Travail sur un article de Mochizuki concernant la théorie des corps locaux p-adiques

Stage de second semestre de M1

Béranger Seguin

Stage sous la direction de
M. Szamuely Tamás

Effectué à l'institut Rényi Alfréd,
13-15 Reáltanoda utca,
Budapest

2018

Sommaire

1 Déroulement du stage

Le stage s'est déroulé à Budapest, où j'ai atterri le dimanche 25 mars 2018 et d'où je suis reparti le vendredi 17 août 2018.

1.1 Organisation

J'ai rencontré mon maître de stage, SZAMUELY Tamás, le mardi 27 mars et, à partir de là, de manière systématique au moins une fois par semaine les mardis, pendant une heure et demi en général. À notre premier rendez-vous, il m'a proposé un sujet que j'ai accepté puis il m'a conduit à la bibliothèque de l'institut pour que j'y emprunte les livres nécessaires.
Je travaillais principalement chez moi, ce qui me permettait de répartir mon temps de travail comme je le voulais. En cas de difficulté, je pouvais le contacter par mail et il était toujours très réactif. Généralement, lors de nos rendez-vous, il me demandait de lui expliquer ce que j'avais fait et compris durant la semaine, commentait, puis me demandait de comprendre une autre chose d'ici à la semaine suivante.
Le stage s'est globalement décomposé en trois parties : d'abord, pendant le premier mois, j'ai dû beaucoup lire. J'ai notamment lu des parties importantes de *Corps Locaux* de SERRE et de *Algebraic Number Theory* de NEUKIRCH (qui fait des choses similaires mais avec des explications parfois plus claires). Ensuite, j'ai commencé à essayer de comprendre l'article de MOCHIZUKI sur lequel je travaillais, tout en continuant de lire d'autres livres au fur et à mesure que des connaissances nouvelles étaient requises. Finalement, mon maître de stage m'a proposé de faire soit un mémoire soit un exposé pour expliquer l'article (à l'oral, au tableau, en anglais, pendant un peu plus d'une heure) à un collègue à lui, spécialiste de géométrie arithmétique mais ignorant tout de l'article. J'ai choisi l'exposé (même si, d'après mon maître de stage, mes notes d'exposé auraient pu faire office de mémoire), et tant mon maître de stage que son collègue se sont dits satisfaits de ma présentation finale.

1.2 Apports sur le plan personnel

— Pour la première fois, j'ai été directement confronté au monde de la recherche : lire et comprendre un article de recherche, essayer de comprendre des arguments incomplets ou peu clairs, apprendre à me documenter dans des références,... mais aussi les conférences, les bureaux, les chercheurs et chercheuses... J'ai par exemple vu un exposé de Roger HEATH-BROWN sur le dénombrement des points rationnels sur les coniques et un exposé de qualité excellente de Terence TAO sur la conjecture de CHOWLA (aucun des deux n'ayant de rapport avec mon sujet de stage).
— J'ai appris beaucoup de choses, mathématiquement parlant.
— Je suis parti en stage parce que je commençais à me désintéresser de l'enchaînement cours/partiels/examens, qui me lassait progressivement de mon activité. Au cours du stage, j'ai repris goût aux mathématiques et j'ai retrouvé un peu de ma curiosité.
— Budapest est une ville fantastique dont j'ai eu beaucoup de plaisir à explorer les coins et recoins. Elle est également très proche de nombreuses capitales d'Europe centrale que j'ai également eu le temps de visiter.
— J'ai eu de très nombreuses interactions en anglais (y compris avec des locuteurs natifs, américains, anglais et australiens) ainsi qu'en allemand (principalement avec des locuteurs natifs). Mon hongrois a également beaucoup progressé.

1.3 Ce qui était bien, ce qui était moins bien

Points positifs :
— Le sujet était intéressant, suffisamment compliqué pour m'occuper tout mon stage, et j'étais ravi d'en avoir une bonne compréhension à la fin.

— J'ai noué une bonne relation avec mon maître de stage, avec qui je parlais quelquefois de musique, de la Hongrie, et d'autres choses. Une fois que j'avais cuisiné des éclairs au chocolat, je lui en ai offert et il les a trouvés bons. Il s'est dit content de moi à la fin du stage (pour des raisons mathématiques, je l'espère, et non pas uniquement pour les éclairs).
— La façon dont le stage était organisé était suffisamment contraignante pour me motiver et m'occuper et suffisamment libre pour que je puisse profiter des activités à Budapest et aux alentours.
— La vie en Hongrie est très peu chère pour un français. J'ai notamment pu trouver un appartement spacieux en centre-ville, à dix minutes à pied du lieu de mon stage, pour un prix raisonnable.
— J'ai pu voir énormément de concerts à Budapest, dont des œuvres rarement jouées de LISZT, de BERNSTEIN, de JANÁČEK, ... J'ai même pu voir Martha ARGERICH et Yuja WANG jouer en vrai.

Points négatifs :

— Je suis un peu déçu de n'avoir pas eu l'occasion de trouver des résultats « nouveaux », le sujet étant extrêmement pointu. Cela dit, l'article de MOCHIZUKI ayant une forte tendance à l'ellipse et aux arguments imprécis, j'ai eu beaucoup d'occasions de passer des nuits blanches à chercher comment les faire fonctionner. Je pense donc avoir quand même eu une petite expérience de la recherche.
— À cause de problèmes administratifs, j'ai commencé mon stage fin mars et l'ai fini en août. Cela signifie que j'ai suivi pendant une partie importante du semestre des cours à l'ÉNS que je n'ai jamais validés, et que j'ai eu peu de vacances. Mais j'ai su profiter de l'été à Budapest malgré tout.
— Le sujet étant très spécifique, j'ignore encore à quel point les connaissances que j'ai développées lors du stage seront réutilisables. Cependant, j'aimerais bien continuer à faire des choses similaires. C'est une des raisons qui m'ont fait choisir le master de mathématiques fondamentales l'an prochain.
— Mon stage ayant eu lieu dans un institut de recherche et non dans une université, il fut compliqué pour moi de faire la connaissance de gens de mon âge, en tout cas pendant les premières semaines. En particulier, je n'ai jamais trouvé de collectif ou de groupe où faire de la musique régulièrement, même si j'allais quelquefois à des open jams publiques.

