Anabelian geometry over local fields

Internship Report

BAGET Martin

Supervised by YAMASHITA Go

La réalisation de ce stage a été intégrée au projet *Arithmetic and Homotopic Galois Theory* (AHGT), soutenu par le réseau de recherche international CNRS France-Japon AHGT entre le RIMS Kyoto University, le LPP de l'université de Lille University, et le DMA de l'ENS PSL.

RIMS 京都大学 数理解析研究所 Research Institute for Mathematical Sciences, Kyoto University

Arithmetic & Homotopic Galois Theory
A France-Japan International Research Network

Contents

1. Preliminaries

We assume no knowledge about local fields, and as such first recall the definition and the basic properties of such a field. We asume, however, knowledge of the general theory of extensions of fields (Galois theory, ramification theory, etc).

Definition 1.1 — Local Field. We say that a field K is a local field if there exists a valuation, that is a morphism $v : K^\times \to \mathbb{Z}$ satisfying $\forall x,y \in K^\times,\ v(x+y) \geqslant min\{v(x), v(y)\}$, such that

1. K is complete for the absolute value defined by $\forall x \in K\ |x|_K = exp(-v(x))$.
2. the quotient field $\{x \in K \mid v(x) \geqslant 0\}/\{x \in K \mid v(x) \geqslant 1\}$ is finite.

For such a field K,

- the ring $\mathcal{O}_K = \{x \in K \mid v(x) \geqslant 0\} = \{x \in K \mid |x|_K \leqslant 1\}$ is called the ring of integers of K.
- its ring of integers is local of maximal ideal $\mathfrak{m}_K = \{x \in K \mid v(x) > 0\} = \{x \in K \mid v(x) \geqslant 1\} = \{x \in K \mid |x|_K < 1\}$ and the units are exactly the elements of valuation 0, or equivalently of norm 1.
- the quotient field $k = \mathcal{O}_K/\mathfrak{m}_K$ is called the residue field of K.
- an element of $\mathfrak{m}_K$ of minimal valuation is called an uniformizer of K. Equivalently, an uniformizer is a generator of the ideal $\mathfrak{m}_K$.
- the norm $|.|_K$ satifies not only the triangle inequality, but the stronger ultrametric inequality:

$$\forall x,y \in K,\ |x+y|_K \leqslant max\{|x|_K, |y|_K\}$$

1.1 Finite extensions of local fields

The typical example of a local field is $\mathbb{Q}_p$ for p a prime, with ring of integers $\mathbb{Z}_p$ and residue field $\mathbb{F}_p$. In fact, one can prove that any local field of characteristic zero is a finite extension of Q_p. Our interest lies in the converse:

Theorem 1.1 Let K be a local field and L a finite extension of K. Let $N_{L/K} : L^\times \to K^\times$ be the norm morphism, and for $x \in L$, $|x|_L = |N_{L/K}(x)|_K$. Then L is a local field for the absolute value $|.|_L$.

Note that the results of this section do not form the core of the subject, but they are used implicitly many times in the following sections. For examples, in the next section we will talk about "the" ramification index of an extension of local fields: one has to understand that we are talking about the ramification index respective to the maximal ideals (and thus we are implicitly using this theorem).

The proof of this theorem is not at all as easy as one could think. It uses the following important lemma:

Proposition 1.1 — Hensel's lemma. Let K be a local field, $f \in \mathcal{O}_K[X]$, $\overline{g}, \overline{h} \in k[X]$ such that $f = \overline{g}\overline{h}$ modulo $\mathfrak{m}_K$ and $gcd(\overline{g}, \overline{h}) = 1$. Then then are polynomials $g, h \in \mathcal{O}_K[X]$ such that $f = gh$ with $g = \overline{g}$ modulo $\mathfrak{m}_K$, $h = \overline{h}$ modulo m_K, $deg(g) = deg(\overline{g})$.

Moreover, if we suppose that f, $\overline{g}$, $\overline{h}$ are monic and add the condition that g and h need to be monic, then g and h are unique.

Proof. We fix ω a uniformizer of K and a set of representatives of k giving $\phi : k \to \mathscr{O}_K$ a right-inverse of the projection $\mathscr{O}_K \to k$. We then have a bijection

$$\psi : k^{\mathbb{N}} \to \mathscr{O}_K,\ (a_n)_n \mapsto \sum_{n\in\mathbb{N}} \phi(a_n)\omega^n$$

Beware that ϕ and ψ do not respect any structure. ψ gives a bijection

$$\overline{\psi} : k[\![X]\!]^{\mathbb{N}} \to \mathscr{O}_K[\![x]\!],\ (\sum_{k\in\mathbb{N}} a_{n,k}X^k)_n \mapsto \sum_{k\in\mathbb{N}}(\sum_{n\in\mathbb{N}} \phi(a_{n,k})\omega^n)X^k$$

Moreover, the polynomials on $\mathscr{O}_K$ are exactly given by the families of polynomials on k with a uniform bound on their degrees, and in this case the degree of the polynomial given by $\overline{\psi}$ is the maximum of the degrees of the polynomials on $k[X]$.

Now let us reformulate what we want to prove. If we denote by $(f_n)_n$ the inverse image of f by $\overline{\psi}$, saying that $f = gh$ in $\mathscr{O}_K[X]$ with $g = \overline{g}$ modulo $\mathfrak{m}_K$ and $h = \overline{h}$ modulo m_K is equivalent to saying that there exist two families $(g_n)_n$, $(h_n)_n$ of polynomials of $k[X]$ of bounded degrees such that

$$\forall n \in \mathbb{N},\ f_n = \sum_{k=0}^{n} g_k h_{n-k}$$

with $g_0 = \overline{g}$ and $h_0 = \overline{h}$.

But proving the existence of such families is easy. Indeed, the above condition can be written as follows:

$$\forall n \in \mathbb{N}^*,\ g_0 h_n + g_n h_0 = f_n - \sum_{k=1}^{n-1} g_k h_k$$

and (g_n) and (h_n) can be defined by induction using the fact that the ideal generated by g_0 and h_0 is the whole ring $k[X]$. Moreover we know that we can impose $deg(g_n) < deg(g_0)$ for $n \in \mathbb{N}^*$ so that we get $deg(g) = deg(g_0) = deg(\overline{g})$ as stated. The fact that f and g are polynomials in $\mathscr{O}_K[X]$ implies that h is too, or we can check by induction that $deg(h_n) \leqslant deg(f) - deg(\overline{g})$ for $n \in \mathbb{N}$.

For $n \in \mathbb{N}^*$, g_n is determined modulo a multiple of g_0, and if want g monic we should have $deg(g_n)) < deg(g_0)$ therefore (g_n) is uniquely determined. Then (h_n) is determined by (g_n) and we have the unicity. ■

Corollary 1.1 Let $P \in K[X]$ be an irreducible polynomial whose leading and constant coefficients are in $\mathscr{O}_K$. Then $P \in \mathscr{O}_K[X]$.

Proof. Fix ω a uniformize of K. Suppose that $P \notin \mathscr{O}_K[X]$, and let $m \in \mathbb{N}^*$ be the smallest integer such that $\omega^m P \in \mathscr{O}_K[X]$. Modulo $\mathfrak{m}_K$, the polynomial $\omega^m P \in \mathscr{O}_K[X]$ is non-zero but divisible by X. If we write it $X^e\overline{h}$ with $e \in \mathbb{N}^*$, $\overline{h} \in k[X]$, $\overline{h}(0) \neq 0$, then by Hensel's lemma $f = gh$ for some $g, h \in \mathscr{O}_K[X]$, $deg(g) = e$. By the irreducibility of f in $K[X]$, we have $f = \lambda g$ for some $\lambda \in K$. But since the leading coefficient of f vanishes modulo $\mathfrak{m}_K$, $deg(g) = e \leqslant e + deg(\overline{h}) < deg(f)$. Therefore we get a contradiction. ■

Proof of the theorem. The valuation associated to $|.|_L$ is indeed a morphism with values in $\mathbb{Z}$. We need to prove that $|.|_L$ satifies the ultrametric inequality. It is sufficient to prove that $|1+x|_L < 1$ if $x \in L$, $|x|_L < 1$. Let P be the minimial polynomial of x over K, so that $P(X-1)$ is the minimal polynomial of $1+x$ over K, $|x|_L = |P(0)|_K^m < 1$, $|1+x|_L = P(-1)|_K^m$ where m is the degree of L over $K[x]$. P has leading coefficient $1 \in \mathscr{O}_K$ and constant coefficient $P(0) \in \mathscr{O}_K$ by hypothesis. By the previous corollary, $P \in \mathscr{O}_K[X]$, and therefore $P(X-1) \in \mathscr{O}_K[X]$. In particular $P(-1) \in \mathscr{O}_K$, or equivalently $|1+x|_L < 1$ as we wanted.

The completeness of L is a particular case of a much more general statement: any finite-dimensional vector space on a complete field is complete for any norm (it is true for the norm given by the maximum of the coordinates in a fixed basis, and so for any norm by the equivalence of norms). In our case, we apply this result to $|.|_L^{1/dim_K(L)}$ which is homogeneous and still satifies the ultrametric inequality.

Finally, we prove that l/k is a field extension of degree at most $n = dim_K(L)$, where l is the residue field of L. Let $(\overline{x_1},...,\overline{x_{n+1}})$ be elements of l and $(x_1,...,x_{n+1})$ in L representants of these elements. Then we have elements $(\lambda_1,...,\lambda_{n+1})$ of L, with at least one non-zero, such that

$$\sum_{k=1}^{n+1} \lambda_k x_k = 0$$

Fix $i \in [\![1;n+1]\!]$ such that λ_i is non-zero of minimal valuation. Then

$$x_i + \sum_{k \neq i} \frac{\lambda_k}{\lambda_i} x_i = 0$$

with $\frac{\lambda_k}{\lambda_i} \in \mathscr{O}_K[X]$ for any k. In the quotient by $\mathfrak{m}_K$, we get a relation between the elements $(\overline{x_1},...,\overline{x_{n+1}})$ with a coefficient 1 in front of $\overline{x_i}$. Hence the result. ∎

Theorem 1.2 Let K be a local field, L, M two finite extensions of K. Then:

1. Any morphism of K-algebras $L \to M$ induces a morphism of k-algebras $l \to m$ (their residue fields). If L is unramified, then this is a 1-1 correspondence.
2. The unramified finite extensions of K are in 1-1 correspondence with the finite extensions of k by taking their residue fields.
3. For any $n \in \mathbb{N}^*$, K has exactly one unramified extension of degree n, denoted K_n.
4. If L/K is an unramified extension, then L/K is Galois of Galois group $Gal(L/K) \simeq Gal(l/k) \simeq \mathbb{Z}/dim_K(L)\mathbb{Z}$. In particular L/K is an abelian extension.

Proof. 1. Let $f : L \to M$ be a morphism of K-algebras. We have to show that $f(\mathscr{O}_L) \subseteq \mathscr{O}_M$ and $f(\mathfrak{m}_L) \subseteq \mathfrak{m}_M$. Let $x \in \mathscr{O}_L$ and P the minimal polynomial of x over K, so that $v(P(0)) \geqslant 0$ by hypothesis. The polynomial P vanishes at $f(x)$ and is irreducible so P is the minimal polynomial of $f(x)$, thus $f(x) \in \mathscr{O}_M$. Similarly, $x \in \mathfrak{m}_L$ if and only if $v(P(0)) > 0$ and we get that $f(\mathfrak{m}_L) \subseteq \mathfrak{m}_M$. Therefore f induces a morphism of k-algebras $l \to m$.
Now we suppose that L is unramified. Let $\alpha \in l$ be a generator of $l^\times$ and $\overline{g} \in k[X]$ its minimal polynomial. Let $g \in \mathscr{O}_K[X]$ be a monic representant of $\overline{g}$. g is still irreducible in $\mathscr{O}_K[X]$. And since $\overline{g} = (X-\alpha)\overline{h}$ for some $\overline{h} \in l[X]$ that doesn't have α as root (a finite field is perfect), by Hensel's lemma $g = (X-a)h$ for some unique $a \in \mathscr{O}_L$ a representant of α, $h \in \mathscr{O}_L[X]$ a representant of $\overline{h}$. Since g is irreducible over $K[X]$, g is the minimal polynomial of a and the equality $deg(g) = deg(\overline{g}) = dim_k(l) = dim_K(L)$ (L being unramified) implies that $L = K[a]$. Then we prove that

$$\begin{aligned} Hom_{K-algebras}(L,M) &\simeq \{b \in \mathscr{O}_M \mid g(b) = 0\} \\ &\simeq \{\beta \in m \mid \overline{g}(\beta) = 0\} \\ &\simeq Hom_{k-algebras}(l,m) \end{aligned}$$

Indeed, the first isomorphism is simply because a morphism of K-algebras from L is determined by the image of a, which must be an element of $\mathscr{O}_M$ of minimal polynomial g. The second isomorphism is a consequence of Hensel's lemma: a root of $\overline{g}$ in m can be uniquely lifted as a root of g in $\mathscr{O}_M$. The third isomorphism is because a morphism of k-algebras from l is determined by the image of α.

2. The unicity is a consequence of the previous point. Fix l a finite extension of k and let us prove that there exist L an unramified extension with residue field l. Let α be a generator of $l^\times$, $\overline{g}$ its minimal polynomial over k and g a representant of $\overline{g}$ in $\mathscr{O}_K[X]$. g is still irreducible by Hensel's lemma. Let $L = K[a]$ be a rupture field of g. L has degree $deg(g) = deg(\overline{g}) = dim_k(l)$ over K, and the residue field of L contains the subfield generated by the image of a which is isomorphic to l over k (because the minimal polynomial of the image of a is $\overline{g}$). This implies that L has residue field l and is unramified.
3. It follows from the previous statement and the unicity of $\mathbb{F}_{p^n}$ for $n \in \mathbb{N}^*$.
4. We write $L = K[a]$ with $\alpha, \overline{g}, g, a$ as in the proof of 2. An extension of finite fields is always Galois, thus $\overline{g}$ has all its roots in l and they are distinct. Then by Hensel's lemma, the roots of g are in L and they are distinct.. This proves that L/K is Galois. The equality between the Galois groups of L/K and l/k is then classical ramification theory.

■

1.2 Ring of integers of a local field

The properties of the ring of integers of a number field F are well-known: $\mathscr{O}_F$ is a free $\mathbb{Z}$-module of rank $dim_{\mathbb{Q}}(F)$, and the units of $\mathscr{O}_F$ form a finitely-generated $\mathbb{Z}$-module of rank $r+s-1$, where r is the number of embedding of F in $\mathbb{R}$, and s the number of pairs of embeddings of F in $\mathbb{C}$ (Dirichlet's unit theorem). For p-adic fields, the situation is much simpler, as stated by the following theorem:

Theorem 1.3 Let L/K be an extension of local fields.
- There exists $a \in \mathscr{O}_L$ such that $L = K[a]$ and $\mathscr{O}_L = \mathscr{O}_K[a]$. In particular, $\mathscr{O}_L$ is a free $\mathscr{O}_K$-module of rank $dim_K(L)$.
- Assume that $K = \mathbb{Q}_p$. Then the multiplicative group $1+\mathfrak{m}_L$ is a $\mathbb{Z}_p$-module isomorphic to $\mathbb{Z}_p^{dim_{\mathbb{Q}_p}(L)} \oplus \mathbb{Z}/p^r\mathbb{Z}$ for some $r \in \mathbb{N}$. $\mathscr{O}_L^\times$ is a $\hat{\mathbb{Z}}$-module isomorphic to $\mathbb{Z}_p^{dim_{\mathbb{Q}_p}(L)} \oplus \mathbb{Z}/p^r\mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z}$ where q is the cardinal of the residue field of L.

