representations of Weil groups, what explains why they are uncomputable in general.

Chapter 4

The geometric objects case

4.1 The general picture

Let X be a scheme of finite type over Spec $\mathbb{Z}$, the residue field at a closed point $x \in X$ is finite, let $\mathbb{N}(x)$ denote its order. The zeta function of X is defined to be the Euler product

$$\zeta(X,s) = \prod_{x \in \overline{X}} \frac{1}{1 - \mathbb{N}(x)^{-s}},$$

where $\overline{X}$ is the set of closed point of X, the product is absolutely convergent for $\Re(s) > \dim\ X$ and we have in particular :

$$\zeta(X,s) = \begin{cases} \zeta(s) & \text{if } X = \operatorname{Spec} \mathbb{Z} \\ \zeta(s-n) & \text{if } X = \operatorname{Spec} \mathbb{Z}[T_1, \ldots, T_n] \\ \zeta_K(s) & \text{if } X = \operatorname{Spec}(\mathcal{O}_K) \end{cases} .$$

4.1.1 Étale and l-adique cohomology

The good settings to study these zeta functions is by cohomology. Étale cohomology has been constructed in order to prove the Weil conjectures in the general case and appears to be the correct basis for any further theory. For a general presentation of the subject I refer to Milne's notes [32]. In this section we introduce what is necessary to define l-adic cohomology.

If X and Y are non-singular varieties over an algebraically closed field a morphism $X \to Y$ is étale at a point if the corresponding map of tangent space is an isomorphism. In the case of schemes the definition is more involved. The term "étale" means "local isomorphism", in the case of schemes an *étale morphism* is a flat and unramified morphism:

Definition 4.1.1 *(flatness)*
A homomorphism of rings $A \to B$ is flat if the corresponding functor: $M \to M \otimes_A M$ from $A-$modules to $B-$modules is exact.

A morphism of schemes $\phi : X \to Y$ is flat if, for all $x \in X$, the corresponding local homomorphism $\mathcal{O}_{Y,\phi(x)} \to \mathcal{O}_{X,x}$ is flat.

Definition 4.1.2 *(ramification)*
A local homomorphism of local rings $f : A \to B$ is unramified if $B/f(m_A)B$ is a finite separable extension of A/m_A.
A morphism $\psi : X \to Y$ is unramified if it is of finite type (for the definition see [20] p. 84) and if, for all, $x \in X$ the map $\mathcal{O}_{Y,\phi(x)} \to \mathcal{O}_{X,x}$ is unramified.

Definition 4.1.3 *(Étale morphisms)*
A morphism of schemes $\phi : X \to Y$ is étale if it is flat and unramified (hence of finite type).

For the properties of étale morphism see [32] chap. 2.

In order to prove the Weil conjecture, one may hope to define a cohomology theory on schemes for which a Lefschetz fixed point formula holds as was remarked by Weil. Grothendieck in a paper of 1957 constructed a general topology theory for categories. The ambient space is a category and the topology on is defined by *a site.*

Definition 4.1.4 *(sites)*
Let $\mathbf{C}$ be a category. A site on $\mathbf{C}$ is defined by giving for every $U \in Ob(\mathbf{C})$ a set of families of arrows, $(U_i \to U)_{i\in U}$, called a coverings of U, subject to the following compatibility conditions:

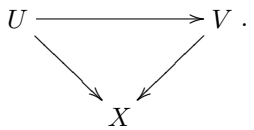
1. *for any covering $(U_i \to U)_{i\in I}$ and any arrow $V \to U$ of $\mathbf{C}$ the fiber products $U_i \times_U V$ exist and $(U_i \times_U V \to V)_{i\in I})$ is a covering of V;*

2. *if $(U_i \to U)_{i\in I})$ is a covering of U and if for each $i \in I$, $(V_{ij} \to U_i)_{j\in J_i}$, is a covering of U_i, then the composed family $(V_{ij} \to U)_{i,j}$ is a covering of U;*

3. *for any $U \in Ob((C))$ the family $(U \xrightarrow{id} U)$ is a covering of U.*

A compatible system of coverings on $\mathbf{C}$ is called a (Grothendieck) topology and a category $\mathbf{C}$ together with such a topology is called a site

If X is a scheme or a variety, we define the *étale site* on X, denoted X_{et} as the category Et/X whose objects are étales morphisms $U \to X$ and whose arrows are commutative triangles



The coverings of X_{et} being the families of étales morphism $(U_i \to U)_{i\in I}$.

A sheaf of sets on X_{et} (resp. groups, rings, A-modules...) is a contravariant functor $\mathcal{F} : Et/X \to \mathbf{Sets}$ (resp.$\mathbf{Ab}, \mathbf{Rg}, \mathbf{A\text{-}mod}, \ldots$) such that the following sheaf axiom is satisfied:

For any $(U \to X) \in Et/X$ (étale) and for any étale covering $(U_i \to U)_{i\in I}$, the following sequence is exact:

$$(\textit{sheaf axiom}) \quad \mathcal{F}(U) \to \prod_{i\in I} \mathcal{F}(U_i) \rightrightarrows \prod_{i,j} \mathcal{F}(U_i \times_U U_j)$$

With some technicalities, we can define a category, $\mathbf{Sh}(X_{et})$,whose objects are sheaves of abelian groups on Et/X and whose arrows are natural transformations. It can be shown (cf. [32]) that this category is abelian and possess enough injectives. The functor

$$\begin{array}{ccc} \mathbf{Sh}(X_{et}) & \longrightarrow & \mathbf{Ab} \\ \mathcal{F} & \longmapsto & \Gamma(X, \mathcal{F}) \end{array}$$

is left exact. So we can define classically the cohomology groups, $H^r(X_{et}, \cdot)$, by taking the rth right derived functor (cf. [23] for the corresponding theory).

There is a natural way to associate to $H^r(X_{et}, \cdot)$ a vector space with good properties ; the first step is to define

$$H^r(X_{et}, \mathbb{Z}_l) = \text{proj lim}_n H^r(X_{et}, \mathbb{Z}/l^n\mathbb{Z}),$$

where l is prime and $\mathbb{Z}/l^n\mathbb{Z}$ stands for the constant sheaf. Actually, there is a general construction for what are called l-adic sheafs but we don't need it. Then we define the vector spaces of l-adic cohomology by:

$$\forall r \geq 0, H^r(X_{et}, \mathbb{Q}_l) := H^r(X_{et}, \mathbb{Z}_l) \otimes \mathbb{Q}_l,$$

this space is also denoted $H^r_{et}(X, \mathbb{Q}_l)$.

4.1.2 Zeta functions for schemes over finite fields

Let X be a scheme over a finite field $\mathbb{F}_q$ ($q = p^f$). For all closed point $x \in \overline{X}$ (the set of closed points), the residue field $k(x)$ at x is a finite extension of $\mathbb{F}_q$, hence its cardinal is of the form $\mathbb{N}(x) = q^{\deg(x)}$ for $\deg(x) = [k(x) : \mathbb{F}_p]$. We define the "big" zeta function of X by

$$Z(X, t) = \prod_{x\in\overline{X}} \frac{1}{1 - t^{\deg(x)}},$$

whereas the classical zeta function is

$$\zeta(X, s) = Z(X, q^{-s}) = \prod_{x\in\overline{X}} \frac{1}{1 - \mathbb{N}(x)^{-s}}.$$

It can be shown (cf. [31]) by taking the developpement of log Z that:

$$Z(X,t) = \exp\left(\sum_{l=1}^{\infty} \text{Card } X(\mathbb{F}_{q^l})\ \frac{t^l}{l}\right),$$

where $X(\mathbb{F}_{q^l})$ is the number of point of X in $\mathbb{F}_{q^l}$.

The particular properties of Zeta functions over finite field are the subject of the celebrated Weil's conjectures of Weil (1949) whose proofs were completed by Deligne in 1973. They rest on the fact that a Lefschetz fixed-point formula holds for endomorphisms acting on étale cohomology groups.

More precisely

Definition 4.1.5 *The Frobenius morphism $F : X \to X$ of a scheme X over $\mathbb{F}_q$ is defined on every affine subscheme Spec $A \subset X$ by the ring homomorphism $a \mapsto a^q$; on the topological space, X, F acts as the identity.*

The Lefschetz-fixed point formula implies that

$$\text{Card } X(\mathbb{F}_{q^l}) = \sum_r (-1)^r \text{Tr}(F^l | H^r_{et}(X, \mathbb{Q}_l)),$$

where $\text{Tr}(\cdot)$ is the trace. This can be used to prove the rationality of $Z(X,s)$.

But the l-adic cohomology space are fundamental for other reasons.

One of them is that they furnish the correct point of view for Zeta and L-functions of varieties and schemes.

Let X be a non-singular projective variety over a finite field $\mathbb{F}_q$, $\overline{\mathbb{F}_q}$ the algebraic closure of $\mathbb{F}_q$ and $X^{ex} = X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ the variety obtained by extensions of scalars. For $l \neq p$ and for $m \geq 0$, we can define the l-adic cohomology space $H^m_{et}(X^{ex}, \mathbb{Q}_l)$ on which the Frobenius morphism acts by functoriality as an endomorphism $F_{l,m}$. Then we can define

$$P_{l,m}(X,T) = \det(1 - TF_{l,m} | H^m_{et}(X^{ex}, \mathbb{Q}_l)).$$

Then the following functions

$$\tilde{Z}(X,T) = \prod_{m=0}^{2\dim X} P_{l,m}(T)^{(-1)^{m+1}}$$

are taken as the basic zeta functions and equal the preceding definition in specialized cases.

4.1.3 The global case

In order to simplify the exposition, we consider only varieties in this section. The general case of scheme has been dealt with principally by Grothendieck and Deligne and can be found in the SGAs (Séminaire de Géométries Algébriques).

For details I refer to the text of Serre [46], it is to his merit to expose the principal ideas and conjectures of the subject.

Let K be a local field, we denote by M_K and M_K^∞ the sets of place and of finite places respectively. If $\mathfrak{p} \in M_K$ we denote by $K_\mathfrak{p}$ the local field obtained by completion of K at $\mathfrak{p}$ and by $\mathcal{O}_\mathfrak{p}$, $k(\mathfrak{p})$ and p the ring of integers, the residue field and the residue characteristic at $\mathfrak{p}$ respectively. For simplicity we suppose that $k(\mathfrak{p})$ is finite. The construction depends essentially on the finite field case.

Let X be a non-singular projective variety over K. Let $S \subset M_K$ be a finite subset such that X has good reduction apart from S. This means that, for all $\mathfrak{p} \in M_K \setminus S$, there exists a smooth projective $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})-$scheme, $X_\mathfrak{p}$, such that $X_\mathfrak{p} \times_{\mathcal{O}_\mathfrak{p}} K_\mathfrak{p} \cong X \times_K K_\mathfrak{p}$. For such an $X_\mathfrak{p}$, we denote $X(\mathfrak{p}) = X_\mathfrak{p} \times_{\mathcal{O}_\mathfrak{p}} k(\mathfrak{p})$ its reduction modulo $\mathfrak{p}$.

As $X(\mathfrak{p})$ verifies the Weil conjecture, we can associate a polynomial $P_{m,\mathfrak{p}} \in \mathbb{Z}[T]$ to it, as done in the previous section, its degree B_m is the $m-th$ Betti number of X.

Then we can define

$$\zeta_S(s) = \prod_{\mathfrak{p} \in M_K \setminus S} \frac{1}{P_{m,\mathfrak{p}}(\mathfrak{N}(\mathfrak{p})^{-s})}$$

which is absolutely convergent in the right half plane $\Re(s) > 1 + m/2$. It implies that $\zeta_S(s)$ is holomorphic in this right half plane and that is the sum of a Dirichlet series with integral coefficients.

The question of analytic continuation and of functional equation is difficult. We know that, for abelian varieties of C.M. type, we there is an analytic continuation to the left of $\Re(s) > m + 1$ and for certain cases of automorphy or modularity as for elliptic curves over $\mathbb{Q}$ with help of Wiles' big theorem.

In all these cases, their exist an rational number $A > 0$, a polynomial $P_{m,\mathfrak{p}}$ for each $\mathfrak{p} \in S$, and gamma factors, $\Gamma_\mathfrak{p}(s)$ for $\mathfrak{p} \in M_K^\infty$ such that if we put

$$\zeta(s) = \zeta_S(s) \prod_{\mathfrak{p} \in S} \frac{1}{P_{m,\mathfrak{p}}(\mathfrak{N}(\mathfrak{p})^{-s})}, \text{ and then } \quad \xi(s) = A^{s/2}\zeta(s) \prod_{\mathfrak{p} \in M_K^\infty} \Gamma_\mathfrak{p}(s)$$

then the following functional equation holds:

$$(*) \qquad \xi(s) = w\,\xi(m+1-s), \quad w = \pm 1.$$

Jean-Pierre Serre in [46] gives precise conjectures about the possible definition of the previous factors A and $P_{m,\mathfrak{p}}$, $(\mathfrak{p} \in S)$. The previous ones seem to depend on the l-adic cohomology of the varieties $X \times_K K_\mathfrak{p}$ whereas the $\Gamma_\mathfrak{p}$, $(\mathfrak{p} \in M_K^\infty)$, depend on the Hodge decomposition of the complex cohomology of $X \times_K K_\mathfrak{p}$.

The bad reduction case: $\mathfrak{p} \in S$ Let $\mathfrak{p}$ be a finite place of K, let $\overline{K_\mathfrak{p}}$ and $G = \mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$. Let $l \neq p = \mathrm{char}(k(\mathfrak{p}))$, to (V, ρ), an l-adic representation, i.e. V is a d-dimensional vector space over $\mathbb{Q}_l$ and

$$\rho : G \longrightarrow \mathrm{Aut}(V)$$

a continuous representation , Serre associates in [46] two non-negative integers ϵ and δ which define the "ramification" of ρ in some sense. He defines $f(\mathfrak{p}) = \epsilon + \delta$.

Remind that we supposed that $k(\mathfrak{p})$ is finite. If I is the inertia group, G/I comes with the Frobenius generator ϕ that induces an automorphism of V^I called the geometric Frobenius and denoted F_ρ. Then we define

$$P_\rho(T) = \det(1 - TF_\rho | V^I).$$

If X is a non-singular projective variety over $K_\mathfrak{p}$, if $m \geq 0$ is an integer and if $l \neq p$ we define

$$V_l = H^m_{et}(X \times_{K_\mathfrak{p}} \overline{K_\mathfrak{p}}).$$

Then $G = Gal(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ acts on V_l which defines an l-adic representation ρ_l. Serre's conjecture C_8 in [46] permits to define:

$$P_{m,\mathfrak{p}} = det(1 - TF_{\rho_l} | V_l^I), \text{ for } \mathfrak{p} \in S.$$

The gamma factors:$\mathfrak{p}|\infty$ The definition of Γ-factors depend on Hodge structures on the complex cohomology space and on the theorem of Hodge given below.

An integral complex Hodge structure of weight $k \in \mathbb{Z}$ on a complex vector space $V_\mathbb{C}$, is a decomposition

$$V_\mathbb{C} = \bigoplus_{p+q=k} V^{p,q}, \quad \text{such that } V^{p,q} = \overline{V^{q,p}} \quad \text{(the complex conjugate)}.$$

A real integral Hodge structure of weight k on a complex vector space $V_\mathbb{C}$ is a complex decomposition of wight k together with an automorphism J of $V_\mathbb{C}$ such that $J^2 = 1$ and $J(V^{p,q}) = V^{q,p}$ for all $p + q = k$.

Let X be a complex variety, we denote by $A^k_\mathbb{C}(X)$ the space of complex differential forms of degree k on X. Elements of $A^k_\mathbb{C}(x)$ are $\mathcal{C}^\infty$ sections of the vector bundle Ω^k_X of differential forms of degree k. We have a natural (De Rham) complex given by the exterior differential d

$$d : A^k_\mathbb{C} \longrightarrow A^{k+1}_\mathbb{C}$$

such that $d \circ d = 0$. This allows to define the k-th complex cohomology group by:

$$H^k(X, \mathbb{C}) := \frac{\text{Ker}(d : A^k_\mathbb{C}(X) \to A^{k+1}_\mathbb{C}(X))}{\text{Im}(d : A^{k-1}_\mathbb{C}(X) \to A^k_\mathbb{C}(X))}$$

. The following due to Hodge is proved in [56] in which Claire Voisin develop Hodge theory and more.

Theorem 4.1.1 *(Hodge)$H^k(X, \mathbb{C})$ admits a Hodge decomposition*

$$H^k(X, \mathbb{C}) = \bigoplus_{p+q=k} H^{p,q}(X) \quad \textit{such that } H^{p,q}(X) = \overline{H^{q,p}(X)},$$

where $H^{p,q}(X)$ is given by the set of closed forms of type (p, q) on each $x \in X$.

If X is a complex non-singular variety over a global field K there are two cases of infinite places

- If $\mathfrak{p}$ is a complex place of K, then from what Hodge theorem we can consider the group $H^k(X(K_\mathfrak{p}), \mathbb{C})$ and the corresponding Hodge decomposition.
- If $\mathfrak{p}$ is a real place of K, $\mathbb{C}$ is a quadratic extension of $K_\mathfrak{p}$ and we can consider the group $H^k(X(\mathbb{C}), \mathbb{C})$ and its Hodge decomposition. Furthermore, complex conjugation on $\mathbb{C}$ induces a real Hodge structure on this space.

To clarify the exposition, we will suppose that the following spaces and their decomposition are the preceding ones without mentioning them.

Definition 4.1.6 *(Gamma factor at complex places)*
If $V^k = \bigoplus V^{p,q}$ is a complex vector spaces endowed with a Hodge structure we define

$$\Gamma_V = \prod_{p+q=k} \Gamma_{\mathbb{C}}(s - \inf(p,q))^{\dim\ V^{p,q}}.$$

where $\Gamma_{\mathbb{C}}$ is the gamma function defined in 1.3.2

If $V = \bigoplus_{p+q=k} V^{p,q}$ is a real Hodge decomposition with automorphism J, Serre defines a decomposition

$$V^{n,n} = V^{n,+} \oplus V^{n,-}$$

from the invariance of $V^{n,n}$ under J, where:

$$V^{n,+} = \{x \in V^{n,n} | J(x) = (-1)^n x\}$$
$$V^{n,-} = \{x \in V^{n,n} | J(x) = (-1)^{n+1} x\}$$

Definition 4.1.7 *(Gamma factors at real places). With the preceding notations, if $V^k = \bigoplus V^{p,q}$ is a real Hodge decomposition, we define the gamma factor*

$$\Gamma_V(s) = \prod_{2n=k} \Gamma_{\mathbb{R}}(s-n)^{\dim\ V^{n,+}} \Gamma_{\mathbb{R}}(s-n+1)^{\dim\ V^{n,-}} \prod_{p<q, p+q=k} \Gamma_C(s-p)^{\dim\ V^{p,q}},$$

where $\Gamma_{\mathbb{C}}$ and $\Gamma_{\mathbb{R}}$ are defined in 1.3.2 .