2 Travail mathématique

Mon stage consistait principalement à accumuler suffisamment de connaissances pour être capable de comprendre et d'expliquer un article de S. MOCHIZUKI intitulé *A Version of the* Grothendieck *Conjecture for p-adic Local Fields*. Cet article prouve essentiellement le résultat suivant, sous une forme plus précise : si deux corps locaux p-adiques (c'est-à-dire des extensions finies de $\mathbb{Q}_p$) ont leurs groupes de GALOIS absolus respectifs isomorphes et que l'isomorphisme vérifie une propriété supplémentaire (il préserve les sous-groupes de ramification), alors les corps sont isomorphes.

2.1 Énoncé précis du théorème

Soit K un corps local p-adique (une extension finie de $\mathbb{Q}_p$). On pose $\Gamma_K = \mathrm{Gal}(\bar{K} \mid K)$. Si L est une extension finie de K et $i \in \{-1, 0, 1, 2, 3, \ldots\}$, on définit :

$$\mathrm{Gal}(L \mid K)_i = \{\sigma \in \mathrm{Gal}(L \mid K) \mid \forall x \in L, v_L(\sigma(x) - x) \geq i + 1\}$$

où v_L est l'unique extension de la valuation p-adique à L. Ceci définit une filtration de $\mathrm{Gal}(L \mid K)$:

$$\mathrm{Gal}(L \mid K) = \mathrm{Gal}(L \mid K)_{-1} \supset \mathrm{Gal}(L \mid K)_0 \supset \mathrm{Gal}(L \mid K)_1 \supset \dots$$

qui induit par passage à la limite projective une filtration, dite de ramification :

$$\Gamma_K \supset (\Gamma_K)_0 \supset (\Gamma_K)_1 \supset (\Gamma_K)_2 \supset (\Gamma_K)_3 \supset \dots$$

et on définit de même la filtration $(\Gamma_{K'})_i$ associée à un deuxième corps p-adique K'. On dira d'un isomorphisme entre Γ_K et $\Gamma_{K'}$ qu'il préserve la filtration de ramification s'il envoie $(\Gamma_K)_i$ sur $(\Gamma_{K'})_i$.
Notons d'abord $\mathrm{Isom}_{\mathbb{Q}_p}(K, K')$ l'ensemble des isomorphismes continus de $\mathbb{Q}_p$-algèbre entre K et K'. Soit f, s'il en existe, un élément de $\mathrm{Isom}_{\mathbb{Q}_p}(K, K')$. On peut alors l'étendre (non uniquement) à un isomorphisme $\tilde{f}$ entre $\overline{K}$ et $\overline{K'}$. On peut en déduire un isomorphisme $\Phi(f)$ entre Γ_K et Γ'_K :

$$\forall g \in \Gamma_K, \Phi(f)(g) = \tilde{f} \circ g \circ \tilde{f}^{-1}$$

Cet isomorphisme $\Phi(f)$ préserve clairement la filtration de ramification. Si on a deux prolongements $\tilde{f}$ différents, cela ne fait que composer $\Phi(f)$ à gauche par un automorphisme intérieur de $\Gamma_{K'}$. On définit donc $\mathrm{Out}_{\mathrm{Filt}}(\Gamma_K, \Gamma_{K'})$ l'ensemble des isomorphismes entre Γ_K et $\Gamma_{K'}$ qui préservent la filtration de ramification, modulo les automorphismes intérieurs de $\Gamma_{K'}$.
Le théorème prouvé par MOCHIZUKI s'énonce alors simplement : il dit l'application naturelle (qu'on vient de décrire)

$$\bar{\Phi} : \mathrm{Isom}_{\mathbb{Q}_p}(K, K') \to \mathrm{Out}_{\mathrm{Filt}}(\Gamma_K, \Gamma_{K'})$$

est une bijection. La partie réellement intéressante du théorème est la suivante : si l'ensemble de droite est non vide, alors l'ensemble de gauche est non vide.

2.2 Plan de la preuve

La preuve se découpe en deux temps, très différents du point de vue des idées employées :

1. Soit K, K' deux corps p-adiques dont les groupes de GALOIS absolus sont liés par un isomorphisme α qui préserve la filtration. Soit V un $\mathbb{Q}_p$-espace vectoriel de dimension finie muni d'une action continue de Γ_K (et donc de $\Gamma_{K'}$, via α). Alors si on définit $d_V(i) = \dim_{\mathbb{Q}_p}((V(-i) \otimes_{\mathbb{Q}_p} \overline{K}^{\wedge})^{\Gamma_K})$ et $d'_V(i)$ similairement en remplaçant K par K', on a $d_V(i) = d'_V(i)$ (ici $V(-i)$ désigne V muni d'une action particulière de Γ_K, définie à l'aide du caractère cyclotomique). Par la suite, nous dirons que α préserve les poids de HODGE-TATE.
2. Soit K, K' deux corps p-adiques dont les groupes de GALOIS absolus sont liés par un isomorphisme α qui préserve les poids de HODGE-TATE. Alors K et K' sont isomorphes.

Ces deux parties m'ont pris des temps à peu près équivalents pour les comprendre. La deuxième est nettement plus difficile que la première du point de vue des idées (mais, en l'abordant, j'avais déjà compris beaucoup de choses qu'il n'y avait plus besoin de recomprendre). De ce point de vue là, cet article était assez bien adapté pour un stage.
Des explications plus précises sur la preuve sont présentes dans les notes de mon exposé final, jointes à la suite de cette section.

