GALOIS REPRESENTATIONS

Msc thesis

by

Péter Kutas

Advisor: Gergely Zábrádi
Department of Algebra and Number Theory
Eötvös Loránd University

Contents

0 Introduction

Galois-representations are finite-dimensional representations of absolute Galois groups. The most important example is the absolute Galois group of $\mathbb{Q}$.Why is this an important question? According to the Tannakian philosophy one can reconstruct a group from the category of its finite dimensional representations. This group is of great importance in algebraic number theory. The following is a very important question formulated first by Emmy Noether:

Question 1. *Is every finite group a Galois group of a finite extension of* $\mathbb{Q}$.

An equivalent formulation of this is that every finite group is a quotient of $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$. As it turns out studying the groups $\mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p)$ is an important tool in studying the absolute Galois group of $\mathbb{Q}$. So in this thesis I will give a short introduction to this theory.

The first chapter will give a short introduction to the theory of local fields. This is mainly based on [N 10] and [M1 7]. The second and third chapter are about Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p)$. However there is a big difference between representations on vector space over $\mathbb{Q}_p$ and on a vector space over $\mathbb{Q}_l$ where $l \neq p$. The second chapter discusses the case $l \neq p$. This is much easier than the other case and much more is known about it. However the whole theory is so large that I only wanted to give a general picture. The main theorem here is Grothendieck's monodromy theorem. At the end of the chapter I give a brief introduction of étale cohomology as it is a very useful tool studying l-adic representations. The third chapter deals with p-adic representations. The main goal here is to prove Fontaine's theorem which states that the category of finite dimensional $\mathbb{Q}_p$-representations of $\mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p)$ is equivalent to the category of étale (ϕ, Γ)-modules over $B_{\mathbb{Q}_p}$. This is a fundamental result in the theory of p-adic Galois representations. The theory of p-adic Galois representations is difficult and not much is known to this day. However, this area is given increasing interest over the years. The fourth chapter is about the local Langlands programme which is the main focus in this area. In the l-adic case we state the result of Harris and Taylor which proves the Langlands conjecture in that case. In the p-adic case we state Colmez's result which proves the Langlands correspondence for 2-dimensional representations. However if we consider higher dimension, we do not even know the exact formulation of such a conjecture (it is likely that the classical Langlands correspondence does not hold in that case).

I am deeply thankful for the help Gergely Zábrádi provided me during the writing of the thesis. His help doesn't only consisted of consulting and correcting errors but also of of great encouragement. I also like to thank my family and friends for their constant support.

1 Local fields

In this section we will study the field of p-adic numbers and their extensions. In order to define the field of p-adic numbers we will start with the notion of an absolute value.

Let K be a field. An **absolute value** is a function $x \mapsto |x| : K \to \mathbb{R}$ with the following properties.

1. $|x| \geq 0$ and $|x| = 0 \iff x = 0$
2. $|xy| = |x||y|$
3. $|x| + |y| \geq |x + y|$

The third property is known as the triangle inequality. We call an absolute value **nonarchimedian** if the following stronger version of the triangle inequality holds:

3.' $|x + y| \leq \max(|x|, |y|)$

This property is called the **ultrametric** property.

Example 1.1. *1. For any number field K and embedding $\sigma : K \mapsto \mathbb{C}$, $|a| = |\sigma(a)|$ defines an archimedian absolute value (the usual absolute value of $\mathbb{C}$). We will deonte this by $||_\infty$*

*2. Let r be a rational number and p a prime number. Lets write r in the following form: $r = \frac{a}{b} \cdot p^k$, where $(a, b) = 1$ and p does not divide either a nor b. Then $|r| = p^{-k}$ will define an absolute value on $\mathbb{Q}$ which is nonarchimedian.This is called the **p-adic absolute value** and will be referred to as $|\cdot|_p$*

An absolute value on a number field makes the number field into a metric space, hence creates a topology. Nonarchimdean topology is very different from the archimedian one. Some strange strange properties are mentioned in the following proposition.

Proposition 1.2. *1. The set $\{m \cdot 1 | m \in \mathbb{Z}\}$ is bounded.*

2. The set $\{|x| \leq 1 | x \in K\}$ is closed under additon.

3. If two spheres intersect then one contains the other.

Proof. The first two are trivial consequences of the ultrametric property. In order to prove the third we will define the following notion:

$D(a, r) = x \in K | |x - a| < r$

We will show that if $b \in D(a, r)$ then $D(a, r) = D(b, r)$. First we show, that $D(b, r) \subseteq D(a, r)$. $x \in D(b, r)$ means, that $|x-b| < r$. $|x-a| = |(x-b)+(b-a)| \leq \max(|x - b|, |b - a|) < r$ because $b \in D(a, r)$. Now we show that $D(a, r) \subseteq D(b, r)$. $x \in D(a, r)$ means, that $|x - a| < r$. $|x - b| = |(x - a) + (a - b)| \leq \max(|x - a|, |b - a|) < r$ and we are done. Here we used that $|x| = | - x|$ which is a trivial consequence of the definition. □

Actually the first property characterizes nonarchimedian absolute values:

Proposition 1.3. *An absolute value is nonarchimedian if an only if the set* $\{m \cdot 1 | m \in \mathbb{Z}\}$ *is bounded.*

The proof is left to the reader. The following corollary is even more interesting:

Corollary 1.4. *If char* $K \neq 0$ *then* K *has only nonarchimedian absolute values.*

Proof. The set $\{m \cdot 1 | m \in \mathbb{Z}\}$ is finite, hence bounded. □

Our first goal will be to classify absolute values on $\mathbb{Q}$. We consider two absolute values **equivalent** if they define the same topology. This definition is rather difficult to check, however the following is true.

Proposition 1.5. *Let* $|\cdot|_1$ *and* $|\cdot|_2$ *be two equivalent absolute values on a field* K*. Then there exists* $s > 0$ *that:*

1. $||_1 = ||_2^s$

For inequivalent absolute values we have a statement which is very similar to the Chinese remainder theorem.

Theorem 1.6 (Approximation theorem)**.** *Let* $||_1, \ldots, ||_n$ *be pairwise inequivalent absolute values of the field* K *and let* $a_1, \ldots, a_n \in K$ *be given elements. Then for every* $\epsilon > 0$ *there exists an* $x \in K$ *such that*

$$|x - a_i|_i < \epsilon \text{ for all } i = 1, \ldots, n \tag{1}$$

We will not prove this but will use it later.A proof can be found in [10]. Now we are ready to state Ostrowski's theorem.

Theorem 1.7 (Ostrowski)**.** *Let* $|\cdot|$ *be a nontrivial absolute value on* $\mathbb{Q}$*. Then:*

1. *If* $|\cdot|$ *is archimedian then it is quivalent to* $|\cdot|_\infty$
2. *If* $|\cdot|$ *is nonarchimedian then it is equivalent to* $|\cdot|_p$ *for exactly one prime* p

Proof. Let $||$ be a nonarchimedian absolute value on $\mathbb{Q}$. Then as we have proved $|n| \leq 1$. There exists a prime number p such that $|p| < 1$ because then for every $r \in \mathbb{Q}^*$ we would have $|r| = 1$ because an absolute value is multiplicative and each integer is a product of primes. The set $A = a \in \mathbb{Z} | |a| < 1$ is an ideal of $\mathbb{Z}$ satisfying $p\mathbb{Z} \subseteq A \neq \mathbb{Z}$ and since $p\mathbb{Z}$ is a maximal ideal they are equal. Let $a \in \mathbb{Z}$ and $a = bp^m$ with $(p, b) = 1$. Then $|b| = 1$ because b is not in A. Hence $|a| = |p|^m = |a|_p^s$ where $||_p$ denotes the p-adic absolute value and $s = -\log|p|/\log p$. Hence $||$ is equivalent to the p-adic absolute value.

Now let $||$ be archimedian. Let $m, n > 1$ be two natural numbers. We may write

$$m = a_0 + a_1 n + \ldots !a_r n^r \tag{2}$$

where $a_i \in 0, 1, \ldots, n-1$ and $n^r \leq m$(this is the key step of the proof). Hence, observing that $r \leq \log m/\log n$ and $|a_i| \leq a_i|1| \leq n$ one gets the inequality

$$|m| \leq \sum |a_i||n|^i \leq \sum |a_i||n|^r \leq (1 + \frac{\log m}{\log n}) n \cdot |n|^{\log m/\log n}. \tag{3}$$

Substituting here m^k for m, taking k-th roots on both sides and letting k tend to ∞, one obtains

$$|m| \leq |n|^{\log m \log n}, \text{ or } |m|^{1 \log m} \leq |n|^{1 \log n}. \tag{4}$$

Swapping m with n gives the following identity:

$$|m|^{1 \log m} = |n|^{1 \log n} \tag{5}$$

Putting $c = |n|^{1 \log n}$ we have $|n| = c^{logn}$ and putting $c = e^s$ yields, for every positive rational number $r = a/b$:

$$|r| = e^{slogr} = |r|^s. \tag{6}$$

Therefore $||$ is equivalent to $||_\infty$, the usual absolute value on $\mathbb{Q}$. □

So now we have classified the absolute values on $\mathbb{Q}$. There are several ways to construct real numbers from the field of rational numbers. One approach is the 'complete' $\mathbb{Q}$. The field of rational numbers is not complete in the sense that not every Cauchy sequence converges. One way to contruct real numbers is to consider the equivalence classes of Cauchy sequences constituting of rational numbers(we consider two sequences a_{nn} and b_{nn} equivalent if $a_n - b_{nn}$ tends to zero). Their multiplication, and addition will be coordinatewise. We will not go into details here but the resulting field will be the field of real numbers. In this contruction we considered the usual (archimedian) absolute value of $\mathbb{Q}$. Actually the following generalization of Ostrowski's theorem is true:

Theorem 1.8. *Let K be a field which is complete with respect to an archimedian absolute value $||$. Then there is an isomorphism σ from K onto $\mathbb{R}$ or $\mathbb{C}$ satisfying*
$|a| = |\sigma a|^s$ for all $a \in K$
for some fixed $s \in (0, 1]$.