The constant A Remind that we consider a number $f(\mathfrak{p})$ attached to an l-adic representation of $\mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ for $\mathfrak{p}$ a place of bad reduction. This factor is completely defined in [46] and we associate to it a divisor

$$\mathfrak{f} = \sum_{\mathfrak{p} \in S} \mathfrak{p}^{f(\mathfrak{p})}$$

and its corresponding norm

$$\mathfrak{N}(\mathfrak{f}) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{f(\mathfrak{p})}.$$

Moreover, we define

$$D = \begin{cases} |d_{K/\mathbb{Q}}|, & \text{if } K \text{ is a number field} \\ q^{2g-2}, & \text{if } K \text{ is a function field of genus } g \text{ over } \mathbb{F}_q \end{cases}$$

The constant A of the functional equation is then conjecturally equal to

$$A = \mathfrak{N}(\mathfrak{f}) D^{B_m},$$

where B_m is the m-th Betti number of X.

Conjecture 4.1.1 *With the preceding definition, and with*

$$\xi(s) = A^{s/2}\zeta(s) \prod_{\mathfrak{p}|\infty} \Gamma_{\mathfrak{p}}(s)$$

the following functional equation holds :

$$\xi(s) = w\xi(m+1-s), \quad \textit{with } w = \pm 1.$$

4.2 L-functions

Here we present L-function with the help of what we previously learned.

4.2.1 Weil groups again: The Weil-Deligne group

We saw that l-adic representations are of special importance in the theory of L-functions. However some l-adic representations of usual Weil's group don't provide good objects because we can't associate them continuous complex representations which are natural in the theory of L-functions.

The reason for this is that, if K is a local non-archimedean field, a complex representation $\rho : W_K \to Gl_n(\mathbb{C})$ is by definition a continuous group homomorphism. In order to be continuous, it is necessary and sufficient (cf. [42]) that ρ be trivial on a open subgroup of I_K (the inertia group seen as a subgroup of $\mathrm{Gal}(\overline{K}/K)$ with the Krull topology), whereas it is not true for important cases of l-adic representations. The way to bypass this is to consider representations of a larger group: *the Weil-Deligne group*

Let K be an non-archimedean local field. Remind from **1.3.3 Special cases**, that we have an identification

$$W_K = \bigcup_{n\in\mathbb{Z}} \Phi^n I_K,$$

where Φ maps to the inverse of the Frobenius endomorphism of $Gal(\overline{k}/k)$ for k the residue field of K. There is a natural quasi-character ω of W_K given by

$$\omega : \begin{array}{ccc} W_K & \longrightarrow & \mathbb{C}^\times \\ I_K & \longmapsto & \{1\} \\ \Phi & \longmapsto & q^{-1} \end{array},$$

ω is unramified by definition.

Definition 4.2.1 *(Weil-Deligne group)*
The Weil-Deligne group $\mathcal{W}_K$ of K is the semidirect product

$$\mathcal{W}_K := W_K \ltimes \mathbb{C}$$

where the action of W_K on $\mathbb{C}$ is given by

$$\forall g \in W_K, \forall z \in \mathbb{C}, \quad gzg^{-1} = \omega(g)z.$$

Actually the Weil-Deligne group may be seen as a group scheme over $\mathbb{Q}$ as in [55] (definition (4.1.1)) or [9] (8.3.6) but we don't need this.

If L/K is a finite separable extension of K and if Φ_L is an inverse Frobenius of L, i.e. if Φ_L is mapped to the geometric Frobenius F_L de $\mathrm{Gal}(\overline{k}/l)$ then as an element of $\mathrm{Gal}(\overline{k}/k)$, $F_L = F^{f(L/K)}$, where F is the geometric Frobenius of $\overline{k}/k$ and $f(L/K)$ is the residue class degree. So $\omega(\Phi_L) = q_L^{-1}$ and

$$\omega | W_L = \omega_L.$$

Hence, $\mathcal{W}_L$ may be viewed as a subgroup of $\mathcal{W}_K$.

A representation of $\mathcal{W}_K$ over a complex vector space V is a continuous homomorphism

$$\rho : \mathcal{W}_K \to GL(V).$$

This is equivalent to the following definition

Definition 4.2.2 *A (resp. l-adic) representation of $\mathcal{W}_K$ over a (resp. $\mathbb{Q}_l$)complex vector space V (resp. V_l) is a pair $\rho' = (\rho, N)$ (resp. (σ_l, N_l)) consisting of*

1. *a homomorphism $\rho : \mathcal{W}_K \to GL(V)$ (resp.V_l) which is trivial on an open subgroup of I_K.*
2. *a nilpotent endomorphism N of V (resp. N_l of V_l) such that $\rho(g)N\rho(g)^{-1} = \omega(g)N$, for all $g \in W_K$. (resp. $\sigma_l(g)N_l\sigma_l(g)^{-1} = \omega(g)N_l$)*

One obtains a representation of $\mathcal{W}_K$ by putting:

$$\rho'(gz) = \rho(g)exp(zN), \text{ for } g \in W_K \text{ and } z \in \mathbb{C},$$

so that

$$N = \frac{\log \sigma'(z)}{z}$$

which as a sense because ([42], p.129) $\sigma'(z)$ is unipotent.

It is straightforward to verify that if $\sigma' = (\sigma, N)$ and $\tau' = (\tau, P)$ are two representations of $\mathcal{W}_K$:

- $\sigma' \oplus \tau' = (\sigma \oplus \tau, N \oplus P)$
- $\sigma' \otimes \tau' = (\sigma \otimes \tau, N \otimes 1 \oplus 1 \otimes P)$, 1 being the adequate identity automorphism.

What are of particular importance for us are l-adic representations σ_l of $\mathrm{Gal}(\overline{K}/K)$, i.e. continuous group homomorphism

$$\sigma_l : Gal(\overline{K}/K) \to Gl(V_l),$$

where V_l is a finite dimensional $\mathbb{Q}_l$-vector space. The reason for us to consider Weil-Deligne groups and their representations is that there is a simple method, due to Grothendieck and Deligne, for associating to an l-adic representation σ_l of $Gal(\overline{K}/k)$ a complex representation $\sigma'_{l,\imath}$ of $\mathcal{W}_K$ for an embedding $\imath : \mathbb{Q}_l \to \mathbb{C}$.

Actually, if σ_l is an l-adic representation of $\mathcal{W}_K$, composing it with the extension of scalars $Gl(V_l) \hookrightarrow Gl(\mathbb{C} \otimes_\imath V_l$ gives

$$\sigma_{l,\imath} : \mathcal{W} \to Gl(\mathbb{C} \otimes_\imath V_l).$$

Similarly, applying extension of scalars $End(V_l) \hookrightarrow End(\mathbb{C} \otimes_\imath V_l)$ gives $N_{l,\imath}$.

So representations of the Weil-Deligne group will be of use to us.

Definition 4.2.3 *A representation $\sigma' = (\sigma, N)$ of $\mathcal{W}_K$ is called Φ-semisimple or admissible if σ is semisimple.*

A representation σ' is called indecomposable if it space can not be written as a direct sum of invariant spaces.

Actually, a representation σ' is Φ-semisimple if $\sigma(\Phi)$ is semi-simple for some inverse Frobenius element Φ.

There is a particular representation which play a central role, they are called special representations and defined by :

Definition 4.2.4 *(Special representation)*

Let $e_0, e_1, \ldots, e_{n-1}$ be the canonical basis for $\mathbb{C}^n$. The special representation of dimension n, denoted $sp(n)$, is the representation $\sigma' = (\sigma, N)$ of $\mathcal{W}_K$, where :

- $\forall g \in \mathcal{W}_K, \forall \quad 0 \leq j \leq n-1, \qquad \sigma(g)e_j = \omega(g)^j e_j$
- $\forall\, 0 \leq j \leq n-2,\ Ne_j = e_{j+1},\ and\ Ne_{n-1} = 0$

The special representation is admissible, indecomposable, n-dimensional. (e.g. see [42] p. 132). Special representations appears in particular if we want to characterize admissible indecomposable representation which is the purpose of the following proposition.

Proposition 4.2.1 *([42] p. 133) Every admissible indecomposable representation of $\mathcal{W}_K$ is equivalent to a representation of the form $\pi \otimes sp(n)$, where π is an irreducible representation of $\mathcal{W}_K$ and n is a positive integer.*

It is a proposition of Deligne in *Modular functions in one variable II, Formes modulaires et representations of Gl(2)*

Furthermore, admissible indecomposable representations of $\mathcal{W}_K$ satisfy the equivalence of Schur's lemma for this case.

Rohrlich in [42] page 133 prove the following corollary by induction on virtual representations.

Proposition 4.2.2 *([42] p. 133)*
Let σ' be an admissible representation of $\mathcal{W}_K$. Then

$$\sigma' = \bigoplus_{j=1}^{s} \pi_j \otimes sp(n_j)$$

where π_j is an irreducible representation of $\mathcal{W}_K$ and n_j is a positive integer. Furthermore, if

$$\sigma' = \bigoplus_{j=1}^{t} \rho_j \otimes sp(m_j)$$

then $s = t$, and after renumbering the summands $n_j = m_j$ and $\pi_j \cong \rho_j$.

There is a natural Φ-semisimple representation associated to any representation of $\mathcal{W}_K$.

Definition 4.2.5 *([55] (4.1.3) and [9] (8.5)) Remind that ω denote the unramified character of $\mathcal{W}_K$ which takes the value q^{-1} on any Frobenius element. Thus there exists a map $v : W_K \to \mathbb{Z}$ such that $\omega(g) = q^{-v(g)}$*

Let $\sigma' = (\sigma, N)$ be a representation of $\mathcal{W}_K$ on a vector space V, there exists a unique unipotent automorphism u of V such that u commutes with N and $\sigma(W_K)$ and such that $\exp(aN)\rho(g)u^{-v(g)}$ is a semisimple automorphism of V for all $a \in K$ and all $g \in W_K \setminus I$. Then $\sigma'_{ss} = (\sigma u^{-v}, N)$ is called a $(\Phi-)$semisimplification of σ' and σ' is $(\Phi-)$semisimple if and only if $\sigma' = \sigma'_{ss}$, which means that the Frobenius acts semisimply.

4.2.2 Conductors and ϵ-factors

As usual, let $\mathcal{O}_K$ and π_K be the ring of integers and a uniformizer of K. If $\sigma' = (\sigma, N)$, is a representation of the Weil-Deligne group $\mathcal{W}_K$, Deligne in [9] define the conductor of σ'. It is an ideal of $\mathcal{O}_K$, denoted $\mathfrak{N}(\sigma')$, hence it takes the form :

$$\mathfrak{N}(\sigma') = \pi_K^{a(\sigma')}\mathcal{O}_K.$$

The exponent of the conductor of σ', i.e. $a(\sigma')$ is an integer which is related to the exponent of the conductor, $a(\sigma)$ of σ by :

$$a(\sigma') = a(\sigma) + b(\sigma'),$$

where $b(\sigma') = \mathrm{Codim}(V_N^I)$ for $V_N^I = V^I \cap \ker N$ and V^I is the invariant subspace of V under the inertia. In order to define $a(\sigma)$ we need more framework.

Remind that the inertia can be defined as $I = \mathrm{Gal}(\overline{K}/K^{ur})$ where $\overline{K}$ is a separable closure of K and K^{ur} is the maximal unramified subextension of $\overline{K}/K$. At present, let R be a finite Galois extension of K^{ur} such that σ is trivial on the subgroup $\mathrm{Gal}(\overline{K}/R)$, and put $G = \overline{Gal}(R/K^{ur})$. If v_R is the valuation on R then we have a filtration $G = G_0 \supset G_1 \supset G_2 \supset \cdots$ by higher ramification groups :

$$G_j = \{g \in G | v_R(g(\pi_R) - \pi_R) \geq j + 1\},$$

where π_R is a uniformizer on R. Then we define :

$$a(\sigma) = \sum_{j=0}^{\infty} \frac{\mathrm{Card}(G_j)}{\mathrm{Card}(G)} \mathrm{Codim}(V^{G_j}).$$

This generalize the case of characters. This exponent satisfies the following properties (e.g. [42] p. 141)

Proposition 4.2.3 *([42] p. 141) Let σ' and τ' be representations of $\mathcal{W}_K$, let L be a finite subextension of $\overline{K}/K$, $d(L/K)$ (resp. $f(L/K)$) be the exponent of the relative discriminant of L/K (resp. the residue class degree of L over K) and ρ' a representation of $\mathcal{L}$, then*

1. $a(\sigma' \oplus \tau') = a(\sigma') + a(\tau')$
2. $a(Ind_{L/K}\rho') = dim(\rho')d(L/K) + f(L/K)a(\rho')$

In the case of admissible indecomposable representations, Rohrlich proved the following proposition :

Proposition 4.2.4 *([42] p.141) Let $\sigma' = \pi \otimes sp(n)$ be an admissible indecomposable representation (proposition 4.2.1), where π is an irreducible representation of $\mathcal{W}_K$ and n is a positive integer. Then*

$$a(\sigma') = \begin{cases} na(\pi) & \text{if } \pi \text{ is ramified} \\ n-1 & \text{if } \pi \text{ is unramified} \end{cases}.$$

ϵ-factors We defined previously ϵ-factors in the case where we are given a tuple $(K, \overline{K}, \psi, dx, V, \sigma)$ (theorem 3.3.3) and we would like to define a similar constant for a representation $\sigma' = (\sigma, N)$ of $\mathcal{W}_K$. It was done by Deligne in [9] but the exposition of Rohrlich in [42] is straightforward.

Definition 4.2.6 *(ϵ-factors) Let $K, \overline{K}, \psi$ and dx be as usual (theorem 3.3.3) and let now $\sigma' = (\sigma, N)$ be a representation of $\mathcal{W}_K$. Let $\epsilon(\sigma, \psi, dx)$ be the epsilon factor of theorem 3.3.3, then :*

$$\epsilon(\sigma', \psi, dx) = \epsilon(\sigma, \psi, dx)\delta(\sigma'),$$

where

$$\delta(\sigma') = \det(-\sigma(\Phi)|V^I/V_N^I).$$

For this, we have properties given in 3.3.3 together with :

- $\delta(\sigma' \oplus \tau') = \delta(\sigma')\delta(\tau')$
- $\delta(\mathrm{Ind}_{L/K}\rho') = \delta(\rho')$

with the preceding notations (e.g. proposition 4.2.3). The article of Rohrlich [42] contains the essential formulas, from which the following will be of importance to us.

- ([42] Lemma p.144) If ψ is a character of K there exists a unique Haar measure dx_ψ on K such that the Fourier transform on the Schwartz space $\mathcal{S}(K)$ is an isometry of the L^2 norm. We call such a measure a *self-dual measure.*

  Let σ'

4.2.3 L-$\star$

Definition 4.2.7 *Let $\sigma' = (\sigma, N)$ be a representation of $\mathcal{W}_K$ on a complex vector space V and I the inertia group of $\overline{K}/K$. As usual $V^I = V^{\sigma(I)}$ is the $I-$invariant subspace of V. Let $V_N^I = V^I \cap \ker N$, as two inverse Frobenius element differ by an element of I, the action of $\sigma(\Phi)$ on V_N^I is independent of the inverse Frobenius Φ. Thus the following definition of the L-factor attached to σ' makes sense :*

$$L(\sigma', s) = \det(1 - q^{-s}\sigma(\Phi)|V_N^I)$$

This definition is similar to the definition of Artin L-functions we are know far from our Riemann-Dirichlet's origins. The similarity goes further :

Proposition 4.2.5 *([42] p. 137-138)*
Let σ' and τ' be representation of $\mathcal{W}_K$, L/K a finite extension and ρ' a representation of $\mathcal{W}_L$. Then :

- $L(\sigma' \otimes \tau', s) = L(\sigma', s)L(\tau', s)$
- $L(Ind_{L/K}\rho', s) = L(\rho', s)$

If l is a prime different from the characteristic p and $\sigma'_l : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V_l)$ is an l-adic representation they are two natural way to construct an L-factor.

- The first one, in the continuation of what precede, is to consider an embedding $\imath : \mathbb{Q}_l \to \mathbb{C}$ and then to construct the representation $\sigma'_{l,\imath} = (\sigma_{l,\imath}, N_{l,\imath})$ of the Weil-Deligne group $\mathcal{W}_K$ which gives us $L(\sigma'_{l,\imath}, s)$
- The other way is, given an embedding $\imath : \mathbb{Q}_l \to \mathbb{C}$, to define :

$$L(\sigma'_l, \imath, s) = \imath(\det(1 - x\sigma'_l(\Phi)|V_l^I))^{-1}|_{x=q^{-s}}$$

Actually, this two definitions agree :

Proposition 4.2.6 *([42] p. 139)With the previous notations :*

$$L(\sigma'_l, \imath, s) = L(\sigma'_{l,\imath}, s)$$

Furthermore, we define the root number associated to an algebraically closed extension of local field $\overline{K}/K$, an Haar measure dx on K, a character ψ of K and a representation σ' of the Weil-Deligne group $\mathcal{W}_K$ by

$$W(\sigma', \psi) = \frac{\epsilon(\sigma', \psi, dx)}{|\epsilon(\sigma', \psi, dx)|}.$$

Usually, we take for dx a self-dual measure with respect to dx and denote the resulting factor by $W(\sigma')$.

Part II

Parity conjecture for elliptic curves

Chapter 5

Elliptic Curves

For basic facts about algebraic geometry and elliptic curves see [20], [27], [52] and, [53], among others.