2.3 Théories mathématiques étudiées, lectures

Pour comprendre l'article de MOCHIZUKI, j'ai eu besoin :

— de connaissances générales sur les corps locaux (p-adiques), principalement obtenues par la lecture de *Corps Locaux* (SERRE) et de *Algebraic Number Theory* (NEUKIRCH) ;

— d'une compréhension de la théorie de la cohomologie des groupes, principalement obtenue par la lecture d'une publication très concise et claire d'Atiyah et Wall intitulée *Cohomology of groups* ;
— d'une connaissance élémentaire de la théorie des corps de classe locaux, principalement apportée par des explications directes de mon maître de stage et par la lecture d'une partie d'un cours de J.S. Milne intitulé *Class Field Theory* ;
— d'un peu de théorie de Hodge p-adique, notamment pour la compréhension d'un théorème, cité et prouvé dans *Abelian l-adic Representations and Elliptic Curves* (Serre).

2.4 Apport personnel

Mon apport personnel principal a été, puisque je ne suis pas familier de ce domaine et que je n'ai donc pas connaissance des arguments classiques, de « boucher les trous » dans la preuve, afin d'être convaincu de sa validité et de comprendre les passages balayés par Mochizuki soit par l'absence de détails là où il semble en falloir (j'ai dû me poser des questions comme « Mais comment récupère-t-il l'action de Γ_K ? Cet argument ne permet que de récupérer la structure d'anneau. », question qui s'est soldée par une invocation inattendue de la théorie de Kummer) soit par des ellipses déroutantes pour moi ("... and then conclude via a standard general nonsense argument." est une expression utilisée dans l'article, qui m'a conduit à lire des bouts d'un article sur la conjecture birationnelle anabélienne pour trouver le détail d'un argument similaire décrit proprement). Je n'ai pas eu le temps de m'intéresser aux diverses généralisations ou aux résultats connexes qui existent, ni de tenter de réfléchir à des questions ouvertes.

3 Notes d'exposé

Ce qui suit (à partir de la page suivante) est le document comportant mes notes (en anglais) pour l'exposé final, donné devant mon maître de stage et son collègue Zábrádi Gergely. Sans être forcément destiné à être relu par quelqu'un d'autre que moi, il contient un inventaire relativement complet (si on le compare à l'article initial) des remarques que j'ai dû rajouter à l'article pour qu'il soit compréhensible pour moi. Tout n'est pas écrit, et certains passages que j'étais parfaitement capable d'expliquer à l'oral sans notes sont décrits soit très rapidement soit pas du tout. Il s'agit de l'unique production mathématique écrite durant mon stage (outre mes innombrables brouillons et mes très nombreuses annotations et notes de lecture).

Filtration-preserving isomorphisms between absolute Galois groups of p-adic local fields are geometric

1 Introduction

Let K, K' be two fields and $\overline{K}, \overline{K'}$ two fixed separable closures of K, K'. Define $\Gamma_K = Gal(\overline{K} \mid K)$ and $\Gamma'_K = Gal(\overline{K'} \mid K')$.

1.1 History and motivation

As was proved partially by Neukirch and then completed by Uchida, Iwasawa and Ikeda, if K and K' are two algebraic number fields whose absolute Galois groups are isomorphic (as topological groups), then K and K' are isomorphic. To be more precise, if K, K' are two algebraic number fields, then :

$$Isom(K, K') \overset{\Phi}{\simeq} Out(\Gamma_K, \Gamma_{K'}) := Out(\Gamma_K, \Gamma_{K'})$$

Where where Φ is defined as such : if $f \in Isom(K, K')$, let $\tilde{f} \in Isom(\overline{K}, \overline{K'})$ be an isomorphism extending f. Then if $\phi \in \Gamma_K$, we define $\Phi(\phi)$ as the projection on $Out(\Gamma_K, \Gamma_{K'})$ of the morphism $\tilde{f} \circ \phi \circ \tilde{f}^{-1}$. It is clear that it doesn't depend on the choice of $\tilde{f}$ and therefore is well-defined. The theorem then states that Φ is a bijection.

This result lead to the question of knowing whether a similar result could be obtained for p-adic local fields.

1.2 The result

Mochizuki proved the following result : let p be a prime number ; if K, K' are two p-adic local fields and if there exists an isomorphism $\alpha : \Gamma_K \to \Gamma_{K'}$ such that the ramification groups of Γ_K (in the upper numbering) are mapped onto the corresponding ramification groups of $\Gamma_{K'}$ by α (we shall say that σ is filtration-preserving), then K and K' are isomorphic. More precisely :

$$Isom_{\mathbb{Q}_p}(K, K') \overset{\Phi}{\simeq} Out_{Filt}(\Gamma_K, \Gamma_{K'})$$

Where $Isom_{\mathbb{Q}_p}(K, K')$ is the set of isomorphisms between K and K' seen as $\mathbb{Q}_p$-algebras, $Out_{Filt}(\Gamma_K, \Gamma_{K'})$ is the set of filtration-preserving outer isomorphisms between their absolute Galois groups and Φ is defined similarly as before.

1.3 Why do we need filtration-preserving group isomorphisms ?

Let's assume the result as stated for algebraic number fields holds for p-adic local fields. Then we have, for any finite extensions K, K' of $\mathbb{Q}_p$, the following result :

$$Isom(K, K') \simeq Out(\Gamma_K, \Gamma_{K'})$$

In particular, for $K = K' = \mathbb{Q}_p$:

$$Aut(\mathbb{Q}_p) \simeq Out(\Gamma_{\mathbb{Q}_p})$$

Let's prove that $Aut(\mathbb{Q}_p) = 1$. Let σ be an element of $Aut(\mathbb{Q}_p)$. If σ is continuous (for the p-adic valuation), since $\mathbb{Q}$ is a dense σ-invariant subset of $\mathbb{Q}_p$, it follows that $\sigma = 1$. Therefore it suffices to proves that σ is continuous. We'll prove that it is actually valuation-preserving.

Let :

$$U = \{x \in \mathbb{Q}_p \mid v_p(x) = 0\}$$

Let's prove that $\sigma(U) \subset U$.