The proof can be found in [10]. The result shows that if we want to study archimedian absolute values, then there is actually 'nothing' to study, complete fields are just $\mathbb{R}$ and $\mathbb{C}$. Let us observe that we can make the same construction in the nonarchimedian case! So we take the rational numbers and complete with respect to the p-adic absolute value for some prime p. This way we get the field of **p-adic numbers**, denoted by $\mathbb{Q}_p$. This construction is very natural and is due to the Hungarian mathematician József Kürschák. However it is not easy to handle equivalence classes of Cauchy sequences in terms of counting. So we will now describe the p-adic numbers in a different way which is similar to the decimal expansion of real numbers.

Theorem 1.9. *Every p-adic number can be written in the following form:*
$a_{-n}p^{-n} + \ldots + a_0 + a_1 p + a_2 p^2 \ldots$
where $a_i \in 0, 1, \ldots, p-1$. Additon, multiplication

A proof can be found in [7]. Now we will introduce a notion which is very closely related to the notion of absolute values. However later for technical reasons it will be important.

Definition 1.10. *A valuation is a function $v : K \mapsto \mathbb{R} \cup \infty$ verifying the properties*

1. $v(x) = \infty \iff x = 0$

2. $v(xy) = v(x) + v(y)$

3. $v(x+y) \geq \min(v(x), v(y))$

Let us observe that if we have an absolute value $||$ on K then $v(x) = -\log|x|$ for $x \neq 0$ and $v(0) = \infty$ will be a valuation on K.

Proposition 1.11. *The subset $O = \{x \in K | v(x) \geq 0\}$ is a ring with group of units $O^* = x \in K | v(x) = 0$ and the unique maximal ideal $P = \{x \in K | v(x) > 0\}$.*

O is an integral domain with field of fractions K and is also a valuaton ring. O/P is field (because P is maximal) and is called the **residue class field** of K. A valuation is called **discrete** if $v(K^*) = s\mathbb{Z}$ with some $s > 0$. It is called **normalized** if s=1. Dividing by s we may always pass tp a normalized valuation without changing O, O^*, P. Let us observe that every element of K^* can be written in the following form:

$x = u\pi^m$

where $m \in \mathbb{Z}$, $u \in O^*$, $v(\pi) = 1$ for some $\pi \in O$ and π is a prime element of O. The following proposition describes the structure of O

Proposition 1.12. *O is a principal ideal domain, hence a discrete valuation ring(beacuse it has a unique maximal ideal).*

It is easy to see that the p-adic valuation we defined is a discrete valuation.$\mathbb{Q}_p$ was also complete with respect to this valuation. A natural question is the following: what is $O, O^*, P, O/P$ in the case of p-adic numbers. It is quite easy to compute, however we leave the details to the reader but we will sum up the results in the next proposition.

Proposition 1.13.

$O = a_0 + a_1 p + a_2 p^2 \ldots | a_i \in 0, 1, \ldots, p-1$. *These numbers are called **p-adic integers** and the set will be denoted by $\mathbb{Z}_p$*

$O* = a \in O | a_0 \neq 0$

$P = a \in O | a_0 = 0$

$O/P = \mathbb{F}_p$

An important remark is that $\mathbb{Z}_p$ can also be realized as the projective limit of $\mathbb{Z}/p^n\mathbb{Z}$(This is easy to see from the first part of the proposition). We saw earlier how we can represent p-adic numbers as infinite series. This is usually very useful in terms of computations. Now our next goal will be to s how that if we have a field which is complete with respect to a valuation also admits such a representaion. We will denote the completitions of O and K with $\hat{O}$ and $\hat{K}$ respectively.

Theorem 1.14. *Let $R \subseteq O$ be a system of representatives for $\kappa = O/P$, such that $0 \in R$ and let $\pi \in O$ be a prime element. Then every $x \neq 0$ in $\hat{K}$ admits a unique representaion as a convergent series*

$$x = \pi^m (a_0 + a_1 \pi + \ldots) \tag{7}$$

where $a_i \in R$, $a_0 \neq 0$,$m \in \mathbb{Z}$.

Proof. First we will prove that

$$\hat{O}/\hat{P} \cong O/P \tag{8}$$

Let us consider the homomorphism $O \to \hat{O}/\hat{P}$, $a \mapsto a \mod P$. Its kernel is P. For every $x \in \hat{O}$ there exists an $a \in O$ such that $v(x-a) \geq 1$ therefore $x - a \in \hat{P}$ hence $x \equiv a \mod \hat{P}$. So this maps is also surjective and the homomorphism theorem gives us the needed isomorphism. Now we will use this result to prove the original theorem. Let $x = \pi^m u$ with $u \in \hat{O}*$. Since $\hat{O}/\hat{P} \cong O/P$, the class $u \mod \hat{P}$ has a unique representative $a_0 \in R$, $a_0 \neq 0$. We thus have $u = a_0 + \pi b_1$ for some $b_1 \in \hat{O}$.Assume now that $a_0, \ldots, a_{n-1} \in R$ have been found satisfying

$$u = a_0 + a_1\pi + \ldots + a_{n-1}\pi^{n-1} + \pi^n b_n \tag{9}$$

for some $b_n \in \hat{O}$ and that the a_i are uniquely determined by this equation. Then the representative $a_n \in R$ of $b_n \mod \pi\hat{O} \in \hat{O}/\hat{P} \cong O/P$ is also uniquely determined by u and we have $b_n = a_n + \pi b_{n+1}$, for some $b_{n+1} \in \hat{O}$. Hence

$$u = a_0 + a_1\pi + \ldots + a_n\pi^n + \pi^{n+1}b_{n+1}. \tag{10}$$

In this way we find an infinite series (ide kell egy szumma) which is uniquely determined by u. It converges to u because the remainder term $\pi^{n+1}b_{n+1}$ tends to zero(in the nonarchimedean case it is easy to see that this is sufficient and this is the point where we use that $\hat{K}$ is complete). □

This lemma will come in useful in proving a very interesting theorem, Hensel's lemma. If we want to study the extensions of $\mathbb{Q}_p$ or any other complete nonarchimdean field, we need to study the irreducible polynomials of that field. This lemma will relate the irreducible polynomials of K (or O, which is the same due to Gauss's lemma) and of $\kappa = O/P$, the residue class field. This is very useful, beacuse local fields have finite residue class fields which are quite simple. First we need to introudec the notion of a primitve polynomial.

Definition 1.15. *A polynomial $f \in O[x], f(x) = a_0 + a_1x + \ldots + a_nx^n$ is called **primitive** if $max\{|a_0|, \ldots, |a_n|\} = 1$.*

Theorem 1.16 (Hensel's lemma)**.** *Let K be a complete valued field. If a primitive polynomial $f(x) \in O[x]$ admits modulo P a factorization*

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \mod O \tag{11}$$

into relatively prime polynomials $\overline{g}, \overline{h} \in \kappa[x]$ then $f(x)$ admits a factorization

$$f(x) = g(x)h(x) \tag{12}$$

into polynomials $g, h \in O[x]$ such that $\deg(g) = \deg(\overline{g})$ and

$$g(x) \equiv \overline{g}(x) \mod P, \quad h(x) \equiv \overline{h}(x) \mod P \tag{13}$$

So a polynomial in O can only be irreducible if it is modulo P irreducible. Note that an irreducible polynomial of κ is not necessarily irreducible in O(so the statement is not an 'if and only if'statement).

Proof. Let $g_0, h_0 \in O[x]$ such that $\deg(g_0) = \deg(\overline{g})$ and $\deg(h_0) \leq \deg(f) - \deg(\overline{g})$ and $g_0 \equiv \overline{g} \mod P$ and $h_0 \equiv \overline{h} \mod P$. Since $\overline{g}$ and $\overline{h}$ are relatively prime, there exist polynomials $a(x), b(x) \in O[x]$ satisfying $ag_0 + bh_0 \equiv 1 \mod P$. Among the coefficients of the two polynomials $f - g_0h_0$ and $ag_0 + bh_0 - 1 \in P[x]$ we pick one with minimum value and call it π. Let us look for the polynomials in the following form:

$$g = g_0 + p_1\pi + p_2\pi^2 + \ldots h = h_0 + q_1\pi + q_2\pi^2 + \ldots \tag{14}$$

where $p_i, q_i \in O[x]$ are polynomials of degree$<$ $\deg(\overline{g})$, respectively $\leq \deg(f) - \deg(\overline{g})$. We then determine successively the polynomials

$$g_{n-1} = g_0 + p_1\pi + p_2\pi^2 + p_{n-1}\pi^{n-1} h_{n-1} = h_0 + q_1\pi + q_2\pi^2 + q_{n-1}\pi^{n-1} \tag{15}$$

in such a way that one has

$$f \equiv g_{n-1}h_{n-1} \mod \pi^n \tag{16}$$

Passing to the limit as $n \to \infty$ we will finally obtain the identity $f = gh$. Here we use that the field is complete and so K satisfies the previous proposition. For $n = 1$ the congruence is satisfied in view of our choice of π. Let us assume that it is already established for some $n \geq 1$. Then in view of the relation

$$g_n = g_{n-1} + p_n\pi^n, h_n = h_{n-1} + q_n\pi^n \tag{17}$$

the condition on g_n, h_n reduces to

$$f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + hn - 1p_n)\pi^n \mod \pi^{n+1} \tag{18}$$