Proof of the first point. Let α be a generator of l over k, $\overline{g}$ the minimal polynomial of α over k, $g \in \mathscr{O}_K[X]$ a monic representant of $\overline{g}$, $a \in \mathscr{O}_L$ the root of g corresponding to α (by Hensel's lemma). Also fix π a uniformizer of L. Now define $b = a$ if $g(a) \notin \mathfrak{m}_L^2$, and $b = a+\pi$ otherwise. In the second case, we have $g(b) = g(a) + \pi g'(a) + \pi^2 c$ for some $c \in \mathscr{O}_L$ with $g(a) \in \mathfrak{m}_L^2$ and $g'(a) \notin \mathfrak{m}_L$ (for if $g'(a) \in \mathfrak{m}_L$, $\overline{g}'(\alpha) = 0$ and this can't happen because an extension of finite fields is separable). We conclude that in both case we have the two following properties : (1) The image of b in l is a generator of l over k. (2) $g(b) \in \mathfrak{m}_L \backslash \mathfrak{m}_L^2$. The second property means that $g(b)$ is a uniformizer of L. The two equalities $L = K[b]$ and $\mathscr{O}_L = \mathscr{O}_K[b]$ follow. Since b has a minimal polynomial monic with coefficients in $\mathscr{O}_K$, it implies that $\mathscr{O}_L$ is a free $\mathscr{O}_K$-module of rank $deg(b) = dim_K(L)$. ■

We first have to describe how to make $\mathscr{O}_L^\times$ into a $\hat{\mathbb{Z}}$-module. We have the following exact sequence

$$0 \to 1+\mathfrak{m}_L \to \mathscr{O}_L^\times \to l^\times \to 0$$

This sequence admits a natural section, more exactly there is exactly one multiplicative section $l^\times \to \mathscr{O}_L^\times$ called the Teichmüller map ω. Let us first prove the unicity: since all elements of $l^\times$ have $q-1$ power equal to 1 (where q is the cardinal of the residue field), ω must have image in the $q-1$ roots of unity in L. By Hensel's lemma, for each $x \in l^\times$, there is exactly one $q-1$ root of unity in L of image x in the residue field. Thus ω is unique, and defined this way we see that it is indeed a multiplicative section.

Now we describe how to make $1+\mathfrak{m}_L$ into a $\mathbb{Z}_p$-module. We will define x^a for $x \in 1+\mathfrak{m}_L$, $a \in \mathbb{Z}_p$. First note the following: write $x = 1+p^m y$ for some $m \in \mathbb{N}^*$, $y \in \mathscr{O}_L$, then

$$x^p = 1 + p^{m+1}y + p^{2m}z \in 1 + p^{m+1}\mathscr{O}_L$$

for some $z \in \mathcal{O}_L$. By induction, we get that $x^{p^k} \in 1 + p^{m+k}\mathcal{O}_L$. It follows that if $a \in \mathbb{Z}_p$ is written $\sum_{i=0}^{+\infty} a_i p^i$, then the sequence of powers of x by the partial sums

$$\left(x^{\left(\sum_{i=0}^{k} a_i p^i\right)} \right)_k$$

is a Cauchy sequence, and thus converges. It is its limit that is denoted x^a.

The proof of point 2 of the theorem is based on the p-adic exponential and logarithm :

$$exp(x) = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$$

$$ln(1+x) = \sum_{n=1}^{+\infty} \frac{(-1)^{n+1}x^n}{n}$$

By giving an approximation of the p-adic valuation of $n!$ (with Legendre's formula), one can prove that $exp(x)$ is well-defined for $x \in \mathfrak{m}_L^k$ for $k > \frac{e(L/\mathbb{Q}_p)}{p-1}$ where $e(L/\mathbb{Q}_p)$ is the ramification index of L over $\mathbb{Q}_p$. We also prove that $ln(1+x)$ is well-defined for $x \in \mathfrak{m}_L$. We have the usual properties that the exponential and logarithm are morphisms between the additive and the multiplicative groups and that their composition is the identity when well-defined.

Proof of the second point. By properties of the exponential and the logarithm, for $k > \frac{e(L/\mathbb{Q}_p)}{p-1}$ we have that

$$ln : 1 + \mathfrak{m}_L^k \to \mathfrak{m}_L^k$$

is an isomorphism. Moreover, the quotient group

$$(1+\mathfrak{m}_L)/(1+\mathfrak{m}_L^k)$$

is finite. Indeed, for π a uniformizer and $i \in [\![1; k-1]\!]$, consider the map

$$(1+\mathfrak{m}_L^i)/(1+\mathfrak{m}_L^{i+1}) \to l,\ x \mapsto \ the\ class\ of\ \frac{x-1}{\pi^i}$$

Then it is a bijection, thus the cardinal of $(1+\mathfrak{m}_L)/(1+\mathfrak{m}_L^k)$ is equal to q^{k-1}.

It follows from those two facts that $1+\mathfrak{m}_L$ is a finitely-generated $\mathbb{Z}_p$-module. From the structure theorem of finitely-generated modules over principal ideal domains, $1+\mathfrak{m}_L$ is of the form $\mathbb{Z}_p^d \oplus \mathbb{Z}_p/p^r\mathbb{Z}_p$ for some $d, r \in \mathbb{N}$. Note that

$$\mathbb{Z}_p/p^r\mathbb{Z}_p \simeq \mathbb{Z}/p^r\mathbb{Z}$$

Finally, since $(1+\mathfrak{m}_L)/(1+\mathfrak{m}_L^k)$ is finite, d is also the rank of $1+\mathfrak{m}_L^k \simeq \mathfrak{m}_L^k$, and $\mathfrak{m}_L/\mathfrak{m}_L^k$ is also finite, so d is the rank of $\mathfrak{m}_L$ over $\mathbb{Z}_p$, that is $dim_{\mathbb{Q}_p}(L)$ by point 1. Point 2 of the theorem follows since

$$\mathcal{O}_L = (1+\mathfrak{m}_L) \oplus l^\times \simeq (1+\mathfrak{m}_L) \oplus \mathbb{Z}/(q-1)\mathbb{Z}$$

■

1.3 Profinite groups

Recall that a profinite group G is an inverse limit of a system (G_i) of finite groups indexed by a set I,

$$G = \varprojlim G_i$$

We are interested in the basic properties of these groups because the Galois group of an algebraic Galois extension L/K is naturally a profinite group

$$Gal(L/K) = \varprojlim Gal(M/K)$$

where M runs through the finite Galois subextensions of L. More generally, the étale fundamental group, defined later, is always a profinite group.

A profinite group is thus defined as a closed subgroup of the product $\prod G_i$, and we will always consider that it is endowed with the restriction of the product topology (where each G_i has the discrete topology). Note that the product and inverse maps are continuous for this topology. As a corollary of Tychonov's theorem, any profinite group is compact.

Proposition 1.2 In a profinite group G, the open subgroups are exactly the closed subgroups of finite index.

Proof. Let H be any subgroup of G. If we choose (g_i) representants of G modulo H, then we can write G as the disjoint union of the g_iH. Now suppose H is closed of finite index. Then we get that $G\backslash H$ is a finite union of closed subsets, thus closed, so H is open. Similarly, we get that if H is open of finite index, then it is also closed.

To conclude, we only need to prove that any open subgroup H of G is of finite index. Write G as the disjoint union of the g_iH as before. Then the g_iH are all open, and as a consequence of the compacity this union must be finite. This is the desired result. ■

We now describe how an abelian profinite group G can be seen as a $\hat{\mathbb{Z}}$-module. Denote $p_i : G \to G_i$ the natural projection. First note that we can suppose that the p_i are surjective: indeed, if we replace G_i by $Im(p_i)$, we have another system of finite groups giving G. In the rest of the section, we make this assumption. Then G_i can be seen as the quotient of G by the kernel of the projection $G \to G_i$, and this kernel is a normal open (because closed of finite index) subgroup of G. Even if we add the normal open subgroups not appearing in this inverse limit, it doesn't change the group:

Proposition 1.3

$$G = \varprojlim G/N$$

where N runs through every open normal subgroup of G.

Proof. Since $ker(p_i)$ is an open normal subgroup of G for each i, the natural map $G \to \varprojlim G/N$ is injective.

The key point to prove the surjectivity is the following lemma: given N an open subset of G, there is a finite subset $J \subseteq I$ such that $\bigcap_{j\in J} ker(p_j) \subseteq N$. As in the proof of the previous proposition, write $N = N' \cap G$ where N' is open in the product $\prod G_i$. By definition of the product topology, there is a finite subset $J \subseteq I$ such that

$$\prod_{j\in J} 1_{G_j} \times \prod_{i\in I\backslash J} G_i \subseteq N'$$

Then this subset J gives the result.

The surjectivity follows. Indeed, let $x \in \varprojlim G/N$. Keeping only the coordinates in the open normal subgroups $ker(p_i)$, we have an element $x' \in \varprojlim G_i = G$. Then let N be any open normal subgroup N and J given by the previous paragraph. Then $x - x' \in \bigcap_{j \in J} ker(p_j)$, thus $x = x'$ in G/N. Since this is true for any N, $x' \in G$ is an antecedent of x. ■

Note that by Proposition 1.2, the quotients G/N are all finite. Then we describe the action of $\hat{\mathbb{Z}}$ on G as follows: for any N, G/N is naturally a $\mathbb{Z}/(Card\ G/N)\mathbb{Z}$-module ; the actions are compatible with the morphims $G/N \to G/N'$ and $\mathbb{Z}/(Card\ G/N)\mathbb{Z} \to \mathbb{Z}/(Card\ G/N')\mathbb{Z}$ if $N \subseteq N'$, so they define an action of $\hat{\mathbb{Z}}$ on G.

This action could in fact have been described directly with the G_i. The interest of writing $G = \varprojlim G/N$ before describing the action is that it automatically proves that the action on G is independent of the G_i chosen. Indeed, if

$$G \simeq \varprojlim G_i \simeq \varprojlim G'_i$$

where the isomorphisms are continuous, then (G_i) and (G'_i) are both subsystems of $(G/N)_N$ and the action on both subsystems is simply the restriction of the one on $(G/N)_N$. Thus they define the same action on G.

It is useful to have the following result in mind:

Proposition 1.4 $\hat{\mathbb{Z}} \simeq \prod_{p\ prime} \mathbb{Z}_p$

Proof. This is a consequence of the Chinese remainders theorem

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{p\ prime} \mathbb{Z}/p^{v_p(n)}\mathbb{Z}$$

by passing to the inverse limit on n on both sides. ■

In a later section, we will consider the the tensor product $G \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell$ for G an abelian profinite group and ℓ a prime. Since G and $\mathbb{Z}_\ell$ are both abelian profinite groups, this tensor product is well-defined. Note that the action of $\hat{\mathbb{Z}}$ on $\mathbb{Z}_\ell$ can be easily described as the multiplication by the ℓ-adic component of an element of $\hat{\mathbb{Z}}$ by the above isomorphism. This tensor product can be seen as the ℓ-adic part of the profinite group G.

Please also note that the above action of $\hat{\mathbb{Z}}$ on $\mathcal{O}_L$ that we have described in the previous section in fact corresponds to the natural action defined in this section when $\mathcal{O}_L$ is seen as the abelian profinite group $\varprojlim \mathcal{O}_L/m_L^n$.

Finally, note that a continuous map between abelian profinite groups is $\hat{\mathbb{Z}}$-linear. All the maps between profinite groups that will appear are continuous.

In the next section, we will use the following result about closed subgroups of profinite groups:

Proposition 1.5 Let $G = \varprojlim G_i$ be a profinite group, $p_i : G \to G_i$ the projection, and H a subgroup. Then H is closed if and only if

$$H = \varprojlim p_i(H)$$

Proof. If $H = \varprojlim p_i(H)$, then by Tychonov's theorem H is compact in G Hausdorff. In particular it is closed.

Conversely, suppose that H is closed. The projections give an inclusion

$$H \subseteq \varprojlim p_i(H)$$

We need to prove that it is surjective: suppose that we have a family (y_i) of elements, with $y_i \in G_i$ and for each i, some element $x_i \in H$ such that $y_i = p_i(x_i)$. G is compact so there is a subsequence of the (x_i) that converges, and since H is closed the limit x of this subsequence will be in H. Then x is sent by the projections to (y_i). ■

1.4 Infinite Galois theory

Theorem 1.4 — Infinite Galois Correspondence. Let L/K be a Galois extension of fields. Then we have inverse bijections between the closed subgroups of $Gal(L/K)$ and the subextensions of L/K given by: $H \mapsto Fix_H(L) = \{x \in L \mid \forall \sigma \in H,\ \sigma(x) = x\}$ and $M \to Gal(L/M)$. Moreover, the open subgroups correspond exactly to the finite subextensions and the normal closed subgroups correspond exactly to the Galois subextensions. If H is a normal closed subroup of $Gal(L/K)$, then $Gal(Fix_H(L)/K) = Gal(L/K)/H$.

Proof. Let M/K be a finite subextension of L/K. Denote by $\tilde{M}$ its Galois closure. Then $Gal(L/M)$ is the inverse image by the projection $Gal(L/K) \to Gal(\tilde{M}/K)$ of the subgroup of elements fixing M. Thus $Gal(L/M)$ is both open and closed. If N/K is any subextension of L/K, then $Gal(L/N)$ is the intersection of $Gal(L/M)$ over the finite subextensions M/K of N/K. Therefore it is closed as an intersection of closed sets. The maps in the statement are well-defined.

We need to check that the two maps defined in the statement are inverse to each other. The equality $Fix_{Gal(L/M)}(L) = M$ for a subextension M/K is proven as for the finite Galois correspondence: if $\alpha \in L \backslash M$, then we can define a field morphism $M[\alpha] \to L$ not fixing α by sending it to one of its conjugates, and then extend this morphism to L using Zorn's lemma.

Next, we consider the equality $Gal(L/Fix_H(L)) = H$ for H a closed subgroup of $Gal(L/K)$. We assume that the result is known when M/K is a finite Galois extension (Artin's lemma). By Proposition 1.5, we can write

$$Gal(L/Fix_H(L)) = \lim_{\leftarrow} Gal(M/Fix_{H_M}(M))$$

$$H = \lim_{\leftarrow} H_M$$

where M runs through the finite Galois subextensions of L/K, and H_M is the image of H by the projection $Gal(L/K) \to Gal(M/K)$. Then the result follows from Artin's lemma.

We then consider the "moreover" sentence in the statement. We saw in the first paragraph that for M/K a finite extension, $Gal(L/M)$ is open. Conversely, suppose H is open and let us prove that $Fix_H(L)$ is a finite extension of K. By Proposition 1.2, H has finite index. Suppose that $Fix_H(L)$ is an infinite extension of K. Then for any $n \in \mathbb{N}^*$, there is a finite Galois subextension N of $Fix_H(L)$ of degree at least n. For each element of $Gal(N/K)$, we can extend it to L. This will give a family of elements of $Gal(L/K)$ that are distinct in the quotient set $Gal(L/K)/H$. Thus the index of H is greater or equal to n, and that for any $n \in \mathbb{N}^*$. We obtain a contradiction.