Let $x \in U$ and $\bar{x}$ its projection in $(\mathbb{Z}/p\mathbb{Z})^\times$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, for every n coprime with $p-1$ there will exist a $\bar{y} \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $(\bar{y})^n = \bar{x}$. If furthermore $p \nmid n$, we obtain by HENSEL's lemma a $y \in \mathbb{Q}_p$ such that $y^n = x$. Therefore, every element of U has n-th roots for an infinite number of values of n. This property is obviously invariant by an automorphism, and so elements of $\sigma(U)$ satisfy the same property. This means that if $x \in U$, then $v_p(\sigma(x))$ is divisible by an infinite number of integers, and therefore $v_p(\sigma(x)) = 0$. We obtain $\sigma(U) \subset U$ as desired.

Now if $v_p(x) = n$, we can write $x = p^n u$ where $u \in U$, and then $\sigma(x) = p^n\sigma(u)$, whence we get :

$$\forall x \in \mathbb{Q}_p, v_p(\sigma(x)) = v_p(x)$$

This proves that $Aut(\mathbb{Q}_p) = 1$. Now we need the additional knowledge that $Out(\Gamma_{\mathbb{Q}_p})$ is non-trivial [1], which leads to an immediate contradiction.

1.4 Plan of attack

Surprisingly enough, MOCHIZUKI's proof uses some results of p-adic HODGE theory. The proof can actually be divided into two parts :

1. Let K, K' two p-adic local fields whose absolute GALOIS groups are linked by a filtration-preserving isomorphism α. Let V be a finite dimensional $\mathbb{Q}_p$-vector space upon which Γ_K (and therefore $\Gamma_{K'}$) acts continuously. Then, if $d_V(i) = \dim_{\mathbb{Q}_p}((V(-i) \otimes_{\mathbb{Q}_p} \overline{K}^\wedge)^{\Gamma_K})$ and $d'_V(i)$ is defined similarly with K' instead of K, we have $d_V(i) = d'_V(i)$ (we shall say that α preserves HODGE-TATE weights).
2. Let K, K' two p-adic local fields whose absolute GALOIS groups are linked by an isomorphism which preserves HODGE-TATE weights. Then K and K' are isomorphic.

One of MOCHIZUKI's student, YUICHIRO HOSHI, went further to explore how geometric morphisms of GALOIS groups preserving properties linked with HODGE-TATE decompositions are, the word « geometric » meaning « arising from a field morphism ».

1.5 Notations

We fix a prime number p and a p-adic local field K. We define the following objects :

— $d = [K : \mathbb{Q}_p]$

— v_K is the valuation obtained by extending the p-adic valuation ;

— $\mathcal{O}_K$ is the ring of integers of K, m_K its only prime ideal and $U_K = \mathcal{O}_K^\times$;

— k is the residue field of $\mathcal{O}_K$, that is $\mathcal{O}_K/m_K$;

— $q = |k|$, and f is the integer such that $q = p^f$;

— $\bar{K}$ is a fixed separable closure of K ;

— $\Gamma_K = Gal(\bar{K} \mid K)$

We shall say that an object is "recovered group-theoretically" from Γ_K when if two fields K and K' satisfy $\Gamma_K \overset{\alpha}{\simeq} \Gamma_{K'}$ then the object associated to K and the one associated to K' are isomorphic and mapped one onto another by α (or the most natural isomorphism it induces).

2 What every isomorphism of absolute GALOIS groups preserves

2.1 Recovering the cyclotomic character

We want to be able to recover the character $\chi : \Gamma_K \to \mathbb{Z}_p$, defined by the action of Γ_K on the roots of unity in $\bar{K}$, group-theoretically. We notate $\mathbb{Z}_p(1)$ the module $\mathbb{Z}_p$ equipped with the Γ_K-action induced by χ.

Lemma 1. *We can recover the Γ_K-module $\mathbb{Z}_p(1)$ group-theoretically from Γ_K.*

Proof. Let M be a $\mathbb{Z}_p$-module of finite length equipped with a continuous Γ_K-action. We want to be able to tell whether M is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}(1)$ using only group-theoretic information. If we succeed, they we'll be able to recover the isomorphism classes of $\mathbb{Z}/p^n\mathbb{Z}(1)$ for every n and therefore $\mathbb{Z}_p(1)$ (by taking the inverse limit).

Let n be an integer and M be isomorphic as a $\mathbb{Z}_p$-module to $\mathbb{Z}/p^n\mathbb{Z}$. We need to be able to tell whether the Γ_K-action on M is the same as the one on $\mathbb{Z}/p^n\mathbb{Z}(1)$. We have the following isomorphism :

$$H^i(K, M) \simeq H^{2-i}(K, M^\vee(1))^\vee$$

Where "$\vee$" represents a PONTRYAGIN dual. First of all :

1. This fact is described in *Cohomology of Number Fields* by NEUKIRCH, SCHMIDT and WINGBERG, pp. 420ff.

$$H^2(K, \mathbb{Z}/p^n\mathbb{Z}(1)) = H^0(K, \mathbb{Z}/p^n\mathbb{Z}^\vee)^\vee = H^0(K, \mathbb{Z}/p^n\mathbb{Z})^\vee = \mathbb{Z}/p^n\mathbb{Z}^\vee = \mathbb{Z}/p^n\mathbb{Z}$$

So if $M \simeq \mathbb{Z}/p^n\mathbb{Z}(1)$, we have $H^2(K, M) = \mathbb{Z}/p^n\mathbb{Z}$. Conversely, if $H^2(K, M) \simeq \mathbb{Z}/p^n\mathbb{Z}$ then :

$$H^0(K, M^\vee(1)) \simeq \mathbb{Z}/p^n\mathbb{Z}^\vee = \mathbb{Z}/p^n\mathbb{Z}$$

Which means $M^\vee(1)$ is Γ_K-invariant, therefore :

$$M^\vee(1) \simeq \mathbb{Z}/p^n\mathbb{Z}$$

(in other words, it is equipped with a trivial action). Then :

$$M \simeq (M^\vee(1))^\vee(1) = (\mathbb{Z}/p^n\mathbb{Z}^\vee)(1) = \mathbb{Z}/p^n\mathbb{Z}(1)$$