Dividing by π^n we get

$$g_{n-1}q_n + hn - 1p_n = g_0q_n + h_0p_n \equiv f_n \mod \pi \tag{19}$$

where $f_n = \pi^{-n}(f - g_{n-1}h_{n-1}) \in O[x]$. Since $g_0a + h_0b \equiv 1 \mod \pi$ one has

$$g_0af_n!h_0bf_n \equiv f_n \mod \pi \tag{20}$$

At this point we would like to put $q_n = af_n$ and $p_n = bf_n$ but the degrees might be too big (so the remainder of the proof is to make sure that g and h have the right degrees). So we write

$$b(x)f_n(x) = q(x)g_0(x) + p_n(x) \tag{21}$$

where $\deg(p_n) < \deg(g_0) = \deg(\overline{g})$. Since $g_0 \equiv \overline{g} \mod P$ the highest coefficient of g_0 is a unit; hence $q(x) \in O[x]$ and we obtain the congruence

$$g_o(af_n + h_0q) + h_0p_n \equiv f_n \mod \pi \tag{22}$$

Omitting now from the polynomial $af_n + h_0q$ all coefficients divisible by π we get a polynomial q_n such that $g_0q_n!h_0p_n \equiv f_n \mod \pi$ and which in view of $\deg(f_n) \leq \deg(f)$, $\deg(g_0) = \deg(\overline{g})$ and $\deg(h_0p_n) < (\deg(f) - \deg(\overline{g})) + \deg(\overline{g}) = d$, has degree $\leq \deg(f) - \deg(\overline{g})$ as required. □

Now we will illustrate how to use Hensel's lemma in practice.

Example 1.17. *We will show that* $(x^2-2)(x^2-17)(x^2-34)=0$ *has a solution in* $\mathbb{Q}_p$ *for* $(p,34)=1$. *Let us consider the polynomial* $\mod p$. *It has a solution if either 2 or 17 or 34 is a quadratic residue* $\mod p$. *This will be the case because the Legendre symbol is multiplicative and* $2\cdot 17=34$ *and therefore it is impossible that each of them has Legendre symbol -1. So it has a solution* $\mod p$ *and now applying Hensel's lemma tells us that it has a solution in* $\mathbb{Q}_p$.

To check this result just using the definition of p-adic numbers would be extremely uncomfortable. This also illustrates the close relationship between finite fields and local fields. Now we will prove a proposition which can be easily deduced from Hensel's lemma but will come in handy later.

Proposition 1.18. *Let the field* K *be complete with respect to a nonarchimedean valuation* $||$. *Then for every irreducible polynomial* $f(x)=a_0+a_1x+\ldots+a_nx^n\in K[x]$*such that* $a_0a_n\neq 0$ *one has*

$$|f|=max\{|a_0|,|a_n|\}. \tag{23}$$

In particular, $a_n=1$ *and* $a_0\in O$ *imply that* $f[x]$.

Proof. After multiplying by a suitable element of K we may assume that $f(x)\in O[x]$ and $|f|=1$. Let a_r be the first one among the coefficients $a_0,a_1,\ldots,a_n$ such that $|a_r|=1$. So we have:

$$f(x)\equiv x^r(a_r+a_{r+1}x+\ldots+a_nx^{n-r}) \mod P \tag{24}$$

If one had $max\{|a_0|,|a_n|\}<1$ then $0<r<n$ and the congruence would contradict Hensel's lemma. □

This result is quite surprising if we compare it to irreducible polynomials over $\mathbb{Z}$ but it also illustrates that the importance of the valuation. Now we will consider the extensions of complete nonarchimedean fields. First we will prove a theorem that we can uniquely extend the valuation to the new field and if the extension is finite it will even remain complete.

Theorem 1.19. *Let* K *be a complete nonarchimedean field, with valuation* $|\cdot|$. *Then* $||$ *may be extended uniquely to any algebraic extension* L *of* K. *The extension is given by the formula*

$$|\alpha|=\sqrt[n]{|N_{L|K}(\alpha)|} \tag{25}$$

when $L|K$ *has finite degree* n. *In this case* L *again is complete.*

Note that an infinite extension of K is never complete!(we will not prove this)

Proof. First we will show that this is indeed a valuation on L (it is obviously an extension of the valuation of K because the norm map on K is just raising to the nth power.). Let O be the valuation ring of K and O' its integral closure in L. Then one has

$$O'=\{\alpha\in L|N_{L|K}\in O\} \tag{26}$$

The implication $\alpha\in O'\Rightarrow N_{L|K}(\alpha)\in O$ is evident. Conversely let us consider the minimal polynomial f of α over K: $f(x)=x^d+a_{d-1}x^{d-1}+\ldots+a_0$. $N_{L|K}(\alpha)=a_0$ hence $a_0\in O$. According to the proposition we proved $f(x)\in O[x]$ and so $\alpha\in O'$. Note that $O'=\{\alpha\in L||\alpha|\leq 1\}$ is trivially true after this description. The first two conditions of a valuation

will be trivially true. In order to check the strong triangle inequality we need to prove that $|\alpha+\beta| \leq max\{|\alpha|,|\beta|\}$. If we divide by β we get that we have to prove the implication

$$|\alpha| \leq 1 \Rightarrow |\alpha+1| \leq 1 \tag{27}$$

Now this is trivial because O' is subring because it is an integral closure. Now we have to prove the uniqueness. Let $||'$ be another extension with valuation ring $O"$. Let P' resp. $P"$ be the maximal ideal of O' and $O"$. We will show that $O' \subseteq O"$. Let $\alpha \in O' \backslash O"$ and let

$$f(x) = x^d + a_1 x^{d-1} + \ldots + a_d \tag{28}$$

be the minimal polynomial of α over K. Then one has $a_1, \ldots, a_d \in O$ and $\alpha^{-1} \in P"$, hence $1 = -a_1\alpha^{-1} - \ldots - a_d(\alpha^{-1})^d \in P"$, a contradiction. This shows the inclusion $O' \subseteq O"$. In other words we have that $|\alpha| \leq 1 \Rightarrow |\alpha|' \leq 1$ and this implies that the valuation $||$ and $||'$ are equivalent due to the approximation theorem. They are equal on K so they are not only equivalent but equal. The completeness is the consequence of the well-known fact that every norm of a finite dimensional vector space is equivalent to the maximum norm. We will leave the details to the reader. □

In this proof we only used Hensel's lemma. Hensel' lemma is not only true for complete fields. A field is actually called **henselian** if Hensel's lemma is true in that field. So the extension theorem will be also true for henselian fields. The following theorem shows that the converse is also true.

Theorem 1.20. *A nonarchimedean valued field $(K,||)$ is henselian if and only if the valuation can be extended uniquely to any algebraic extension.*

Now let us consider finite Galois extensions.From now on K will be a local field. A famous unsolved problem is the so-called 'inverse Galois' problem: which finite groups can be realized as the Galois groups of finite Galois extension of $\mathbb{Q}$. A natural question would be to ask the same question with $\mathbb{Q}_p$. However this turns out to be much easier. Every Galois group will be solvable. Our goal will be now to prove this result. First we consider unramified extensions.

Definition 1.21. *Let $L|K$ be a finite extension, and λ, κ be their residue fields. If $\lambda|\kappa$ is a separable extension, and $|\lambda:\kappa| = |L:K|$ then we call the extension* ***unramified****.*

We will prove that the Galois group of an unramified extension is isomorphic to the Galois group of the residue field extension and is therefore cyclic.

Theorem 1.22. *Let L be a finite extension of K and let l be the residue field of L. The map $K' \mapsto k'$ sending an unramified extension K' of K contained in L to its residue field k' is a one-to-one correspondence between the sets*

$$\{K' \subset L,\ \textit{finite and unramified over } K\ \} \leftrightarrow \{k' \subset l, finiteover k\} \tag{29}$$

Moreover:

1. *if $K' \leftrightarrow k'$ and $K" \leftrightarrow k"$, then $K' \subset K" \Leftrightarrow k' \subset k"$,*
2. *if $K' \leftrightarrow k'$ then K' is Galois over K if and only if k' is Galois over k in which case there is a canonical isomorphism $Gal(K'|K) \rightarrow Gal(k'|k)$*