Suppose that H is a normal subgroup of $Gal(L/K)$ and let us check that $Fix_H(L)/K$ is a Galois extension. We need to prove that for $\sigma \in Gal(L/K)$, $\sigma(Fix_H(L)) = Fix_H(L)$. If $x \in Fix_H(L)$, then for any $\tau \in H$, there is τ' in H such that $\tau\sigma(x) = \sigma\tau'(x) = \sigma(x)$. Thus $\sigma(x) \in Fix_H(L)$. It is also true for σ^{-1} so we get the desired equality. Now suppose that M/K is a Galois subextension of L/K. Then for any $\sigma \in Gal(L/K)$, $\tau \in Gal(L/M)$, $x \in M$, we have $\sigma(x) \in M$ so $\sigma^{-1}\tau\sigma(x) = \sigma^{-1}\sigma(x) = x$. This proves that $\sigma^{-1}Gal(L/M)\sigma \subseteq Gal(L/M)$ and so that $Gal(L/M)$ is a normal subgroup of $Gal(L/K)$. The last statement of the theorem is a consequence of the equality $Gal(L/Fix_H(L)) = H$. ■

2. Anabelian geometry for local fields

The natural starting point for anabalian geometry is Neukirch's theorem (1969), which states that if two number fields have isomorphic absolute Galois groups, then they are isomorphic as fields. I say that this is the natural starting point because number fields are more concrete than local fields, that Galois theory is older and more well-known than scheme theory, and because this theorem is often called the first result in anabelian geometry. However, the proof of Neukirch's theorem, whose skeleton is exposed in Appendix D.1, needs some basic results from anabelian geometry of local fields (points 1 and 2 in Theorem 2.2 below). In fact, one could argue that the starting point of anabelian geometry is class field theory, developed in the previous decades. The distinction between class field theory and anabelian geometry for fields is thin: essentially, it is a difference in the point of view - in class field theory, we start from a field and we want to understand the structure of its absolute Galois group in terms of the structure of the field; in anabelian geometry for fields, we start from the absolute Galois group, and we want to reconstruct information on the field in a manner that is preserved by group isomorphisms. But this difference of point of view doesn't prevent the methods and results used to be similar, in particular group cohomology (though this is not developed here). Over local fields, anabelian geometry is deduced from local class field theory, as we will explain below. For global fields however, the proof of Neukirch's theorem doesn't use the main results of global class field theory, with the exception of a local-global principle for the second cohomology groups used in his characterization of decomposition subgroups. The other tools of the global theory of anabelian geometry are Chebatorev's density theorem and the local theory - in the same manner that global class field theory is deduced from local class field theory.

Before continuing on the subject of anabelian geometry for local fields, we would like to explain in greater generality what is anabelian geometry and where does it comes from. The term "anabelian geometry" comes from Alexandre Grothendieck's "Esquisse d'un programme" ("Sketch of a program", 1984). Grothendieck insists on the enormous quantity of information contained in the non-commutative (or anabelian) part of a group, which is set aside by traditional algebra. He writes:

> "anabelian algebraic geometry", whose starting point is a study (for the moment limited to characteristic zero) of the actions of "absolute" Galois groups (mainly $Gal(\overline{K}/K)$ for K a finitely-generated extension of the prime field) on (profinite) geometric fundamental groups of algebraic varieties (defined over K), and in particular (going against a deep-rooted tradition) fundamental groupes that are very far from abelian groups (and that I name for this reason "anabelian")
>
> (...)
>
> It is also during this work (as well as in distinct notes) that appears the main theme of anabelian algebraic geometry, which is to reconstruct some varieties X called "anabelians" on an absolute field K from their mixed fundamental group, extension of $Gal(\overline{K}/K)$ by $\pi_1(X_{\overline{K}})$;
>
> (...)
>
> the isomorphism class of an anabelian algebraic curve on a number field K (finite extension of $\mathbb{Q}$) is known when its mixed fundamental group is given (or, which amonts

to the same, the outer action of $Gal(\overline{K}/K)$ on its profinite geometric fundamental group)

Note that the last quote is a conjecture that Grothendieck is making, often called "Grothendieck's conjecture on anabelian geometry", and proven by the Japanese school of algebraic geometry in 1996. The original view of anabelian geometry by Grothendieck has been twisted by modern mathematics, and anabelian geometry is now usually stated as:

> What information on a scheme X can be retrieved from its étale fundamental group $\pi_1(X)$?

In particular, we see that the "anabelian" property is not considered so critical as Grothendieck did, but the name stayed nevertheless. In the case of a field K, we have $\pi_1(K) = Gal(\overline{K}/K)$ where, as in all of the document, $\overline{K}$ is a separable closure of K (which the reader should think of as the maximal Galois extension of K). For a field, the anabelian geometry can therefore be summarized as:

> What information on a field K can be retrieved from its absolute Galois group $Gal(\overline{K}/K)$?

We now start to answer this question in the case of a local field. As a consequence of Theorem 1.2, there is exactly one maximal unramified extension of a local field K

$$K_{unram} = \bigcup_{n\in\mathbb{N}^*} K_n$$

and K_{unram}/K is a Galois extension of Galois group isomorphic to $\hat{\mathbb{Z}}$. The Frobenius element is defined to be the element of the Galois group corresponding to $1 \in \hat{\mathbb{Z}}$.

Theorem 2.1 — Local Class Field Theory. Let K be a local field. We set π a uniformizer and $f = \pi X + X^q$ where q is the cardinal of the residual field. Then:

- There exists one and only one $F_\pi \in \mathcal{O}_K[\![X,Y]\!]$ satisfying the following properties : (1) $F_\pi(X,0) = X$ and $F_\pi(0,Y) = Y$. In particular, F_π has no constant term and thus define a law $\mathfrak{m}_K^2 \to \mathfrak{m}_K$. (2) This law is associative and commutative. (3) f is an endomorphism for the law F_π, that is $f(F_\pi(X,Y)) = F_\pi(f(X), f(Y))$. F_π is called the Lubin-Tate formal group law associated to π.
- For each $a \in \mathcal{O}_K$, there exists one and only one $[a]_\pi \in \mathcal{O}_K[X]$ satisfying the following properties : (1) $[a]_\pi$ is equal to aX modulo the polynomials of degree at least two. In particular, $[a]_\pi$ defines a function $\mathfrak{m}_K \to \mathfrak{m}_K$. (2) $[a]_\pi$ is an endomorphism for the law F_π.
- (Existence theorem) F_π and $[a]_\pi$ for $a \in \mathcal{O}_K$ define maps on $\mathfrak{m}_{\overline{K}}$ where $\overline{K}$ is a separable closure of K. We set
$$K_\pi = \bigcup_{n\in\mathbb{N}} K(ker([\pi^n]_\pi))$$
where $[\pi^n]_\pi$ is seen as a map on $\mathfrak{m}_{\overline{K}}$. Finally, we also set
$$K_{ab} = K_\pi K_{unram}$$
The extension K_{ab} is independant of the choice of the uniformizer π and is the only maximal abelian extension of K. The map $L \mapsto N_{L/K}(L^\times)$ is a bijection from the finite abelian extensions of K (i.e. the finite subextensions of K_{ab}/K) onto the open subgroups of $K^\times$ of finite index.
- There are non canonical isomorphisms
$$Gal(\overline{K}/K)^{ab} \simeq Gal(K_{ab}/K) \simeq Gal(K_\pi/K) \times Gal(K_{unram}/K) \simeq \mathcal{O}_K^\times \times \hat{\mathbb{Z}}$$

- (Local reciprocity) For each finite Galois extension L of K, there exists a natural isomorphism
$$\theta_{L/K} : Gal(L/K)^{ab} \to K^\times/N_{L/K}(L^\times)$$
The maps $\omega_{L/K} : K^\times \to Gal(L/K)^{ab}$ obtained by precomposing $\theta_{L/K}^{-1}$ by the projections commute with the restrictions. Thus we can define a map $\omega_{K_{ab}/K} : K^\times \to Gal(K_{ab}/K)$. This map is characterized by the two following properties : (1) $\omega_{K_{ab}/K}(\pi)$ acts trivially on K_π and acts like the Frobenius on K_{unram}. (2) For $a \in \mathscr{O}_K^\times$, $\omega_{K_{ab}/K}(a)$ acts like $[a]_\pi$ on K_π and acts trivially on K_{unram}. As a consequence, the map $\omega_{K_{ab}/K}$ induces a natural isomorphism between $\mathscr{O}_K^\times$ and the image of the inertia subgroup $I \subseteq Gal(\overline{K}/K)$ in the abelianization.

Proof. Admitted. ■

Theorem 2.2 Let p, p' be two primes numbers, K a finite extension of $\mathbb{Q}_p$, K' a finite extension of $\mathbb{Q}_{p'}$. We denote by k, k' their respective residue fields, and by O_K, $O_{K'}$ their respective rings of integers. We suppose that there is an isomorphism $f : Gal(\overline{K}/K) \to Gal(\overline{K'}/K')$. Then:
- $p = p'$ and K and K' have the same dimension over $\mathbb{Q}_p$.
- f induces an isomorphism $k^\times \to k'^\times$. Thus k and k' have the same dimension over $\mathbb{F}_p$ and K and K' have the same ramification index.
- f induces an isomorphism between the inertia subgroups I and I'. Moreover, the isomorphism $Gal(\overline{K}/K)/I \to Gal(\overline{K'}/K')/I'$ sends the Frobenius element to the Frobenius element.
- f induces an isomorphism $K^\times \to K'^\times$ preserving the rings of integers.

Proof. We denote $G = Gal(\overline{K}/K)$, $G' = Gal(\overline{K'}/K')$.
- Let ℓ be a prime number. Since $\mathbb{Z}_\ell$ is a principal ideal domain, we can compute the rank of the $\mathbb{Z}_\ell$-module $G^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell$. By Theorem 2.1, point 4, we have a non canonical isomorphism $G^{ab} \simeq \mathscr{O}_K^\times \times \hat{\mathbb{Z}}$ and by Theorem 1.3, $\mathscr{O}_K^\times \simeq \mathbb{Z}_p^{dim_{\mathbb{Q}_p}(K)} \oplus \mathbb{Z}/p^r\mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z}$ where q is the cardinal of the residue field and $r \in \mathbb{N}$. Thus
$$rk_{\mathbb{Z}_\ell}(G^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_l) = 1 + rk_{\mathbb{Z}_l}(\mathbb{Z}_p^{dim_{\mathbb{Q}_p}(K)} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell)$$
Now note the following: if $\ell \neq p$, then $\mathbb{Z}_p \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell = 0$ because for any $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_\ell$,
$$a \otimes b = 1 \otimes ab$$
and the multiplication ab in $\hat{\mathbb{Z}} = \prod_{q\ prime} \mathbb{Z}_q$ is zero. Thus we get that this rank is equal to 1 if $\ell \neq p$, and $1 + dim_{\mathbb{Q}_p}(K)$ if $\ell = p$. p is therefore characterized as the only prime for which this rank is at least 2, and the dimension over $\mathbb{Q}_p$ is computed by substracting 1 to this rank.
- According to Theorem 2.1, point 5 and point 3, there is a natural isomorphism
$$G^{ab} \simeq \hat{K^\times} = \lim_{\leftarrow} K^\times/N_{L/K}(L^\times) = \lim_{\leftarrow} K^\times/S$$
where L runs through the abelian extensions of K and S runs through the open subgroups of $K^\times$ of finite index. Using this map and the Teichmüller character $\omega : k^\times \to \mathscr{O}_K^\times$, we get a morphism
$$k^\times \to (G^{ab})_{tor \neq p}$$
where have defined $(G^{ab})_{tor \neq p} = \{x \in G^{ab} \mid x^n = 1\ for\ some\ n \in \mathbb{N}^*\ prime\ to\ p\}$. We will prove that this morphism is in fact an isomorphism. First, we need to check that the map $K^\times \to \hat{K^\times}$ is injective. This is because if we fix a uniformizer π, then $K^\times \simeq \mathscr{O}_K^\times \times \mathbb{Z}$

and $\hat{K^\times} \simeq \mathcal{O}_K^\times \times \hat{\mathbb{Z}}$ (Theorem 2.1, points 4 and 5), and the map $K^\times \to \hat{K^\times}$ corresponds to the identity on $\mathcal{O}_K^\times$ and the inclusion $\mathbb{Z} \to \hat{\mathbb{Z}}$. Thus we have an injective morphism $k^\times \to (G^{ab})_{tor \neq p}$ and to conclude we only need to prove that both sides have same cardinality. This is a consequence of Theorem 1.3 and Theorem 2.1, point 4, that is the non canonical isomorphisms

$$\mathcal{O}_K^\times \simeq \mathbb{Z}_p^{dim_{\mathbb{Q}_p}(K)} \oplus \mathbb{Z}/p^r\mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \text{ and } G^{ab} \simeq \mathcal{O}_K^\times \times \hat{Z}$$

where q is the cardinal of the residue field and $r \in \mathbb{N}$.

- We first prove that we have the equality $I = Gal(\overline{K}/K_{unram})$. If $\sigma \in I$, then for any $n \in \mathbb{N}^*$, by definition, it acts trivially on the residue field k_n of the unramified extension K_n of K of degree n. Now $Gal(K_n/K) \simeq Gal(k_n/k)$ so σ is the identity of K_n. Thus σ is the identity of K_{unram}, that is $\sigma \in Gal(\overline{K}/K_{unram})$.
Now suppose $\sigma \in Gal(\overline{K}/K_{unram})$. Let L be a finite Galois extension of K and I_L the inertia subgroup of L/K. We set $M = Fix_{I_L}(L)$. Then by Artin's lemma $Gal(L/M) \simeq I_L$ and since the map $Gal(L/M) \to Gal(l/m)$ is surjective and, by definition of I_L, of image $\{1\}$, the extension L/M has ramification index equal to its degree. Therefore

$$e(M/K) = \frac{e(L/K)}{e(L/M)} = \frac{e(L/K)}{deg_M(L)} = \frac{e(L/K)}{Card\ Gal(L/M)} = \frac{e(L/K)}{Card\ I_L} = 1$$

M/K is an unramified extension so σ is the identity of M. Thus $\sigma \in Gal(L/M) \simeq I_L$, and since this is true for any L we conclude that $\sigma \in I$.
From the above discussion, we have the equalities

$$I = Gal(\overline{K}/K_{unram}) = \bigcap_{n\in\mathbb{N}^*} Gal(\overline{K}/K_n)$$

Thus to prove that $f(I) = I'$, it is sufficient to see that f sends $Gal(\overline{K}/K_n)$ to $Gal(\overline{K'}/K'_n)$. It is a consequence of the previous points (the ramification index and the dimension over $\mathbb{Q}_p$ are preserved) and the equality

$$e(K_n/K) = \frac{e(K_n/\mathbb{Q}_p)}{e(K/\mathbb{Q}_p)}$$

The proof that f preserves the Frobenius needs many more preliminaries about the structure of an extension of local fields. It is defered to Appendix B.
- We proved in the previous point that f induces an isomorphism between the inertia subgroups. By Theorem 2.1, point 5, the image of the inertia subgroup in the abelianization of the absolute Galois group is naturally isomorphic to the ring of integers. Thus we get an isomorphism between the rings of integers.
Finally, f also naturally induces an isomorphism between $\hat{K^\times}$ and $\hat{K'^\times}$. To see that $K^\times$ is sent to $K'^\times$ by this isomorphism, it is sufficient to see that this morphism preserves the rings of integers (which we have just justified) and that the quotient map $\hat{\mathbb{Z}} \to \hat{\mathbb{Z}}$ sends $\mathbb{Z}$ to $\mathbb{Z}$. This last point is a consequence of the fact that f sends the Frobenius to the Frobenius (i.e. sends 1 to 1).

■

The previous theorem doesn't state that K and K' are isomorphic as fields, and for a good reason: contrary to number fields, this result is not true for local fields. Anabelian geometers say that "local fields are not anabelian" while "number fields are anabelian". It is not so easy to produce a counterexample for local fields though. A reference for this is given in S. Mochizuki, *A Version of the Grothendieck Conjecture for p-adic Local Fields*, https://www.kurims.kyoto-u.ac.jp/

~motizuki/A%20Version%20of%20the%20Grothendieck%20Conjecture%20for%20p-adic%20Local%20Fields.pdf. In the same article, Mochizuki also gives a necessary and sufficient for an isomorphism between the absolute Galois groups to come from a field isomorphism: the preservation of the filtration in the upper numbering (which is not defined here).

3. Anabelian geometry for curves

3.1 Schemes and the étale fundamental group

The goal of this section is to introduce the étale fundamental group, which is necessary to generalize the theory of anabelian geometry from fields as in the previous section to geometric objects on any ring. As of today, important results have only been proved for curves over a field and so we will use this case as the basis of our intuition. The étale fundamental group is a part of scheme theory introduced by Grothendieck in the 1960s, and so we will have to talk about schemes and their properties in this section. However, since our goal is only to study curves, we will try to avoid technicalities: for example, we will describe roughly what is a scheme but without giving the precise definition. We will also admit all the results from algebraic geometry that we are using.