An elliptic curves is an abelian variety of dimension 1, i.e. it is a complete, non-singular, connected curve of genus one with a specified rational point denoted O. What are of particular importance to us are elliptic curves over finite fields, over local fields and ("of course") over number fields. It is worth noting that elliptic curves have a long history going back to the computation of the arc length of ellipses. On $\mathbb{C}$, an elliptic curve is up to homothety of the form $\mathbb{C}/\Lambda$ where Λ is a lattice in $\mathbb{C}$ (i.e. a discrete subgroup which contains an $\mathbb{R}-$ basis), thus an elliptic curve over $\mathbb{C}$ looks like a torus (e.g. [52] ch. VI).

Let E/K be an elliptic curve over a field K, then ([52] Prop. 3.1 p. 63) E can be embedded in the projective plane $\mathbb{P}^2(K)$ as a cubic curve with the following type of equation :

Weierstrass Equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_1, a_2, \cdots, a_6 \in K$ and such that the basepoint O is represented by $(0:1:0)$.

This defining equation can be simplified (e.g. [52] p.46-47) if $\mathrm{char}(\overline{K}) \neq 2$ and $\mathrm{char}(\overline{K}) \neq 2, 3$ as follows.

Weierstrass equation for char$(\overline{K}) \neq 2$

$$Y^2Z = 4X^3 + b_2X^2Z + 2b_4XZ^2 + b_6Z^3.$$

Weierstrass equation for char$(\overline{K}) \neq 2, 3$

$$Y^2Z = X^3 - 27c_4XZ^2 - 54c_6Z^3.$$

Where the coefficients are given by

$$\begin{array}{ll} b_2 = a_1^2 + 4a_2 & c_4 = b_2^2 - 24b_4 \\ b_4 = 2a_4 + a_1a_3 & c_6 = -2b_2^3 + 36b_2b_4 - 216b_6 \\ b_6 = a_3^2 + 4a_6 & \end{array} .$$

Furthermore let us define to important quantity Δ and j called respectively the discriminant and the $j-$invariant of the elliptic curve by

$$\Delta(E) = \frac{c_4^3 - c_6^2}{1728} \qquad j(E) = \frac{c_4^3}{\Delta(E)}.$$

A curve given by a Weierstrass equation has at most one singular point :

Proposition 5.0.7 *(proposition 1.4 p.50 of [52]) The curve given by a Weierstrass equation can be classified as follows.*

1. *It is non-singular if and only if $\Delta \neq 0$.*
2. *It has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.*
3. *It has a cusp if and only if $\Delta = c_4 = 0$.*

Moreover to elliptic curves over K are isomorphic over $\overline{K}$ is and only if they have the same $j-$invariant and every element of $\overline{K}$ can be the $j-$ invariant of an elliptic curve on an appropriate field.

What is a particular characteristic of elliptic curves (and abelian varieties) is that there definition implies that they are endowed with an algebraic group law. Namely, for this law, three points P_1, P_2, P_3 sum to O if and only if the *Weil* divisor $P_1 + P_2 + P_3$ is the intersection of E with a line.

The natural morphisms for elliptic curve are called an isogenies and are defined as follows :

Definition 5.0.8 *(Isogenies) Let E and E' be elliptic curves, an isogeny between E and E' is a morphism*

$$\phi : E \to E'$$

such that $\phi(O) = O$.

From the theory of curves (e.g. [52] ch. II), an isogeny is either trivial or surjective. As an elliptic curve is an algebraic group, we have the following natural isogenies : let m be a positive integer we define the isogeny $[m]$, called the multiplication by m map, by

$$[m]P = \underbrace{P + P + \cdots + P}_{m \text{ times}},$$

for every $P \in E$.

An interesting property of isogenies is that they are nearly "invertible" in the sense of the following theorem

Theorem 5.0.1 *([52] ch. III) Let $\phi : E \to E'$ be an isogeny of degree m.*

- *There exists a unique isogeny, called the dual isogeny,*

$$\hat{\phi} : E' \to E$$

satisfying

$$\hat{\phi} \circ \phi = [m].$$

- *This last isogeny being defined, it also satisfies*

$$\phi \circ \hat{\phi} = [m] \text{ on } E'.$$

If $\phi : E \to E'$ is an isogeny, let us define $E(\phi)$ by $E(K)[\phi] = \ker(\phi : E(K) \to E'(K)$ and $E[\phi] = E(\overline{K})[\phi]$, in particular for the endomorphism $[m]$ we will denote it $E[m]$. This last group is of the following kinds

Proposition 5.0.8 *([52] Ch. III Cor. 6.4 p 89) Let E/K be an elliptic curve over a field K and m be a nonnegative integer then*

1. *If $char(K) = 0$ and if m is prime to $char(K)$, then*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

2. *If $char(K) = p$, prime, then either :*

$$\begin{array}{ll} E[p^e] = \{O\} & \text{for all } e = 1, 2, \ldots; \text{or} \\ E[p^e] = \mathbb{Z}/p^e\mathbb{Z} & \text{for all } e = 1, 2, \ldots. \end{array}$$

When K is of characteristic p and $E[p^e] = \{O\}$ for all e, we say that E is *supersingular* otherwise we say that it is *ordinary*.

From the definition of elliptic curves we can deduce the notable fact that it is an algebraic group, the second notable fact is that *isogenies are actually algebraic group homomorphisms* (e.g. [52] Ch. III Th. 7.5).

From the groups $E[l^n]$ we can construct a Galois representation which is actually the Galois representation that come from $l-$adic cohomology groups H^1(e.g. ch.4) and so can be used to construct the L-functions.

Let E/K be an elliptic curve and $\overline{K}$ the algebraic closure of K. Then $\mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$ because, for $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $P \in E[m]$, $[m]P^\sigma = ([m]P)^\sigma = O$. This gives a representation :

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]).$$

This is far from sufficient for our purpose as we would like $l-$adic representation. The purpose of the following theorem is to define a $\mathbb{Z}_l-$module which tensored by $\mathbb{Q}_l$ will be of use :

Definition 5.0.9 *Let E be an elliptic curve and l a prime. The $l-$adic Tate module of E is :*

$$T_l(E) := proj\ lim_n E[l^n],$$

the inverse limit coming from the natural maps

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]\ .$$

From the previous proposition (prop. 5.0.2) we deduce immediately

Proposition 5.0.9 *The Tate module of E/K is a $\mathbb{Z}_l$ module and has the following structure :*

- $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ *if* $l \neq char(K)$.
- $T_p(E) = 0$ *or* $\mathbb{Z}_p$ *if* $p = char(K) > 0$

Furthermore, the action of $\mathrm{Gal}(\overline{K}/K)$ on each $E[l^n]$ commutes with the multiplication by l map, so it acts on the Tate module $T_l(E)$. Further as $E[m]$ is finite, it is a discrete $\mathrm{Gal}(\overline{K}/K)$-module, so this action is continuous ([38] ch. I prop. (1.1.8)) and the resulting action on $T_l(E)$ is also continuous. To obtain an action over an vector space we put :

$$V_l(E) := T_l(E) \otimes \mathbb{Q}_l,$$

which gives the $l-$adic representation denoted $\rho_{E,l}$:

$$\rho_{E,l} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Q}_l}(V_l(E)).$$

5.1 Basic facts

The natural objects of study are elliptic E curves over number fields K. The notable fact is that the group $E(K)$ is finitely generated, this is known as the Mordell-Weil theorem. However we won't be concerned by this here but by the machinery of number fields, their completion to local fields and the reduction to finite fields. This goes as follows : Let M_K be the set of places of the number field K and $\mathfrak{p} \in M_K$, let $K_\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$, $m_\mathfrak{p}$, $k_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/m_\mathfrak{p}$ be the corresponding completion, ring of integers, its maximal ideal and residue field respectively.

Definition 5.1.1 *With the preceding notations, one says that E/K has good reduction at $\mathfrak{p}$ if one can find a coordinate system in $\mathbb{P}^2(K)$ such that the corresponding equation of E has coefficient in $\mathcal{O}_\mathfrak{p}$ and its reduction mod $m_\mathfrak{p}$ defines a non-singular cubic $\tilde{E}_\mathfrak{p}$, called the reduction of E at $\mathfrak{p}$.*

5.1.1 Elliptic curves over local fields

If E/K is an elliptic curves over a local field, we define its reduction $\tilde{E}(k)$ the corresponding reduction according to the preceding definition (k denote the residue field of the local field K), the reduced curve can be singular in general. We denote $K, \mathcal{O}_K, m_K, k = \mathcal{O}_K/m_K, v : K \to \mathbb{Z}$ a local field, its ring of integer, the corresponding maximal ideal, the residue field and the valuation of K.

We need to define the sets

$$E_0(K) = \{P \in E(K) | \tilde{P} \in \tilde{E}_{ns}(k)\},$$
$$E_1(K) = \{P \in E(K) | \tilde{P} = \tilde{O}\},$$

where $\tilde{E}_{ns}(k)$ denote the set of non-singular point of the curve $\tilde{E}/k$. The following sequence is exact (e.g. [52] ch. VII prop. 2.1)

$$0 \longrightarrow E_1[K] \xrightarrow{\text{injection}} E_0(K) \xrightarrow{\text{reduction}} \tilde{E}_{ns}(k) \longrightarrow 0\ .$$

If $K = K_v$ is the completion of a number field at a finite place $v \in M_K^0$ we denote

$$c_v = (E(K_v) : E_0(K_v))$$

and call it the local Tamagawa number at v.

From all Weierstrass equations that define an elliptic curve over a local field with $a_1, a_2, \ldots, a_6 \in \mathcal{O}_K$ we can select the one for which the valuation of the discriminant is minimal (see [52] ch. VII ğ1).

Definition 5.1.2 *Let E/K be an elliptic curve the minimal Weierstrass equation of E over K is such that $v(\Delta(E))$ is minimal with the condition $a_1, a_2, \ldots, a_6 \in \mathcal{O}_K$.*

The reduction type of E/K is of three kind that we resume in the following theorem.

Theorem 5.1.1 *(Theorem and Definition [52] ch. VII)Let K be a local field, E/K an elliptic curve over K and $\tilde{E}/k$ the reduced curve for a minimal Weierstrass equation :*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- *E has good reduction, one also says stable reduction, over K if $\tilde{E}$ is non-singular. This is the case if and only if $v(\Delta(E)) = 0$.*
- *We say that E has multiplicative reduction, one says semi-stable reduction, over K if $\tilde{E}$ has a node. This is the case if and only if $v(\Delta(E)) > 0$ and $v(c_4) = 0$, if so :*

$$\tilde{E}_{ns}(\overline{k}) \cong \mathbb{G}_m(\overline{k}) \cong \overline{k}^*$$

- *E has additive reduction, one also says unstable reduction, over K if $\tilde{E}$ has a cusp. This is the case if and only if $v(\Delta(E)) > 0$ and $v(c_4) > 0$, if so :*
$$\tilde{E}_{ns}(\overline{k}) \cong \mathbb{G}_a(\overline{k}) \cong \overline{k}^+$$

In the cases of multiplicative and additive reduction we say that E has bad reduction. The reduced curve is an elliptic curve if and only if E has good reduction

Moreover, we can distinguish two types of multiplicative reduction :

Definition 5.1.3 *Let E/K be an elliptic curve with multiplicative reduction. One says that E/K has split multiplicative reduction if the slopes of the tangent lines are in k. Otherwise we say that E/K has non-split multiplicative reduction*

The meaning of "stable", "semi-stable" and "unstable" is given just below.

Definition 5.1.4 *Let E/K be an elliptic curve, one says that E has potential good reduction over K if it acquires good reduction over a finite extension K'/K. One define in the same way potential multiplicative reduction.*

One can show that E/K has potential good reduction if and only if the $j-$invariant is integral, i.e. $j(E) \in \mathcal{O}_K^*$ ([52] ch. VII).

Theorem 5.1.2 *(semi-stable reduction theorem, [52] ch. VII) Let E/K be an elliptic curve.*

- *Let K'/K be a finite unramified extension of K then E has the same reduction type over K and over K'.*
- *Let K'/K be any finite extension, if E has either good or multiplicative reduction over K, it has the same type of reduction over K'.*
- *There exists a finite extension K'/K so that E has either good or split multiplicative reduction over K'*

Recall that if $\mathrm{Gal}(\overline{K}/K)$ acts on a set Σ, we say that Σ is unramified if it is invariant under the inertia group I of K. There is a well known criterion for an elliptic curve to have good reduction :

Theorem 5.1.3 *(Criterion of Néron-Ogg-Shavarevich) Let E/K be an elliptic curve over a local field K, the following are equivalent :*

1. *E ha good reduction over K*
2. *$E[m]$ is unramified for all integers $m \geq 1$ relatively prime to $char(k)$*
3. *The Tate module $T_l(E)$ is unramified for some (all) primes $l \neq char(k)$*
4. *$E[m]$ is unramified for infinitely many integers $m \geq 1$ relatively prime to $char(k)$.*

5.1.2 Formal groups

We saw that an elliptic curve can be defined by Weierstrass equations and that such a curve is equipped with a natural group law. The description of the group law by the coordinates (functions) may be done. The resulting theory is equivalent to the theory of groups but with formal power series in the coordinates. It is known as formal groups. For some details on what is going to be said see [52] ch. IV.

Let E/K be an elliptic curve defined by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We make the following change of variables :

$$z = -\frac{x}{y} \qquad w = -\frac{1}{y}$$

so that the point O of E becomes the point $(z, w) = (0, 0)$ and z is a local uniformizer at O. Furthermore the preceding equation becomes

$$w = f(z, w) := z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3.$$

Proposition 5.1.1 *([52] ch. IV)*

1. *We can reiter the preceding equation ($w = f(z, w) = f(z, f(z, w))\cdots$) this define a power series*

$$w(z) = z^3(1 + A_1z + A_2z^2 + \cdots) \in \mathbb{Z}[a_1, \ldots, a_6][[z]].$$

2. *$w(z)$ is the unique power series satisfying*

$$w(z) = f(z, w(z)).$$

3. *If $\mathbb{Z}[a_1, \ldots, a_6]$ is made into a graded ring by assigning weights $wt(a_i) = i$ then, for all n, A_n is a homogeneous polynomial of weight n*

We have by example

$$A_1 = a_1,\ A_2 = a_1^2 + a_2,\ A_3 = a_1^3 + 2a_1a_2,\ A_4 = a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + a_4 \cdots.$$

From this we deduce the Laurent series for $x(z)$ and $y(z)$:

$$\begin{aligned} x(z) &= \tfrac{z}{w(z)} = \tfrac{1}{z} - \tfrac{a_1}{z} - a_2 - a_3z - (a_4 + a_1a_3)z^2 - \cdots, \\ y(z) &= -\tfrac{1}{w(z)} = -\tfrac{1}{z^3} + \tfrac{a_1}{z^2} + \tfrac{a_2}{z} + a_3 + (a_4 + a_1a_3)z + \cdots. \end{aligned}$$

This give a solution in the quotient field of the ring of formal power series. Further, the inverse of the point with coordinates (z, w) can be easily defined as

$$i(z) = \frac{x(z)}{y(z) + a_1x(z) + a_3} = \frac{z^{-2} - a_1z^{-1} - \cdots}{-z^{-3} + 2a_1z^{-2} + \cdots} \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$$

and the z-coordinate of the sum of the points (z_1, w_1), (z_2, w_2) is a power series of the form (see [52]):

$$\begin{aligned} F(z_1, z_2) = \quad & z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 + z_1 z_2^2) \\ & -(a_3 z_1^3 z_2 - (a_1 a_2 - 3a_3) z_1^2 z_2^2 + 2a_3 z_1 z_2^3) + \cdots \\ & \in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]. \end{aligned}$$

We have thus defined a formal group over the ring $\mathbb{Z}[a_1, \ldots, a_6]$ as the basic definition of a formal group is given by

Definition 5.1.5 *Let R be a ring, a one-parameter commutative formal group defined over R is a power series $F(X, Y) \in R[[X, Y]]$ satisfying*

1. *$F(X, Y) = X + Y +$ (terms of higher degrees).*
2. *$F(X, F(Y, Z)) = F(F(X, Y), Z)$ (associativity).*
3. *$F(X, Y) = F(Y, X)$ (commutativity)*
4. *There is a unique power series $i(T) \in R[[T]]$ such that $F(T, i(T)) = 0$. (inverse)*
5. *$F(X, 0) = X$ and $F(0, Y) = Y$.*

We denote the formal group associated to the elliptic curve by $\hat{E}$. Actually, if E/K is an elliptic curve over a local field K with ring of integers $\mathcal{O}$ and maximal ideal $\mathcal{M}$, the power series $x(z)$ and $y(z)$ converge for $z \in \mathcal{M}$. This gives the following injection : $\mathcal{M} \to E(K)$.

Definition 5.1.6 *With the preceding notations, we denote by $\hat{E}(\mathcal{M})$, called the group associated to the formal group $\hat{E}$, the group whose ambient set is $\mathcal{M}$ and whose laws are given by the law of formal group. Similarly we define the groups $\hat{E}(\mathcal{M}^n)$ for all non-negative integer n*

Proposition 5.1.2 *([52] ch. IV)*

1. *For each $n \geq 1$, the map*

$$\hat{E}(\mathcal{M}^n)/\hat{E}(\mathcal{M}^{n+1}) \to \mathcal{M}^n/\mathcal{M}^{n+1}$$

   induced by the identity map on sets is an isomorphism.

2. *Let p be the characteristic of the residue field k. Then every torsion point of $\hat{E}(\mathcal{M})$ has order a power of p.*

Remind the definition of $E_1(K) = \{P \in E(K) | \tilde{P} = \tilde{O}$, this group is in fact isomorphic to the group associated to $\hat{E}$:

Proposition 5.1.3 *([52] ch. VII prop. 2.2) Let E/K be an elliptic curve over a local field given by a minimal Weierstrass equation, let $\hat{E}/\mathcal{O}_K$ be the associated formal group and let $w(z) \in R[[z]]$ be the previous power series. Then the map*

$$\begin{array}{rl} \hat{E}(\mathcal{M}) & \to E_1(K) \\ z & \to \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right) \end{array}$$

is an isomorphism.

For details about the particular structure of formal groups, the reader is invited to consult the book of Frölich [17].

5.1.3 Elliptic curves over p-adic fields

Elliptic curves over local fields are principally of three type : elliptic curves over $\mathbb{C}$, elliptic curves over $\mathbb{R}$ and elliptic curves over p-adic fields.