So :

$$M \simeq \mathbb{Z}/p^n\mathbb{Z}(1) \Leftrightarrow H^2(K, M) \simeq \mathbb{Z}/p^n\mathbb{Z}$$

So we have a purely group-theoretic condition on M for it to be isomorphic to $\mathbb{Z}/p^n\mathbb{Z}(1)$. Which means we can recover every $\mathbb{Z}/p^n\mathbb{Z}(1)$ group-theoretically, and taking an inverse limit gives us the full cyclotomic character. □

2.2 Recovering q and d

Local class field theory gives us an isomorphism :

$$\Gamma_K^{ab} \overset{LCF_K}{\simeq} (K^\times)^\wedge$$

So that knowing Γ_K^{ab} is enough to recover the group $(K^\times)^\wedge$. Now we have the exact sequence :

$$0 \to U_K \overset{\subseteq}{\to} K^\times \overset{v_K}{\to} \mathbb{Z} \to 0$$

Which can be made into the following exact sequence (because the modulo operation is surjective) :

$$0 \to \widehat{U_K} \to (K^\times)^\wedge \to \widehat{\mathbb{Z}} \to 0$$

Now we know [2] that, for some integer a :

$$U_K \simeq \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$$

And it becomes clear that $\widehat{U_K} = U_K$. So we have a decomposition $(K^\times)^\wedge = U_K \times \widehat{\mathbb{Z}}$ (the exact sequence is split by the morphism $\mathbb{Z} \to K^\times$ which maps 1 to any uniformizing element $\pi \in \mathcal{O}_K$). What we want is to characterize algebraically each one of these terms so that they can be recovered algebraically too.

Let's write the full decomposition of $(K^\times)^\wedge$:

$$\begin{aligned}(K^\times)^\wedge &= \widehat{\mathbb{Z}} \oplus \underbrace{\mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d}_{U_K} \\ &= \left(\bigoplus_{q \neq p} \mathbb{Z}_q\right) \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^{d+1}\end{aligned}$$

What we can deduce of this decomposition is :

- The torsion subgroup of $(K^\times)^\wedge$ is $\mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z}$, and so by taking its prime-to-p part we can recover algebraically $\mathbb{Z}/(q-1)\mathbb{Z}$, and therefore the number $q = |k|$.
- The maximal pro-p quotient of $(K^\times)^\wedge$ is $\mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^{d+1}$, and by quotienting by its torsion group we recover algebraically $\mathbb{Z}_p^{d+1}$, and therefore the number $d = [K : \mathbb{Q}_p]$.

So, q (and therefore f) and d are entirely determined by Γ_K^{ab}.

2. cf. for example *Algebraic Number Theory* by Neukirch, pp.135-141

2.3 Recovering the inertia subgroup

Let H be an open subgroup of Γ_K corresponding to a finite extension $L = \overline{K}^H$ of K (we have $\Gamma_L = H$).

From the last subsection, we can deduce that the number q_L of elements of the residue field of L (and therefore f_L) and the dimension $[L : \mathbb{Q}_p]$ can be recovered group-theoretically from H.

Let's write $q_L = p^{f_L} = q^{f_{L|K}}$ and $q = p^{f_K}$. It follows that $f_{L|K} = \frac{f_L}{f_K}$. Moreover, we know that L is unramified as an extension of K if and only if $e_{L|K} = 1$ (that is, $f_{L|K} = [L : K] = [\Gamma_K : H]$). Since we can recover group-theoretically f_L, f and that we can compute $[\Gamma_K : H]$ from Γ_K and H, it follows that we can always know whether an open subgroup of Γ_K corresponds to an unramified extension of K. By intersecting every open subgroup which does correspond to an unramified extension of K, we obtain the subgroup associated with the maximal unramified extension of K, that is the inertia subgroup of Γ_K.

Therefore, the inertia subgroup of Γ_K can be recovered group-theoretically from Γ_K.

2.4 Recovering the Γ_K-module $\overline{K}$

We have a homomorphism $\log : K^\wedge \to K$.

Lemma 2. *The restriction of* log *induces an isomorphism from U_K modulo torsion to an open subgroup of K (the additive group).*

Proof. First, the logarithm of a torsion element of 0, so the map $U_K/U_{K\text{tors}} \to K$ is well-defined. Now let's show that it is injective.

Recall that if $v_{m_K}(z) > \frac{e}{p-1}$, then [3] $v_{m_K}(\log(1+z)) = v_{m_K}(z)$.

Now assume that for a $x \in m_K$ we have $\log(1+x) = 0$. We need to prove that $1+x$ is in the torsion subgroup [4]. We know that $v_{m_K}(x) > 0$, so for n big enough we'll have $v_{m_K}(x^{p^n}) > \frac{e}{p-1}$. Let's compute $v_{m_K}((1+x)^{p^n} - 1)$:

$$\begin{aligned} v_{m_K}((1+x)^{p^n} - 1) &= v_{m_K}\left(\sum_{j=1}^{p^n} \binom{p^n}{j} x^j\right) \\ &\geq \min\left(\min_{1\leq j\neq p^n}\left(v_{m_K}\left(\binom{p^n}{j} x^j\right)\right), v_{m_K}\left(x^{p^n}\right)\right) \\ &\geq \min\left(\min_{1\leq j\neq p^n}\left(v_{m_K}(p) + j\right), v_{m_K}\left(x^{p^n}\right)\right) \\ &> \min\left(e, \frac{e}{p-1}\right) = \frac{e}{p-1} \end{aligned}$$

From this we can deduce :

$$v_{m_K}((1+x)^{p^n} - 1) = v_{m_K}(\log(1+x)^{p^n}) = p^n v_{m_K}(\log(1+x)) = +\infty$$

And therefore $(1+x)^{p^n} - 1 = 0$, whence we deduce that $1+x$ is in the torsion subgroup.