Classic algebraic geometry is the study of the set of common zeroes in an affine or projective space of some family of polynomials over an algebraically closed field K. One of the first theorem of this subject is Hilbert's Nullstellensatz which asserts that there is an equivalence of categories between algebraic sets and polynomials morphisms on one side, and reduced finitely-generated K-algebras and morphisms of K-algebras on the other. The points of the algebraic set are in 1-1 correspondence with the maximal ideals of the corresponding K-algebra, and the other prime ideals can be interpreted as irreducible components of the algebraic set. This correspondence is useful in both directions: it allows to solve geometric problems by translating it in the algebraic langage, and it allows to visualize some algebraic properties (Krull dimension, integral domain, flatness, local ring, etc).

The startig point for modern algebraic geometry is the following question: why do we confine ourselves to reduced finitely-generated algebras over an algebraically closed field? One answer to that question could be that maximal ideals are not functiorial: the inverse image of a maximal ideal by a ring morphism may not be a maximal ideal. For finitely-generated algebras over an algebraically closed field, this is true (it is consequence of Zariski's lemma). In geometrical terms, this means that a point is sent to a point, and this is what allows us to identify morphisms between varieties with algebra morphisms. In we want to extend the theory, the first step is to replace maximal ideals with prime ideals. Grothendieck's scheme theory basically says that when working with prime ideals, the ideas of algebraic geometry can be extended to any ring - even if the vizualization becomes difficult. In fact, Grothendieck is even a bit more general. He first defines an affine scheme which is the spectrum of a ring R (the set of its prime ideals) endowed with the Zariski topology and a sheaf of functions in a sense. For integral rings, the sheaf of functions corresponds simply to the fraction field K: for an element $\frac{a}{b} \in K$ with $a, b \in R$, and for any prime (= point) $\mathfrak{p}$ in R not containing b, we can evaluate $\frac{a}{b}$ at $\mathfrak{p}$ by taking its image in the fraction field of the quotient $R/\mathfrak{p}$. If for any representation of $\frac{a}{b}$ as a fraction of elements of R the denominator is in $\mathfrak{p}$, then we can't evaluate $\frac{a}{b}$ at $\mathfrak{p}$ and we say that $\frac{a}{b}$ has a pole at the prime (= point) $\mathfrak{p}$. For non-integral rings, functions are defined to be locally quotients of elements of the ring, but we will not give more details. Once an affine scheme is defined, a general scheme is defined to be a topological space with a sheaf of functions that is locally isomorphic to an affine scheme. The advantages of Grothendieck's scheme theory are (at least) fourfold:

- considering scheme instead of simply affine schemes allows us to speak with a common language of both affine and projective geometry ;

- the flexibility of the definition makes it possible to glue schemes, to do product of schemes, etc ;
- by dropping the assumption that the base ring is an algebraically closed field, we can consider problems of an arithmetic nature, as we are interested in ourselves ;
- this common arithmetico-geometric langage gives a new perspective to study arithmetic problems, by looking at the action of (arithmetic) Galois groups on (geometric) cohomology groups.

As stated at the beginning, we will not dive too much into the details of those points. It is however important to have in mind the two types of schemes we will work with:

- a field K can be seen as a scheme with only one point and field of functions K ;
- a curve can be seen as a scheme if we add to it the only prime ideals that is not maximal: the zero ideal, also called the generic point. It is the affine scheme of its ring of coordinates.

Poincaré defined the fundamental group for topological spaces at the very beginning of the twentieth century. This group can be seen in two ways: either has the group of loops in the space modulo deformation, or as the automorphism group of the fiber of the universal covering. Grothendieck generalized the second construction to a scheme. He defined the notion of an étale covering of X which is a smooth unramified morphism $f : Y \to X$ for some scheme Y. It is not so simple as one could think, because the notion of smoothness can not be generalized easily - one must consider flatness, which is a difficult property to vizualize. In this theory, there is no scheme playing the role universal étale covering, but we can still define the universal étale covering of X as the inverse system of the finite étale coverings of X. Then the étale fundamental group is defined in the same way as for the topological case: it is the automorphism group of the fiber above a point.

We have stated that we do not want to deep too much into technical details, but we don't want oversimplified explanations neither. The previous paragraph was a bit oversimplified. We will give some more precisions and introduce useful notions at the same time. Let us first describe what a base change is. In classical algebraic geometry, it corresponds to searching for solutions of the polynomial equation in a field extension - and this is what one needs in mind for the cases we are interested in. For an affine scheme $Spec(B)$ for some ring B over another ring A, and C another ring above A, the base change to C is $Spec(B \otimes_A C)$. The general case then comes by gluing together such affine schemes of tensor products. What we are particularly interested in is that from a scheme X over a field K, we can consider the base change to $\overline{K}$ which we will denote $X_{\overline{K}}$. For a scheme X over a field K, the étale fundamental group is defined for a point $\overline{x} \in X_{\overline{K}}$ and denoted $\pi_1^{\text{ét}}(X, \overline{x})$, and for $f : Y \to X$ a finite étale covering, what we called the fiber above a point is in fact $Hom_X(\overline{x}, Y)$ - that is the morphisms ϕ from the scheme $\overline{x}$ to the scheme Y such that $f \circ \phi(\overline{x})$ is the image of $\overline{x}$ in X. However, the étale fundamental group is independent of the choice of the point $\overline{x}$ up to non-canonical isomorphism, so we will not pay much attention to this.

Even if we didn't define the étale fundamental group correctly, what is important to know is that an analogous result to the infinite Galois correspondence holds: closed subgroups of the étale fundamental group correspond to étale coverings, open subgroups to finite étale coverings, and normal subgroups to Galois coverings. We will mainly use this property.

The following result is fundamental to understand the next section:

Theorem 3.1 — Grothendieck SGA1. Let K be a field, X a quasi-compact quand quasi-separated scheme over K such that $X_{\overline{K}}$ is connected. Then there is a short exact sequence of profinite groups

$$1 \to \pi_1^{\text{ét}}(X_{\overline{K}}) \to \pi_1^{\text{ét}}(X) \to Gal(\overline{K}/K) \to 1$$

Proof. See Grothendieck, SGA1, Exposé IX, Théorème 6.1. ■

The first group that appears in theorem - $\pi_1^{\text{ét}}(X_{\overline{K}})$ - is called the geometric fundamental group.

The idea behind this name is that no matter over which algebraically closed field we look at a variety, the étale fundamental group should always have the same properties. Thus this part can be computed by considering the variety over $\mathbb{C}$, where the toplogical fundamental group has already been defined and studied. Precise comparison theorems between the geometric and topological fundamental groups are given after some more comments on the theorem.

The previous theorem allows us to see the étale fundamental group $\pi_1^{\text{ét}}(X)$ as the data of the absolute Galois group of K, the geometric fundamental group of X and a group morphism $Gal(\overline{K}/K) \to Out(\pi_1^{\text{ét}}(X_{\overline{K}}))$. Here $Out(G)$ denotes the outer automorphisms of the group G, that is the quotient of the automorphisms group by the subgroup of the inner automorphisms. The morphism is defined in the following way: take an element $x \in Gal(\overline{K}/K)$, a lift $y \in \pi_1^{\text{ét}}(X)$ of x. As a corollary of the theorem, the geometric fundamantal group is a normal subgroup of its étale fundamental group so y defines by conjugation an automorphism of $\pi_1^{\text{ét}}(X_{\overline{K}})$. Now if y' is another lift of x, then y and y' differ by multiplication by an element of $\pi_1^{\text{ét}}(X_{\overline{K}})$ so the automorphisms defined differ by composition by an inner automorphism. Therefore the image in the outer automorphisms group depends only on x, and this give the desired morphism. Once this result is known, the missing part to use this theory is to determine the geometric fundamental group. Grothendieck also considered this question, and proved important theorems, notably:

Theorem 3.2 — Grothendieck SGA1. Let K be a field of characteristic 0, X a proper scheme over K. Then the geometric fundamental group of K is naturally isomorphic to the profinite completion of the topological fundamental group of X seen as a complex manifold.

Proof. See Grothendieck, SGA1, Exposé XII, Corollaire 5.2. ■

This theorem is not sufficient in our case because we also want to consider curves with punctured points. However, Raynaud proved that the theorem still holds in this case:

Theorem 3.3 — Raynaud SGA1. The previous theorem also holds if X is an open subset of a proper nonsingular curve over a field of characteristic 0 obtained by puncturing a finite number of points.

Proof. See Grothendieck, SGA1, Exposé XIII, Corollaire 2.12. ■

Then to compute the geometric fundamental group, we only have to know the topological fundamental group. In the case we are interested in, this can be done using Van Kampen's theorem.

Theorem 3.4 The topological fundamental group of the curve over $\mathbb{C}$ of genus g with r punctured points is generated by $2g+r$ elements satisfying one relation. More precisely, it is

$$< \alpha_1, \beta_1, ..., \alpha_g, \beta_g, \gamma_1, ..., \gamma_r \mid [\alpha_1, \beta_1]...[\alpha_g, \beta_g]\gamma_1...\gamma_r = 1 >$$

3.2 Anabelian geometry for hyperbolic curves over local fields

Theorem 3.5 Let p, p' be two primes numbers, K a finite extension of $\mathbb{Q}_p$, K' a finite extension of $\mathbb{Q}_{p'}$. Let X and X' be hyperbolic curves of genus g and g' with r and r' punctured points over K and K' respectively. Let Π and Π' denote the arithmetical fundamental group of X and X' respectively, and Δ and Δ' their geometric fundamental groups respectively. Let $f : \Pi \to \Pi'$ be an isomorphism of fundamental groups. Then:

- $f(\Delta) = \Delta'$. As a consequence, K and K' have isomorphic absolute Galois groups and Theorem 2.2 can be applied.
- X is affine if and only if X' is affine.

- $g = g'$ and $r = r'$.

Proof.

- Let A be an open subgroup of Π, $B = A \cap \Delta$, $C = A/B$. First note that $\Delta \subseteq A$ if and only if $[\Pi : A] = [Gal(\overline{K}/K) : C]$. Indeed, since A is open, the indexes of A, B, C in Π, Δ, $Gal(\overline{K}/K)$ respectively are finite and we have the equality

$$[\Pi : A] = [\Delta : B][Gal(\overline{K}/K) : C]$$

Thus we have

$$\begin{aligned} \Delta \subseteq A &\iff B = \Delta \\ &\iff [\Delta : B] = 1 \\ &\iff [\Pi : A] = [Gal(\overline{K}/K) : C] \end{aligned}$$

Therefore we have an inclusion

$$\Delta \subseteq \bigcap_A A$$

where the intersection is on the open subgroups A satisfying the above equality of indexes. This inclusion is in fact an equality: indeed, let $x \in \Pi$ which is not in the image of Δ. Then the image σ of x in $Gal(\overline{K}/K)$ is non-trivial. Consider $\alpha \in \overline{K}$ such that $\sigma(\alpha) \neq \alpha$ and A the inverse image of $Gal(\overline{K}/K[\alpha])$ in Π. Then A is an open subgroup, satifies the equality of indexes (because $\Delta \subseteq A$) and doesn't contain x. This proves the desired equality.
Now we must prove that the condition $[\Pi : A] = [Gal(\overline{K}/K) : C]$ can be expressed only in term of A (C has been defined using Δ, but here we want to characterize Δ). We will prove that we have the following equality:

$$[Gal(\overline{K}/K) : C][K : \mathbb{Q}_p] = rk_{\mathbb{Z}_p}(A^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p) - rk_{\mathbb{Z}_\ell}(A^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell)$$

for $\ell \neq p$ a prime. To prove this, let L be the finite extension of K defined by C. We first write the following equalities:

$$[L : \mathbb{Q}_p] = [L : K][K : \mathbb{Q}_p] = [Gal(\overline{K}/K) : C][K : \mathbb{Q}_p]$$

By the computations in the proof of point 1 of Theorem 2.2, which follow from local class field thoery, we have:

$$[L : \mathbb{Q}_p] = rk_{\mathbb{Z}_p}(C^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p) - rk_{\mathbb{Z}_\ell}(C^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell)$$

Moreover, we have the following exact sequence:

$$1 \to \overline{B} \to A^{ab} \to C^{ab} \to 1$$

where $\overline{B}$ is the image of B in the abelianization of A. $\mathbb{Z}_p$ and $\mathbb{Z}_\ell$ are flat $\hat{\mathbb{Z}}$-modules, thus:

$$rk_{\mathbb{Z}_p}(C^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p) = rk_{\mathbb{Z}_p}(A^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p) - rk_{\mathbb{Z}_p}(\overline{B}^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p)$$

$$rk_{\mathbb{Z}_\ell}(C^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell) = rk_{\mathbb{Z}_\ell}(A^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell) - rk_{\mathbb{Z}_\ell}(\overline{B}^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell)$$

Claim: $\overline{B}/\overline{B}_{torsion}$ is a free $\hat{\mathbb{Z}}$-module of finite rank.
We admit this claim for now. Then we have:

$$rk_{\mathbb{Z}_p}(\overline{B}^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p) = rk_{\mathbb{Z}_\ell}(\overline{B}^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell)$$

and by replacing the two previous equalities of ranks in the formula for $[L : \mathbb{Q}_p]$, we obtain the desired equality.
With this, we can prove three things:

1. $p = p'$
2. $[K:\mathbb{Q}_p] = [K':\mathbb{Q}_{p'}]$
3. For A an open subgroup of Π satisfying

$$[\Pi : A][K:\mathbb{Q}_p] = rk_{\mathbb{Z}_p}(A^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p) - rk_{\mathbb{Z}_\ell}(A^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell)$$

$A' = f(A)$ is an open subgroup of Π' satisfying

$$[\Pi' : A'][K':\mathbb{Q}_{p'}] = rk_{\mathbb{Z}_{p'}}(A'^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_{p'}) - rk_{\mathbb{Z}_\ell}(A^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell)$$

In fact, the third point is a direct consequence of points 1 and 2, and by the two previous paragraphs this third point implies that $f(\Delta) = \Delta'$.
Using as in the previous paragraph the computations in the proof of Theorem 2.2, point 1, and the fact that the image of Δ in the abelianization of Π, when quotiented by its torsion part, is a free $\hat{\mathbb{Z}}$-module, we see that p is characterized as the only prime for which

$$rk_{\mathbb{Z}_p}(\Pi^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p) - rk_{\mathbb{Z}_\ell}(\Pi^{ab} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_\ell)$$

for any other prime ℓ. This condition is preserved by f so it proves the first point. Moreover, it value gives $[K:\mathbb{Q}_p]$ so we have also proved the second point.
The proof of the clam is the topic of Appendix C.1. We only sketch the proof.