Elliptic curves over $\mathbb{C}$ are torus of the form $\mathbb{C}/\mathbb{Z}+\tau\mathbb{Z}$ which can be realized via the map $z \to \exp(2\pi i z)$ as $\mathbb{C}^*/q^{\mathbb{Z}}$, where $q^{\mathbb{Z}} = \{q^n | n \in \mathbb{Z}\}$ with $|q| \in \mathbb{C}^*$. For elliptic curves over $\mathbb{Q}_p$, we can't define a torus because $\mathbb{Q}_p$ has no non-trivial lattices because if $0 \neq t \in \Lambda$ an hypothetical lattices, then $\lim_n p^n t = 0$ so that Λ can't be discrete. However a definition as $\mathbb{Q}_p^*/q^{\mathbb{Z}}$ with $|q|_p < 1$ defines an elliptic curve over $\mathbb{Q}_p$. Actually there are many similarities between the theory of elliptic curves over this different local fields.

Basic facts about elliptic curves over p-adic fields, i.e. finite extensions of $\mathbb{Q}_p$, are stated and prove in the chapter V of [53]. The essential theorem being :

Theorem 5.1.4 *(Tate, [53] ch. V 3) Let K be a p-adic field with absolute value $|\cdot|$, let $q \in K^*$ satisfy $|q| < 1$, and let*

$$s_k(q) = \sum_{n \geq 1} \frac{n^k q^n}{1-q^n}, \quad a_4(q) = -5s_3(q), \quad a_6(q) = -\frac{5s_3(q)+7s_5(q)}{12}.$$

- *The series $a_4(q)$ and $a_6(q)$ converge in K. We define the Tate curve, denoted E_q, by the equation*

$$E_q \ : \ y^2 + xy = x^3 + a_4(q)x + a_6(q).$$

- *The Tate curve is an elliptic curve over K with discriminant*

$$\Delta = q\prod_{n \geq 1}(1-q^n)^{24}$$

and $j-$invariant

$$j(E_q) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n \geq 0} c(n)q^n,$$

where the $c(n)$ are integers.

- *The series*

$$\begin{array}{c} X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q), \\ Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q) \end{array} ,$$

converge for all $u \in \overline{K} \setminus q^{\mathbb{Z}}$ and define a surjective homomorphism

$$\begin{array}{rccl} \phi: & \overline{K}^* & \to & E_q(\overline{K}) \\ & u & \mapsto & \begin{cases} (X(u,q), Y(u,q)) & \text{if } u \notin q^{\mathbb{Z}} \\ O & \text{if } u \in q^{\mathbb{Z}}. \end{cases} \end{array}$$

The kernel of ϕ is $q^{\mathbb{Z}}$.

- *The map ϕ is compatible with the action of the Galois group $Gal(\overline{K}/K)$ in the sense that*

$$\forall u \in \overline{K}^*, \forall \sigma \in Gal(\overline{K}/K), \quad \phi(u^\sigma) = \phi(u)^\sigma.$$

In particular, for any algebraic extension L/K there is an isomorphism

$$L^*/q^{\mathbb{Z}} \cong E_q(L).$$

Actually $|j(E_q)| = |\frac{1}{q}| > 1$ and every element of $\overline{\mathbb{Q}_p}$ is the $j-$invariant of a Tate curve ([53] ch. V lemma 5.1.).

The next theorem due also to Tate is called the $p-$adic uniformization theorem, it build the bridge between elliptic curves over $p-$adic fields and their parametrization by Tate curve. It is equivalent to the usual uniformization over $\mathbb{C}$ (see [52] ch. VI 5) and the parametrization by Weierstrass functions.

Theorem 5.1.5 *(Tate, $p-$adic uniformization theorem, e.g. [53] ch. V 5) Let K be a $p-$adic field and E/K be an elliptic curve with $|j(E)| > 1$, and define*

$$\gamma(E/K) = -\frac{c_4}{c_6} \in K^*/K^{*2}.$$

- *$\gamma(E/K)$ is well defined as an element of K^*/K^{*2}, i.e. independent of the Weierstrass equation for E/K.*
- *Let E'/K be an other elliptic curve with $j(E') \neq 0, 1728$. Then E and E' are isomorphic over K if and only if*

$$j(E) = j(E') \qquad \text{and} \qquad \gamma(E/K) = \gamma(E'/K).$$

- *Let E/K and E'/K be elliptic curve with $j(E) = j(E') \neq 0, 1728$ and suppose that $\gamma(E/K) \neq \gamma(E'/K)$ so that $L(\sqrt{\gamma(E/K)/\gamma(E'/K)})$ is a quadratic extension. Let $\chi : Gal(\overline{K}/K) \to Gal(L/K) \to \{\pm 1\}$ be the quadratic character associated to L/K. Then there exists an isomorphism $\psi : E \to E'$ with the property that*

$$\forall \sigma \in Gal(\overline{K}/K), \forall P \in E(\overline{K}), \quad \psi(\sigma(P)) = \chi(\sigma)\psi(P).$$

- *There is a unique $q \in \overline{K}^*$ with $|q| < 1$ such that E is isomorphic over $\overline{K}$ to the Tate curve E_q. Further, $q \in K$.*
- *Let q be chosen by the previous item. Then the following conditions are equivalent*
  1. *E is isomorphic to E_q over K*
  2. *$\gamma(E/K) = 1$*
  3. *E has split multiplicative reduction*

5.2 L-functions of elliptic curves

We saw at the beginning of this chapter that there is a natural l-adic Galois representation associated to an elliptic curve E/K over a local field K for l different from the residue characteristic. It is given by the action of $\mathrm{Gal}(\overline{K}/K)$ on the $l-$adic Tate module $T_l(E)$ and the associated $\mathbb{Q}_l$-vector space $V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and reads

$$\rho_{E/K,l} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V_l(E)).$$

However we saw in the first part of this text that the "natural" way to define $L-$factors associated to non-archimedean local fields is via étale cohomology (Part I ch. 4 sec. 4.1). It turns out that the $l-$adic representation coming from $H^1(E, \mathbb{Q}_l)$ is the contragredient representation to $\rho_{E/K,l}$. It's a good point because the definition of $\rho_{E/K,l}$ is clear. At present we put :

$$\sigma'_{E/K,l} = \check{\rho'_{E/K,l}} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V_l(E)^*),$$

where $V_l(E)^*$ is the dual of $V_l(E)$. Now we know (Part I ch.4 sec 4.2) that to an $l-$adic representation $\sigma'_{E/K,l}$ of $\mathrm{Gal}(\overline{K}/K)$ and to an embedding $\imath : \mathbb{Q}_l \hookrightarrow \mathbb{C}$ we can associate a representation $\sigma'_{E/L,l;\imath} = (\sigma_{E/K,l,\imath}, N_{E/K,l,\imath}$ of the Weil-Deligne group $\mathcal{W}_K$.

In [42], it is proved that $\sigma_{E/K,l,\imath}$ is actually independent of l and $\imath$. The proof breaks in to case according to the semi-stable reduction theorem (Part. II ch.5 th. 5.1.2.): the case of potential good reduction and the case of potential multiplicative reduction.

The first case depends on the criterion of Néron-Ogg-Shafarevich, on the semi-simplicity of $\sigma_{E/K,l,\imath}$ and then on the reduction to its character which is known to be independent by a theorem of Serre and Tate. The proposition of Rohrlich reads

Proposition 5.2.1 *([42] sec.14 p.148) Suppose E has potential good reduction. Then $\sigma'_{E/K,l,\imath}$ is independent of l and $\imath$. Further, dropping the subscripts $N_{E/K} = 0$ and $\sigma_{E/K}$ is semisimple and E has good reduction if and only if $\sigma_{E/K}$ is unramified.*

The second case follows by extending K to a quadratic extension where E acquires split multiplicative reduction and as we saw on the section on elliptic curves over $p-$adic fields, such a curve is isomorphic to a Tate curve. After some work this gives the following proposition

Proposition 5.2.2 *([42] sec. 15 p. 150) Suppose that E has potential multiplicative reduction, and let χ be a character of the Weil group W_K such that $\chi^2 = 1$ and the twist E^χ has split multiplicative reduction. Then $\sigma_{E/K,l,\imath} \cong \chi\omega^{-1} \otimes sp(2)$ is independent of l and $\imath$. In particular, $N_{E/K} \neq 0$, so that $\sigma'_{E/K}$ (subscripts deleted) is ramified. Furthermore, χ is trivial, unramified but nontrivial, or ramified according as E/K has split multiplicative reduction, nonsplit multiplicative reduction, or additive reduction.*

The $L-$factors for elliptic curves are known basically by defining the $L-$function from the zeta function of the curve. Actually, what was presented on the use of $l-$adic cohomology is theoretically motivated and finally the definition agree.

If E/K is an elliptic curve over a local field K we define its $L-$factors has the $L-$factor of the corresponding representation :

$$L(E/K, s) = L(\sigma'_{E/K}, s).$$

Proposition 5.2.3 *([42] sec. 17 p.151)*

1. *If E has good reduction, put $a = 1 - |\tilde{E}(k)| + q$ where q is the cardinal of the residue field k. Then*

$$L(E/K, s) = \frac{1}{1 - aq^{-s} + q^{1-2s}}.$$

2. *If E has multiplicative reduction, then*

$$L(E/K, s) = \frac{1}{1 - \alpha q^{-s}},$$

where α is 1 or -1 according as E has split or non-split multiplicative reduction.

3. *If E has additive reduction, then $L(E/K, s) = 1$.*

If E/K is an elliptic curve over a number field, we define the L-function of E/K by means of its local factors at finite places:

$$L(E/K, s) = \prod_{v \in M_K^0} L(E/K_v, s),$$

where M_K^0 denote the set of finite places. This function is absolutely convergent for $\Re(s) > 3/2$.

5.3 Selmer and Shafarevich-Tate groups

For more de tails about the contents of this section, the reader is invited to consult [7], [38], [40], [50] or [52].

5.3.1 Basic group cohomology

Let G be a group and Mod_G the category of G-module, i.e. of $\mathbb{Z}[G]$-modules now considered as a module in the "usual" sense. There exists a functor from the category of $G-$module to itself given by

$$Mod_G \ni A \longmapsto A^G \in Mod_G,$$

where $A^G = \{a \in A | \forall g \in G,\ ga = a\}$ is the set fixed by G. This functor is left-exact and covariant, that is to say that if we have a exact sequence of $G-$module

$$0 \to A \to B \to C \to 0$$

then the functor gives rise to the exact sequence

$$0 \to A^G \to B^G \to C^G$$

but the last arrow is not surjective in general, i.e. the functor is not right-exact. It is the subject of group cohomology to complete this last sequence.

Theorem 5.3.1 *(Existence and uniqueness of the cohomological extension) There exists one and only one cohomological extension of the functor $A \mapsto A^G$ up to canonical equivalence. This means that there is a sequence of left-exact functors $H^i(G,-)$ for $i \geq 0$ and natural transformations $\delta : H^i(G,-) \to H^{i+1}(G,-)$ such that $H^0(G,A) = A^G$ and*

1. *For all exact sequence of $G-$modules*

$$0 \to A \to B \to C \to 0$$

the following infinite sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G,A) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^n(G,A) \longrightarrow H^n(G,B) \longrightarrow H^n(G,C) \xrightarrow{\delta} H^{n+1}(G,A) \longrightarrow \cdots$$

is exact. It is called the long cohomology sequence.

2. *Furthermore, if we have a commutative diagram with exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

Then we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & \xrightarrow{\delta} & H^1(G,A) \longrightarrow \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A'^G & \longrightarrow & B'^G & \longrightarrow & C'^G & \xrightarrow{\delta} & H^1(G,A') \longrightarrow \cdots \end{array}$$

Usually, for the purpose of study of Galois groups actions, we usually study this for profinite groups G and discrete $G-$modules on which it acts continuously. Remind that a profinite group is the projective limit of discrete groups or, what amounts to be the same, a compact totally disconnected topological group. The $H^q(G,A)$ are called *cohomology group of G with coefficients in A.*

This group cohomology can be described in terms of cochains, cocycles and coboundaries as the usual cohomology theories. If $A \in Mod_G$ we denote $C^n(G,A)$ as the set of all continuous maps from G^n to A. The coboundary is a map

$$\partial : C^n(G,A) \to C^{n+1}(G,A)$$

defined by the formula

$$\begin{array}{rl} (\partial f)(g_1,\ldots,g_{n+1}) = & g_1 \cdot f(g_2,\ldots,g_{n+1}) \\ & +\sum_{i=1}^{n}(-1)^i f(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_{n+1}) \\ & +(-1)^{n+1} f(g_1,\ldots,g_n) \end{array}$$

The groups $C^*(G,A)$ form a complex (i.e. $d \circ d = 0$) and the cohomology groups $H^i(G,A)$ are the cohomology groups of this complex :

$$H^i(G,A) = \{i-cocycle\}/\{i-coboundaries\},$$

where i-cocycles are the element of the image of ∂ and i-boundaries are the element of the kernel of ∂.

The elements of $H^1(G,A)$ are called *crossed homomorphism*, they are the continuous functions $x : G \to A$ such that

$$\forall \sigma,\tau \in G, \quad x(\sigma\tau) = x(\sigma) + \sigma x(\tau).$$

Restriction and Inflation

If $f : G \to G'$ is a homomorphism of groups, it induces a homomorphism

$$f^* : H^q(G,A) \to H^q(G',A)$$

for any $G-$module A.(see e.g. [7] ch. IV or [50])

In particular, taking $G' = H$ to be a subgroup of G and f to be the embedding $H \to G$, we have, on one hand, *restriction* homomorphisms :

$$\mathrm{Res} : H^q(G,A) \to H^q(H,A).$$

On the other hand, if H is a normal subgroup of G we can consider $G \to G/H$ and for any $G-$module A we have the $G/H-$module A^H, hence a homomorphism $H^q(G/H, A^H) \to H^q(G, A^H)$. By composing it with the embedding $A^H \hookrightarrow A$, we obtain the *inflation* homomorphism :

$$\mathrm{Inf} : H^q(G/H, A) \to H^q(G, A).$$

Proposition 5.3.1 *(Restriction-Inflation sequence) Let H be a normal subgroup of G, and let A be a $G-$module. Then the sequence*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{Inf} H^1(G, A) \xrightarrow{Res} H^1(G, A)$$

is exact.

5.3.2 Selmer and Shafarevich-Tate groups

Let L/K be a Galois extension, then $\mathrm{Gal}(L/K)$ is the projective limit of the groups $\mathrm{Gal}(L_f/K)$ where L is a finite Galois subextension of $\mathrm{Gal}(L/K)$, thus is a profinite group. We are interested in the cohomology groups $H^q(\mathrm{Gal}(K/k), A)$, $q \geq 0$. If k is a field we denote $H^q(k, A) := H^q(\mathrm{Gal}(\overline{k}/k), A)$, where $\overline{k}$ denote the algebraic closure of k.

Of particular importance for us are the groups of K-points, $A = E(K)$, or the torsion points $E[m]$, of an elliptic curves on which Galois groups acts naturally for a number field K. Let E/K and E'/K be two elliptic curves over a number field K and $\phi : E \to E'$ an isogeny defined over K (e.g. $\phi = [m]$, we have a short exact sequence of
$G_K := \mathrm{Gal}(\overline{K}/K)-$modules

$$0 \longrightarrow E[\phi] \longrightarrow E(\overline{K}) \xrightarrow{\phi} E'(\overline{K}) \longrightarrow 0 \ .$$

Galois cohomology yields the long exact sequence :

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K)$$

$$\xrightarrow{\delta} H^1(G_K, E[\phi]) \longrightarrow H^1(G_K, E(\overline{K})) \xrightarrow{\phi} H^1(G_K, E'(\overline{K})).$$

We can cut this sequence in the third term and fifth term and completing we obtain the following short exact sequence

$$0 \longrightarrow \frac{E'(K)}{\phi(E(K))} \xrightarrow{\delta} H^1(G_K, E[\phi]) \longrightarrow H^1(G_K, E(\overline{K}))[\phi] \longrightarrow 0$$

The preceding sequence is often called *Kummer sequence* because Kummer first extract such a sequence in the case of fields and their groups of roots of 1.

Similarly, let M_K be the set of places of K and $v \in M_K$, we can identify $\overline{K}$ with the algebraic closure of K inside $\overline{K}_v$ which yields the embedding

$$\begin{array}{rcl} G_v := \mathrm{Gal}(\overline{K}_v/K) & \hookrightarrow & G_K := \mathrm{Gal}(\overline{K}/K) \\ \sigma & \mapsto & \sigma|_{\overline{K}} \end{array}$$

whose image is a decomposition group at v. As G_v acts on $E(\overline{K}_v)$ and $E'(\overline{K}_v)$ we can repeat the preceding procedure which yields

$$0 \longrightarrow \tfrac{E'(K_v)}{\phi(E(K_v))} \xrightarrow{\delta} H^1(K_v, E[\phi]) \longrightarrow H^1(K_v, E(\overline{K}_v))[\phi] \longrightarrow 0 \ .$$

Furthermore, for each $v \in M_K$ we have a composed morphism, denoted Res_v

$$\mathrm{Res}_v : \ H^q(K, E(\overline{K})) \xrightarrow{\mathrm{Res}} H^q(K_v, E(\overline{K})) \longrightarrow H^q(K_v, E(\overline{K}_v)) \ .$$

Taking together the different embedding yields the following diagram with exact rows and columns

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E'(K)}{\phi(E(K))} & \xrightarrow{\delta} & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E(\overline{K})) & \longrightarrow & 0 \ . \\ & & \downarrow & & \downarrow & \searrow & \downarrow & & \\ 0 & \longrightarrow & \prod_{v\in M_K} \frac{E'(K_v)}{\phi(E(K_v))} & \xrightarrow{\delta} & \prod_{v\in M_K} H^1(K_v, E[\phi]) & \longrightarrow & \prod_{v\in M_K} H^1(K_v, E(\overline{K}_v))[\phi] & \longrightarrow & 0 \end{array}$$

Definition 5.3.1 *(Selmer and Shafarevich-Tate group) Let $\phi : E/K \to E'/K$ be a rational isogeny. The ϕ-Selmer group of E/K is the subgroup of $H^1(K, E[\phi])$ defined by*

$$S^{(\phi)}(E/K) = ker\left\{ H^1(K, E[\phi]) \to \prod_{v\in M_K} H^1(K_v, E(\overline{K}_v)) \right\}$$

The Shafarevich-Tate group of E/K is the subgroup of $H^1(K, E(\overline{K}))$ defined by

$$Ш(E/K) = ker\left\{ H^1(K, E(\overline{K})) \to \prod_{v\in M_K} H^1(K_v, E(\overline{K}_v)) \right\}.$$

More generally, we could define $Ш^q(E/K)$ by replacing H^1 by H^q in the preceding definition

Proposition 5.3.2 *Let $\phi : E/K \to E'/K$ be a rational isogeny, $S^{\phi}(E/K)$ and $Ш(E/K)$ be the Selmer group and the Shafarevich-Tate group respectively, then*

1. *There is an exact sequence*

$$0 \to E'(K)/\phi(E(K)) \to S^{\phi}(E/K) \to Ш(E/K)[\phi] \to 0$$

.