Now let's show that $\log(U_K)$ is an open subgroup of K. Let $y = \log(x)$, $x \in U_K$. Choose a z such that $n := v_{m_K}(z-y) > \frac{e}{p-1}$, then $z - y = \log(u)$ where u is an element of $U^{(n)}$, and $z = y + \log(u) = \log(x) + \log(u) = \log(xu)$ with $xu \in U_K$. So we have a ball around y included in $\log(U_K)$ which proves the openness of $\log(U_K)$, which is obviously a subgroup of the additive group K. □

So, the p-adic logarithm defines an isomorphism between U_K modulo torsion and an open subgroup H of K. It is clear that $H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq K$ and therefore we have an isomorphism $U_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq K$ (there is no need to eliminate the torsion because it is removed when we localize). We shall call this isomorphism log as well.

If we have a subgroup $\Gamma_L \subset \Gamma_K$ corresponding to a finite extension $L \mid K$, we can write the following commutative diagram :

$$\begin{array}{ccc} U_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p & \xrightarrow{\subseteq} & U_L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \\ \big\downarrow{\scriptstyle \log} & & \big\downarrow{\scriptstyle \log} \\ K & \xrightarrow{\quad\subseteq\quad} & L \end{array}$$

We also have these two exact sequences :

3. Because for $n > \frac{e}{p-1}$, log is an isomorphism between $U^{(n)}$ and m_K^n, cf. *Algebraic Number Theory* by Neukirch, pp.136-137
4. It is enough to do this verification for elements in $U^{(1)}$ because $U_K = \mu_{q-1} \times U^{(1)}$ and μ_{q-1} is a torsion group.

$$\begin{array}{ccccccccc} 1 & \to & I_K^{ab} & \to & \Gamma_K^{ab} & \to & Gal(K^{nr} \mid K)^{ab} & \to & 1 \\ 1 & \to & U_K & \to & (K^\times)^\wedge & \to & \widehat{\mathbb{Z}} & \to & 0 \end{array}$$

Where K^{nr} is the maximal non-ramified extension of K and I_K is the inertia subgroup (i.e. $Gal(\bar{K} \mid K^{nr})$). Now the local class field theory gives isomorphisms :

$$\Gamma_K^{ab} \simeq (K^\times)^\wedge$$

$$\begin{aligned} Gal(K^{nr} \mid K)^{ab} &\simeq \varprojlim_{L|K \text{ non-ramified}} Gal(L \mid K)^{ab} \\ &\simeq \varprojlim_{L|K \text{ non-ramified}} K^\times / N_{L|K} L^\times \\ &\simeq \varprojlim_{L|K \text{ non-ramified}} (\pi)U_K/(\pi^d)U_K \simeq \varprojlim_{d \in \mathbb{N}} \mathbb{Z}/d\mathbb{Z} \simeq \widehat{\mathbb{Z}} \end{aligned}$$

(We used $K^\times = (\pi)U_K$, $L^\times = (\pi^d)U_L$ and $N_{L|K}U_L = U_K$, where $d = [L : K]$)

And therefore (because of the two exact sequences) there must be an isomorphism $U_K \simeq I_K^{ab}$, which means we can recover U_K (and similarly for U_L) group-theoretically (using the previous subsection to recover the inertia subgroup).

We also need to recover the inclusion morphism $U_K \to U_L$. In terms of absolute Galois groups, they correspond to the transfer/Verlagerung map [5] $Ver : \Gamma_K^{ab} \to \Gamma_L^{ab}$. In other words we have the following commutative diagram :

$$\begin{array}{ccc} U_K & \xrightarrow{\subseteq} & U_L \\ \wr\vert & & \wr\vert \\ I_K^{ab} & \xrightarrow{Ver} & I_L^{ab} \end{array}$$

Now the Verlagerung is a purely algebraic construction, computed using only the inertia subgroups, which we can recover, and therefore the morphism $U_K \to U_L$ can be recovered group-theoretically.

This means we can also recover the morphisms $U_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to U_L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and subsequently $K \to L$.

We have the isomorphism given by Kummer theory :

$$H^1(\Gamma_L, \mu_n(1)) \simeq L^\times/(L^\times)^n$$

(we used that $\bar{K}^n = \bar{K}$ because it's the separable closure)

We know that we can recover $H^1(\Gamma_L, \mu_\infty(1))$ from Γ_L group theoretically, because we only need the corresponding cyclotomic character. Now there is an action of Γ_K on $H^1(\Gamma_L, \mu_n)$: if ϕ is a 1-cocycle $\Gamma_L \to \mu_n$, $g \in \Gamma_K$ and $g' \in \Gamma_L$, we define $(g.\phi)(g') = g.\phi(g')$. Being defined using the cyclotomic character for Γ_K, this action can be algebraically recovered. This action is sent onto the natural action of Γ_K on $L^\times/(L^\times)^n$ by the Kummer isomorphism [6] . Therefore we can recover the Γ_K-action on $L^\times/(L^\times)^n$ group-theoretically.

By taking inverse limits on both sides :

$$H^1(\Gamma_L, \mu_\infty(1)) \simeq \widehat{L^\times}$$

Which proves that we can recover the Γ_K-module $\widehat{L^\times}$ (and therefore the Γ_K-action on L). Doing this for all subgroups of Γ_K of finite index, we can obtain every finite extension L as a Γ_K-module.

3 Filtration-preserving isomorphisms preserve Hodge-Tate weights

3.1 Recovering $\mathcal{O}_K$

Remember that we know $f_K = \log_p(q)$ and therefore $e_K = \frac{[K:\mathbb{Q}_p]}{f_K}$.

Assume that we know an inertia subgroup Γ_K^v for some $v = re_K$ with $r \geq 2$. Then, by local class field theory, we also know $U_K^v = 1 + m_K^v$ (which is its direct image by the isomorphism between Γ_K^{ab} and $\widehat{K^\times}$).

5. cf. *Algebraic Number Theory* by Neukirch, pp.296-297

6. Let $g \in \Gamma_K$ and $a \in L^\times$ such that $a = \alpha^n$ ($\alpha \in \bar{K}$). Then the image of a is $\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$ and the image of $g.a = (g.\alpha)^n$ is $\sigma \mapsto \frac{\sigma(g.\alpha)}{g.\alpha} = g.\left(\frac{\sigma(\alpha)}{\alpha}\right)$.