Proof. Let k' be a finite extension of k. We can write $k' = k[a]$(every finite extension is simple over a perfect field). Let $f_0(x)$ be the minimum polynomial of a over k, and let $f(x)$ be any lifting to $O[x]$(O is the valuation ring of K). As a is a simple root of $f_0(x)$ (the extension is separable), Hensel's lemma shows that there is a unique $\alpha \in L$ such that $f(\alpha) = 0$ and $\alpha \equiv a$ mod P. Now we define K' as the simple extension of K by α ($K' = K[\alpha]$). This obviously has residue field k'. So the mapping $K' \to k$ is surjective. Suppose that K' and K" are unramified extensions of K in L with the same residue field k'. $K' \cdot K$ is an unramified(this is not obvious, but not difficult to prove)extension of K with residue field k'. Hence

$$[K' \cdot K" : K] = [k' : k] = [K' : K] \tag{30}$$

Both equations are true because they are unramified(that's the definition). K' is contained in $K' \cdot K$" and has the same degree over K. This implies that $K' = K' \cdot K$" so $K" = K'$. Now we proved the one-to-one correspondence. Statement (1) is obvious. Now lets turn to (2). Assume K' is Galois over K. Then Gal$(K'|K)$ preserves O'(the valuation ring in K') and its maximal ideal, and so we get a map $Gal(K'|K) \to$ Aut$(k'|k)$. Write $k' = k[a]$ and let $g(x) \in O[x]$ be such that $\overline{g} \in k[x]$ is the minimum polynomial of a. Let $\alpha \in O'$ be the unique root of $g(x)$ such that $\overline{\alpha} = a$. Because K' is Galois over K $g(x)$ splits in $O'[x]$ and this implies that $\overline{g}$ splits in $k'[x]$, and so k' is Galois over k. Let $f = [k' : k] = [K' : K]$, and let $\alpha_1, \ldots, \alpha_f$ be the roots of $g(x)$. These are the Galois conjugates of α. Because $\overline{g}$ is separable, the α_i are distinct mod P and this shows that the image of the map $Gal(K'|K) \to Gal(k'|k)$ has order f and hence is an isomorphism. Conversely, suppose $k'|k$ is Galois. Again write $k' = k[a]$, an $\alpha \in O$ lift a. It follows from Hensel's lemma that O' contains all the conjugates of α and hence that K' is Galois over K. □

An important corollary of the theorem is that there exist a largest unramified extension of K. Now we turn to the general case and we introduce ramification groups. Let $L|K$ be a finite Galois extension. Let Π be a prime element of L.Let $G = Gal(L|K)$ and $B = \{\alpha \in L || \alpha| \leq 1\}$ and $P = \{\alpha \in L || \alpha| < 1\}$.

Definition 1.23. *Let $G \supset G_0 \supset G_1 \ldots$ be a sequence of subgroups which satisfy the following condition:*

$$\sigma \in G_i \Leftrightarrow |\sigma\alpha - \alpha| < |\pi_L|^i forall \alpha \in B \tag{31}$$

*The group G_0 is called the **inertia group**, the group G_1 is called the **ramification group** and the groups $G_i, i > 1$ are called the **higher ramification groups** of L over K.*

Lemma 1.24. *The G_i are normal subgroups of G, and $G_i = 1$ for i large enough.*

Proof. Let $\tau, \sigma \in G$.

$$|\tau^{-1}\sigma\tau\alpha - \alpha| = |\sigma(\tau\alpha) - (\tau\alpha)| \tag{32}$$

because $|\tau x| = |x|$. As α runs through B, so also does $\tau\alpha$ and so $\tau^{-1}\sigma\tau \in G_i$ exactly when σ does. This proves that the G_i are normal subgroups. If $\sigma \neq 1$ then $\sigma\alpha \neq \alpha$ for some $\alpha \in B$. Hence if i is large enough $|\sigma\alpha - \alpha| > |\pi_L|^i$ because $|\pi_L| < 1$ so $|\pi_L|^i$ tends to zero as i tends to infinity. This means that for every $\sigma \in G$ there exists a bound k_σ that if i is bigger than that G_i will not contain σ. G is finite so if i is large enough G_i will be trivial. □

Theorem 1.25. *Let $L|K$ be a finite Galois extension and assume that the residue field extension $l|k$ is separable(if K is a local field this will be automatic).*

1. *The fixed field of G_0 is the largest unramified extension K_0 of K in L, and $G/G_0 = \mathrm{Gal}(K_0|K) = \mathrm{Gal}(l|k)$.*

2. *For $i \geq 1, G_i = \{\sigma \in G_0 || \sigma\pi_L - \pi_L| < |\pi_L|^i\}$*

Proof. 1. Let K_0 be the largest unramified extension in L. Then σK_0 is also unramified, and so it is contained in K_0. Thus K_0 is Galois over K, and the canonical map $\mathrm{Gal}(K_0|K) \to \mathrm{Gal(l|k)}$ is an isomorphism. By definition G_0 is the kernel of $G \to \mathrm{Gal}(l|k)$, and so K_0 is its fixed field.

2. Let O_0 be the valuation ring in K_0. Then $B = O_0[\pi_L]$. Since G_0 fixes O_0, in order to check that $\sigma \in G_i$ it suffices to check that $|\sigma\alpha - \alpha| < |\pi_L|^i$ for the element $\alpha = \pi_L$.

□

Corollary 1.26. *We have an exhaustive filtration*

1. $G/G_0 = \mathrm{Gal}(l|k)$

2. $G_0/G_1 \hookrightarrow l^*$

3. $G_i/G_{i+1} \hookrightarrow l$

Therefore $\mathrm{Gal}(L|K)$ *is solvable.*

Proof. Let $\sigma \in G_0$; then $\sigma\Pi$ is also a prime element and so $\sigma\Pi = u\Pi$ with u a unit in B.The map $\sigma \to u \mod P$ is a homomorphism $G_0 \to l^*$ with kernel G_1. Let $\sigma \in G_i$. Then $|\sigma\Pi - \Pi| \leq |\Pi|^{i+1}$, and so $\sigma\Pi = \Pi + a\Pi^{i+1}$ for some $a \in B$. The map $\sigma \mapsto a \mod P$ is a homomorphism $G_i \to l$ with kernel G_{i+1}. □

To conclude the chapter we will state an important result without proof. A proof can be found in [10].

Theorem 1.27. *The local fields are precisely the finite extensions of the fields $\mathbb{Q}_p$(if the characteristic of the field is 0) and $\mathbb{F}_p((t))$(if the characteristic of the field is $p > 0$).*

2 Galois representations, the $l \neq p$ case

Let K be a local field with residual characteristic p.In this section we will study representations of the absolute Galois group of the field K. First we will define the basic notions.

Definition 2.1. *Let l be a prime number different from p. An **l-adic representation**of a group G is a continuous homomorphism $\rho : G \to GL_n(\mathbb{Q}_l)$. If $G = \mathrm{Gal}(\overline{K}|K)$ then we call it an l-adic **Galois representation**.*

This homomorphism can be regarded as a linear action of the group G on a $\mathbb{Q}_l$-vectorspace. We will denote the absolute Galois group of a field K by G_K. Now let us see some examples of such representations.

Example 2.2. *There is a unique continuous homomorphism of groups $\chi_l : G_{\mathbb{Q}} \to \mathbb{Z}_l \subset \mathbb{Q}_l$ such that for all l^nth roots of unity $\zeta \in \mu_\infty$ and $\sigma \in G_{\mathbb{Q}}$, $\sigma(\zeta) = \zeta^{\chi_l \sigma}$. This is well defined because $\zeta \in \mu_\infty$, so if n is large enough ζ^{l^n} will be 1. This is a 1-dimensional representation of $G_{\mathbb{Q}}$ and is called the **cyclotomic character**.*

Example 2.3. *Let E be an elliptic curve over $\overline{\mathbb{Q}}$. Let $E[m]$ denote the set of points P on E which satisfy the condition $mP = O$. If we consider E over $\mathbb{Z}/l\mathbb{Z}$ then $E[l^n] \simeq \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$ (proof in Silverman). So it is natural to consider the inverse limit of the groups $E[l^n]$, where the transition morphisms are given by $E[l^{n+1}] \to E[l^n]$, $x \to lx$, because it will give us a $\mathbb{Z}_l$ module of rank 2.*

$$T_l(E) = \varprojlim E[l^n] \tag{33}$$

*is called the **Tate-module** of E. This will give rise to a 2-dimensional representation of $G_{\mathbb{Q}}$ because the absolute Galois group acts naturally on the points of E, so it will act on the Tate-module as well(let us keep in mind that $\mathbb{Z}_l \subset \mathbb{Q}_l$).*

The following theorem states that if the curve does not have complex multiplication(i.e. multiplying by $m \in \mathbb{Z}$ are the only endomorphisms of the curve) then this representation will be almost always irreducible.

Theorem 2.4 (Serre)**.** *Let E be an elliptic curve over a field K. Then for all but finitely many primes l, there are no G_K invariant subgroups of $E[l]$.*

A proof can be found in [11]. Observe that this means, that the Tate-module will satisfy the same condition, because if it would have a $G_{\mathbb{Q}}$ invariant subspace then the $\mathbb{F}_l$ subspace consisting of the first coordinates would be an invariant subgroup of $E[l]$. We can construct the cyclotomic representation in the same fashion as we constructed the Tate module of an elliptic curve.

Example 2.5. *The groups $\mu_{l^n} \in \overline{\mathbb{Q}}$ form an inverse system with the raising to lth power map.*

$$T_l(\mu) = \varprojlim \mu_{l^n} \tag{34}$$

This called the Tate module of $\mathbb{Q}$. Since

$$\mu_{l^n} \cong \mathbb{Z}/l^n\mathbb{Z} \tag{35}$$

$T_l(\mu)$ will be isomorphic to $\mathbb{Z}_l$, so it is a free $\mathbb{Z}_l$ module of rank 1. We will define an action(called the Tate twist) on this module. Let t be a generator,$t = (\epsilon_n)_{n\in\mathbb{N}}$ and $\epsilon_0 = 1, \epsilon_1 \neq 1, \epsilon_n = \epsilon_{n+1}^l$. $\lambda \in \mathbb{Z}_l$ acts on t in the following manner:

$$\lambda t = (\epsilon_n^{\lambda_n})_{n\in\mathbb{N}}, \lambda_n \in \mathbb{Z}, \lambda_n \equiv \lambda \mod l^n\mathbb{Z}_l \tag{36}$$

We will denote this by $\mathbb{Z}_l(1)$ and its tensor product with $\mathbb{Q}_l$ by $\mathbb{Q}_l(1)$.