- We will prove that we can detect if X is affine by looking purely at its geometric fundamental group Δ, which can be recovered by the previous point. First note that X affine is equivalent to $r > 0$. Indeed, a complete curve is not affine but it becomes affine if we puncture at least one point. Next note that if $r > 0$, then Δ is simply the free profinite group generated by $2g + r - 1$ generators (we can express γ_r with the other generators). If $r = 0$, it "appears" that Δ is not a free profinite group and this is how we will detect that X is affine. To make this argument precise, we need to use group cohomology (see Appendix A). By the last theorem of Appendix A and the above remark, if X is affine then $H^2(\Delta, M) = 0$ for any abelian group M where the action of Δ on M is trivial. Now suppose X is not affine, then there is an exact sequence
$$1 \to H \to F \to \Delta \to 1$$
where F is the free profinite group with $2g$ generators $\alpha_1, \beta_1, ..., \alpha_g, \beta_g$ and H is the profinite subgroup generated by $[\alpha_1, \beta_1]...[\alpha_g, \beta_g]$. Thus in the long exact sequence of cohomology we get
$$H^1(F,M) \xrightarrow{u} H^1(H,M) \to H^2(\Delta,M) \to H^2(F,M)$$
By the last theorem of Appendix A, $H^1(H,M) = M$ and $H^2(F,M) = 0$. We want to prove that $H^2(\Delta,M) = H^1(H,M) = M$. It is sufficient to prove that u is the zero map. To that end, we use the explicit description of group cohomology. Take $f : F \to M$ a 1-cocycle, that is continuous and satisfying
$$\forall g_1, g_2 \in F,\ f(g_1 g_2) = g_1.f(g_2) + f(g_1)$$
But here, since the action is trivial, this condition exactly means that f is a group morphism. Since M is an abelian group, f vanishes on the communators. H is topologically generated by products of commutators (this is where we use that $r = 0$) so $u(f) = 0$. Therefore we did prove that for X not affine, $H^2(\Delta,M) \neq 0$ for $M \neq 0$.
- Here g and r can not be retrieved solely by looking at the geometric fundamental group. Indeed, if $r, r' > 0$ and $2g + r = 2g' + r'$, then Δ and Δ' are both free profinite groups generated by $2g + r - 1 = 2g' + r' - 1$ elements. However, we can, by the previous point, detect if $r = 0$ or $r > 0$. If $r > 0$, then for M a finite abelian group, $H^1(\Delta,M)$ is finite of cardinal

$(Card\ M)^{2g+r-1}$. Thus we can recover the value $2g+r-1$. If $r=0$, then considering the same exact long sequence of cohomology as before, we have

$$H^0(F,M) \to H^0(H,M) \to H^1(\Delta,M) \to H^1(F,M) \xrightarrow{u} H^1(H,M)$$

and we have justified that u is the zero map. We also have $H^0(F,M) = H^0(H,M) = M$ and the map between them in the exact sequence is an isomorphism, and $H^1(F,M) = M^{2g}$. Then the map $H^1(\Delta,M) \to H^1(F,M)$ is an isomorphic, and thus for M finite, by taking the cardinal we can recover $2g$. Therefore if $r=0$, g can be recovered geometrically.
The recovering of the number of punctured points and the genus in the affine case are conducted in Appendix C.2. This is without a doubt the most technical part of this report, and we use many results without proof.

■

A. Group cohomology

Group cohomology is an important tool for proving the results of local class field theory. This Appendix A was supposed to define group cohomology and the Tate cohomology groups and then prove the important results of the domain used in local class field thoery, mainly Tate-Nakayama theorem. It should have been followed by an Appendix B using these results to prove local class field theory. However, due to a lack of time, these two Appendix never came to be and the results of local class field theory are admitted. Group cohomology, though, is still used in chapter 3, to detect properties of a curve from its geometric fundamental group. That is why this Appendix A still exists, but is concerned only with defining group cohomology, stating its basic properties and proving the theorem about the cohomology of free groups that we need.

We fix G a profinite group. In the following, we will say G-module for $\mathbb{Z}[G]$-module. $\mathbb{Z}[G]$ can be thought as the group G endowed with a formal addition. We consider the category of G-modules where the maps between two G-modules are continous and linear. We want to construct a cohomology theory consisting of G-modules $H^i(G,M)$, for any $i \in \mathbb{N}$ and M a G-module, satisfying the following property: for any exact sequence of G-modules

$$0 \to M' \to M \to M'' \to 0$$

we have a functorial long exact sequence of G-modules in cohomology

$$\dots \to H^{i-1}(G,M'') \to H^i(G,M') \to H^i(G,M) \to H^i(G,M'') \to H^{i+1}(G,M') \to \dots$$

with $H^i(G,M') = H^i(G,M) = H^i(G,M'') = 0$ for $i < 0$ and $H^0(G,M') = Hom_G(\mathbb{Z},M')$, $H^0(G,M) = Hom_G(\mathbb{Z},M)$, $H^0(G,M'') = Hom_G(\mathbb{Z},M'')$.

There are two possible ways to construct such a cohomology theory. The first way can be achieved if we have the following result: for any G-module M, there exists an injection of M into a G-module I such that the functor $Hom_G(.,I)$ is exact (such a module is called injective). Take as an axiom that the cohomology of an injective module is zero for $i > 0$. For any module M, we have an exact sequence

$$0 \to M \to I \to N \to 0$$

for some modules I, N, with I injective. Then the long exact sequence, plus the above axiom, give us that $H^1(G,M) = Hom_G(\mathbb{Z},N)/Im(Hom_G(\mathbb{Z},I))$ and $H^{i+1}(G,M) = H^i(G,N)$ for $i > 0$. We can repeat the process by taking an injection of N into an injective modulo to compute $H^1(G,N) = H^2(G,M)$, and so on. In a more concise way, we are showing that the cohomology can be computed in the following way: take a long exact sequence

$$0 \to M \to I_0 \to I_1 \to I_2 \to \dots$$

with I_i injective for any $i \in \mathbb{N}$. Then the cohomology of G at M is the homology of the complex

$$0 \to Hom_G(\mathbb{Z},I_0) \to Hom_G(\mathbb{Z},I_1) \to Hom_G(\mathbb{Z},I_2) \to \dots$$

Now let us describe the other way of constructing such a cohomology theory. In the previous paragraph, we considered an injective resolution of M and then applied $Hom_G(\mathbb{Z},.)$. We can use the dual construction: we consider a projective resolution of $\mathbb{Z}$ by $Z[G]$-modules, and then apply the functor $Hom_G(.,M)$. The fact that those two constructions satisfy the long exact sequence property is a consequence of the snake lemma. From the definition of injective and projective modules, it is also possible to prove that in both cases the cohomology is independent of the resolution chosen (up to isomorphism).

The first construction is often taken as a definition of group cohomology, while the second has the advantage of being easier to compute. Indeed, it is possible to give a concrete example of projective resolution of $\mathbb{Z}$ and thus an explicit formula for the cohomology, as stated by the theorem below. From this explicit formula, it is possible to prove that injective modules have zero cohomology and therefore that the two definitions coincide.

Theorem A.1 Let G be a profinite group, M a G-module. The cohomology of G at M is the homology of the complex

$$0 \to K^0 \xrightarrow{d^0} K^1 \xrightarrow{d^1} K^2 \xrightarrow{d^2} \dots$$

where K^i is the G-modules of the continuous functions $G^i \to M$, and for $f \in K^i$, $g_1, \dots, g_{i+1} \in G$,

$$d^i(f)(g_1, \dots, g_{i+1}) = g_1.f(g_2, \dots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j f(g_1, \dots, g_j g_{j+1}, \dots, g_{i+1}) + (-1)^{i+1} f(g_1, \dots, g_i)$$

We use the following theorem for the proof of Theorem 3.5:

Theorem A.2 Let F be the free group with n generators and M a group considered as a G-module with trivial action. Then:

$$H^q(F,M) = \left| \begin{array}{ll} M & if\ q=0 \\ M^n & if\ q=1 \\ 0 & if\ q \geqslant 2 \end{array} \right.$$

Proof. Since the action of F on M is trivial, $H^0(F,M) = Fix_F(M) = M$. Using the explicit description of the cohomology groups, we also see that the group $H^1(F,M)$ corresponds to continuous linear morphims $F \to M$. Since F is topologically generated by n elements, the data of such a morphim is equivalent to the data of the images of the n elements. Therefore $H^1(F,M) = M^n$.

To prove that the cohomology is zero for $q \geqslant 2$, we consider the exact sequence

$$0 \to K \to \mathbb{Z}[F] \to \mathbb{Z} \to 0$$

where the map $\mathbb{Z}[F] \to \mathbb{Z}$ sends any element of F to 1, and K is the kernel of map. Denote by $g_1, \dots, g_n$ generators of F. We will prove that K is a free $\mathbb{Z}[F]$ module of rank $n-1$. In particular the above exact sequence is a projective resolution of $\mathbb{Z}$, and so we can compute the cohomology from this resolution. Since this resolution has only two non-zero modules, this gives the desired result.

First note that K is a free $\mathbb{Z}$-module with basis $g-1$ for $g \in F \backslash \{0\}$. We have either $g = hg_i$ or $g = hg_i^{-1}$ for some $h \in F$ which is shorter than g when written in terms of the $g_1, \dots, g_n$, and some index i. In the first case, write

$$g - 1 = h.(g_i - 1) + (h-1)$$

In the second case, write

$$g - 1 = -g(g_i - 1) + (h-1)$$

By iterating the process on h, we see that $g-1$ can be written as a sum of terms of the form $g'(g_i - 1)$ for $g' \in F$, $i \in [\![1;n]\!]$. The two relations above can be inverted to prove the converse: any element of the form $g'(g_i - 1)$ can be written as a sum of terms of the form $g-1$ for $g \in F$. Thus $g(g_i - 1)$ is another $\mathbb{Z}$-basis of K. It follows that $g_i - 1$ is a $\mathbb{Z}[F]$-basis of K, and this is the desired result. ∎

B. Totally tamely ramified extensions and the Frobenius

The goal of this Appendix is to prove that the Frobenius of $Gal(\overline{K}/K)/I$ is preserved by a continuous isomorphism between the absolute Galois groups of two p-adic local fields, as stated in Theorem 2.2, point 3. To that end, we characterize the Frobenius by its action on I/P where P is the wild inertia subgroup. We first define totally ramified extensions and tamely ramified extensions and prove some of their properties; then we define the wild inertia subgroup, link this notion to the previous ones to further understand the structure of the absolute Galois group of a local field, and describe the action of the Frobenius on the quotient I/P; finally, we prove that an isomorphism between absolute Galois groups preserve the wild inertia subgroup and this action.

Definition B.1 Let L/K be a finite extension of local fields. This extension is called totally ramified if its ramification index is equal to its degree.

Proposition B.1 Let L/K be a finite extension of local fields. Then there exists a subextension M/K such that M/K is unramified and L/M is totally ramified.

Proof. Consider $\tilde{L}$ the Galois closure of L and $I \subseteq Gal(\tilde{L}/K)$ the the inertia subgroup of the extension $\tilde{L}/K$. Define M to be the elements of $\tilde{L}$ fixed by I. We justified in the proof of Theorem 2.2, point 3, that M/K is unramified and that $\tilde{L}/M$ is totally ramified. To conclude, we must prove that $M \subseteq L$. By Theorem 1.3, point 1, we can write $M = K[a]$ for some $a \in \mathscr{O}_M$. $a \in \tilde{L}$ means that for some element σ of $Gal(\tilde{L}/K)$, we have $\sigma(a) \in L$. But by Theorem 1.2, point 4, any unramified extension is Galois. Thus $\sigma(a) \in M$ and $M = K[\sigma(a)] \subseteq L$. ∎

Proposition B.2 A finite extension L/K of local fields is totally ramified if and only if $\mathscr{O}_L = \mathscr{O}_K[\pi]$ for any uniformizer π of L. Moreover, the minimal polynomial of a uniformizer π over K is an Eisenstein polynomial.

Proof. Denote by n the degree of the extension, by v the valuation on $\mathscr{O}_L$ and fix π a uniformizer of L. Suppose that L/K is totally ramified. The family π^i, $i \in [\![0; n-1]\!]$, is free over $\mathscr{O}_K$ because their valuations are distinct modulo $n\mathbb{Z} = v(\mathscr{O}_K)$. It is a family of cardinal n so it is a base of $\mathscr{O}_L$ over $\mathscr{O}_K$.

Suppose that $\mathscr{O}_L = \mathscr{O}_K[\pi]$. The minimal polynomial of π is of degree n:

$$f = X^n + \sum_{i=0}^{n-1} a_i X^i$$

Since $f(\pi) = 0$ and $v(\pi^n) = n$, we must have $v(a_i\pi^n) = n$ for some $i \in [\![0; n-1]\!]$. But for $i \neq 0$, $v(a_i\pi^n) \neq 0$ modulo $n\mathbb{Z}$. Thus $v(a_0) = n$, i.e. $a_0 \in \mathfrak{m}_K \backslash \mathfrak{m}_K^2$, and $\pi^n - a_0 \in \mathfrak{m}_K^2$. Then $\pi^2 | a_1\pi$, so $a_1 \in \mathfrak{m}_K$, so $\pi^3 | a_2\pi^2$, so $a_2 \in \mathfrak{m}_K$, and so on by induction. We conclude that f is indeed an Eisenstein polynomial.

We have $\mathfrak{m}_L^n \subseteq \mathfrak{m}_L^{e(L/K)} = m_K\mathscr{O}_L$. Let $x \in \mathfrak{m}_K\mathscr{O}_L$ that we write $x = a_0x'$ for some $x' \in \mathscr{O}_L$. Then

$$
\begin{aligned}
x &= -\left(\pi^n + \sum_{i=1}^{n-1} a_i\pi^i\right)x' \\
&= -\pi^n x' - \pi\left(\sum_{i=1}^{n-1} a_i\pi^{i-1}\right)x'
\end{aligned}
$$

Since f is an Eisenstein polynomial, $a_i \in \mathfrak{m}_K$ for $i \in [\![1;n-1]\!]$. Thus $x \in \mathfrak{m}_L^n + \mathfrak{m}_L\mathfrak{m}_K$. We can repeat the same process on

$$\left(\sum_{i=1}^{n-1} a_i\pi^{i-1}\right)x'$$

and by induction we will be able to conclude that $x \in \mathfrak{m}_L^n + \mathfrak{m}_L^{n+1} = \mathfrak{m}_L^n$. Thus L/K is totally ramified. ■

Definition B.2 Let L/K be a finite extension of local fields, and denote by p the residual characteristic. The extension is called tamely ramified if p does not divide the ramification index, and widly ramified otherwise. We denote that maximal tamely ramified extension by K_{tame}:

$$K_{tame} = \underset{\leftarrow}{lim}\, L$$

where L runs trough the finite tamely ramified extension of K.

An extension that is both totally ramified and tamely (resp. widly) ramified is called totally tamely (resp. widly) ramified.

Proposition B.3 Let K be a local field, $a \in \mathscr{O}_K^\times$, $b \in \overline{K}$ such that $b^n = a$ for some $n \in \mathbb{N}^*$ that is not divisible par the residual characteristic p of K. Then the extension $K[b]/K$ is unramified.

Proof. We write L for $K[b]$. Note that since $b^n \in \mathscr{O}_K^\times$, $b \in \mathscr{O}_L^\times$. The minimal polynomial P of b over K in therefore in $\mathscr{O}_K[X]$. $\overline{P}$ denotes its image in $k[X]$, and $\overline{a}$ the image of a in $k^\times$. By assumption, $\overline{P}|X^n - \overline{a}$. The derivative of $X^n - \overline{a}$ is nX^{n-1} which is non-zero (because p does not divide n) and prime to $X^n - \overline{a}$ (because $\overline{a} \neq 0$, i.e. $a \notin \mathfrak{m}_K$). Thus $X^n - \overline{a}$ has only simple roots, and as a consequence $\overline{P}$ too. If we write the decomposition of $\overline{P}$ in r irreducible polynomials, each irreducible polynomial will be prime to the others, and thus by Hensel's lemma P can be decomposed in r polynomials. Since P is irreducible, we can conclude that $r = 1$, i.e. that $\overline{P}$ is also irreducible. Thus $[l:k] = deg(\overline{P}) = deg(P) = [L:K]$, and this exactly means that L/K is unramified. ■

Theorem B.1 For $\sigma \in Gal(K_{tame}/K_{unram})$, π a uniformizer of K, $\ell \in \mathbb{N}^*$ a prime number different from the residual characteristic p of K, $n \in \mathbb{N}^*$, $\pi^{1/\ell^n} \in \overline{K}$ a ℓ^n-th root of π, we define

$$\phi_{\ell^n}(\sigma) = \frac{\sigma(\pi^{1/\ell^n})}{\pi^{1/\ell^n}}$$

Then ϕ_{ℓ^n} is independent of the choice of π and its ℓ^n-th root, and has value an element of μ_{ℓ^n} the ℓ^n roots of unity in $\overline{K}$. Moreover, the map

$$\phi : \sigma \mapsto (\phi_{\ell^n}(\sigma))_{\ell,n}$$

is a continous group isomorphism between the Galois group $Gal(K_{tame}/K_{unram})$ and $\prod_\ell \underset{\leftarrow}{lim}\, \mu_{\ell^n}$, which is itself non canonically isomorphic to $\prod_{\ell \neq p \ prime} \mathbb{Z}_\ell$.