2. *$S^{\phi}(E/K)$ is finite and as a consequence the m-torsion $Ш(E/K)[m]$, is finite for every integer m*

Actually, $H^1(K, E(\overline{K}))$ classify principal homogeneous spaces over K under E, i.e. varieties X over K equipped with a fully faithful action of E (a morphism $E \times X \to X$ for which the induced action of $E(\overline{K})$ on $X(\overline{K})$ such that for each $x_1, x_2 \in X(\overline{K})$ there is a unique $P \in E(\overline{K})$ such that $Px_1 = x_2$). Principal homogeneous spaces over K under E are also called $K-$torsors. A $K-$torsors is called locally trivial if it is in the kernel of every Res_v, or equivalently if $X(K_v)$ is not empty for every v. Thus $Ш(E/K)$ is geometrically the set of locally trivial $K-$torsors under E, thus elements of $Ш(E/K)$ correspond to $K-$torsor that violate the Hasse principle.

The classical and important conjecture being that $Ш(E/K)$ is finite. It is known that as G_K is a profinite group, the cohomology groups $H^q(K, E(\overline{K}))$ are torsion groups for $q \geq 1$ which means that every element has finite order. Hence $Ш(E/K) \subset H^1(K, E(\overline{K}))$ is a torsion group and we can write

$$Ш(E/K) = \bigoplus_p Ш_{p^\infty}(E/K),$$

where $Ш_{p^\infty}$ is the p-primary part of $Ш(E/K)$, i.e. the subgroup of elements killed by a power of p. By abelian groups theory, we can write

$$Ш_{p^\infty} = (\mathbb{Q}_p/\mathbb{Z}_p)^{n_p} \times \left(\frac{\mathbb{Z}}{p^{s_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p^{s_l}\mathbb{Z}} \right)$$

for some integers $n_p, s_1, \ldots, s_l$. That's why if the Shafarevich-Tate group is finite, the Mordell-Weil rank is equal to the $p-$Selmer rank, defined as the Mordell-Weil rank plus the nunmber of copies of $\mathbb{Q}_p/\mathbb{Z}_p$ in Ш. This is used to motivate the form of the parity conjecture (see section 5.4.3) proved by Tim and Vladimir Dokchitser in their article.

Concerning the finiteness of Ш we have the following expectation due to Goldfeld and Szpiro in [19]

Conjecture 5.3.1 *(Goldfeld-Szpiro) Let K be a number field, E/K an elliptic curve of conductor $\mathfrak{N}(E/K)$ (see 4.2.2 and the next section) then for any constant $\epsilon > 0$, there is a constant $C_\epsilon(K)$ such that*

$$Card\, Ш(E/K) \leq C_\epsilon(K) N_{K/\mathbb{Q}}(\mathfrak{N}(E/K))^{1/2+\epsilon}.$$

5.3.3 The Cassels-Tate pairing

In [5], J.W.S constructed a pairing over the Shafarevich-Tate group with nice properties :

Theorem 5.3.2 *(Cassels [5]) Let E/K be an elliptic curve over an algebraic number field and Ш be its Shafarevich-Tate group, then there exists a skew-symmetric form*

$$< \cdot, \cdot >: Ш \times Ш \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

This pairing has the following property : Let m be a natural number and suppose that $<\xi,\eta>=0$ for all $\xi \in Ш$ such that $m\xi = 0$ then $\eta = m\alpha$ for some $\alpha \in Ш$.

Here the kernel of the Cassels-Tate pairing is $Ч = \bigoplus(\mathbb{Q}/\mathbb{Z}_p)^{n_p}$, the set of infinitely divisible, which is conjecturally trivial, elements of Ш so that it defines alternate, non-degenerate pairing on $Ш/Ч$.

5.4 BSD and parity conjectures

5.4.1 L-functions again

Let E/K be an elliptic curve over a number field K and denote M_K and M_K^0 the sets of places and of finite places respectively. We know that the $l-$adic representations associated to E are essentially unique. We denote by $\sigma'_{E/K}$ the corresponding representation of the Weil-Deligne group $\mathcal{W}_K$. We defined in section 4.2.2 the conductor $\mathfrak{N}(\sigma')$ for a representation of the Weil-Deligne group of a local field. By proposition 3.2.2 a representation σ' of the Weil-Deligne group of a global field define representations of the local Weil-Deligne group. Hence, if K is a global field we define

$$\mathfrak{N}(E/K) = \prod_{v \in M_K^0} \mathfrak{N}(E/K_v)$$

seen as an ideal of the integer ring $\mathcal{O}_K$.

Furthermore, for D the absolute value of the discriminant of K, we define

$$A(E/K) = \prod_{v \in M_K^0} A(E/K_v) = \prod_{v \in M_K^0} D_v^2 N(\mathfrak{N}(E/K_v)) = D^2 N(\mathfrak{N}(E/K)).$$

Like in 4.2.3 where we defined the local root numbers $W(\sigma')$ for representations of local Weil-Deligne groups, which we denote by $W(E/K_v)$ in our context, we define the global root number of E/K as

$$W(E/K) = \prod_{v \in M_K} W(E/K_v) = (-1)^{r_1+r_2} \prod_{v \in M_K^0} W(E/K_v).$$

The completed L-function (see part I) then is given by

$$\Lambda(E/K,s) = A(E/K)^{s/2}(2(2\pi)^{-s}\Gamma(s))^n L(E/K,s).$$

One conjectures that this function has an analytic continuation to an entire function and that it satisfies the following functional equation

$$\Lambda(E/K,s) = W(E/K)L(E/K,2-s)$$

which implies that

$$W(E/K) = (-1)^{\mathrm{ord}_{s=1}L(E/K,s)}.$$

5.4.2 The Birch and Swinnerton-Dyer conjecture

Remind the following formula of I.2.1

$$\mathrm{res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{Reg}(K)}{d_K^{1/2}\omega}.$$

The equivalent formula for L-functions of elliptic curves is conjectural and known as the Birch and Swinnerton-Dyer conjecture. The weak Birch and Swinnerton-Dyer conjecture asserts that

$$L(E/K,s) \sim_{s=1} c(s-1)^{-r} + \text{ higher order terms},$$

where

$$r = \mathrm{rank}\, E(K).$$

We can be more precise about the constant c, it is the subject of the complete conjecture which many believe to be true for empirical and numerical signs.

The equivalent of the regulator of the field K is called the elliptic regulator of the elliptic curve E/K for K a number field. This regulator which we denote $\mathrm{Reg}(E/K)$ is defined in term of the Néron-Tate pairing of E/K, i.e. in terms of the canonical *height* of the elliptic curve. For the definition of the (canonical) Néron-Tate height and the corresponding pairing see [52].

If we denote by $\hat{h}$ the canonical height of E/K, the canonical pairing is the following bilinear form

$$< , >: E(\overline{K}) \times E(\overline{K}) \to \mathbb{R}$$

defined by

$$< P, Q >= \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

Definition 5.4.1 *(Elliptic regulator) Let E/K be a elliptic curve over a number field K. Remind from Mordell-Weil theorem that the group of $K-$rational points $E(K)$ is of finite type. The elliptic regulator of E/K, denoted $Reg(E/K)$ is the volume of a fundamental domain of $E(K)/E_{tors}(K)$, computed with respect to the Néron-Tate height. In other words, if $P_1, \ldots, P_r \in E(K)$ generate $E(K)/E_{tors}(K)$ then*

$$Reg(E/K) = \det(< P_i, P_j >)_{1\leq i,j\leq r}.$$

For $v \in M_K$, let K_v be the corresponding completion and μ_v be the Haar measure on K_v, normalized so that for each open $U \subset K_v$ and $x \in K_v$:$\mu_v(xU) = |x|_v\mu_v(U)$.

The Birch and Swinnerton-Dyer conjecture takes the form

Conjecture 5.4.1 *(Birch and Swinnerton-Dyer) Let E/K be an elliptic curve over a number field K and $L(E/K,s)$ its L-function then*

$$\lim_{s\to 1}\frac{L(E/K,s)}{(s-1)^{rank\, E(K)}} = C_{E/K}\cdot\frac{Card(Ш(E/K))Reg(E/K)}{\sqrt{|d_K|}(Card\, E(K)_{tors})^2},$$

where $C_{E/K}$ is a constant which is the product of local Tamagawa numbers and periods and d_K is the discriminant of K.

5.4.3 The parity conjecture

From the two preceding sections we may conjecture that the parity of the analytic rank, that we define $(-1)^{\mathrm{ord}_{s=1}L(E/K,s)}$, may be equal to the parity of Mordell-Rank, $(-1)^{\mathrm{rank}\,E(K)}$, both being equal to the $\pm$ sign of the functional equation. This is the basic parity conjecture, one can see it as a very weak form of the Birch and Swinnerton-Dyer conjecture.

Conjecture 5.4.2 *(Basic parity conjecture) The parity of the analytic rank of an elliptic curve over a number field is equal to the parity of its Mordell-Weil rank:*

$$ord_{s=1}\, L(E/K,s) \equiv\ rank\, E(K) \pmod 2.$$

As discussed in section 5.3.2, when $Ш(E/K)$ is finite, the Mordell-Weil rank is equal, for every p, to the $p-$Selmer rank defined by

$$s_p(E/K) = \mathrm{rank}\, E(K) + \mathrm{rank}_{\mathbb{Z}_p} Ш(E/K),$$

and the analytic rank by

$$rk_{an}(E/K) = \mathrm{ord}_{s=1}\, L(E/K).$$

Then a refined version of the parity conjecture reads

Conjecture 5.4.3 *(Parity conjecture for Selmer groups) For some prime p*

$$s_p(E/K) \equiv rk_{an}(E/K) \pmod 2.$$

Combining the different conjectures we can expect the following conjecture as propose by Tim and Vladimir Dokchitser in their paper [14].

Conjecture 5.4.4 *($p-$parity conjecture) For any (some) prime p, the root number agrees with the parity of the $p-$Selmer rank :*

$$W(E/K) = \sigma(E/K,p),$$

where $\sigma(E/K,p) = (-1)^{s_p(E/K)}$.

This is this conjecture which has been dealt with recently, in particular, Tim and Vladimir Dokchister in [14] prove the following theorem (see the next chapter for a discussion of the paper)

Theorem 5.4.1 *([14] theorem 2) If E/K has a rational isogeny of prime degree $p \geq 3$, and E is semistable at all primes over p, then the p-parity conjecture holds for E/K and p. It also holds for $p = 2$ under the additional assumption that E is not supersingular at primes above 2.*

In the case of elliptic curves over the rational numbers, Jan Nekovář ([33], [34], [35] and [36]), proved the following result

Theorem 5.4.2 *(Nekovář [34]) Let E be an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p. Then the parity conjecture for Selmer groups holds for E and p.*

The proof of the preceding theorems are not of the same nature, as the techniques are different over a number field or over $\mathbb{Q}$. Actually it is difficult to compare this two theorem : they really live in different worlds.

5.5 Néron Models

An almost complete presentation of Néron models can be found in [3], in the case of elliptic curves the books of Silverman [53] and of Liu [27] are sufficient at least for our purposes.

Let E/K be an elliptic curve over a complete field K with respect to a discrete valuation v and with ring of integers R and residue field k. R is a discrete valuation ring and K is its fraction field. For instance K can be the completion of a number field at a non-archimedean place, then $R = \mathcal{O}_K$ and $k = \mathbb{F}_q$. A minimal equation of E/K over R define a scheme over $\mathrm{Spec}(R)$ which can be singular. However if we resolve the singularities of this scheme we obtain a scheme $\mathcal{C}/\mathrm{Spec}(R)$ whose generic fiber is E/K and whose special fiber is a union of curves over k. If we choose $\mathcal{C}/\mathrm{Spec}(R)$ minimal with respect to $\mathcal{C} \to \mathrm{Spec}(R)$ then it is unique up to unique homomorphism. The subscheme $\mathcal{E} \subset \mathcal{C}$ obtained by discarding all the singular points of the special fiber of $\mathcal{C}$ is called the *Néron minimal model* of E/K, in what follows we will be more precise.

5.5.1 Algebro-geometric preliminaries

Remind that a integral domain is called normal if it is integrally closed in its field of fractions. A scheme X is called normal at the point x if the corresponding local ring $\mathcal{O}_X, x$ is normal, a scheme is normal if every local rings are normal.

Furthermore a scheme X with structural sheaf $\mathcal{O}_X$ is called *noetherian* if it can be covered by a finite number of open affine sets X_i such that the rings $\mathcal{O}_X$ are noetherian (i.e. its ideals are finitely generated). A scheme is said *locally noetherian* if every point has a Noetherian open neighborhood. Following Liu [27], we define

Definition 5.5.1 *A normal locally noetherian scheme of dimension 0 or 1 is called a Dedeking scheme.*

Definition 5.5.2 *(fibered surfaces) Let S be a Dedekind scheme. A integral, noetherian, flat S-scheme $X \to S$ is called a fibered surface.*

A regular fibered surface $X \to S$ over a Dedekind scheme of dimension 1 is called an arithmetic surface, the definition of flatness has been given in chapter 4 definition 4.1.1..

Remark: Integral means that for every open set $U \subseteq X$, $\mathcal{O}_X(U)$ is an integral domain. The definition of flatness has been given in chapter 4.

As a consequence, the generic fiber of a fibered surface over a scheme of dimension 1 is a curve over $K(S)$ normal if X is normal and the special fibers X_s, for $s \in S$, is a projective curve over the residue field $k(s)$ ([27] ch. 8 lemma 3.3). Furthermore the set of singular points of X is a finite set of closed points. It is called an arithmetic surface because it is a one dimensional family of one-dimensional varieties.

As a particular case of what preceded we can take $S = \mathrm{Spec}(R)$ where R is a Dedekind domain. The principal theorem of the theory been the theorem of existence and uniqueness of regular minimal models for curve of genus ≥ 1, more precisely

Theorem 5.5.1 *(Existence and uniqueness of minimal regular models, [53] ch. IV, [27] ch. 9). Let R be a Dedekind domain with fraction field K, and C/K a non-singular projective curve over K.*

1. *(Existence) There exists a regular arithmetic surface $\mathcal{C}/R$, proper over R, whose generic fiber is isomorphic to C/K. It is called a proper regular model for C/K.*

2. *(minimality) Suppose that the genus of C is ≥ 1 then there exists a proper regular model $\mathcal{C}^m/R$ of C/K which is minimal with respect to the following property :*

   If $\mathcal{C}'/R$ is another proper regular model, the $R-$birational map induced from a fixed isomorphism between their generic fibers :

   $$\mathcal{C} \dashrightarrow \mathcal{C}^m$$

   is an $R-$isomorphism.

   $\mathcal{C}^m/R$ is called a proper regular model for C/K.

$\mathcal{C}^m/R$ is unique up to unique isomorphism.

Loosely speaking, a Néron model of an elliptic curve is a scheme-theoretic model of the elliptic curve which is universal in some sense, more precisely :

Definition 5.5.3 *Let R be a Dedekind Domain with fraction field K, and let E/K be an elliptic curve. A Néron model for E/K is a smooth group scheme $\mathcal{E}/R$ whose generic fiber is E/K such that every K-rational map between curve $\phi_R : X/K \to E/K$ extend, for every smooth $R-$scheme Ξ/R with generic fiber X/K, to a morphism $\phi_R : \Xi/R \to \mathcal{E}/R$.*

This definition implies that if $\mathcal{E}/R$ is a Néron model for E/K then

$$\mathcal{E}(R) \cong E(K).$$

The following theorem and its generalization (e.g. [27]) is fundamental

Theorem 5.5.2 *(Existence and uniqueness of Néron models, [53] ch. IV)*

1. *(Existence) Let R be a Dedekind domain with function field K and let E/K be an elliptic curve, let $\mathcal{C}/R$ be a minimal regular model for E/K and let $\mathcal{E}/R$ be the largest subscheme of $\mathcal{C}/R$ which is smooth over R. Then $\mathcal{E}/R$ is a Néron model for E/K.*

2. *(Uniqueness) The Néron model is unique up to unique isomorphism.*

Actually, if the elliptic curve E/K has good reduction,the subscheme $\mathcal{W}^0$ obtained as the largest subscheme of the scheme defined by a Weierstrass equation, is a Néron modél for E/K.

5.5.2 The fibers of Néron models

The principal result of the theory of Néron models over a discrete valuation ring is that they can be classified according to their special fiber.