We now have some examples of Galois-representations. We could create a lot more using direct sums, tensor products exterior products, etc. The second example is somewhat astonishing, as it comes purely from geometry. We will get to that back later and give other examples that come from algebraic geometry. Our primary goal is to study representations of $G_{\mathbb{Q}}$. The following theorem tells us, that if we know $G_{\mathbb{Q}_l}$ for a lot of l-s then we can determine $G_{\mathbb{Q}}$ from it. This important beacuse those groups are a lot easier to study.

Theorem 2.6. *Let S be a set of prime numbers of density 1. Let $\rho : G_{\mathbb{Q}} \to V$ be a representation. If we know $\rho|_{G_{\mathbb{Q}_l}}$ for all $l \in S$ then we can determine ρ from it.*

Now we will study l-adic representations of G_K, K being a local field (finite extension of $\mathbb{Q}_p$). It would be somewhat natural to consider representations which are homomorphisms into $GL_n(\overline{\mathbb{Q}_l})$ instead of $GL_n(\mathbb{Q}_l)$ but we will later prove that if $\rho : G_K \to GL_n(\overline{\mathbb{Q}_l})$ then the image ρ is contained in $GL_n(L)$ where L is a finite extension of $\mathbb{Q}_l$ in $\overline{\mathbb{Q}_l}$. In order to prove this we will need two lemmas first.

Lemma 2.7 (Krasner)**.** *Let $\alpha, \beta \in \overline{K}$ and assume that α is separable over$K[\beta]$. If α is closer to β than any conjugate of α then $K[\alpha] \subset K[\beta]$.*

Proof. Let σ be an embedding of $K[\alpha, \beta]$ into $\overline{K}$ fixing $K[\beta]$. By Galois theory it suffices to show that σ fixes α.

$$|\sigma\alpha - \beta| = |\sigma\alpha - \sigma\beta| = |\alpha - \beta| \tag{37}$$

because σ fixes β.

$$|\sigma\alpha - \alpha| = |\sigma\alpha - \beta + \beta - \alpha| \leq |\alpha - \beta| \tag{38}$$

Here we used the ultrametric property and the previous equation. Now $\sigma\alpha = \alpha$ because $\sigma\alpha$ is closer to α than to β. So we have completed the proof. □

An important consequence of this lemma is that the completion of an algebraically closed field will be algebraically closed (see [M1, 7]). The following result can be easily deduced from this fact[see [K, 6]].

Lemma 2.8. *$\overline{\mathbb{Q}}$ is dense in $\overline{\mathbb{Q}_l}$.*

Now we have everything we need to prove our theorem.

Theorem 2.9. *Let $\rho : G_K \to GL_n(\overline{\mathbb{Q}_l})$ be a continous representation. Then $\rho(G_K) \subset GL_n(L)$ where L is a finite extension of $\mathbb{Q}_l$.*

Proof. Let $\alpha \in \overline{\mathbb{Q}}$. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the $G_{\mathbb{Q}_l}$ conjugates of α. If we take a β that satisfies the equation below:

$$|\alpha - \beta| \leq |\alpha - \alpha_i| \text{ for } i = 1, 2, \ldots, n \tag{39}$$

Then by Krasner's lemma $\mathbb{Q}_l(\alpha) \subset \mathbb{Q}_l(\beta)$. Therefore the number of finite extensions of $\mathbb{Q}_l$ contained in $\overline{\mathbb{Q}_l}$ is countable because $\overline{\mathbb{Q}}$ is a countable set. The field $\overline{\mathbb{Q}_l}$ is a filtered union of finite extensions E_i of $\mathbb{Q}_l$ where i ranges over some countable index set I. Similarly we have $GL_n(\overline{\mathbb{Q}_l}) = \bigcup GL_n(E_i)$. Recall that a topological space X is a Baire space if and only if given any countable collection of closed sets F_i in X, each with empty interior in X, their union $\bigcup F_i$ has also empty interior. The image $\rho(G_K)$ is compact in $GL_n(\overline{\mathbb{Q}_l})$ and therefore complete as a metric space and in particular a Baire space. Let F_i be the closure of $GL_n(E_i) \bigcap \rho(G_K)$ in the space $\rho(G_K)$. Then $\bigcup F_i$ has non-empty interior inside $\rho(G_K)$ so there exists an $i \in I$ such that F_i contains a non-empty open subset U of $\rho(G_K)$. After translating and shrinking U we may assume it is an open subgroup of $\rho(G_K)$. The quotient $\rho(G_K)/U$ is covered by the sets $GL_N(E_j) \bigcap \rho(G_K)$ with j ranging over all the elements of I such that $E_i \subset E_j$. Because the quotient $\rho(G_K)/U$ is finite, we need only a finite number of such j-s. The compositum L of the fields E_j is then finite over E_i and so this L will have the desired property. □

In my opinion this proof is extremely interesting. First the result is astonishing. Second, the proof uses a tool from general topology, and almost no algebra! The main reason why this claim is true is that if you consider a compact topological group then their open subgroups must be of finite index. This proof shows that if we consider local fields we must seriously take topological aspects into account because pure algebraic results are consequences of topological theorems.

Our next goal will be to prove a general result, called Grothendieck's monodromy theorem. Now we will also consider the case when the residue field is not finite(although this is now the most important case). In the first chapter we have introduced ramification groups. However we only considered the case, where $K|L$ was a finite Galois extension. Almost everything is the same if we switch to algebraic extensions(see Milne). Now we consider the case where $G = \mathrm{Gal}(\overline{K}|K)$. $I_K = G_0$ is called the inertia subgroup and its p-Sylow subgroup P_K is called the wild inertia subgroup of G_K. Let k be the residue field of K. It is easy to see that we have the following exact sequences:

$$1 \to I_K \to G_K \to G_k \to 1. \tag{40}$$

$$1 \to P_K \to G_K \to G_K/P_K \to 1. \tag{41}$$

Let l be a fixed prime number $l \neq p$. Then there is the following isomorphism([4]):

$$I_K/P_K \simeq \hat{\mathbb{Z}}'(1) = \prod_{l \neq p} \mathbb{Z}_l(1) = \mathbb{Z}_l(1) \times \prod_{l' \neq l,p} \mathbb{Z}_{l'}(1) \tag{42}$$

We define $P_{K,l}$ to be the inverse image of $\prod_{l' \neq l,p} \mathbb{Z}_{l'}(1)$ in I_K and $G_{K,l}$ the quotient group to make the short exact sequences:

$$1 \to P_{K,l} \to G_K \to G_{K,l} \to 1. \tag{43}$$

$$1 \to \mathbb{Z}_l(1) \to G_{K,l} \to G_k \to 1. \tag{44}$$

We will state the following proposition(for a proof see [4]):

Proposition 2.10. *Let ρ be finite dimensional l-adic representation of G_K. Then $\rho(P_{K,l})$ is finite.*

Now we will define the necessary notions in order to proceed.

Definition 2.11. *Let V be an l-adic representation of G_K with $\rho : G_K \to Aut_{\mathbb{Q}_l}(V)$.*

1. *V has **good reduction** if I_K acts trivially.*
2. *V has **potentially good reduction** if $\rho(I_K)$ is finite, in other words, if there exists a finite extension K' of K contained in $\overline{K}$ sich that V as an l-adic representation of $G_{K'}$ has good reduction.*
3. *V is **semi-stable** if I_K acts unipotently(or equivalently the semi-simplification of V has good reduction).*
4. *V is **potentially semi-stable** if there exists a finite extension K' of K contained in $\overline{K}$ sucht that V is a semi-stable representation of $G_{K'}$.*

The last definition is equivalent to the condition that there exists an open subgroup of I_K which acts unipotently or that the semi-simplification has good reduction.

The monodromy theorem vaguely states that if the residue field of K satisfies certain conditions then the representation is potentially semi-stable. Our next goal will be to prove this in the case where the residue field is finite.

Theorem 2.12. *Assume that the group $\mu_{l^\infty}(K(\mu_l)) = \{\epsilon \in K(\mu_l) | \exists n \text{ such that } \epsilon^{l^n} = 1q\}$ is finite. Then any l-adic representation of G_K is potentially semi-stable. As $\mu_{l^\infty}(k) \simeq \mu_{l^\infty}(K)$, this is the case if k is finite.*

Proof. Replacing K with a suitable finite extension we may assume that $P_{K,l}$ acts trivially (if we prove the theorem for a finite extension of K then the theorem is true for K as the composite of finite extension is finite). Here we used the proposition above. So ρ factors through $G_{K,l}$. Let $\overline{\rho}$ denote the map from $G_{K,l}$ to $Aut_{\mathbb{Q}_l}(V)$ that ρ induces. Consider the exact sequence:

$$1 \to \mathbb{Z}_l(1) \to G_{K,l} \to G_k \to 1. \tag{45}$$

Let t be a topological generator of $\mathbb{Z}_l(1)$. So $\overline{\rho}(t) \in \mathrm{Aut}_{\mathbb{Q}_l}(V)$. Choose a finite extension E of $\mathbb{Q}_l$ such that the characteristic polynomial of $\overline{\rho}(t)$ is a product of polynomials of degree 1. Let $V' = E \otimes_{\mathbb{Q}_l} V$. It is quite natural to consider this vector space as $\overline{\rho}(t)$ will have eigenvalues(because the characteristic polynomial has roots in E) and $G_{K,l}$ acts on V' by

$$g(\lambda \otimes v) = \lambda \otimes g(v). \tag{46}$$

Let $\overline{\rho} : G_{K,l} \to Aut_E(V')$ be the representation over E, let a be an eigenvalue of $\overline{\rho}(t)$. Let $v \neq 0$ be an eigenvector associated to a. If $g \in G_{K,l}$ then $gtg^{-1} = t^{\chi_l(g)}$ where $\chi_l : G_{K,l} \to \mathbb{Z}_l^*$ is a character because of the exact sequence we stated at the beginning of the proof(and because t is a topological generator). Now our goal will be to prove that if a is an eigenvalue then $a^{\chi_l(g)}$ is also an eigenvalue for any $g \in G_{K,l}$.