Proof. Let π' be another uniformizer of K, and π'^{1/ℓ^n} a ℓ^n-th root of π'. Write $\pi' = a\pi$ for some $a \in \mathscr{O}_K^\times$. Then $\pi'^{1/\ell^n} = b\pi^{1/\ell^n}$ for some $b \in \overline{K}$ such that $b^{\ell^n} = a$. Then by Proposition B.3 above, $K[b]/K$ is unramified. By definition of σ, it implies that b is fixed by σ. Therefore:

$$\frac{\sigma(\pi'^{1/\ell^n})}{\pi'^{1/\ell^n}} = \frac{\sigma(b\pi^{1/\ell^n})}{b\pi^{1/\ell^n}} = \frac{b\sigma(\pi^{1/\ell^n})}{b\pi^{1/\ell^n}} = \frac{\sigma(\pi^{1/\ell^n})}{\pi^{1/\ell^n}}$$

We have proved that ϕ is well-defined.

The injectivity of ϕ results from the above propositions B.1 and B.2. Suppose that $\phi(\sigma) = 1$, and let L/K be any tamely ramified extension. By proposition B.1, there is an unramified subextension M/K such that L/M is totally ramified. σ acts trivially on M by definition, and by Proposition B.2 $L = M[\pi^{1/n}]$ for some π a uniformizer of M (or equivalently of K, since M/K is unramified) and $n \in \mathbb{N}^*$ not divisible by the residual characteristic p of K. Write $n = \ell_1^{n_1} \dots \ell_r^{n_r}$ for $\ell_1, \dots, \ell_r$ primes, $n_1, \dots, n_r \in \mathbb{N}*$. Then the hypothesis means that σ acts trivially on $\pi^{1/\ell_i^{n_i}}$ for any i, and thus σ also acts trivially on $\pi^{1/n}$. Therefore we proved that σ fixed L and L is arbitrary so σ is the identity of K_{tame}.

Next we consider the surjectivity of ϕ. Fix π a uniformizer of K. For any $N \in \mathbb{N}^*$ not divisible by p, we can consider

- the Galois extension M_N of K obtained by adjoining the N-th roots of unity to K. By Proposition B.3, M_N/K is unramified.
- the Galois extension L_N of K obtained by adjoining the N-th roots of π to M_N. By Proposition B.2, L_N/M_N is totally ramified of degree N.

As above, we have an injective morphism

$$\begin{array}{rcl} Gal(L_N/M_N) & \to & \prod_\ell \mu_{\ell^{v_\ell(N)}} \\ \sigma & \mapsto & (\phi_{\ell^{v_\ell(N)}}(\sigma)) \end{array}$$

and since both sides have the same cardinal, it is actually an isomorphism. If we have $y \in \prod_\ell \underleftarrow{lim}\, \mu_{\ell^n}$, then for any such N, y determines an element of $\prod_\ell \mu_{\ell^{v_\ell(N)}}$ and thus an element $\sigma_N \in Gal(L_N/M_N)$. We have natural projections maps $Gal(L_{N'}/M_{N'}) \to Gal(L_N/M_N)$ if $N|N'$ and the familty $(\sigma_N)_N$ is compatible with these projections. Thus this family define an element σ in the Galois group of $\underleftarrow{lim}\, L_N$ over $\underleftarrow{lim}\, M_N$. Now, using Proposition B.1 and Proposition B.2, the compositum of $\underleftarrow{lim}\, L_N$ with K_{unram} is K_{tame}. Moreover, the intersection of $\underleftarrow{lim}\, L_N$ with K_{unram} is $\underleftarrow{lim}\, M_N$ and σ acts trivially on this intersection. We can extends σ to K_{tame} by setting it as the identity on the remaining part of K_{unram}, and we obtain an element of $Gal(K_{tame}/K_{unram})$ of image by ϕ equals to y. ■

We now come to the definitions of the wild inertia subgroup. We define more generally the following filtration of the Galois group.

Definition B.3 Let L/K be a Galois extension of local fields of Galois group G. For each $i \in \mathbb{N}$, we defined the i-th ramification group (in lower numbering) by

$$G_i = \{\sigma \in G \mid \forall\, M/K \text{ finite Galois subextension, } \forall x \in M,\ \sigma(x) - x \in \mathfrak{m}_M^{i+1}\}$$

G_0 is the inertia subgroup. G_1 is called the wild inertia subgroup.

Note that G_i is a subgroup of $Gal(L/K)$ for all i because of the relations

$$\sigma\tau(x) - x = (\sigma(\tau(x)) - \tau(x)) + (\tau(x) - x)$$

$$\sigma^{-1}(x) - x = -\sigma^{-1}(\sigma(x) - x)$$

Proposition B.4 Let L/K be a finite Galois extension of residual characteristic p and G_i the ramification groups. Then the order of G_0/G_1 is prime to p, and the order of G_i/G_{i+1} for $i \in \mathbb{N}^*$ is a power of p.

Proof. First we should justify that G_{i+1} is normal in G_i. Consider $\sigma \in G_i$, $\tau \in G_{i+1}$ and $x \in L$. We want to prove that $(\sigma^{-1}\tau\sigma)(x) - x \in \mathfrak{m}_L^{i+1}$. Then we write

$$\sigma^{-1}\tau\sigma(x) - x = \sigma^{-1}(\tau\sigma(x) - \sigma(x))$$

to conclude.

Now choose π a uniformizer of K. Then we can define a map

$$\begin{array}{rcl} G_i/G_{i+1} & \to & (1+\mathfrak{m}_K^i)/(1+\mathfrak{m}_K^{i+1}) \\ \sigma & \mapsto & \frac{\sigma(\pi)}{\pi} \end{array}$$

where the image as the structure of a multiplicative group, except in the case $i = 0$ where $1+\mathfrak{m}_K^i$ should be replaced by $\mathscr{O}_K^\times$ to make things work.

Note that the value $\frac{\sigma(\pi)}{\pi}$ is independent of the choice of π, because we consider elements of the inertia subgroup. As a consequence, this map is in fact a group morphism. Indeed,

$$\sigma \circ \tau \mapsto \frac{\sigma \circ \tau(\pi)}{\pi} = \frac{\sigma \circ \tau(\pi)}{\tau(\pi)} \frac{\tau(\pi)}{\pi} = \frac{\sigma(\pi)}{\pi} \frac{\tau(\pi)}{\pi}$$

where the last equality uses the previous remark and the fact that $\tau(\pi)$ is an uniformizer. Therefore we have defined a group morphism and we prove, by playing with the definitions a bit, that this morphism is injective.

Now for $i = 0$, we have

$$\mathscr{O}_K^\times/(1+\mathfrak{m}_K) \simeq k^\times$$

and this group is of cardinal $p^{f(K/\mathbb{Q}_p)} - 1$ prime to p, thus we deduce by Lagrange's theorem that the cardinal of G_0/G_1 is also prime to p.

For $i \in \mathbb{N}^*$, given a uniformizer π, we have a non-canonical bijection

$$\begin{array}{rcl} (1+\mathfrak{m}_K^i)/(1+\mathfrak{m}_K^{i+1}) & \to & k \\ x & \mapsto & \text{the class of } \frac{x-1}{\pi^i} \end{array}$$

Therefore $(1+\mathfrak{m}_K^i)/(1+\mathfrak{m}_K^{i+1})$ is of cardinal $p^{f(K/\mathbb{Q}_p)}$, and as a consequence G_i/G_{i+1} is of cardinal a power of p. ■

Proposition B.5 For the extension $\overline{K}/K$, we have

- $G_0 = Gal(\overline{K}/K_{unram})$.
- $Gal(\overline{K}/K)/G_0 = Gal(K_{unram}/K) \simeq \hat{\mathbb{Z}}$
- $G_1 = Gal(\overline{K}/K_{tame})$.
- $G_0/G_1 = Gal(K_{tame}/K_{unram}) \simeq \prod_\ell \varprojlim \mu_{\ell^n}$.

Proof.
- Justified in the proof of Theorem 2.2, point 3.
- It is a consequence of the previous point, of the Galois correspondence and of Theorem 1.2.
- If L/K is a finite Galois tamely ramified extension, then by Proposition B.4 G_1 is a subgroup of G_0 of cardinal a power of p. But by hypothesis the cardinal of G_0 is not divisible by p, so G_1 must be trivial. This proves the inclusion $G_1 \subseteq Gal(\overline{K}/K_{tame})$.
  Conversely, take some $\sigma \in Gal(\overline{K}/K_{tame})$ and let L/K be a finite Galois extension. Denote by P the wild inertia subgroup in $Gal(L/K)$ and by M the fixed field of P in L. The extension M/K is Galois of Galois group $Gal(L/K)/P$ and thus tamely ramified by Proposition B.4. Thus $\sigma \in Gal(L/M) = P$. This proves the inclusion $Gal(\overline{K}/K_{tame}) \subseteq G_1$.

- It is a consequence of the points 1 and 3, of the Galois correspondence and of Theorem B.1. ■

In the following, K is a local field, we write G for the absolute Galois group of K, I for the inertia subgroup and P for the wild inertia subgroup. Then we can define an action of G/I on I/P by conjugation. For this action to be well-defined, we need to check that for any $\sigma, \tau \in I$, $\sigma\tau\sigma^{-1} = \tau$ in I/P. We prove this by using Proposition B.5, point 4, and the explicit isomorphism of Theorem B.1. We only have to check that for π a uniformizer of K, ℓ a prime, $n \in \mathbb{N}^*$, π^{1/ℓ^n} a ℓ^n-th root of π, $\sigma\tau\sigma^{-1}(\pi^{1/\ell^n}) = \tau(\pi^{1/\ell^n})$. Write

$$\sigma(\pi^{1/\ell^n}) = a\pi^{1/\ell^n}$$
$$\tau(\pi^{1/\ell^n}) = b\pi^{1/\ell^n}$$

where a,b are ℓ^n-th roots of unity, and recall that by Proposition B.3 the extensions $K[a]/K$ and $K[b]/K$ are unramified, which means that a and b are fixed by σ and τ. Thus by applying σ^{-1} to the first equality, we get

$$\pi^{1/\ell^n} = \sigma^{-1}(a\pi^{1/\ell^n}) = a\sigma^{-1}(\pi^{1/\ell^n})$$

or equivalently

$$\sigma^{-1}(\pi^{1/\ell^n}) = a^{-1}\pi^{1/\ell^n}$$

Now we can prove the desired equality:

$$\begin{aligned}
\sigma\tau\sigma^{-1}(\pi^{1/\ell^n}) &= \sigma\tau(a^{-1}\pi^{1/\ell^n}) \\
&= a^{-1}\sigma\tau(\pi^{1/\ell^n}) \\
&= a^{-1}\sigma(b\pi^{1/\ell^n}) \\
&= a^{-1}b\sigma(\pi^{1/\ell^n}) \\
&= a^{-1}ba\pi^{1/\ell^n} \\
&= b\pi^{1/\ell^n} \\
&= \tau(\pi^{1/\ell^n})
\end{aligned}$$

Therefore we have a well-defined action of G/I on I/P. We can easily describe this action, starting with the Frobenius element $F \in G/I$. We keep the same notations as above and also let c be a ℓ^n-th root of unity such that $F(\pi^{1/\ell^n}) = c\pi^{1/\ell^n}$. F acts like the p-th power on elements which define an unramified extension, so in particular on b and c. We deduce that F^{-1} acts on b and c like the q-th power, where q in the inverse of p modulo ℓ^n. Thus if we apply F^{-1}, we get

$$\pi^{1/\ell^n} = c^q F^{-1}(\pi^{1/\ell^n})$$

or equivalently

$$F^{-1}(\pi^{1/\ell^n}) = c^{-q}\pi^{1/\ell^n}$$

We can then compute the action of F:

$$\begin{aligned}
F\tau F^{-1}(\pi^{1/\ell^n}) &= F\tau(c^{-q}\pi^{1/\ell^n}) \\
&= c^{-pq}F\tau(\pi^{1/\ell^n}) \\
&= c^{-1}F(b\pi^{1/\ell^n}) \\
&= c^{-1}b^pF(\pi^{1/\ell^n}) \\
&= c^{-1}b^pc\pi^{1/\ell^n} \\
&= b^p\pi^{1/\ell^n} \\
&= \tau^p(\pi^{1/\ell^n})
\end{aligned}$$

We deduce from this computation that the action of F on I/P corresponds to the p-th power map. Moreover, for any element $s \in (G/I) \backslash \{F\}$, we have some $\ell \neq p$ prime, some $n \in \mathbb{N}^*$ and some ℓ^n-th root of unity d such that $s(d) = d^{p^k}$ with $k \in [\![2; \ell^n - 1]\!]$. Then s doesn't act like the p-th power on I/P. Therefore this action of F characterizes F, and with this information in mind we will finally be able to prove the theorem that is the goal of this section.

Theorem B.2 Let K, K', f be as in Theorem 2.2, G and G' the absolute Galois groups of K and K' respectively, I and I' the inertia subgroups of K and K' respectively, P and P' the wild inertia subgroups of K and K' respectively, F and F' the Frobenius in G/I and G'/I' respectively. Then:

- $f(I) = I'$
- $f(P) = P'$
- $f(F) = F'$

Proof. We already proved the first point in chapter 2. For the point 2, consider L any finite Galois extension of K. By the infinite Galois correspondence, L corresponds by f to a finite Galois extension L' of K' and their Galois groups over K and K' respectively are isomorphic. We know that f preserves the inertia subgroups of G and G', so the induced map between $Gal(L/K)$ and $Gal(L'/K')$ also preserves the inertia subgroups. By Proposition B.4, the wild inertia subgroups in $Gal(L/K)$ and $Gal(L'/K')$ are the only p-Sylow subgroups of the inertia subgroups. Thus the induces map $f : Gal(L/K) \to Gal(L'/K')$ preserves the wild inertia subgroups. Since this is true for any finite Galois extension, $f : G \to G'$ preserves the wild inertia subgroups.

Finally, to prove that the induced map $f : G/I \to G'/I'$ preserves the Frobenius, we use the above characterization: F acts like the p-th power map on I/P, so $f(F)$ acts like the p-th power map on $f(I)/f(P) = I'/P'$. This exactly means that $f(F) = F'$. ■

C. The weight filtration

The general theory of the weight filtration of the ℓ-adic cohomology of a scheme is developed by Deligne in *Théorie de Hodge I* (1970), II (1971) and III (1974). The theory for the homology (the Tate module) of curves over local fields is already developed in SGA7 (1967-69), Exposé IX, by Grothendieck. For a curve X, the weight filtration consists of two canonical subspaces W_{-2} and W_{-1} of the ℓ-adic cohomology $W_0 = H^1(X, \mathbb{Q}_\ell)$. Beware that in this notation W_i represents the subspace of weight at most i - the weight i part is thus the quotient W_i/W_{i-1}. In SGA7, Grothendieck calls the subspaces appearing in the dual of the weight filtration the fixed part and the toric part. The level of this appendix is above our own level in algebraic geometry, and as such we apologize for the imprecisions and errors that are due to appear.

We didn't define the ℓ-adic cohomology and we will not. For our purpose, the reader must only know (or admit) that in our setting the ℓ-adic cohomology groups $H^i(X, \mathbb{Q}_\ell)$ are finite-dimensional $\mathbb{Q}_\ell$-vector spaces. We also need the following theorem relating the geometric fundamental group and the ℓ-adic cohomology. It can be thought of as an ℓ-adic version of Hurewicz's theorem.

Theorem C.1 In our setting, the maximal pro-ℓ abelian quotient of the geometric fundamental group, when tensorized by $\mathbb{Q}_\ell$, is naturally isomorphic to the dual of the first ℓ-adic cohomology group $H^1(X, \mathbb{Q}_\ell)$.

The intuition behind the weight filtration is that it is possible to distinguish in the ℓ-adic cohomology groups of a variety X the part that is already present in the compactification of X, and the parts appearing when removing a subvariety in the compactification. In the case of a curve of genus g with r punctured points, we will be able to distinguish in the first cohomology group the part coming from the compactification (which has dimension $2g$) and the part appearing after removing the punctured points (which has dimension $r-1$ if $r>0$).