Moreover, the logarithm defines an isomorphism between U_K^v and m_K^v (because $v > e_K \geq \frac{e_K}{p-1}$), and the fact that $\log(u^{p^{-r}}) = p^{-r}\log(u)$ shows that the logarithm also defines an isomorphism between $p^{-r}U_K^v$ and $p^{-r}m_K^v = \mathcal{O}_K$ (the last equality is true because $p^n\mathcal{O}_K = m_K^{e_K n}$).

Thus, we can recover the Γ_K-module $\mathcal{O}_K$ using only the information we assumed we knew (Γ_K^v, v and e_K). This can be summarized by this figure :

$$\Gamma_K^v \xrightarrow{\text{LCF}} U_K^v \to p^{-r}U_K^v \xrightarrow{\log} \mathcal{O}_K$$

3.2 Finite extensions, and where the filtration-preserving hypothesis is used

Let Γ_L be a subgroup of Γ_K of finite index and L the corresponding finite extension of K. In a similar fashion to what we just dit, if suffices to know a Γ_L^v for some $v = re_L$ ($r \in \{2, 3, \ldots\}$) to recover $\mathcal{O}_L$.

For some fixed number v, let's try to recover Γ_L^v using only knowledge about Γ_K and its ramification subgroups, in the upper numbering.

$$\Gamma_L^v = (\Gamma_L)_{\psi_{\bar{L}|L}(v)} = (\Gamma_K)_{\psi_{\bar{L}|L}(v)} \cap \Gamma_L = (\Gamma_K)^{\varphi_{\bar{K}|K}(\psi_{\bar{L}|L}(v))} \cap \Gamma_L$$

Here, it was necessary to use the lower numbering because it is the appropriate one for subgroups.

We know that : $\varphi_{\bar{K}|K} = \varphi_{L|K} \circ \varphi_{\bar{K}|L} = \varphi_{L|K} \circ \varphi_{\bar{L}|L} = \varphi_{L|K} \circ \psi_{\bar{L}|L}^{-1}$ and thus : $\varphi_{\bar{K}|K} \circ \psi_{\bar{L}|L} = \varphi_{L|K}$.

So, to compute Γ_L^v, we need to know the function $\varphi_{L|K}$. Its inverse map is $\psi_{L|K}$ whose definition is :

$$\psi_{L|K}(v) = \int_0^v (G^0 : G^w)dw$$

To compute that, we need to know $G^0 = (\Gamma_K/\Gamma_L)$ and $G^w = (\Gamma_K/\Gamma_L)^w = \Gamma_K^w\Gamma_L/\Gamma_L$. Notice that this time the upper numbering was used, because we have quotients. To compute G^w, it is clear that we need to know the group Γ_K^w for every $w \in]0, v[$. This is the reason why knowing only some ramification subgroups isn't enough (otherwise, there is no way to link the upper numbering and the lower one).

If we know Γ_K^w for every $w \in]0, v[$, then we also know Γ_L, Γ_L^v and finally $\mathcal{O}_L$ (similarly to what we did with K) .

In particular, if we know Γ_K^w for every $w \in \mathbb{R}$, we can recover $\mathcal{O}_K$ but also the Γ_K-module $\mathcal{O}_L$ associated with every subgroup of Γ_K corresponding to a finite extension (the argument to recover the action is the same as to recover the Γ_K-action on L).

3.3 Recovering $\mathcal{O}_{\bar{K}}$ and $\bar{K}^\wedge$

Consequently, if we know all the ramification groups, we can recover the Γ_K-module :

$$\mathcal{O}_{\bar{K}} = \varinjlim_{L|K \text{ finite extension}} \mathcal{O}_L$$

and therefore we can also recover $\bar{K}^\wedge$, which is the p-adic completion of $\mathcal{O}_{\bar{K}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We needed to recover $\mathcal{O}_{\bar{K}}$ for this, in order to be able to reconstruct the p-adic valuation on $\bar{K}$ and to compute the p-adic completion.

3.4 Recovering Hodge-Tate weights

We recovered $\bar{K}^\wedge$ as a Γ_K-module.

Let V be a finite dimensional $\mathbb{Q}_p$-vector space upon which Γ_K acts continuously. We want to compute :

$$V(-i) = V \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(-1)^{\otimes i} = V \otimes_{\mathbb{Q}_p} Hom(\mathbb{Q}_p(1), \mathbb{Q}_p)^{\otimes i}$$

Where $\mathbb{Q}_p(1) = \mathbb{Z}_p(1) \otimes \mathbb{Q}_p$ and $\mathbb{Z}_p(1)$ is obtained via a projective limit of Γ_K-modules :

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}(1)$$

The action of Γ_K on $\mathbb{Z}/p^n\mathbb{Z}$ being given by its action on the primitive p^n-th roots of unit in $\bar{K}$, which we can recover (it's the cyclotomic character). Therefore we know $V(-i)$ and thus $V(-i) \otimes_{\mathbb{Q}_p} \bar{K}^\wedge$ with its Γ_K-action. It is clear that we can compute the dimension of the space of its Γ_K-invariants, that is $d_V(i)$.

Therefore, we proved the first half of the theorem.

4 Isomorphisms which preserve Hodge-Tate weights are geometric

4.1 Uniformizing modules

Here is the crucial part of the theorem. Mochizuki defines the following notion :

Definition 3 (Uniformizing module). *Let E be a finite* Galois *extension of $\mathbb{Q}_p$ containing K and V be a $E[\Gamma_K]$-module of dimension one over E, so that the action of Γ_K on V is given by a representation $\rho_V : \Gamma_K^{ab} \to E^\times$ satisfying, for $g \in \Gamma_K$ and $x \in V$, $g.x = \rho_V(g).x$.*

V is said to be uniformizing if there exists an open subgroup I of U_K and a morphism $f : K \to E$ such that the following diagram commutes :

$$\begin{tikzcd} & U_K \arrow[r, "\subseteq"] & K \arrow[r, "f"] & E \\ I \arrow[ur, "\subseteq"] \arrow[r, "\subseteq"] & U_K \arrow[r, "LCF"] & \Gamma_K^{ab} \arrow[r, "\rho_V"] & E^\times \arrow[u, "\subseteq"'] \end{tikzcd}$$

The very powerful remark by Mochizuki, deduced from a result by Serre is the following lemma :

Lemma 4. *V is uniformizing if and only if $d_V(0) = [E : K]([K : \mathbb{Q}_p] - 1)$ and $d_V(1) = [E : K]$.*

Thanks to this lemma, we can know whether V is uniformizing by only looking at the Hodge-Tate weights, which we know. We will prove this lemma later. Let us first see how it allows us to conclude.