$$\overline{\rho}(gtg^{-1})(v) = \overline{\rho}(t^{\chi_l(g)})(v) = a^{\chi_l(g)}(v). \tag{47}$$

Therefore

$$\overline{\rho}(t)(g^{-1}(v)) = t(g^{-1}v) = (tg^{-1})(v) = g^{-1}(a^{\chi_l(g)}v) = a^{\chi_l(g)}g^{-1}v. \tag{48}$$

If we find a $g \in G_{K,l}$ such that $\chi_l(g) = n, n \in \mathbb{Z}$ then a^n is also an eigenvalue. The condition $\mu_{l^\infty}(K(\mu_l))$ is finite is equivalent to $Im(\chi_l)$ being open in $\mathbb{Z}_l^*$. An open subgroup of $\mathbb{Z}_l$ must contain infinitely many integers, so a must be a root of 1. Therefore there exists $N \geq 1$ such that t^N acts unipotently(because all its eigenvalues are 1-s).The closure of the subgroup generated by t^N acts unipotently and is an open subgroup of $\mathbb{Z}_l(1)$. Since $I_K \twoheadrightarrow \mathbb{Z}_l(1)$ is surjective, the theorem now follows because we found an open subgroup of I_K that acts unipotently. □

I think this is an interesting proof which illustrates that passing to finite extensions makes it easier to proceed. Now we will turn to the case where the residue field is infinite. This is the less important case but it will indicate the closeness between representations and geometry. We will state a theorem where the terms are not yet well defined but will be at the at the end of the chapter.

Theorem 2.13. *Let K be a local field. Then any l-adic representation of G_K coming from algebraic geometry is potentially semi-stable.*

We will not prove this here(as we have not yet defined the term 'coming from algebraic geometry') but it can easily be deduced from the previous theorem.

However if k is algebraically closed then the converse is also true.

Theorem 2.14. *If k is algebraically closed then any potentially semi-stable l-adic representation comes from algebraic geometry.*

Proof. We proceed the proof in two steps. First we note that k being algebraically closed implies that $I_K = G_K$.

Step 1. First, we assume that the Galois representation is semi-stable. Then the action of $P_{K,l}$ must be trivial from above discussions, hence the representation factors through $G_{K,l}$. Identify $G_{K,l}$ with $\mathbb{Z}_l(1)$ and let t be a topological generator of this group. Let V be such a representation, then as in the previous proof $\overline{\rho}(t)$(defined in the previous proof)will lie in $\mathrm{Aut}_{\mathbb{Q}_l}(V)$.

For each integer $n \geq 1$ there exists a unique (up to isomorphism) representation V_n which is semi-stable and in-decomposable. Write it as $V_n = \mathbb{Q}_l^n$, and we can assume that $\overline{\rho}(t)$ (as a matrix)has 1-s in the main diagonal and in the diagonal above (this is the Jordan normal form of the matrix $\overline{\rho}(t)$.

As $V_n \simeq \mathrm{Sym}^{n-1}_{\mathbb{Q}_l}(V_2)$ it is enough to prove that V_2 comes from algebraic geometry(there is a general procedure in algebraic geometry producing $\mathrm{Sym}^{n-1}(C)$ as a representation coming from geometry once we obtained V this way). Write

$$0 \to \mathbb{Q}_l \to V_2 \to \mathbb{Q}_l \to 0, \tag{49}$$

where V_2 is a non-trivial extension. It is enough to produce a non-trivial extension of two l-adic extensions of dimension 1 coming from algebraic geometry. We apply the case for some $q \in m_K, q \neq 0$. Then from Tate's theorem(see [11]), let E be an elliptic curve over K such that $E(\overline{K}) \simeq (\overline{K})^*/q^{\mathbb{Z}}$ with

$$E(\overline{K}))_{l^n} = \{a \in \overline{K})^* | \exists m \in \mathbb{Z} \text{ such that } a^{l^n} = q^m\}/q^{l^n} \tag{50}$$

and

$$V_l(E) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(E), T_l(E) = \varprojlim E(\overline{K}))_{l^n}. \tag{51}$$

An element $\alpha \in T_l(E)$ is given by

$$\alpha = (\alpha_n)_{n\in\mathbb{N}}, \alpha_n \in E(\overline{K})_{l^n}, \alpha_{n+1}^l = \alpha_n. \tag{52}$$

Consider the following exact sequence:

$$0 \to \mu_{l^n}(K) \to E(\overline{K})_{l^n} \to \mathbb{Z}/l^n\mathbb{Z} \to 0. \tag{53}$$

If we take projective limits and tensor with $\mathbb{Q}_l$ we get:

$$0 \to \mathbb{Q}_l(1) \to V_l(E) \to \mathbb{Q}_l \to 0. \tag{54}$$

The action of G_K on the left $\mathbb{Q}_l(1)$ of the above exact sequence is trivial, since it comes from the action of an unramified extension. And the extension $V_l(E)$ is non-trivial.

Step 2. Assume the representation is potentially semi-stable. Then the restriction of ρ to some open subgroup $H \leq G_K$ is semi-stable and comes from geometry. There is a general procedure called Weil-restriction which produces induced representations. ρ is a subrepresentation of $\mathrm{ind}_H^G \rho$ by Frobenius reciprocity hence comes from geometry. □

In the remainder of the chapter we will give a brief description of étale cohomology and its relations to Galois-representations.

2.1 Étale cohomology

Étale cohomology was originally developed by Grothendieck (and was a little bit modified by Artin) in order to prove the Weil conjectures. However, soon it became a very useful tool in algebraic geometry and number theory. We will define some notions which are necessary to define étale cohomology.

Definition 2.15. *Let X be a topological space. A **presheaf** F attaches to every open set U an abelian group $F(U)$ and to any $V \subset U$ a map $\rho : F(U) \to F(V)$, called the restriction map with the following properties:*

(1) $\rho_U^U = \mathrm{id}_F(U)$

(2) *whenever $W \subset V \subset U$ $\rho_W^U = \rho_W^V \circ \rho_V^U$*

The elements of $F(U)$ are called sections of F over U, the elements of $F(X)$ are called the global sections of F. Note that F is a contravariant functor from the category of open sets of X to the category of abelian groups.

A presheaf is called a sheaf if it has the following properties:

(a) *a section $f \in F(U)$ is determined by its restrictions $\rho_U^{U_i}(f)$ to the sets to the sets of an open covering $(U_i)_{i\in I}$ of U;*

(b) *a family of sections $f_i \in F(U_i)$ for $(U_i)_{i\in I}$ an open covering of U arises by restriction from a section $f \in F(U)$ if $f_i|U_i \cap U_j = f_j|U_i \cap U_j$ for all i and j.*

To understand this definition we give an example which led to this definition.

Example 2.16. *Let X be the complex plane. If U is an open set then $F(U)$ will be the continuous(or holomorph) functions from U to any topological group Λ. These obviously form and additive abelian group. The restriction maps are the restrictions of functions. If Λ has the discrete topology then every continuus map $f : U \to \Lambda$ is constant on each connected component of U and hence factors through $\pi_0(U)$, the space of connected components of U. When this last space is discrete, $F(U)$ is the set of all maps $\pi_0(U) \to \Lambda$. In this case, we call F the constant sheaf defined by the abelian group Λ.*

We will now define morphisms between sheaves, making them into a category.

Definition 2.17. *Let F and G be sheaves on a topological space X. A **morphism** $\phi : G \to F$ consists of a morphism $\phi(U) : G(U) \to F(U)$ for each open set $U \subset X$ subject to the condition that this morphism is compatible with restrictions. In other words if $V \subset U$ is an open set then the following diagram commutes:*

$$\begin{array}{ccc} G(U) & \xrightarrow{\phi(U)} & F(U) \\ {\scriptstyle \rho_V^U}\downarrow & & {\scriptstyle \rho_V^U}\downarrow \\ G(V) & \xrightarrow{\phi(V)} & F(V) \end{array}$$

Definition 2.18. *F' is a subsheaf of F if for each open set $U \subset X$ $F'(U) \subseteq F(U)$ and $\rho_U^V(F') = \rho_U^V(F)|F'$ (so the restriction maps are the same).*

Now we define the notion of **abelian**category.

Definition 2.19. (1) *If A and B are objects of the category then* $\mathrm{Hom}(A, B)$ *is an abelian group and the composition of morphisms is bilinear.*

(2) *We can form finite direct sums and direct products.*

(3) *Every morphism has a kernel and a cokernel.*

(4) *Every monomorphism is a kernel of a morphism and every epimorphism is a cokernel of morphism.*

Grothendieck showed that the sheaves form an abelian category(see [5]). This allows us to define injective sheaves.