The weight filtration over a finite field $\mathbb{F}_q$ is deeply linked to the eigenvalues of the map induced by the Frobenius on the ℓ-adic cohomology. To justify this fact, we need the following result. It is a fundamental tool to study the weight filtration.

Theorem C.2 — Riemann hypothesis over finite fields, Weil, Grothendieck, Deligne, 1973. Let Z be a nonsingular projective variety over a finite field $\mathbb{F}_q$ of characteristic p, and $\ell \neq p$ another prime. For any $i \in [\![1; 2n-1]\!]$, and any λ an eigenvalue of the automorphism of $H^i(Z, \mathbb{Q}_\ell)$ induced by the Frobenius map $Z \to Z$, the minimal polynomial of λ has coefficients in $\mathbb{Z}$ independent of ℓ. The complex roots of this polynomial all have complex norm $q^{i/2}$. We say that λ has weight i.

An equivalent statement of the above theorem is that the part of weight i of the ℓ-adic cohomology corresponds exactly to the direct sum of the eigenspaces with eigenvalues of weight $q^{i/2}$. We didn't define the weight filtration so we can't prove this fact rigorously, but we can justify it in our setting using the intuition that we gave. The theorem says exactly that a nonsingular projective variety has only one weight, which corresponds to the intuition since it is its own compactification. Now suppose X is an open subvariety of Z compact projective, with complementary Y which is a finite number of points. Then we have a long exact sequence in cohomology:

$$\ldots \to H^0(Y, \mathbb{Q}_\ell) \to H^1(X, \mathbb{Q}_\ell) \to H^1(Z, \mathbb{Q}_\ell) \to H^1(Y, \mathbb{Q}_\ell) \to \ldots$$

and we see that the eigenvalues of the Frobenius on $H^1(X, \mathbb{Q}_\ell)$ will be either weight 1, in which case they come from the compactification, or weight 0, in which case they come from the punctured points.

In section 2 we will use the duality of the weight filtration. For curves, the statement is as follows:

Theorem C.3

$$W_0/W_{-1} \simeq W_{-2}$$

C.1 An explicit description of the weight filtration

The goal of this section is to describe the proof of the following result, used for Theorem 3.5, point 1: if A is an open subgroup of Π, $B = A \cap \Delta$, then the image of B in the abelianization of A is a free $\hat{\mathbb{Z}}$-module of finite rank. Here Π and Δ are respectively the étale and the geometric fundamental groups of a variety X over a p-adic field K. Then A is the étale fundamental group of Y for Y a finite étale covering of X, and one can prove that B is then the geometric fundamental group of Y. Thus, if we replace X by Y, we are reduced to proving that the image of Δ in the abelianization of Π is a free $\hat{\mathbb{Z}}$-module of finite rank. Equivalently, the image of Δ can also be seen as the image of Δ^{ab}.

We only describe the main steps of the proof:

1. If there is a section $Gal(\overline{K}/K) \to \Pi$, the image of Δ in the abelianization of Π is the quotient of Δ^{ab} under the action of $Gal(\overline{K}/K)$.
2. If we replace X by some finite étale covering Y of X, we can suppose that there is a section as in the first point. The images of the geometric fundamental groups in the étale fundamental groups for X and Y only differ by torsion.
3. There is an explicit filtration $0 \subseteq T^t \subseteq T^f \subseteq T = \Delta^{ab}$ of the abelianization of Δ. After taking the maximal pro-ℓ quotient, the tensor product by $\mathbb{Q}_\ell$, and the dual, it gives the weight filtration on the ℓ-adic cohomology, thus the title of the section.
4. T^t has image zero in the quotient by the action of the absolute Galois group.
5. T^f/T^t has image zero in the quotient by the action of the absolute Galois group.
6. $T/T^f \simeq H^1(\Gamma) \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ where Γ is the dual graph of X. $H^1(\Gamma)$ is stable under the action of the absolute Galois group.

We deduce from the three last point that the quotient of Δ^{ab} by the action of the absolute Galois group is the tensor product by $\hat{\mathbb{Z}}$ of the quotient of $H^1(\Gamma)$ by the action of the absolute Galois group. Since $\mathbb{Z}$-modules are well-known, the result follows.

C.2 Reconstructing the weight filtration

The goal of this section is to describe how to reconstruct the weight filtration from the étale fundamental group - or equivalently from the geometric fundamental group Δ and the morphism $Gal(\overline{K}/K) \to Out(\Delta)$. In fact, what we want to prove is that we can recover either the genus of the number of punctured points, as stated in Theorem 3.5, point 3. However, if we know that the weight filtration is preserved by isomorphism of étale fundamental groups, and admitting some properties of the weight filtration, the conclusion follows from simple computations. We start by doing those simple computations.

We write $W_{-2} \subseteq W_{-1} \subseteq W_0$ for the weight filtration of X, a curve as in Theorem 3.5, and $W'_{-2} \subseteq W'_{-1} \subseteq W'_0$ for the weight filtration of the compactification of X. The dimension over $\mathbb{Q}_\ell$ of W_0 is the rank over $\hat{\mathbb{Z}}$ of Δ^{ab}, that is $2g + r - 1$. The equality between dimension and rank is also true for the compactification, and this time the result is $2g$. We admit that $W_0/W_{-1} \simeq W'_0/W'_{-1}$ and $W_{-1}/W_{-2} \simeq W'_{-1}/W'_{-2}$, and we also recall that the duality Theorem C.3 gives $W'_0/W'_{-1} \simeq W'_{-2}$.

Then we write

$$\begin{aligned}
r-1 &= dim_{\mathbb{Q}_\ell}(W_0) - dim_{\mathbb{Q}_\ell}(W_0') \\
&= dim_{\mathbb{Q}_\ell}(W_0/W_{-1}) + dim_{\mathbb{Q}_\ell}(W_{-1}/W_{-2}) + dim_{\mathbb{Q}_\ell}(W_{-2}) \\
&\quad - dim_{\mathbb{Q}_\ell}(W_0'/W_{-1}') - dim_{\mathbb{Q}_\ell}(W_{-1}'/W_{-2}') - dim_{\mathbb{Q}_\ell}(W_{-2}') \\
&= dim_{\mathbb{Q}_\ell}(W_{-2}) - dim_{\mathbb{Q}_\ell}(W_{-2}') \\
&= dim_{\mathbb{Q}_\ell}(W_{-2}) - dim_{\mathbb{Q}_\ell}(W_0'/W_{-1}') \\
&= dim_{\mathbb{Q}_\ell}(W_{-2}) - dim_{\mathbb{Q}_\ell}(W_0/W_{-1})
\end{aligned}$$

If we know how to reconstruct the weight filtration from the étale fundamental group, then this implies that we can get the number of punctured points, and as a corollary the genus.

We stated in the introduction that the weight filtration was "canonical", but canonical only means that an isomorphism of varieties respect the weight filtration. Here, we don't know that the varieties are isomorphic, or even that they are on the same field. However, we know how to reconstruct the first ℓ-adic cohomology group (Theorem 3.5, point 1, and Theorem C.1) and the Frobenius element in G/I (Theorem 3.5, point 1, and Theorem 2.2., point 2, proved as Theorem B.2). We want to generalize the correspondence between the weight filtration and the eigenspaces of the Frobenius described in the introduction of this appendix. The Frobenius element is defined modulo an element of the inertia subgroup, so in general it does not make sense to speak of the eigenspaces of the Frobenius. However, when it does make sense, this correspondence still holds.

Theorem C.4 In our setting, and if we suppose moreover that the eigenvalues of the elements of the inertia subgroup on the first ℓ-adic cohomology group are roots of unity, then the part of weight i corresponds to the direct sum of the eigenspaces with eigenvalue of weight i for any lift of the Frobenius.

Even though one can think at first that the hypothesis is restrictive, in fact one can always suppose that it is satisfied, using the following theorem. We give its proof since it does not use algebraic geometry.

Theorem C.5 — Grothendieck's Local Monodromy Theorem, 1968. Let K be a local field, ℓ a prime distinct from the residual characteristic of K and $\rho : Gal(\overline{K}/K) \to V$ a continuous representation of the absolute Galois group of K on a finite-dimensional $\mathbb{Q}_\ell$-vector space V. There exists a finite extension L of K such that the restriction of ρ to the inertia subgroup of $Gal(\overline{L}/L)$ has only roots of unity as eigenvalues.

Proof. Take W a $\mathbb{Z}_\ell$-lattice in V. Then W is open in V, and $GL(W)$ is open in $GL(V)$. By continuity, $\rho^{-1}(GL(W))$ is open in $G = Gal(\overline{K}/K)$, so the quotient $G/\rho^{-1}(GL(W))$ is finite. Consider W' the $\mathbb{Z}_\ell$-module obtained by adding to W the images of a set of representants of the above quotient. Then by construction the image of ρ is included in $GL(W')$. Moreover, W' is a torsion-free finitely-generated $\mathbb{Z}_\ell$-module and $\mathbb{Z}_\ell$ is a principal ideal domain, so W' is free, so that $GL(W')$ is isomorphic to $GL_n(\mathbb{Z}_\ell)$ where n is the dimension of V. In the rest of the proof, we consider that the image of ρ is included in $GL_n(W')$.

For $A \in M_n(\mathbb{Z}_l)$, we have $I_n + \ell A \in GL_n(\mathbb{Z}_\ell)$ because its inverse is

$$\sum_{k=0}^{+\infty} (-\ell A)^k$$

which is well-defined. The subset $I_n + \ell M_n(\mathbb{Z}_\ell)$ is an open subgroup of $GL_n(\mathbb{Z}_\ell)$. Now recall that by Proposition B.4, the wild inertia subgroup P of G is a pro-p group. Then it is a corollary of Lagrange's theorem that for $g \in P$, $g^{p^k} \to 1$ when $k \to +\infty$. Suppose that $\rho(g) \in I_n + \ell M_n(\mathbb{Z}_\ell)$, written $\rho(g) = I_n + \ell M_n(\mathbb{Z}_\ell)$ for some $A \in M_n(\mathbb{Z}_\ell)$. Then:

$$\rho(g^{p^k}) = \rho(g)^{p^k} = (I_n + \ell A)^{p^k} = I_n + p^k \ell A + \ell^2 B$$

for some matrix $B \in M_n(\mathbb{Z}_\ell)$ depending on k. This expression tends to zero, so for k great enough we have that $p^k \ell A + \ell^2 B$ is divisible by ℓ^2. Since $\ell \neq p$, it follows that A is divisible by ℓ. Write $A = \ell A'$ for some matrix A'. Similarly, we get

$$p^k \ell^2 A' + \ell^4 B' \to 0$$

for some matrix B' depending on k, and we deduce that ℓ^2 divides A', so ℓ^3 divides A. By induction we deduce that A is divisible by any power of ℓ, and thus that $A = 0$.

We noted that $I_n + \ell M_n(\mathbb{Z}_\ell)$ is an open subgroup of $GL_n(\mathbb{Z}_\ell)$, so by continuity $G' = \rho^{-1}(I_n + \ell M_n(\mathbb{Z}_\ell))$ is an open subgroup of G, corresponding to a finite extension L of K. In the previous paragraph, we proved that the wild inertia subgroup P' in G' has trivial image by ρ, thus we can consider ρ as a group representation of the quotient G'/P'. Consider I' the inertia subgroup of G', and recall that by the computations before Theorem B.2, if $F \in G'$ is a lift of the Frobenius, F acts by conjugation on I'/P' as the p-th power. Now consider an eigenvalue λ of $\rho(g)$ for some $g \in I'/P'$ with eigenvalue x, and let us prove as stated that λ is a root of unity. We write:

$$\lambda \rho(F)(x) = \rho(F)(\lambda x) = \rho(F) \circ \rho(g)(x) = \rho(FgF^{-1}F)(x) = \rho(g^p) \circ \rho(F)(x)$$

We proved that λ is an eigenvalue of ρ^p. By induction, λ is an eigenvalue of ρ^{p^k} for all $k \in \mathbb{N}^*$. But ρ has only a finite number of eigenvalues, so there must be an eigenvalue μ of ρ and two indexes $k < l$ such that $\lambda = \mu^k = \mu^l$. Then $\mu^{l-k} = 1$ so $\lambda^{l-k} = (\mu^{l-k})^k = 1$, and this ends the proof. ■

With this theorem we can finally prove that the number of punctured points can be reconstrucuted from the étale fundamental group. Consider X, X', f as in Theorem 3.5. For each finite étale covering Y of X, with Y defined over a finite extension L of K, choose F a lift of the Frobenius element in the the absolute Galois group of L. Denote ρ the representation of the absolute Galois group of L on the first ℓ-adic cohomology group of Y. Then we can compute the value of

$$1 + dim_{\mathbb{Q}_\ell}\Big(\bigoplus_{\lambda \text{ of weight } -2} Ker(Id - \lambda\rho(F))\Big) - dim_{\mathbb{Q}_\ell}\Big(\bigoplus_{\lambda \text{ of weight } 0} Ker(Id - \lambda\rho(F))\Big)$$

The two previous theorems state that this sequence converges, and its limit is

$$1 + dim_{\mathbb{Q}_\ell}(W_{-2}) - dim_{\mathbb{Q}_\ell}(W_0/W_{-1})$$

which is also by the computations above the number of punctured points of X. Now f gives a correspondence between the finite étale coverings of X and X', sends a representant of the Frobenius to a representants of the Frobenius, and gives an isomorphism between the first ℓ-adic cohomology groups. Therefore the computation of the limit above is invariant by f, and we obtain that the number of punctured points of X and X' are equal.

D. Anabelian geometry over global fields

The internship was originally supposed to speak about anabelian geometry on both p-adic fields and number fields. However, due to both a lack of available space in the report and a lack of time to complete the proofs, the two following sections about anabelian geometry over global fields have been removed from the main chapters of the report. The first one is incomplete.

D.1 Neukirch's theorem

Theorem D.1 — Neukirch, 1969. Let K, K' be two number fields. We suppose that $Gal(\overline{K}/K)$ and $Gal(\overline{K'}/K')$ are isomorphic. Then K and K' are isomorphic.

There are four main steps in the proof of Neukirch's result. The first one is to associate to each prime of K a prime in K' with isomorphic decomposition subgroups. The second step is to prove that these two primes have the same inertia index. The third step is to deduce the global statement for Galois extensions of $\mathbb{Q}$ by using Chebotarev's density theorem. The fourth step is to generalize the result to non-Galois extensions.

This section contains an incomplete proof of Neukirch's theorem. In particular, the fourth step is not described here at all. It is not, though, the most difficult: if local class field theory and Chebotarev's density theorem are admitted, the most difficult step the first one. The key result is a characterization of decomposition subgroups in the absolute Galois groups of number fields (see below) that is admitted here.

We begin the proof of the first step by linking the decomposition subgroup of a prime with the Galois group of the completed field at this prime. We will need the following result:

Proposition D.1 — Krasner's lemma. Let K be a local field, $\alpha, \beta \in \overline{K}$, and let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ be the conjugates of α. Suppose that $|\alpha - \beta| < |\alpha - \alpha_i|$ for $i \in [\![2;n]\!]$, the norm being computed in $K[\alpha_i, \beta]$. Then $K[\alpha] \subseteq K[\beta]$.