Theorem 5.5.3 *(Kodaira, Néron, see e.g. [53] ch. IV) Let R be a discrete valuation ring with maximal ideal $\mathfrak{p}$, fraction field K, and algebraically closed residue field k. Let E/K be an elliptic curve and let $\mathcal{C}/R$ be a minimal proper regular model for E/K. Further, put $c_{\mathfrak{p}} = (E(K) : E_0(K))$, where $E_0(K)$ is defined according to the section 5.1.1. and put $\upsilon(\Delta)$ the valuation of the discriminant of E. Then the special fiber $\mathcal{C}_{\mathfrak{p}} = \mathcal{C} \times_{Spec\, R} Spec(k)$ and the number $c_{\mathfrak{p}}$ are of the following forms :*

- *Type I_0 $\mathcal{C}_p$ is a non-singular curve and $c_{\mathfrak{p}} = 1$. Good reduction. $\upsilon(\Delta) = 0$*
- *Type I_1 $\mathcal{C}_p$ is a rational curve with a node and $c_{\mathfrak{p}} = 1$. Multiplicative reduction.*
- *Type $I_n, n \neq 2$ $\mathcal{C}_p$ consists of n non-singular rational curves arranged in the shape of an n-gon and $c_{\mathfrak{p}} = n$.Multiplicative reduction. $\upsilon(\Delta) = n$*
- *Type II $\mathcal{C}_p$ is a rational curve with a cusp and $c_{\mathfrak{p}} = 1$. Additive reduction. $\upsilon(\Delta) = 2$*
- *Type III $\mathcal{C}_p$ consists of two non-singular rational curves which intersect tangentially at a single point and $c_{\mathfrak{p}} = 2$. Additive reduction. $\upsilon(\Delta) = 3$*
- *Type IV $\mathcal{C}_p$ consists of three non-singular rational curves which intersect at a single point and $c_{\mathfrak{p}} = 3$. Additive reduction. $\upsilon(\Delta) = 4$*
- *Type I_0^* $\mathcal{C}_p$ is a non-singular rational curve of multiplicity two with four non-singular curves of multiplicity 1 attached and $c_{\mathfrak{p}} = 4$. Additive reduction. $\upsilon(\Delta) = 6$*
- *Type I_n^* $\mathcal{C}_p$ consists of a chain of $n+1$ non-singular rational curves of multiplicity two with two non-singular rational curves of multiplicity one attached to either ends and $c_{\mathfrak{p}} = 4$. Additive reduction.$\upsilon(\Delta) = 6 + n$*

- *Type IV^* For this more complex case see for instance the pictures in the appendix C of [52] or the chapter IV of [53].* $c_{\mathfrak{p}} = 3$. *Additive reduction.*$\upsilon(\Delta) = 8$
- *Type III^* For this more complex case see for instance the pictures in the appendix C of [52] or the chapter IV of [53].*$c_{\mathfrak{p}} = 2$. $\upsilon(\Delta) = 9$
- *Type II^* For this more complex case see for instance the pictures in the appendix C of [52] or the chapter IV of [53].*$c_{\mathfrak{p}} = 1$. *Additive reduction.* $\upsilon(\Delta) = 10$

Chapter 6

Parity conjecture with a cyclic isogeny

6.1 Presentation of the article of Tim and Vladimir Dokchitser

Recall that the p-parity conjecture says that the sign of the global root number $W(E/K)$ shall be equal to $\sigma(E/K,p) = (-1)^{s_p(E/K)}$ where $s_p(E/K)$ is the $p-$Selmer rank of E/K. The article has the following main directories: computing the root number by local root numbers, computing $\sigma(E/K,p)$ by a local method due to Cassels and Fisher for $p \geq 3$ (see the next section), making the corresponding computation in the case of a $2-$isogeny. This is what we present in the remaining of the text.

First of all, the computation of the local roots number and of a kind of local $p-$Selmer rank leads to the following result

Theorem 6.1.1 *([14] theorem 3) Let K be a number field and p be an odd prime. Let E/K be an elliptic with a rational $p-$isogeny ϕ, and assume that E has semistable reduction at all primes above p. Then for all place v of K*

$$W(E/K_v) = (-1, K_{v,\phi}/K_v)\sigma_\phi(E/K_v).$$

Where $W(E/K_v)$ are local root numbers, $\sigma_\phi(E/K_v)$ are local factors (defined below) whose product gives the parity of the $p-$Selmer rank and $(-1, K_{v,\phi}/K)$ is defined as a by-product of the norm residue symbol (defined in section 3.2.3).

Precisely, $K_{v,\phi}$ is the completion of the field K_ϕ which is the smallest field over which the point of $\ker(\phi)$ are defined and $(-1, K_{v,\phi})$ is the composition

$$K^* \xrightarrow{loc.rec.} \mathrm{Gal}(K_\phi/K) \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^* .$$

The last embedding coming from the faithful action of $\ker(\phi)$, which has cardinal p, on $\mathrm{Gal}(K_\phi/K)$. Thus $(-1, K_\phi/K) = 1$ if -1 is a norm from K_ϕ/K and it equals -1 otherwise.

For $p = 2$, the existence of a $2-$isogeny is equivalent to the existence of a $2-$torsion point. For if ϕ is a $2-$isogeny and if $\hat{\phi}$ is its dual, there exists a point P such that $\phi(P) = O$ which gives $[2]P = \hat{\phi} \circ \phi P = O$. A similar argument shows that the kernel of a $p-$isogeny is contained in $E[p]$. By using a translation wa can assume that the 2-torsion point is $(0, 0)$, then there exists a model of the curve of the following form

$$E: \quad y^2 = x^3 + ax^2 + bx, \quad a, b \in \mathcal{O}_K$$

and they use the following 2-isogeny

$$\begin{array}{rccl} \phi: & E & \to & E' \\ & (x, y) & \mapsto & (x + ax + bx^{-1}, y - bx^{-2}y) \end{array}$$

where E' is the curve with model

$$y^2 = x^3 - 2ax^2 + \delta x, \quad \delta = a^2 - 4b.$$

Then, by making a "case by case" computation they deduce the following result

Theorem 6.1.2 *([14] theorem 4) Suppose E/K has either ordinary or multiplicative reduction at all prime above 2. Then for all places v of K,*

$$W(E/K_v) = (a, -b)_{K_v}(-2a, \delta)_{K_v}\sigma_\phi(E/K_v),$$

where $(\ ,\ )_{K_v}$ denotes the Hilbert symbol (define below).

Hence the product formulas, given in proposition 3.2.1 and in section 6.2 below, imply that the parity conjecture holds in the conditions of the previous two theorems. I insist on the fact that almost all results of [14] remain on "case-by-case" computations.

The most notable result of this article being the already stated

Theorem 6.1.3 *([14] theorem 2) If E is an elliptic curve over a number field K which has a rational isogeny of prime degree $p \geq 3$ and that E is semistable at all primes above p, then the p-parity conjecture (conjecture 5.4.4) holds for E/K and p. It also holds for $p = 2$ under the additional assumption that E is not supersingular at primes above 2.*

6.2 The $p-$Selmer rank

6.2.1 Basis for computation of parity of $p-$Selmer ranks

In the appendix of an article of Vladimir Dokchitser, [15], Tom Fisher gives results which are essential in the computation of the $p-$Selmer rank. It allows us to define the parity of the $p-$Selmer rank $\sigma(E/K, p)$ (see section 5.4.3) as a product of local factors which turn out to be computable. This is what makes the existence of a $p-$isogeny (isogeny of prime degree p) essential in [14].

Proposition 6.2.1 *Let E/K and E'/K be two elliptic curves over K and $\phi : E \to E'$ be a rational isogeny of prime degree p. Denote by $\hat{\phi}$ the dual isogeny. Then*

$$T(E, E', \phi) := \frac{|E'(K)[\hat{\phi}]|\,|S^{\phi}(E/K)|}{|E(K)[\phi]|\,|S^{\hat{\phi}}(E'/K)|} = p^e$$

for some integer e such that

$$e \equiv s_p(E/K) \pmod 2,$$

where $s_p(E/K)$ is the $p-$Selmer rank defined in 5.4.3..

Proof : First of all, from the exact sequence of proposition 5.3.2. the quotient is equal to

$$\frac{|E'(K)[\hat{\phi}]|\,|E'(K)/\phi(E(K)|}{|E(K)[\phi]|\,|E(K)/\hat{\phi}(E'(K)|}\,\frac{|Ш(E/K)[\phi]|}{|Ш(E'/K)[\hat{\phi}]|}.$$

On one hand, as $\phi\hat{\phi} = [p]$ and $\hat{\phi}\phi = [p]$, on E' and E respectively, hence we have the inclusion

$$Ш(E/K)[\phi] \subset Ш(E/K)[p] \subset Ш(E/K)[p^\infty]$$
$$Ш(E'/K)[\hat{\phi}] \subset Ш(E'/K)[p] \subset Ш(E'/K)[p^\infty]$$

so the $\phi-$torsion of the Shafarevech-Tate group has order a power of p as a subgroup of the $p-$torsion. Moreover we have the following exact sequence

$$0 \longrightarrow Ш(E/K)[\phi] \longrightarrow Ш(E/K)[p] \xrightarrow{\phi} Ш(E'/K)[\hat{\phi}] \longrightarrow 0\ .$$

Hence

$$\frac{|Ш(E/K)[\phi]|}{|Ш(E'/K)[\hat{\phi}]|} = \frac{|Ш(E/K)[\phi]|^2}{|Ш(E/K)[p]|}.$$

Moreover we know (section 5.3) that the $p-$primary part of Ш takes the form

$$Ш(E/K)[p^\infty] = (\mathbb{Q}_p/\mathbb{Z}_p)^{n_p} \times (\mathbb{Z}/p^{s_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{s_l}\mathbb{Z}).$$

Each factor $\mathbb{Q}_p/\mathbb{Z}_p$ contains p elements of order p, so there are p^{n_p}. And each $\mathbb{Z}/p^s\mathbb{Z}$ contains also p elements of order p. But the Cassels-Tate pairing is non-degenerate and skew-symmetric on this "finite" part. As a finite group equipped with a non-degenerate skew-symmetric form has square order, the order of the "finite" part of the $p-$torsion is of the form p^{2b} for some natural integer b. Hence

$$\frac{|Ш(E/K)[\phi]|}{|Ш(E'/K)[\hat{\phi}]|} = p^{n_p+2b}, \quad \text{for} \quad n_p = \operatorname{corank}_{\mathbb{Z}_p} Ш(E/K).$$

On the other hand, we know from he Mordell-Weil theorem that $E(K) \cong (\mathbb{Z})^g \times E_{tors}(K)$, where E_{tors} is the finite abelian group of torsion points of $E(K)$. Similarly $E'(K)$ has the same form with the same rank g because E

and E' are isogenous. We denote by $E_\infty(K)$ and $E'_\infty(K)$ the "infinite" parts of $E(K)$ and $E'(K)$. We have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_{tors}(K) & \longrightarrow & E(K) & \longrightarrow & E_\infty(K) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \\ 0 & \longrightarrow & E'_{tors}(K) & \longrightarrow & E'(K) & \longrightarrow & E'_\infty(K) & \longrightarrow & 0 \end{array}$$

Taking kernel and cokernel we obtain

$$\frac{|E'(K)/\phi(E(K))|}{|E(K)[\phi]|} = \frac{|E'_{tors}(K)/\phi(E_{tors}(K))|\,|E'_\infty(K)/\phi(E_\infty(K))|}{|E_{tors}(K)[\phi]|\,|E_\infty(K)[\phi]|}.$$

Moreover, as $E_{tors}(K)$ and $E'_{tors}(K)$ are finite groups we have

$$\frac{|E'_{tors}(K)/\phi(E_{tors}(K))|}{|E_{tors}(K)[\phi]|} = \frac{|E'_{tors}(K)|}{|E_{tors}(K)|}$$

and $|E_\infty(K)[\phi]| = 1$ because $E_\infty(K)$ is a free group. Using the dual isogeny we obtain similar results for $\hat{\phi} : E' \to E$, thus

$$\frac{|E'(K)[\hat{\phi}]|\,|E'(K)/\phi(E(K)|}{|E(K)[\phi]|\,|E(K)/\hat{\phi}(E'(K)|} = \frac{|E'_\infty(K)/\phi(E_\infty(K))|}{|E_\infty(K)/\hat{\phi}(E'_\infty(K))|}\frac{|E'_{tors}(K)|^2}{|E_{tors}(K)|^2}.$$

Finally, as the E_∞s are free of rank g

$$|E'_\infty(K)/\phi(E_\infty(K))||E_\infty(K)/\hat{\phi}(E'_\infty(K))| = p^{\text{rank } E(K)}.$$

The result follows.

$\diamond$

If $v \in M_K$ is non-archimedean we denote by μ_v the additive Haar measure normalized so that $\mu_v(\mathcal{O}_v) = 1$. If v is archimedean, $\mu_v = dx$ is the usual Lebesgue measure if $K_v \cong \mathbb{R}$ and $\mu_v = 2dxdy$ if $K_v \cong \mathbb{C}$. If ω is an invariant differential on E/K, following Cassels we define

$$\mu_v(\omega, E) = \int_E |\omega|_v \mu_v.$$

If E/K and E'/K are two isogenous elliptic curves and if ω (resp. ω') is an invariant differential on E (resp. E'), then from [28], for almost all $v \in M_K$

$$\mu_v(\omega, E(K_v)) = \mu_v(\omega', E(K_v)) = \frac{N_v}{N(v)},$$

where N_v is the number of points in the reduced curve and $N(v)$ is the norm of v (norm of the corresponding prime ideal). Hence the following product is well defined :

$$\prod_{v \in M_K} \frac{\mu_v(\omega, E(K_v))}{\mu_v(\omega', E'(K_v))}.$$

Proposition 6.2.2 *With the preceding definitions*

$$\frac{\mu_v(\phi^*\omega', E(K_v))}{\mu_v(\omega', E'(K_v))} = \frac{|E(K_v)[\phi]|}{|E'(K_v)/\phi(E(K_v))|}$$

Proof : This relation can be rewritten as

$$\int_{E(K_v)} |\phi^*\omega'|_v \mu_v = \frac{|\ker(\phi : E(K_v) \to E'(K_v))|}{|\mathrm{coker}(\phi : E(K_v) \to E'(K_v))|} \int_{E'(K_v)} |\omega'|_v \mu_v,$$

which is clear by considering the corresponding coverings.

◇

Corollary 6.2.1 *If we define* $\sigma(E/K, p) = (-1)^{s_p(E/K)}$ *then*

$$\sigma(E/K) = \prod_{v \in M_K} \sigma_\phi(E/K_v),$$

where we define $\sigma_\phi(E/K_v) = \pm 1$ *and equal to one if and only if the power of* p *in* $\frac{|E(K_v)[\phi]|}{|E'(K_v)/\phi(E(K_v))|}$ *is even.*

Proof This is a direct consequence of theorem 6.0.4 and proposition 6.0.1.

◇

Theorem 6.2.1 *(Cassels [5] theorem 1.1) Let* $\phi : E/K \to E'/K$ *be a rational isogeny of elliptic curves over a number field and let* $\hat{\phi}$ *then*

$$T(E, E', \phi) = \frac{|E'(K)[\hat{\phi}]|\,|S^{\phi}(E/K)|}{|E(K)[\phi]|\,|S^{\hat{\phi}}(E'/K)|} = \prod_{v \in M_K} \frac{|E(K_v)[\phi]|}{|E'(K_v)/\phi(E(K_v))|}.$$

What preceded is the basis of the computation of the parity of the $p-$Selmer rank in the article of Tim and Vladimir Dokchitser. They also use a result of Schaefer, [51], which says that if we define the number α by $\phi^*\omega' = \alpha\omega$ for ω and ω' invariant differential on E and E' respectively. It is always possible since elliptic curves are of dimension one. And if $v \in M_K^0$ is a finite place of K then

$$\frac{|E(K_v)[\phi]|}{|E'(K_v)/\phi(E(K_v))|} = |\alpha|_v^{-1} \frac{c_v(E')}{c_v(E)}.$$

The the computation of the "local Selmer" factors reduces to the computation of the p-order of the quotients $c(E')/c(E)$ and of $|\alpha|_v$ this is done mainly in the article [14] but it also rests on a result of Tom Fisher in the appendix of [15]. We finish this section by presenting these ideas.

Proposition 6.2.3 *(lemma 11 of [14]) Let* E/K *be an elliptic curve over an* l*-adic field* K*. Suppose* $\phi : E \to E'$ *is a cyclic* $p-$*isogeny (the kernel is a cyclic group of cardinality* p*) defined over* K *for a prime number* $p \geq 3$*. Denote*

$c(E) = (E(K) : E_0(K))$ and $c(E') = (E'(K) : E'_0(K))$ the Tamagawa numbers, and let $\delta = \pm 1$ such that $\delta = 1$ unless $p = 3$, $\mu_3 \not\subset K$ and E/K has Néron-Kodaira type IV or IV* (e.g. section 5.5.2). Then

$$ord_p \frac{c(E')}{c(E)} = \begin{cases} 0, \text{ if } E \text{ has good or non-split multiplicative reduction,} \\ \pm 1, \text{ if } E \text{ has split multiplicative reduction,} \\ 0, \text{ if } E \text{ has additive reduction and } \delta = 1, \\ \pm 1, \text{ if } E \text{ has additive reduction and } \delta = -1. \end{cases}$$

Proof : We distinguish the corresponding cases :

- E has good reduction In this case we have by definition $c(E) = c(E') = 1$.
- E has non-split multiplicative reduction By Tate algorithm ([53] ch. IV 9 step 2) E and E' $c(E), c(E') = 1$ or 2, hence the quotient is prime to p.
- E has split multiplicative reduction In this case we use the following lemma:

  Lemma 6.2.1 *(Tom Fisher [15]) If E has split multiplicative reduction the either*

  1. *$E[\phi] \simeq \mathbb{Z}/p\mathbb{Z}$ over K, and*
  $$\frac{c(E')}{c(E)} = \frac{1}{p}, \text{ or}$$
  2. *$E[\phi] \simeq \mu_p$ over K and*
  $$\frac{c(E')}{c(E)} = p.$$

  This justify the second case of the proposition.

- This last case is explain in [14]

Next we reformulate some results of [14]. Just remark that the number α that we defined by $\phi^*\omega' = \alpha\omega$ is also the leading coefficient for the action of ϕ on formal groups.

Proposition 6.2.4 *Let K be an $l-$adic field and E/K an elliptic curve with a cyclic $p-$isogeny, ϕ, for p a prime ≥ 3. Furthermore let α be define as the leading coefficient of the action of ϕ on formal groups.*

1. *For $l \neq p$, α is a unit.*
2. *for $l = p$, $ord_p|\alpha|_l$ is even if and only if $(-1, F_\phi/F) = 1$*

Proof : The first item is trivial since in this case, ϕ induce an isomorphism on formal groups.

The second item is not obvious and depends on three lemmas of Tim and Vladimir Dokchitser.