Definition 2.20. *I is an injective sheaf if for any subsheaf F' of a sheaf F every homomorphism $F' \to I$ extends to a homomorphism $F \to I$.*

Theorem 2.21. *Every sheaf can be embedded into an injective sheaf*

This gives us the opportunity to consider an injective resolution of a sheaf F. This means that there exists a left exact sequence

$$0 \to F \to I^0 \to I^1 \to I^2 \to \dots \tag{55}$$

with each I^r being injective. We set $H^r(X,F)$ equal to the rth cohomology group of the complex of abelian groups

$$0 \to I^0(X) \to I^1(X) \to I^2(X) \to \dots \tag{56}$$

These are the sheaf cohomology groups. Now we will turn to étale cohomology groups. Let X and Y be smooth varieties over an algebraically closed field k. A map ϕ is **étale** at a point if $d\phi$ is an isomorphism between the tangent spaces. This is exactly the condition of the inverse mapping theorem in calculus. So this means that if a map is étale at a point then it has an open neighbourhood for which it is a local isomorphism. A map is called étale, if it is étale at every point. This condition is easily computable because this means that the Jacobi matrix at that point is nonsingular. The topology to be defined is not a usual topology but a so called Grothendieck-topology[citation]

Now let X be a smooth variety. The open sets of the étale topology are étale morphisms $U \to X$ (for every $U \subset X$ being open). A family of étale morphisms $(U_i \to U)_{i\in I}$ over X is a covering of U if $U = \cup\phi_i(U_i)$.

An étale neighbourhood of a point $x \in X$ is an étale morphism $U \to X$ together with a point $u \in U$ mapping to x. Let Et/X be the category whose objects are the étale morphism $U \to X$. If we have two morphisms $\Phi_1 : U \to X$ and $\Phi_2 : V \to X$ and there exists a map $\alpha : U \to V$ which makes them into a commutative diagram. This will be the morphism between the objects.

We have a topological space (the étale topology) so we can define sheaves on this space. These sheaves will form an abelian category with enough injectives, so we can define the cohomology groups for this sheaf which gives us the étale cohomology groups $H^r(X_{et},F)$(F being the sheaf). If we take F to be the constant sheaf with the abelian group Λ then we get the group $H^r(X_{et},\Lambda)$.

Let $X(\mathbb{C})$ be a smooth variety over $\mathbb{C}$ the singular cohomology groups $H^r(X(\mathbb{C}),\Lambda)$ are very important in algebraic topology and algebraic geometry. We will not define them here, for a definition see (Milne LEC). The only thing which is important is that $H^r(X(\mathbb{C}),\mathbb{Q}_l)$ will be a vectorspace over $\mathbb{Q}_l$. So if $G_{\mathbb{Q}_l}$ acted on this we would get a representation. Unfortunately such action doesn't seem likely if we take the original definition into account. However such a Galois action is quite visible with the étale cohomology groups! So if we could establish a link between the two we would get a representation. Fortunately, the following is true:

Theorem 2.22 (Comparison theorem)**.** *For any finite abelian group* Λ $H^r(X_{et},\Lambda)$ *and* $H^r(X(\mathbb{C}),\Lambda)$ *are isomorphic.*

We do not quite have what we want as $\mathbb{Q}_l$ is not finite. However let's take $\Lambda = \mathbb{Z}/l^n\mathbb{Z}$. If we take the inverse limits of $H^r(X(\mathbb{C}),\mathbb{Z}/l^n\mathbb{Z})$ then we get $H^r(X(\mathbb{C}),\mathbb{Z}_l)$. So as we can extend the Galois-action to inverse limits and so we get a Galois action on $H^r(X(\mathbb{C}),\mathbb{Z}_l)$. Finally we take into account that $H^r(X(\mathbb{C}),\mathbb{Q}_l) = H^r(X(\mathbb{C}),\mathbb{Z}_l)\otimes\mathbb{Q}_l$ and so we get the required Galois action as the Galois group also acts on the tensor product.

Note that the first étale cohomology groups action is the same as the action provided by the Tate-module:

$$H^1(E_{et},\mathbb{Z}_l) \simeq T_l(E) \tag{57}$$

where E is an curve (see [M3 9]). The reason we described étale cohomology here is twofold. First it underlines the very important connection between number theory(in our case Galois

representations) and geometry. Secondly there is a famous conjecture of Fontaine and Mazur that relates all l-adic representations to étale cohomology groups! However we will not state this conjecture here precisely as we would need further notions to be defined.

3 p-adic Galois representations

In this chapter we will turn our focus to the $l = p$ case. Our main goal will be to prove Fontaine's theorem which states that the category of p-adic Galois representations is equivalent to another category which is easier to handle. However we will need to introduce some notions in order to begin with the proof. So we will start with defining with vectors and then we will give a brief review on Galois cohomology.

3.1 The ring of Witt vectors

First we introduce perfect rings and perfect p-rings.

Definition 3.1. *R is a **perfect ring** if $p = 0$ and $x \mapsto x^p$ is a bijection.*

Definition 3.2. *A is a perfect p-ring if $R = A/pA$ is a perfect ring, p is not a zero divisor in A and A is seperated and complete for the p-adic topology.*

Now let R be the ring in the previous definition. For each $x \in R$ let $\hat{x} \in A$ be a lift of x. If $x_0 = x \in R$ and for each $i \geq 0$ we choose $x_i \in R$ such that $x_{i+1}^p = x_i$ (we can create this sequence for every x as R is a perfect ring) then the sequence $(\hat{x_i}^{p^i})_{i\geq 0}$ converges in A (as A is complete for the p-adic topology) to an element $[x]$ which only depends on x and which is called the Teichmüller lift of x. The set $\{[x]\}_{x\in R}$ is a set of representatives of R in A so that every element $a \in A$ can be written in a unique way as $a = \sum_{i\geq 0} p^i[a_i]$ with $a_i \in R$.

Let S be the p-adic completion of $\mathbb{Z}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]_{i\geq 0}$ so that S is a perfect p-ring and $S/pS = \mathbb{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]_{i\geq 0}$. Note that $X_i \in S$ is the Teichmüller lift of $X_i \in S/pS$ and likewise for Y_i. There exist elements $S_i \in S/pS$ and $P_i \in S/pS$ such that:

$$\sum_{i\geq 0} p^i X_i + \sum_{i\geq 0} p^i Y_i = \sum_{i\geq 0} p^i [S_i] \tag{58}$$

$$\sum_{i\geq 0} p^i X_i \times \sum_{i\geq 0} p^i Y_i = \sum_{i\geq 0} p^i [P_i] \tag{59}$$

If A is a perfect p-ring and if we choose some elements $\{x_i\}_{i\geq 0}$ and $\{y_i\}_{i\geq 0}$ in $R = A/pA$ then let $\pi : S \to A$ be the ring homomorphism determined by $X_i \mapsto [x_i]$ and $Y_i \mapsto [y_i]$. If we apply π to the above formulas when we get:

$$\sum_{i\geq 0} p^i [x_i] + \sum_{i\geq 0} p^i [y_i] = \sum_{i\geq 0} p^i [S_i(x_j, y_j)] \tag{60}$$

$$\sum_{i\geq 0} p^i [x_i] \times \sum_{i\geq 0} p^i [y_i] = \sum_{i\geq 0} p^i [P_i(x_j, y_j)] \tag{61}$$

.

So now we have a universal formula for addition and multiplication in A as every $x \in A$ can be represented in the form $\sum_{i\geq 0} p^i[x_i]$.

Let J be some set, let $R_J = \mathbb{F}_p[X_J^{p^{-\infty}}]$ and let S_J be the p-adic completion of $\mathbb{Z}_p[X_J^{p^{-\infty}}]$ so that S_J is a perfect p-ring and $S_J/pS_J = R_J$. If R is any perefect ring in which $p = 0$ then R is a quotient of R_J for some J by a perfect ideal I. We then set $W(I)(\{\sum_{i\geq 0} p^i[x_i] \text{where} x_i \in I \text{for all} i \geq 0\}$ so that $W(I)$ is an ideal of S_J. The following theorem will state that any perfect ring in which $p = 0$ can easily be constructed from a certain perfect p-ring.

Theorem 3.3. *If R is a perfect ring in which $p = 0$ then there exists a unique perfect p-ring $W(R)$ such that $W(R/pW(R) = R$. If R' is another perfect ring in which $p = 0$ then any $f : R \to R'$ lifts to a unique $W(f) : W(R) \to W(R')$ (so W is covariant functor from the category of perfect rings in which $p = 0$ and perfect p-rings)*

Proof. Write $R = R_J/I$ as above and set $W(R) = S_J/W(I)$ so that we have $W(R)/pW(R) = S_J/(W(I) + pS_J) = R_J/I = R$. Now we check that $W(R)$ is indeed a perfect p-ring. $W(R)/pW(R)$ is perfect because it equals R. The definition of $W(I)$ shows that if $x \in S_J$ satisfies $px \in W(I)$ then $x \in W(I)$ so that p is not a zero divisor in $W(R)$. The ring S_J is complete for the p-adic topology and hence so is $W(R)$. Finally, $\cap_{n\geq 0}(p^n S_J + W(I)) = W(I)$ so that $W(R)$ is separated.

Any perfect p-ring A such that $A/pA = R$ is then the set of elements of the form $a = \sum_{i\geq 0} p^i[x_i]$ with the x_i's in R addition and multiplication given by the formulas (54) and (55). Two such rings are canonically isomorphic.

If $f : R \to R'$ is a homomorphism, then the unique $g : A \to A'$ lifting f is given by $g(\sum_{i\geq 0} p^i[x_i]) = \sum_{i\geq 0} p^i[f(x_i)]$. Indeed the formulas for $+$ and $\times$ recalled above sjow that g thus defined commutes with $+$ and $\times$. □

The ring $W(R)$ is called the ring of Witt vectors with coefficients in R. It is simply the set of elements of the form $\sum_{i\geq 0} p^i[x_i]$ with the x_i's in R addition and multiplication being given by the formulas (54) and (55).