Proof. First note that the hypothesis implies that $|\alpha - \alpha_i| > 0$ for $i \in [\![2;n]\!]$, or equivalently that α is separable over K. We assume that $K[\alpha]$ is not included in $K[\beta]$. Then $K[\alpha, \beta]$ is a non-trivial extension of $K[\beta]$, and since α is separable over $K[\beta]$, there is $\sigma : K[\alpha, \beta] \to \overline{K}$ that fixes $K[\beta]$ but not α. Then

$$|\alpha - \beta| = |\sigma(\alpha - \beta)| = |\alpha_i - \beta|$$

for some $i \in [\![2;n]\!]$. Then:

$$|\alpha - \alpha_i| \leqslant max\{|\alpha - \beta|, |\alpha_i - \beta|\}$$

Then we get that either

$$|\alpha - \alpha_i| \leqslant |\alpha - \beta|$$

or

$$|\alpha - \alpha_i| \leqslant |\alpha_i - \beta|$$

and in this second case, by applying σ^{-1} and recalling that $\alpha_i = \sigma(\alpha)$, we get

$$|\sigma^{-1}(\alpha) - \alpha| \leqslant |\alpha - \beta|$$

with $\sigma^{-1}(\alpha) \neq \alpha$. In both cases we have a contradiction. ∎

Proposition D.2 Let K be a number field and $\mathfrak{p}_\infty$ a prime in $\overline{K}$. For any finite extension L of K, we write $\mathfrak{p}_L = \mathfrak{p}_\infty \cap \mathcal{O}_L$ and $L_{\mathfrak{p}_L}$ for the $\mathfrak{p}_L$-adic completion of L. Then:

- The ramification index and the inertia index of $L_{\mathfrak{p}_L}$ of $K_{\mathfrak{p}_K}$ are the ones of L at $\mathfrak{p}_L$ over $\mathfrak{p}_K$.
- The union M of the $L_{\mathfrak{p}_L}$ where L runs through the finite extensions L of K is a separable closure of the completion $K_{\mathfrak{p}_K}$.
- The decomposition subgroup of $\mathfrak{p}_\infty$ in $Gal(\overline{K}/K)$ is isomorphic to the absolute Galois group of $K_{\mathfrak{p}_K}$.

Proof.

- The equality of the inertia indexes results from the isomorphism

$$\mathcal{O}_{L_{\mathfrak{p}_L}}/\mathfrak{m}_{L_{\mathfrak{p}_L}}\mathcal{O}_{L_{\mathfrak{p}_L}} \simeq \mathcal{O}_L/\mathfrak{p}_L\mathcal{O}_L$$

which itself results from the isomorphism

$$\mathcal{O}_{L_{\mathfrak{p}_L}} \simeq \underset{\leftarrow}{lim}\ \mathcal{O}_L/\mathfrak{p}_L^n\mathcal{O}_L$$

where n runs through $\mathbb{N}$. For the equality of ramification index, we start from

$$\mathfrak{p}_K\mathcal{O}_L = \prod_{\mathfrak{q}|\mathfrak{p}_K} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p}_K)}$$

and we tensorize it by $\mathcal{O}_{L_{\mathfrak{p}_L}}$ over $\mathcal{O}_L$. The left-hand side becomes $\mathfrak{m}_{K_{\mathfrak{p}_K}}\mathcal{O}_{L_{\mathfrak{p}_L}}$ and, since for $q \neq \mathfrak{p}_L$ the elements of $\mathfrak{q}\backslash\{0\}$ are invertible in $\mathcal{O}_{L_{\mathfrak{p}_L}}$, the right-hand side becomes $\mathfrak{m}_{L_{\mathfrak{p}_L}}^{e(\mathfrak{p}_L/\mathfrak{p}_K)}$. This implies the desired equality.

- We assume that the reader knows the equality

$$dim_K(L) = \sum_{\mathfrak{q}} e(\mathfrak{q}/\mathfrak{p}_K)f(\mathfrak{q}/\mathfrak{p}_K)$$

where the sum is on the primes ideals $\mathfrak{q}$ of L above $\mathfrak{p}_K$. Our interest lies in the inequality $dim_K(L) \geqslant e(\mathfrak{p}_L/\mathfrak{p}_K)f(\mathfrak{p}_K/\mathfrak{p}_K) = e(\mathfrak{m}_{L_{\mathfrak{p}_L}}/\mathfrak{m}_{K_{\mathfrak{p}_K}})f(\mathfrak{m}_{L_{\mathfrak{p}_L}}/\mathfrak{m}_{K_{\mathfrak{p}_K}}) = dim_{K_{\mathfrak{p}_K}}(L_{\mathfrak{p}_L})$ that follows from this equality and the first point. It shows in particular that the union M of the $L_{\mathfrak{p}_L}$ is an algebraic extension of $K_{\mathfrak{p}_K}$. We must now show that it is algebraically closed. Let α be an element that is algebraic over M. Since M is algebraic over $K_{\mathfrak{p}_K}$, α is algebraic over $K_{\mathfrak{p}_K}$. Consider its minimal polynomial $P \in K_{\mathfrak{p}_K}[X]$. Since the fields considered are of characteristic zero, P has no double root, so the quantity $\varepsilon = \underset{i\in[\![2;n]\!]}{min} |\alpha - \alpha_i|$, where $\alpha = \alpha_1, \alpha_2, ..., \alpha_n$ are the conjugates of α, is strictly positive. Since K is dense in $K_{\mathfrak{p}_K}$, for any $\delta \in \mathbb{R}_+^*$ we can approach P by a polynomial $Q \in K[X]$ such that their difference (for the norm that is the sum of the $\mathfrak{p}_K$-adic norm of the coefficients) is smaller that δ. If we choose δ small enough, then Q will have a root β in $\overline{K}$ such that $|\alpha - \beta| < \varepsilon$. Then by Krasner's lemma, $K_{\mathfrak{p}_K}[\alpha] \subseteq K_{\mathfrak{p}_K}[\beta]$ and $K_{\mathfrak{p}_K}[\beta] = K[\beta]_{\mathfrak{p}_{K[\beta]}} \subseteq M$, so $\alpha \in M$ and this concludes the proof.

- It is sufficient to justify that for L a finite Galois extension of K, $L_{\mathfrak{p}_L}/K_{\mathfrak{p}_K}$ is Galois of Galois group isomorphic to the decomposition subgroup of $\mathfrak{p}_L$ in $Gal(L/K)$. By the primitive element theorem, $L = K[\alpha]$ for an α whose conjugates all lie in L. Then $L_{\mathfrak{p}_L} = K_{\mathfrak{p}_K}[\alpha]$ and the conjugates of α all lies in $L_{\mathfrak{p}_L}$, so $L_{\mathfrak{p}_L}/K_{\mathfrak{p}_K}$ is Galois. An element of $Gal(L_{\mathfrak{p}_L}/K_{\mathfrak{p}_K})$ is in particular, by restricting it to L, an element of $Gal(L/K)$ that fixes $\mathfrak{p}_L$. Conversely, any element of the decomposition subgroup of $\mathfrak{p}_L$ in $Gal(L/K)$ extends in a unique way to give an element of $Gal(L_{\mathfrak{p}_L}/K_{\mathfrak{p}_K})$.

■

The following theorem is a converse to this proposition, and the key result of the proof:

Theorem D.2 — Neukirch's characterization of decomposition subgroups. Let K be a number field, and H a subgroup of $Gal(\overline{K}/K)$ that is isomorphic to the absolute Galois group of a local field. Then there is a prime $\mathfrak{p}_\infty$ in $\overline{K}$ such that H is the decomposition subgroup of $\mathfrak{p}_\infty$ over a finite extension of K. Moreover, this prime is unique.

Proof. Admitted. See J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Theorem 12.1.9. ■

We now start the proof of Neukirch's theorem. The isomorphism $Gal(\overline{K}/K) \to Gal(\overline{K'}/K')$ is denoted by f.

First step of the proof of Neukirch's theorem. Let $\mathfrak{p}$ be a prime in K, and fix $\mathfrak{p}_\infty$ a prime of $\overline{K}$ over $\mathfrak{p}$. Then by Proposition D.2, the decomposition subgroup D of $\mathfrak{p}_\infty$ in $Gal(\overline{K}/K)$ is isomorphic to the absolute Galois group of a local field. Thus $f(D)$ is too. By Theorem D.2, this implies that $f(D) \subseteq D'$ where D' is the decomposition subgroup of a prime $\mathfrak{q}_\infty$ of $\overline{K'}$ above a prime $\mathfrak{q}$ of K'. To finish this step, we have to prove that in fact $f(D) = D'$. Equivalently, $f^{-1}(D') \subseteq D$. By using once again Proposition D.2 and Theorem D.2, we have $f^{-1}(D') \subseteq D''$ where D'' is the decomposition subgroup of a prime $\mathfrak{p}'_\infty$ of $\overline{K}$ above a prime $\mathfrak{p}'$ of K. In particular $D \subseteq D''$. Since we also have $D \subseteq D$, the unicity in Theorem D.2 implies that $D = D''$ and as a consequence that $f(D) = D'$. ■

Second step of the proof of Neukirch's theorem. By the first step, there is a $1-1$ correspondence between prime ideals of K and of K'. For $\mathfrak{p}$ a prime in K, denote $f(\mathfrak{p})$ the corresponding prime in K'. Moreover, to those two prime ideals we have associated local fields $K_\mathfrak{p}$ and $K'_{f(\mathfrak{p})}$ that have isomorphic Galois groups by Proposition D.2. Now Theorem 2.2, point 2, and Proposition D.2, point 1, implies that the inertia indexes of $\mathfrak{p}$ and $f(\mathfrak{p})$ are equal. ■

The third step is a corollary of the following (difficult) theorem, that is not proved in this report.

Theorem D.3 — Chebotarev's density theorem, 1922. Let L/K be a finite Galois extension of number fields. For each unramified ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the conjugacy class of Frobenius element associated to a prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ above $\mathfrak{p}$ is independent of the choice of $\mathfrak{q}$, we denote it $\sigma_\mathfrak{p}$. Then for any conjugacy class C of $G = Gal(L/K)$, we have

$$\frac{Card\{\mathfrak{p} \text{ unramified prime ideal of } \mathcal{O}_K \text{ such that } N(\mathfrak{p}) \leqslant x \text{ and } \sigma_\mathfrak{p} = C\}}{Card\{\mathfrak{p} \text{ unramified prime ideal of } \mathcal{O}_K \text{ such that } N(\mathfrak{p}) \leqslant x\}} \underset{x\to+\infty}{\to} \frac{Card\ C}{Card\ G}$$

Proof. As for any result giving an equivalent of an arithmetic quantity, this theorem is proven by writing the partial sum of the coefficients of some L functions as an integral (by Fourier's inverse formula) and then as a sum of residues (by the residue theorem). For Chebotarev's density theorem, Artin's L functions are the ones used. The details are omitted as it would be too long for this report and too far from the subject. See for example J. S. Milne, *Class Field Theory*, https://www.jmilne.org/math/CourseNotes/CFT.pdf, Chapter VIII - Complements, Theorem 7.4. ■

Corollary D.1 — Third step of Neukirch's theorem. Let K, K' be two numbers fields that are Galois over $\mathbb{Q}$. We suppose that for any prime $p \in \mathbb{N}$ that is unramified in both K and K', the inertia indexes of K and K' at p are equal. Then $K = K'$.

Proof. Let p be a prime number. We denote σ_p^K for the conjugacy class defined in the statement of the theorem in $Gal(K/\mathbb{Q})$. We first note that we have the equivalences

$$\begin{aligned} p\ splits\ completely\ in\ KK' &\iff \sigma_p^{KK'} = \{1\} \\ &\iff Any\ represent\ of\ \sigma_p^{KK'}\ is\ the\ identity\ on\ KK' \\ &\iff Any\ represent\ of\ \sigma_p^{KK'}\ is\ the\ identity\ on\ both\ K\ and\ K' \\ &\iff \sigma_p^K = \{1\}\ and\ \sigma_p^{K'} = \{1\} \\ &\iff p\ splits\ completely\ in\ both\ K\ and\ K' \end{aligned}$$

This equivalence and the hypothesis imply that the primes that split completely in K, K' and KK' are exactly the same. But Chebotarev's density theorem implies, by taking $C = \{1\}$, that the density of those primes is equal to the inverse of the dimension of the field extension. Thus

$$dim_{\mathbb{Q}}(K) = dim_{\mathbb{Q}}(KK') = dim_{\mathbb{Q}}(K')$$

and we conclude that the three fields are equal. ■

D.2 Anabelian geometry for hyperbolic curves over global fields

Theorem D.4 — Relative Grothendieck's conjecture - Nakamura, Tamagawa, Mochizuki, 1995. Let X and X' be two hyperbolic curves over a number field F. We suppose that their étale fundamental groups are isomorphic. Then X and X' are isomorphic.

Proof. Mochizuki's first proof, based on the ideas of Nakamura and Tamagawa, is given in *The Profinite Grothendieck Conjecture for Closed Hyperbolic Curves over Number Fields*, https://www.kurims.kyoto-u.ac.jp/~motizuki/The%20Profinite%20Grothendieck%20Conjecture%20for%20Closed%20Hyperbolic%20Curves%20over%20Number%20Fields.pdf. He gave a second proof in *The Local Pro-p Anabelian Geometry of Curves*, https://www.kurims.kyoto-u.ac.jp/~motizuki/The%20Local%20Pro-p%20Anabelian%20Geometry%20of%20Curves.pdf, using a different method and strenghtening its previous results. ■

The above theorem is the conjecture that was mentioned in the introduction of the second chapter.

Theorem D.5 The only topologically finitely-generated closed normal subgroup of the absolute Galois group of a number field is the trivial subgroup.

Here "topologically finitely-generated" means that there exists a finitely-generated subgroup that is dense is the whole group.

Proof. Admitted. See for example M. D. Fried, M. Jarden, *Field Arithmetic*, Springer, 2008, Proposition 16.11.6. ■

Corollary D.2 Let X be an hyperbolic curve over a number field F with arithmetic fundamental group Π and geometric fundamental group Δ. Then Δ is the unique maximal topologically finitely-generated closed normal subgroup of Π.

Proof. Let H be a topologically finitely-generated closed normal subgroup of Π. Then the image of H in $Gal(\overline{F}/F)$ is a topologically finitely-generated closed (because the sequence is split) normal subgroup, thus trivial by Theorem D.5. Il follows that $H \subseteq \Delta$. Δ is a topologically finitely-generated (by its explicit description) closed normal subgroup of Π so we have the conclusion. ■

Corollary D.3 — Absolute Grothendieck's Conjecture. Let X and X' be hyperbolic curves over F and F' respectively, with F, F' two number fields. We suppose that their étale fundamental groups are isomorphic. Then F and F' are isomorphic and X and X' are isomorphic.

Proof. Let f be an isomorphism between their étale fundamental groups. The characterization of the previous corollary implies that f preserve the geometric fundamental groups. Then the quotient map is an isomorphism between the absolute Galois groups of F and F'. By Neukirch's theorem, we can conclude that F and F' are isomorphic and then apply the above theorem of Mochizuki. ■

Bibliography

Lectures notes

[1] P. Allen. *Nonarchimedean Local Fields*. https://faculty.math.illinois.edu/~pballen/research/LocalFields.pdf.

[2] D. Harari. *Théorie du corps de classes, M2, Orsay*. https://www.imo.universite-paris-saclay.fr/~david.harari/enseignement/corpsclass/.

[3] Y. Hoshi. *Reconstruction of a Number Field from the Absolute Galois Group*. https://www.kurims.kyoto-u.ac.jp/~yuichiro/talk20140311.pdf.

[4] J. S. Milne. *Algebraic Number Theory*. https://www.jmilne.org/math/CourseNotes/ANTc.pdf.

[5] S. Mundy. *Algebraic Number Theory Notes: Local Fields*. https://www.math.columbia.edu/~mundy/ANT1.pdf.

[6] A. Sutherland. *Number Theory I*. https://math.mit.edu/classes/18.785/2019fa/LectureNotes11.pdf.

Books

[7] R. Hartshorne. *Algebraic Geometry*. Springer, 1977.

[8] K. Wingberg J. Neukirch A. Schmidt. *Cohomology of Number Fields*. Springer, 2008.

[9] J. Neukirch. *Algebraic Number Theory*. Springer, 1991.

[10] C. A. Weibel. *An Introduction to Homological Algebra*. Cambridge University Press, 1994.

Articles

[11] S. Mochizuki H. Nakamura A. Tamagawa. "The Grothendieck Conjecture on the Fundamental Groups of Algebraic Curves". In: (2001).

[12] S. Mochizuki. "The Absolute Anabelian Geometry of Hyperbolic Curves". In: (2016).