Lemma 6.2.2 *([14] lemma 12) Let $\mathbb{Q}_l \subset K \subset K'$ be finite extension (p odd), with K'/K cyclic Galois of degree dividing $p-1$. Then $(-1, K'/K) = 1$ if and only if one of the following condition is satisfied :*

1. *The residue field k of K is of even degree over $\mathbb{F}$, or*
2. *$\frac{p-1}{e(K'/K)}$ is even, where $e(K'/K)$ denote the ramification degree of K'/K.*

Proof :[14] section 5 .◇

For what follows we denote by K an $l-$adic field and by $\mathcal{O}_K$ the ring of integers , $\mathfrak{m}_K = (\pi)_K$ the maximal ideal and a uniformizer , υ the valuation and $k = \mathcal{O}_K/\mathfrak{m}_K$ its ring of integers. Let $\phi : E/K \to E'/K$ be an cyclic isogeny of prime degree p. Moreover we denote by $\hat{E}(\mathfrak{m}_K)$ and $\hat{E}'(\mathfrak{m}_K)$ the formal groups and by $f : \hat{E}(\mathfrak{m}_K) \to \hat{E}(\mathfrak{m}_K)$ the map induced by ϕ. Then by working directly on formal groups they prove the following lemmas

Lemma 6.2.3 *([14] lemma 13) If α, $(f(T) := \alpha T + \cdots)$, is a unit, then K_ϕ/K is unramified.*

Proof : See [14] section 6.◇

Lemma 6.2.4 *([14] lemma 14) Let $\bar{f} : \overline{\hat{E}} \to \overline{\hat{E}'}$ be the reduction of f modulo $\mathfrak{m}_K$. If $\bar{f}$ is inseparable of degree p, then f has kernel of order p in the maximal unramified extension K^{unr} if and only if $\upsilon(\alpha)$ is a multiple of $p-1$.*

Proof : See [14] section 6.◇

End of the proof of proposition 6.3.4 As $|\alpha|_l = p^{-[k:\mathbb{F}_p]\upsilon(\alpha)}$ we know that if $[k : \mathbb{F}_p$ is even so is $\mathrm{ord}_p(|\alpha|)$ and $(-1, K_\phi/K) = 1$ by the first item of lemma 6.3.2. This prove a special case of the proposition.

So we suppose at present that $[k : \mathbb{F}_p]$ is odd. We denote by e the greatest exponent such that $2^e | (p-1)$. Then $\mathrm{ord}_p |\alpha| \equiv \upsilon(\alpha) \bmod 2$. If $\upsilon(\alpha) = 0$ then by lemma 6.3.3, K_ϕ/K is unramified so $(-1, K_\phi/K) = 1$ since all units are norms in this case.

On the other hand if $\upsilon\alpha > 0$ the reduction $\bar{f}$ is an inseparable isogeny of degree p, so we may apply lemma 6.3.4. This gives that $2^e | \upsilon_{K_\phi}(\alpha)$.

If $\upsilon(\alpha)$ is odd, it follows that the ramification degree of K_ϕ/K is a multiple of 2^e because ([47] ch. II) $v_\phi(\alpha) = e(K_\phi/K)\upsilon(\alpha)$. Hence in this last case $\frac{p-1}{e(K_\phi/K)}$ is odd, so $(-1, K_\phi/K) = -1$ by lemma 6.3.2.

If $\upsilon(\alpha)$ is even. As the valuation of α in the field $K^{unr}\left((\pi_K)^{p-1/2}\right)$ is divisible by $p-1$, lemma 6.3.4 show that $K_\phi \subset K^{unr}\left((\pi_K)^{p-1/2}\right)$ hence the ramification index of K_ϕ/K is not divisible by 2^2 the second case of lemma 6.3.2 applies.

◇

6.2.2 The computation of $p-$Selmer ranks

The purpose of this section is to state and explain the theorem 6 of [14]. This theorem and its consequences is one of the main result of this paper. It is original, in the sense that it stay on the approach of Tim Fisher explained earlier.

Theorem 6.2.2 *([14] theorem 6) For $K = \mathbb{R}$ or $\mathbb{C}$, or $[F : \mathbb{Q}_l] < \infty$ and a prime $p \geq 3$. Let E/K be an elliptic curve with a rational $p-$isogeny ϕ. Define $\sigma_\phi(E/K)$ as in corollary 6.3.1, then*

$$\sigma_\phi(E/K) = \begin{cases} -(-1, K_\phi/K), & \text{if } K \text{ is archimedian} \\ (-1, K_\phi/K), & \text{if } E \text{ has good reduction,} \\ -(-1, K_\phi/K), & \text{if } E \text{ has split multiplicative reduction,} \\ (-1, K_\phi/K), & \text{if } E \text{ has non-split multiplicative reduction,} \\ \delta & \text{if } E \text{ has additive reduction and } l \neq p \end{cases}$$

Proof: Here I reformulate the proof given in [14].

K archimedean

If $K = K_\phi = \mathbb{R}$ or $K = K_\phi = \mathbb{C}$ then $|E'(K)/\phi(E(K))| = 1$ and $|E(K)[\phi]| = p$ so that, by corollary 6.3.1, $\sigma_\phi(E/K) = -1$. If $K = \mathbb{R}$ and $K_\phi = \mathbb{C}$ the generator of $\ker(\phi)$ is only defined over $\mathbb{C}$ so that $|E(K)[\phi]| = 1$ while $E'(K)/\phi(E(K))| = 1$ so that $\sigma_\phi(E/K) = 1$.

This gives $\sigma_\phi(E/K) = -(-1, K_\phi/K)$.

K non-archimedean

Proposition 6.3.3 and 6.3.4 directly implies this case, it only remains to prove that $(-1, K_\phi/K) = 1$ for places $l \neq p$ of semistable reduction this is done by proving that K_ϕ/K is unramified and then applying lemma 6.3.1, see [14] p.4.

6.3 The root number

The purpose of this section is to present one of the main theorem of the article [14], the one dealing with local root numbers of elliptic curves.

Theorem 6.3.1 *([14] theorem 5) Assume $K = \mathbb{R}$ or $\mathbb{C}$, or $[K : \mathbb{D}_l] < \infty$, and let $p \geq 3$ be a prime. Let E/K be an elliptic curve with a rational $p-$isogeny ϕ. Then*

$$W(E/K) = \begin{cases} -1 & \text{if } K \text{ is archimedean,} \\ 1 & \text{if } E \text{ has good reduction,} \\ -1 & \text{if } E \text{ has split multiplicative reduction,} \\ 1 & \text{if } E \text{ has non-split multiplicative reduction,} \\ \delta \cdot (-1, K_\phi/K) & \text{if } E \text{ has additive reduction and } l \neq p. \end{cases}$$

Her $\delta = 1$ unless $p = 3$, $\mu_3 \not\subset K$ and E/K has reduction type IV or IV*, in which case $\delta = -1$.

Proof : The first cases were known before the article [14], for example we can cite the following result of Rohrlich:

Proposition 6.3.1 *(Rohrlich [42] section 19) Let E/K be an elliptic curve over a local field K.*

1. *If E has good reduction over K, then $W(E/K) = 1$.*
2. *Suppose E has potential multiplicative reduction. If E has multiplicative reduction over K itself*

$$W(E/K) = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction,} \\ 1 & \text{if } E \text{ has non-split multiplicative reduction.} \end{cases}$$

If E has additive reduction, let ξ be a character of the Weil group W_K such that the quadratic twist E^{ξ} has multiplicative reduction. Then

$$W(E/K) = \xi(-1).$$

This gives the four first cases. The forme of the case of additive reduction which interest us is dealt with by Tim and Vladimir Dokchitser in [14]. They distinguish three cases : potential multiplicative reduction, potential good reduction with $p \geq 5$, potential good reduction with $p = 3$. This gives rise to three lemma (lemma 8, 9, 10) which fix this different cases.

6.3.1 Potential multiplicative reduction

We begin by proving some elements of the proof of lemma 8 which are not explicit in the text.

Lemma 6.3.1 *(Lemma 8 of [14]) Suppose that K is a $l-$adic field and that E/K is an elliptic curve with additive reduction of potential multiplicative reduction type. Denote the Tate module, for $p \neq l$, of E by $T_p(E) = proj\ lim_n E[p^n]$ and put $V_p(E) = T_p(E) \otimes \mathbb{Q}_p$. Then the action of the inertia subgroup of $Gal(\overline{K}/K)$ over $V_p(E)$ is of the form $\pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, furthermore the action of the full Weil group on $V_p(E)$ is of the form $\begin{pmatrix} \chi & * \\ 0 & \chi^{-1} \| \end{pmatrix}$, for some ramified quasi-character χ. The root number is given by $W(E/K) = (-1, K_\phi/K)$.*

Proof: Suppose first that E/K has split multiplicative reduction. In this case, by theorem 5.1.5, E is isomorphic to a Tate curve E_q for some $q \in K^*$. There is an isomorphism, the $l-$adic uniformization, given by

$$\phi : \overline{K}^* / q^{\mathbb{Z}} \to E_q(\overline{K}).$$

In this isomorphism a p^n-torsion point correspond to a $p^n - th$ root of q. Let us fix such a root, $Q = q^{1/p^n} \in \overline{K}$. Then, naturally, if ζ is a $p^n - th$ root of one in $\overline{K}$ the $l-$adic uniformization (see the section on Tate curves) yields

$$\left(\zeta^{\mathbb{Z}} \cdot Q^{\mathbb{Z}}\right) / q^{\mathbb{Z}} \cong E_q[p^n].$$

On the other hand if σ is an element of the inertia group $I_{\overline{K}/K}$, $\sigma(Q)$ is a $p^n - th$ root of q. Hence there exists an integer $0 \leq b \leq p^n - 1$ such that $\sigma(Q) = \zeta^b Q$. At present we put, $P_1 = \phi(\zeta)$ and $P_2 = \phi(\zeta)$.

It follows from the commutativity of the $l-$adic uniformization with respect to Galois action that $\sigma(P_1) = P_1$ ($K(\zeta)$ is totally ramified) and $\sigma(P_2) = bP_1 + P_2$. So inertia takes the form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Now, it is straightforward to verify that we can take the projective limit over n in what preceded. This yields, in the case of split multiplicative reduction, that the action of inertia on the $p-$adic Tate module is of the form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Moreover b can't be identically 0, for otherwise inertia would act trivially which would contradict the criterion of Néron-Ogg-Shafarevich.

Furthermore, we know from theorem 5.1.1 that if E/K has potential multiplicative reduction it admits split multiplicative reduction over a quadratic extension, and that the corresponding curve are isomorphic over $\overline{K}$. This isomorphism commutes with Galois only by a twist by the quadratic character associated to this extension. This justify the sign $\pm$ in the lemma.

For the action of the full Weil group, recall that inertia is normal in the Weil group, so Frobenius preserve the invariant subspace of inertia. This gives an action of the Weil group of the form

$$\begin{pmatrix} \chi & * \\ 0 & \chi' \end{pmatrix}$$

but the determinant of the l-adic Galois representation of elliptic curves is equal to the cyclotomic character $\|\cdot\|_K$ we deduce that $\chi\chi' = \|\cdot\|_K$ and so, the action of the full Weil group is of the form

$$\begin{pmatrix} \chi & * \\ 0 & \chi^{-1}\|\cdot\| \end{pmatrix}.$$

The fact that χ is ramified comes from the form of inertia. The remaining of the proof is clearly explained in the article [14].

6.3.2 Potential good reduction and $p \geq 5$

This case is dealt with by the following lemma :

Lemma 6.3.2 *([14] lemma 9) Suppose E has potential good reduction and $p \geq 5$. Then the action of the Weil group on $V_p(E)$ is of the form $\begin{pmatrix} \chi & 0 \\ 0 & \chi^{-1}\|\cdot\| \end{pmatrix}$ for some quasi-character χ. The root number is given by $W(E/K) = (-1, K_\phi/K)$.*

Proof : Here I just add some precisions to the original proof given in [14]. The fact that inertia acts via $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ on $E[p]$ from the Galois invariance of the Weil pairing. As $E[p] \cong (\mathbb{Z}/p\mathbb{Z}) \oplus \ker(\phi)$ we want to show that $\ker(\phi)$ is invariant under inertia. Let $e_p(\ ,\ )$ denote the Weil paring on $E'[p]$. Let $A \in \ker(\phi)$ and i an element of inertia. Then for all $B \in E'[p]$

$$e_p(\phi(iA), B) = e_p(iA, \hat{\phi}(B)) = e_p(A, i^{-1}\hat{\phi}(B))^i = e_p(\phi(A), i^{-1}B)^i = 0,$$

by the properties of the Weil pairing ([52] ch. III sec. 8) and the fact that the isogeny is defined over K. As it is true for all B we deduce that $\phi(iA) = O$ and so $\ker(\phi)$ is an invariant one dimensional subspace of $E[p]$ which show that inertia has the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Furthermore in [50] and [48], it is shown that inertia acts via a finite subgroup of order dividing 24, the exact order depending on the Néron classification. So inertia has no element of order $p \geq 5$ (by classical group theory), this show that E/K_ϕ has good reduction by the criteria of Néron-Ogg-Shafarevich. The remaining of proof is clearly stated in the article.

6.3.3 Potential good reduction and $p = 3$

The purpose of this section is to add some clues to the proof of the last case of theorem 6.4.1 (theorem 5 of [14]), namely the case of potentially good reduction with $p = 3$. The result is stated as follow.

Lemma 6.3.3 *([14] lemma 10) Suppose E has potential good reduction and $p = 3$. Then $W(E/F) = \delta(-1, K_\phi/K)$.*

Proof: Inertia of $G = \mathrm{Gal}(K(E[3])/K)$ is of the form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ because it as an invariant one-dimensional subspace, namely $\ker(\phi)$. It is of determinant 1 because the determinant of the action of Galois is the cyclotomic character which gives 1 on inertia. Then an easy computation shows that inertia, I, is one of the following cyclic group C_2, C_3 or C_6. The fact that $I = C_3$ if and only if E has reduction type IV or IV^* can be found in the article of Serre ([50] section 5.6.) in the case $l \neq 2$ and it is a result of Krauss ([25] theorem 2) in the case $l = 2$. In this case, G is either C_3, C_6 if $\mu_3 \subset K$ and the permutation group S_3 otherwise. The first two case are explained clearly in the article, let me explain the third case : $G = S_3$. The remaining of the proof is quite technical, I refer to the original article for it.

I owe the following explaination directly by Tim Dokchitser that I thank for it. We can use Schur's lemma to show that Frob^2 acts as a scalar because $V_3(E)$ is an irreducible representation of of $\mathrm{Gal}(\bar{F}/F)$. But as $\mathrm{Gal}(\bar{F}/F)$ is generated by the Frobenius and ny inertia, it suffice to show that Frob^2 commutes with inertia. On the other hand, inertia acts trough C_3 and is normal in $\mathrm{Gal}(\bar{F}/F)$ so for any element i of inertia $\rho(\mathrm{Frob}^2)\rho(i)\rho(\mathrm{Frob}^2)^{-1})$ is an element of C_3 which

is necessarilly trivial because it acts trivially on $E[3]$ as on $E[3]$ inertia acts by C_3 and Frob acts via a transposition.

6.4 The case of a 2−isogeny

This case is treated by direct computations on the Weierstrass equation :

$$\begin{aligned} &E:\ y^2 = x^3 + ax^2 + bx, \quad a, b \in \mathcal{O}_K \\ &E':\ y^2 = x^3 - 2ax^2 + \delta x, \quad \delta = a^2 - 4b, \\ &\phi(x, y) = (x + a + bx^{-1}, y - bx^{-2}y). \end{aligned}$$

On the other hand the discriminant of E is given by

$$\Delta(E) = 16\delta b^2.$$

Here we present the proof of theorem 4 of [14] which states that if E/K has either good ordinary or multiplicative reduction at all prime above 2. Then for all places v of K,

$$(\star) \quad W(E/K_v) = \sigma_\phi(E/K_v)(a, b)_{K_v}(-2a, \delta)_{K_v}.$$

The proof goes in several steps, namely: infinite places, finite places such that $[K_v : \mathbb{Q}_l] < \infty$ and $l \neq 2$, and the case of finite places with $l = 2$. Actually, the purpose of this theorem is not to compute the local terms which has been done here and in other article, but to correlate local root number and "local Selmer" rank in such a way that the product over all places will prove the parity conjecture.

Next I had a section on Hilbert symbol

6.4.1 Hilbert symbols

Let K be a finite extension of $\mathbb{Q}_p$ with p either finite or infinite. We define the *Hilbert symbol* for $a, b \in K^*$ by

$$(a, b)_K = \begin{cases} 1, & \text{if the from } ax^2 + by^2 - z^2 \text{ has a non-trivial zero in } K \\ -1, & \text{otherwise.} \end{cases}$$

Equivalently $(a, b)_K = 1$ if and only if $a = z^2 - by^2$ for some $y, z \in K$, which means that a is a norm from the quadratic extension $K(\sqrt{b})/K$.

The Hilbert symbol satisfies the following elementary properties

1. $(a, b)_K = (b, a)_K$
2. $(aa', b)_K = (a, b)_K(a', b)_K$ and $(a, bb')_K = (a, b)_K(a, b')_K$.
3. $(a, b)_K = 1$ for all b if and only if $a \in K^{*2}$.
4. $(a, -a)_K = 1$

Furthermore, it satisfies the following product formula : Let K be a number field then

$$\prod_{\mathfrak{p}\in M_K} (a,b)_{K_\mathfrak{p}} = 1.$$

The following results is used twice in the article [14], fist in the case of the local norm residue symbol, second in the lemma 15 which gives the computation of some Hilbert symbols.

Lemma 6.4.1 *(see e.g. [29] ch.2 sec.2) Let K be a finite extension of $\mathbb{Q}_p$ for some finite prime p. Let L be a unramified extension of K. Then every unit of K is a norm of some unit in L.*

In [14] they prove the following lemma

Proposition 6.4.1 *([14] lemma 15) Let $K/\mathbb{Q}_p$ be a finite extension (p finite). Then*

1. *If $|x| < 1$ and $y \in K^*$ then $(1+4x, y) = 1$.*
2. *If $p = 2$, $|x| = 1$ and $y \in \mathcal{O}_K^*$ then $(1+4x, y) = 1$.*
3. *$(-1,-2) = -1$ if and only if $p = 2$ and $[K : \mathbb{Q}_p]$ is odd*

Proof : For odd p, 1) is a consequence of the fact that $1+4x$ is a unit, so the preceding lemma (6.2.1) implies. Similarly, $(-1,-2) = 1$ for odd p.