4.2 Existence of a uniformizing V

Lemma 5. *If E is a finite* Galois *extension of $\mathbb{Q}_p$ which contains K, then there exists a uniformizing $E[\Gamma_K]$-module of dimension one over E.*

Proof. Our goal is to construct a morphism $\rho_V : \Gamma_K^{ab} \to E^\times$ such that this diagram commutes (for $I = U_K$ and f the inclusion morphism) :

$$\begin{tikzcd} U_K \arrow[r, "\subseteq"] \arrow[d, "\subseteq"] & E^\times \\ (K^\times)^\wedge \arrow[r, "LCF"] & \Gamma_K^{ab} \arrow[u, "\rho_V"] \end{tikzcd}$$

One very easy way to do that is to use the morphism $\Gamma_K^{ab} \to U_K$ given by the decomposition :

$$\Gamma_K^{ab} \simeq (K^\times)^\wedge = \widehat{\mathbb{Z}} \oplus \underbrace{\mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d}_{U_K}$$

Obviously, this morphism restricted to U_K is the identity. □

4.3 The key argument

Let K, K' be two local p-adic fields and $\alpha : \Gamma_K \simeq \Gamma_{K'}$ an isomorphism which preserves Hodge-Tate weights. Let E be a Galois extension of $\mathbb{Q}_p$ which contains both K and K' and V be a uniformizing $E[\Gamma_K]$-module.

Using α, we can define an action of $\Gamma_{K'}$ on V, so V can be seen as a $E[\Gamma_{K'}]$ module (which we'll note V'). The Hodge-Tate weights of V and V' are the same, which means that V' is also uniformizing (as we saw, we can recover $[K : \mathbb{Q}_p]$ group-theoretically from Γ_K^{ab} and we can obviously compute $[E : \mathbb{Q}_p]$).

So, using the definition of a uniformizing module, there exists open subgroups $I_1 \subseteq U_K$ and $I_2 \subseteq U_{K'}$ and morphisms $f : K \to E$, $f' : K' \to E$ such that the diagram in the definition commutes. Now note $\Xi : U_K \simeq U_{K'}$ the isomorphism induced by the local class field isomorphism (cf. first section to see why we can recover U_K from Γ_K^{ab}) and define $I = I_1 \cap \Xi^{-1}(I_2)$ and $I' = I_2 \cap \Xi(I_1)$. These are isomorphic open subgroups of U_K and $U_{K'}$ respectively which can be checked to both satisfy the uniformizing hypothesis (we will note $\alpha_I : I \simeq I'$ the restricted isomorphism). Thus, we have this big commutative diagram :

$$\begin{tikzcd}
 & U_K \arrow[r, "\subseteq"] & K \arrow[r, "f"] & E \\
I \arrow[ur, "\subseteq"] \arrow[r, "\subseteq"] \arrow[d, "\alpha_I"] & U_K \arrow[r, "LCF"] \arrow[d, "\Xi"] & \Gamma_K^{ab} \arrow[r, "\rho_V"] \arrow[d, "\alpha"] & E^\times \arrow[u, "\subseteq"] \arrow[d, leftrightarrow, "Id_{E^\times}"] \\
I' \arrow[r, "\subseteq"] \arrow[dr, "\subseteq"] & U_{K'} \arrow[r, "LCF"] & \Gamma_{K'}^{ab} \arrow[r, "\rho_{V'}"] & E^\times \arrow[d, "\subseteq"] \\
 & U_{K'} \arrow[r, "\subseteq"] & K' \arrow[r, "f'"] & E
\end{tikzcd}$$

It is clear on this diagram that $f(I) = f'(I')$. Now let's prove the following lemma (we state and prove it for K and I, but it obviously holds for K' and I').

Lemma 6. *I generates K as a $\mathbb{Q}_p$-vector space.*

Proof. Let Z be the $\mathbb{Q}_p$-sub vector space of K generated by I. For the p-adic topology, U_K is an open subset of K (because K is a local field), and I is an open subset of U_K so I is open in K.

Let $z \in Z$. We know that $z + I = \{z + i \mid i \in I\} \subset Z$ by definition of Z, and $z + I$ is open in K (because I is). Therefore, Z is open in K (each element of Z is surrounded by an open neighbourhood in Z).

Let's prove that a strict subspace of K is not open. Assume P is a strict subspace of K. Let a be an element of $K \setminus P$, then $(p^n a)_{n\in\mathbb{N}}$ is a sequence of elements of $K \setminus P$ whose limit is $0 \in P$, so $K \setminus P$ is not closed, therefore P is not open.

Therefore, Z being an open subspace, we have $Z = K$, which completes the proof of the lemma. □

So we have :

$$f(K) = f(\langle I \rangle) = \langle f(I) \rangle = \langle f'(I') \rangle = f'(\langle I' \rangle) = f'(K')$$

Hence $f(K) = f'(K')$ is a subfield of E isomorphic to both K and K', which means K and K' are isomorphic fields, therefore proving the result.

The final result, as stated in the introduction, can be obtained by seeing that the field isomorphism constructed here is sent to α by the function Φ described before. The key point is that the field isomorphism and the group isomorphism can be compared on U_K, thanks to local class field theory, and that they are mapped onto each other if and only if they are equal on U_K, proving both injectivity and surjectivity.