The item 1) for $p = 2$ is proved in [53] : the series

$$(1+4x)^{1/2} = \sum_{n=0}^{\infty} \begin{pmatrix} -1/2 \\ n \end{pmatrix} (4x)^n$$

converge in K because $|x| < 1$ and

$$\begin{pmatrix} -1/2 \\ n \end{pmatrix} 4^n = (-1)^n \begin{pmatrix} 2n \\ n \end{pmatrix}$$

is an integer. This prove that $1+4x$ is a square in K^*, hence $(1+4x, y) = 1$.

For item 2) they also use the preceding lemma : it suffices to show that $K(\sqrt{1+4x})/K$ is unramified, that is $(1+4x)$ is a square in the unique quadratic unramifed extension L of K. For the remaining of the proof I refer to [14] where it is clearly stated.

$\diamond$

6.4.2 Discussion about the proof of theorem 6.1.2

Here we discuss the proof of the theorem 6.1.2, i.e. of equation $(\star)$. Here E is endowed with a 2-isogeny.

The case of infinite places is clearly explained in the article (sec. 7.1) and depends on the technic of Fisher and on the classification of the groups $E(\mathbb{R})$ and $E'(\mathbb{R})$ which I recall :

Proposition 6.4.2 *([53] corollary 2.3.1 ch. V) Let $E(\mathbb{R})$ be an elliptic curve, and let $\Delta(E)$ be the discriminant of some Weierstrass equation for $E/\mathbb{R}$. There is an isomorphism of real Lie groups*

$$E(\mathbb{R}) \cong \begin{cases} S^1, & if \Delta(E) < 0, \\ S^1 \times (\mathbb{Z}/2\mathbb{Z}), & if \Delta(E) > 0. \end{cases}$$

The case of finite places depends again on the technic of Fisher, presented earlier : we need to compute the parity of the exponent of the power of 2 in $|E(K)[\phi]|/|(E'(K)/\phi(E(K)))| = \frac{c(E')}{c(E)}|\alpha|^{-1}$.

The computation of the Tawagawa is mainly based upon Tate's algorithm which is exposed in [53] chapter IV section 9. In the case of good reduction and of characteristic $l \neq 2$ the global result is easy to obtain. ([14] sec. 7.3). Otherwise the reduction is either potentially good or potentially multiplicative. The cases of characteristic 2 and $\neq 2$ is treated separately.

For potential good reduction and $l \neq 2$ we know that $E/F(E[4])$ has good reduction from a result of Serre and Tate, corollary 3 of [48]. As $E/F(E[4])$ has good reduction the discriminant is a twelve power over that field and as $F(E[4])/F$ is a 2-extension $3|v(\Delta_E)$. According to the classification of Néron-Kodaira the reduction type of E is either III, III^*, I_0^* or I_n^*. With this and with the Weierstrass equations of E and E', Tim and Vladimir Dokchitser obtained the required results. The computation of the root numbers is due mainly to a result of Kobayashi in [26] who computed root numbers of elliptic curves defined by a Weierstrass equation. I recall the result.

Theorem 6.4.1 *(Kobayashi [26] theorem 1.1) Let K be a local field with residue field k and odd characteristic p. Let E/K be an elliptic curve with potential good reduction. let $y^2 = x^3 + ax^2 + bx + c$ be a Weierstrass equation and Δ the discriminant of this cubic polynomial. We denote the quadratic residue symbol on $k^\times$ by $\left(\frac{\ }{k}\right)$ and the Hilbert symbol of K by $(\ ,\ )_K$. We extend the residue symbol by putting $\left(\frac{0}{k}\right) = 1$*

1. *If the Néron-Kodaira type of E is I_0 or I_0^*, then*

$$W(E/K) = \left(\frac{-1}{k}\right)^{\frac{v(\Delta)}{2}}.$$

2. *If the Néron-Kodaira type of E is III or III^*, then*

$$W(E/K) = \left(\frac{-2}{k}\right).$$

3. *If the Néron-Kodaira of E is II, IV, IV^* or II^* there exists a Weierstrass equation such that $3 \nmid v_K(c)$. For such an equation we have*

$$W(E/K) = \delta(\Delta, c)_K \left(\frac{v_K(c)}{k}\right) \left(\frac{-1}{k}\right)^{v(\Delta)(v(\Delta)-1)/2}$$

where $\delta = \pm 1$ and $\delta = 1$ if and only if $\Delta^{\frac{1}{2}} \in K$.

Note that if π is a uniformizer parameter of the l-adic field K with residue field k, the Hilbert symbol $(\cdot, \pi)$ is the same thing as the residue symbol $\left(\frac{\cdot}{k}\right)$.. This explains the table given in section 7.4 of [14].

The case of type III is clear from Néron-Kodaira classification and from $\delta \equiv -4b \bmod \pi^2$ note also that $v(\delta) = 1$ implies that there is a unit u such that $\delta = u\pi$ so $(-2, \delta) = (-2, \pi)(-2, u) = (-2, \pi)$, finally

$$(a, -b)(-2a, \delta) = (a, -b\delta)(-2, \delta) = (a + 4b^2 + O(\pi^3))(-2, \pi) = (-2, \pi)$$

which agree with $(\star)$.

The case III^* is similar, for the type I_0^* they use Tate algorithm ([53] ch. IV sec. 9 p 367). More precisely $c(E) = 1 + |\{\alpha \in k | P(\alpha) = 0\}|$ where $P = T^3 + \frac{a}{\pi}T^2 + \frac{b}{\pi^2}T$. The discriminant of the quadratic equation obtain being $w = \frac{a^2 - 4b}{\pi^2} = \delta\pi^{-2}$, $c(E) = 4$ if and only if w is a square otherwise $c(E) = 2$. But w is a square if and only if $(\pi, \delta) = 1$. And same things for E'. With some easy computations (see [14] p. 12) this gives $(\star)$. The case of type I_n^* goes along the same lines : using Tate's algorithm as explained in [53].

In the case of good ordinary reduction in residue characteristic 2, $W(E/K) = 1$, $c(E) = c(E') = 1$, the only question remaining is $\mathrm{ord}_2|\alpha|$. The model of the curves depend on the fact that the 2-torsion point reduce to $\bar{O}$ or not.

Tim and Vladimir Dokchitser indicate that if E and E' are transformed into their respective minimal model by standard substitutions $(x, y) \mapsto (w^2x + \ldots, w^3y + \ldots)$ and $(x, y) \mapsto (u^2x + \ldots, u^3y + \ldots)$, then $\alpha = uw^{-1}$.

If the 2-torsion point reduce to $\bar{O}$, they manipulate the model (see e.g. [52] Appendix A) of the curve to obtain $w = 1$ and $u = 2$ this gives $\mathrm{ord}_2|\alpha|_K = \mathrm{ord}_2|2|_K$ which is, almost by definition, even if and only if $[K : \mathbb{Q}_2]$ is even which by proposition 6.5.1 (lemma 15 of [14]) is equivalent to $(-2, -1) = 1$. On the other hand by manipulating the equation of E, they obtain $(a, -b)(-2a, \delta) = (-2, -1)$, proving $(\star)$ in this case.

If the 2-torsion point reduce to $\bar{O}$ by using appropriate model they show that $\alpha = 1$.

In the case of multiplicative reduction, they distinguish the case of split multiplicative reduction for which they use the theory of the Tate curve and of non-split reduction for which they reduce to split multiplicative reduction after a twist by a quadratic character.

In the case of split multiplicative reduction, we know from the preceding propositions (6.2.3 and theorem 6.3.1) that $\mathrm{ord}_2(c(E')/c(E)) = \pm 1$ and that $W(E/K) = -1$.They directly use the theory of the Tate curve, which furnishes the 2-torsion points. Their article is clear about this subject, no need to reproduce it here. For non-split multiplicative reduction, they use the theorem of Tate to reduce to split-multiplicative reduction and Tate's algorithm as exposed in [53] ch IV sec. 9 to compute the Tamagawa numbers.

Chapter 7

Conclusion

What can I conclude from this work ? First of all that it was helpful for me. Before the beginning I didn't realize that one must enter the vast territory of modern research by some way, for me it was the article of Tim and Vladimir Dokchitser and its related articles and subjects. I am happy to have gained some knowledge about the rich subject of $L-$functions as there is a gap between the elementary Dirichlet series and the theoretical framework of $L-$functions of algebraic varieties. This work has helped me to understand some basic but important facts that are essential in understanding the far reaching and active field of research linked to the "L" world.

Moreover I reinforced my knowledge of elliptic curves by working on the article [14]. I tried to make the text as self-contained as possible, at least by presenting the definitions, theorems and ideas linked to this article. As everyone working in the field of elliptic curves may be filled with wonder by this fruitful subject, I am satisfied to know some of its technics and results. I was even surprised to observed that I can know read works about it without being too disoriented as I now know some of the main research themes and guidelines.

However, having understood this article, one may be unsatisfied by the fact that there is no clear idea that link root numbers to Selmer ranks. Something important may be missing, not too surprisingly because the notions involved are, up to now, mainly conjectural.

Nonetheless, the essential of my work is not contained in this text. In fact as I want to do research in Mathematics, I consider that the main consequence of my work is that I have gained insight and familiarity with this working activity. It was necessary for me to take the plunge from school mathematics to professional mathematics and I consider that this work was a good step. Actually, I think that it is useful for every student to go from a "passive" school learning to an "active" and personal point of view. This is what gives sense to studies and this

is what I enjoy having (partially) reached, the next step being my thesis.

I am so grateful to the Professor Marc Hindry of Paris 7 University. He has chosen the article [14] and I didn't realize immediately that It would help me so much. The article is quite short (17 p.) but working on it I travelled through important areas of number theory, from algebraic number theory, class field theory, zeta and L functions to the fertile land of elliptic curves. I discovered for myself various new things as suggested in the bibliography. I am also grateful for his two half-semester courses on elliptic curves and on abelian varieties which me and the other students enjoyed so much.

Bibliography

[1] E. Artin, Über eine neue Art von L-Reihen . Hamb. Abh., 89-108 1923, Collected papers nř 3

[2] E. Artin, J. Tate; Class Field Theory, W.A. Benjamin,Inc (1967)

[3] S. Bosch, W. Lütkebohmert and M. Raynaud, Néron Models ; Springer-Verlag (1980)

[4] D. Bump, Automorphic Forms and Representations ; Cambridge Studies in Advanced Mathematics 55 (1998)

[5] J.W.S Cassels, Arithmetic of curve of genus 1 IV Proof of the Hauptvermutung ; J. Reine Angew Math. 211 pp. 95-112 (1962)

[6] J.W.S Cassels, Arithmetic of curve of genus 1 VIII On the conjecture of Birch and Swinnerton-Dyer ; J. Reine Angew Math. 217 pp. 180-199 (1965)

[7] J.W.S Cassels, A. Fröhlich, Algebraic Number Theory ; Academic Press (1967)

[8] C. Chevalley, La théorie du corps de classe ; Annals of Math., **41**, 394-418 (1940). Zbl.25,18

[9] P. Deligne, Les constantes des équations fonctionnellles des fonctions L ; Modular forms in one variable II, SLN 349, Springer-Verlag, New-York, pp. 501-595 (1973)

[10] P. Deligne, Les constantes des équations fonctionnelles ; Séminaire Delange-Pisot-Poitou, Théorie des nombres, vol 11, nř2, 19bis pp 16-28 (1969-1970)

[11] P. Deligne, Valeurs de fonctions L et périodes d'intégrales ; Proceedings of Symposia in Pure Mathematics Vol. 33 (1979), part 2, pp. 313-346

[12] M. Demazure, Motifs des variétés algébriques ; Séminaire N. Bourbaki, 1969-1970, pp. 19-38

[13] F. Diamond, J. Shurmann, A first course on modular forms ; Graduate Texts in Mathematics 228, Springer

[14] T. and V. Dokchitser, Parity of Ranks of Elliptic Curves with a Cyclic Isogeny ; J. Number Theory 128 (2008), 662-679, available on: http://www.dpmms.cam.ac.uk/ vd209/

[15] V. Dokchitser with an appendix of Tom Fisher, Root Numbers of Non-abelian Twists of Elliptic Curves ; Proc. London Math. Soc. (3) 91 (2005) pp 300-324, available on: http://www.dpmms.cam.ac.uk/ vd209/

[16] T. and V. Dokchitser, Regulator constants and the parity conjecture; preprint (2007), available on: http://arxiv.org/abs/0709.2852v1

[17] A. Frölich, Formal Groups ; Lecture Notes in Mathematics 74 (Springer 1968)

[18] A. Frölich, J. Queyrut ; On the functional equation of the Artin L-function for characters of real representations, Invent. Math. 20 (1973), 125-138

[19] D. Goldfield and L. Szpiro, Bounds for the order of the Tate-Shafarevich group ; Compositio Math. **97** (1995) p. 71-87

[20] R. Hartshorne, Algebraic Geometry ; Graduate Texts in Mathematics 52, Springer-Verlag (1977)

[21] D. Husemöler, Elliptic Curves ; Graduate Texts in Mathematics 111, Springer (1987)

[22] K. Iwasawa, Lectures on p-adic L-functions ; Annals of Mathematics Studies PUP (1972)

[23] G. Kato, The heart of cohomology ; Springer (2006)

[24] K. Kramer and J. Tunnel, Elliptic Curves and Local ϵ-factors ; Compositio Mathematica Vol. 46, nř3 p.307-352 (1982)

[25] A. Krauss, Sur le défaut de semi-stabilité des coubes elliptiques à réduction additive ; Manuscripta Math. 69. 353-385 (1990)

[26] Sh. Kobayashi, The Local Root Number of Elliptic Curves with Wild Ramification ; Mathematische Annalen 323, p.609-623 (2002)

[27] Qing Liu, Algebraic Geometry and Arithmetic Curves ; Oxford Graduate texts in Mathematics (2002)

[28] S. Lang, Algebraic groups over finite fields ; Amer. J. Math. (78) (1956) pp. 555-563

[29] S. Lang, Algebraic Number Theory ; Graduate Texts in Mathematics 110, Springer (1970)

[30] Robert P. Langlands, On the Functional Equation of the Artin L-functions ; Available on the website of Robert Langlands

[31] Yu.I. Manin, A.A. Panchishkin, Introduction to Modern Number Theory ; Encyclopaedia Of Mathematical Sciences (Springer 2004)

[32] J.S. Milne, Lecture on étale cohomology ; notes for a course taught at the university of Michigan, available at www.math.lsa.umich.edu/ jmilne/

[33] J. Nekovář, On the parity of ranks of Selmer groups ; Asian J. Math. 4 (2000), No. 2, 437 - 498 (with A. Plater), available at http://www.math.jussieu.fr/ nekovar/pu/

[34] J. Nekovář, On the parity of ranks of Selmer groups II ; Comptes Rendus de l'Acad. Sci. Paris, Serie I, 332 (2001), No. 2, 99 - 104, available at http://www.math.jussieu.fr/ nekovar/pu/

[35] J. Nekovář, On the parity of ranks of Selmer groups III ; Documenta Math. 12 (2007), 243 - 274, available at http://www.math.jussieu.fr/ nekovar/pu/

[36] J. Nekovář, On the parity of ranks of Selmer groups IV ; preprint, 5pp (with an appendix by J.-P. Wintenberger, 4pp), available at http://www.math.jussieu.fr/ nekovar/pu/

[37] J. Neukirch, Algebraic Number Theory ; Springer (1999)

[38] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields ; Grundlehren der Mathematischen Wissenschaften Vol. 323 Springer (2000)

[39] M. Ram Murty, Lecture on Artin L-functions ; notes of a course of lecture given at the Tata Institute of Fundamental Research during 1998-1999 on automorphic forms.

[40] Bjorn Poonen, The Selmer group, the Tate-Shafarevich, and the Mordell-Weil theorem ; math.berkeley.edu/ poonen/f01/weakmw.pdf (2002)

[41] K. Rubin and A. Silverberg, Ranks of Elliptic Curves ; Bul. of the American Math. Soc. Volume 39, Number 4, pp. 455-474 (2002)

[42] D. E. Rohrlich, Elliptic and the Weil Deligne group, Elliptic Curves and Related Topics ; CRM Proceedings and Lecture Notes Vol.4 pp. 125-157 (1994)

[43] D. E. Rohrlich, Galois theory, elliptic curves and root numbers ; Compositio Mathematica, vol. 100, nř3 pp 311-349 (1996)

[44] D. Ramakrishnan and R.J. Valenza, Fourier Ananalysis on Number Fields ; Graduate Texts in Mathematics 186, Springer (1998)

[45] J.-P. Serre, Cours d'arithmétique ; Presse Universitaires de France (1970)

[46] J.-P. Serre, Facteurs locaux des fonctions zêta des variétés algébriques (Définitions et conjectures) ; Séminaire Delange-Pisot-Poitou, Théorie des nombres, vol 11, nř2, nř19 pp 1-15

[47] J.-P. Serre, Corps locaux ; Hermann (1968) (Traduced in english with the title "Local Fields")

[48] J.-P. Serre and J. Tate, Good reduction of abelian varieties ; Annals of Math. 68 (1968), 492-517

[49] J.-P. Serre, Prpriétés galoisienne des points d'ordre fini des courbes elliptiques ; Inventiones math. 15, 259-331 (1972)

[50] J.-P. Serre, Galois Cohomology ; Springer Monographs in Mathematics (1997)

[51] E.F. Shaefer, Class groups and Selmer groups ; J. Number theory 56 (1996), no. 1, 79-114

[52] J. H. Silverman, The arithmetic of elliptic curves ; Graduate Texts in Mathematics 106, Springer

[53] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves ; Graduate Texts in Mathematics 151, Springer

[54] J. Tate, Fourier analysis in number fields and Hecke's zeta function ; Thesis, Princeton (1950)

[55] J. Tate, Number Theoretic Background ; Proceedings of Symposia in Pure Mathematics Vol. 33, part 2 p.3-26 (1979)

[56] C. Voisin, Théorie de Hodge et géométrie algébrique complexe ; Cours spécialisé 10 , Société mathématique de France (2002)

[57] A. Weil, Basic Number Theory ; Classics in Mathematics, Springer 3^{rd} ed. (1974)

[58] A. Weil, Sur la théorie du corps de classe ; J. Math. Soc. Japan (1951)