If R is a perfect ring in which $p = 0$ then the Frobenius map $x \mapsto x^p$ is an automorphism. According to the second part of the theorem it lifts to an endomorphism of $W(R)$.

We will state a generalization of the second part of the theorem:

Theorem 3.4. *If A is a ring which is complete for the p-adic topology and if R is a perfect ring of characteristic p then a map $f : R \to A/pA$ lifts to $W(f) : W(R) \to A$*

If A is complete for the p-adic topology as above let $\mathrm{Perf}(A/pA) = \varprojlim_{x\mapsto x^p} A/pA$ so that $\mathrm{Perf}(A/pA)$ is a perfect ring of characteristic p. If $x = (x_0, x_1, \ldots) \in \mathrm{Perf}(A/pA)$ and for each i we choose a lift $\hat{x}_i \in A$ of x_i then the sequence $(\hat{x}_i^{p^i})_{i\geq 0}$ converges in A to an element $x^{(0)}$ which only depend on x(Teichmüller lift).

Corollary 3.5. *The map $\phi : W(\mathrm{Perf}(A/pA)) \to A$ given by the formula*

$$\sum_{i\geq 0} p^i[x_i] \mapsto \sum_{i\geq 0} p^i x_i^{(0)} \tag{62}$$

is a ring homomorphism.

$W(R)$ will be complete for the p-adic topology. However if R itself admits some topology then we can define a finer topology on $W(R)$ called the weak topology. In all cases we need R will be complete.

First we will state a proposition about the a S_n-s from the sum-formula above.

Proposition 3.6. 1. *S_n is a polynomial in $\{X_i^{p^{i-n}}\}_{0\leq i\leq n}$ and in $\{Y_i^{p^{i-n}}\}_{0\leq i\leq n}$;*

2. *S_n is homogenous of degree 1 if each X_i and Y_i is of weight 1;*

3. *S_n is of the form*

$$S_n = (X_n + Y_n) + (X_{n-1}^{p^{-1}} + Y_{n-1}^{p^{-1}})Rn, n-1 + \ldots + (X_0^{p^{-n}} + Y_0^{p^{-n}})R_{n,0} \tag{63}$$

where $R_{n,i} \in S/pS$.

Let val(.) be some valuation on R for which it is complete. If $k \geq 0$ consider the map $w_k : W(R) \to \mathbb{R} \cup \{+\infty\}$ given by $w_k = \inf_{i \leq k} \text{val}(x_i)$ if $x = \sum_{i \geq 0} p^i[x_i]$. If $x \in W(R)$, then $w_k(x) = +\infty$ if and only if $x \in p^{k+1}W(R)$ and if $x, y \in W(R)$ then $w_k(x+y) \geq \inf(w_k(x), w_k(y))$ so that w_k is a semi-valuation on $W(R)$.

These semi-valuations define a topology on $W(R)$ which is called the weak topology. $W(R)$ will also be complete with respect to this topology.

3.2 Galois cohomology

Here we will give a brief review on Galois-cohomology. First let us consider the abelian case. Let M be an abelian group with a group action of G (which in our case will be a topological group with a continuous action). These objects are called G-modules. A homomorphism of G-modules is a homomorphism of abelian groups which commutes with the group action. As in the previous chapter we can define injective G-modules (if every homomorphism on a submodule can be extended to the entire G-module). This category has enough injectives:

Theorem 3.7. *Every G-module can be embedded into an injective G-module.*

Let $M^G = \{m \in M | gm = m \forall g \in G\}$.This is a functor from G-modules into abelian groups. So now lets take a G-module M and injective resolution:

$$0 \to M \to I_0 \to I_1 \to \ldots \tag{64}$$

If we apply the above functor to this exact sequence we get a left exact sequence which in general is not right exact:

$$0 \to M^G \to I_0^G \to I_1^G \to \ldots \tag{65}$$

Its r-th cohomology group is denoted by $H^r(G, M)$. Note that $H^0(G, M) = M^G$. This definition does not really give us a way to compute these groups. However $H^1(G, M))$ can be computed easily. A crossed homomorphism $\phi : G \to M$ is a map that satisfies

$$\phi(ab) = a\phi(b) + \phi(a), a, b \in G. \tag{66}$$

A principal crossed homomorphism is of the form $g \mapsto gm - m$. $H^1(G, M)$ will be the group of crossed homomorphisms modulo the principal homomorphisms.

Usually G will be a Galois group. Here we will state two cases of M's. First let L be a Galois extension of K and $G = \text{Gal}(L|K)$.

Theorem 3.8 (Hilbert theorem 90)**.**

1. $H^1(G, L*) = 0$
2. $H^r(G, L^+) = 0$ *for all* $r > 0$.

For a proof see [M2]. Now we will turn to the non-abelian case. Let G and M be a topological groups and M is equipped with a continuous G-action such that $g(xy) = g(x)g(y)$ for all $x, y \in M$ and $g \in G$. The 0th cohomology group is defined similarly:

$$H^0(G, M) = M^G = \{m \in M | gm = m \forall g \in G\} \tag{67}$$

. We define 1-cocycles in the following way:

$$Z^1(G, M) = \{f : G \to M \text{continuous} | f(g_1 g_2) = f(g_1) \cdot g_1 f(g_2)\} \tag{68}$$

We say that $f, f' \in Z^1(G, M)$ are cohomologous if there exists $a \in M$ such that $f'(g) = a^{-1} f(g) g(a)$ for all $g \in G$. This defines an equivalence relation on $Z^1(G, M)$. The set of equivalence classes form the group (multiplication is composition) $H^1(G, M)$.

For our purposes it suffices to define only these two cohomology groups. It is easy to see that they are indeed generalizations of the abelian cohomology groups. The following theorem is also called Hilbert 90, because it is its generalization (the generalization of the first claim):

Theorem 3.9. $H^1(\mathrm{Gal}(L|K), GL_n(L)) = 1$

For a proof see [F]. Now we have the sufficient background to prove Fontaine's theorem.

3.3 Fontaine's theorem

Now we will turn to Fontaine's theorem. Our goal will be to state a categorical equivalence between the the category of $\mathbb{Q}_p$ representations of G_K and another category which seems to be more explicit. First we start by defining some necessary notions.

If $0 < \delta < \frac{1}{p-1}$ is a real number then let us consider the ideal I of elements x with $\mathrm{val}_p(x) \geq \frac{1}{p-1} - \delta$. Let $\mathbb{C}_p$ be the completion of $\overline{\mathbb{Q}_p}$ which according to Krasner's lemma is also algebraically closed. We define $\widetilde{E}^+ = \{(x_0, x_1, \ldots) \text{ where } x_i \in O_{\mathbb{C}_p}/I \text{ and } x_{i+1}^p = x_i\}$. Addition and multiplication is componentwise. We denote by θ_n the nth projection map $x \mapsto x_n$. If $x \in \widetilde{E}^+$ then for each i we choose a lift $\hat{x}_i \in O_{\mathbb{C}_p}$ of x_i. The sequence $\hat{x}_{i+j}^{p^j}$ converges as $j \to +\infty$ (the sequence is Cauchy) to some $x^{(i)} \in O_{\mathbb{C}_p}$ which only depends on x. This construction is very similar to the Teichmüller representative described at beginning of the section. The natural multiplicative map $\varprojlim_{x \mapsto x^p} O_{\mathbb{C}_p} \to \widetilde{E}^+$ is therefore a bijection. Now we can see that the definition is independent of the choice of I. If $x \in \widetilde{E}^+$ we define the valuation of x as $\mathrm{val}_E(x) = \mathrm{val}_p(x^{(0)})$. The ring $\widetilde{E}^+$ is a perfect ring of characteristic p and is complete with respect to this valuation. Note that $\overline{\mathbb{F}_p}$ maps into $\widetilde{E}^+$ by $\alpha \mapsto ([\alpha^{1/p^n}])_{n \geq 0}$ and that the residue field of $\widetilde{E}^+$ is $\overline{\mathbb{F}_p}$.

Lemma 3.10. *If $P \subset Q$ are two subsets of $\widetilde{E}^+$ then P is dense in Q if and only if $\theta_n(P) = \theta_n(Q)$ for all $n \geq 0$.*

Proof. Note that if $x \in \widetilde{E}^+$ then $\theta_n(x) = 0$ if and only if $\mathrm{val}_E(x) \geq p^{n+1}\mathrm{val}_p(I)$. Let us assume that $\theta_n(P) = \theta_n(Q)$. If $y \in Q$ then let us take an $x \in P$ such that $\theta_n(x) = \theta_n(y)$. Now we have $\theta_n(x - y) = 0$ which means that $\mathrm{val}_E(x - y) \geq p^{n+1}\mathrm{val}_p(I)$. So as the right side of the inequality tends to infinity we get that for any M and any $y \in Q$ there exists an $x \in P$ such that $\mathrm{val}_E(x) \geq M$ which means exactly that P is dense in Q. The reverse implication is similar. □

This lemma will be very useful later on as we will consider a lot of density arguments(this shows again that proofs here are not merely algebraic, that we need to consider the topology as well).

Let $\epsilon = (1, \zeta_p, \zeta_{p^2}, \ldots) \in \widetilde{E}^+$ and $\pi = \epsilon - 1$ so that $\mathrm{val}_E(\pi) = \frac{p}{p-1}$. We define $\widetilde{E} = \widetilde{E}^+[1/\pi]$ so that $\widetilde{E}$ is a perfect field of characteristic p which contains $\mathbb{F}_p((\pi))$. We denote the Frobenius map $x \mapsto x^p$ on $\widetilde{E}$ by ϕ. The group $G_{\mathbb{Q}_p}$ acts on $\mathbb{C}_p$ and this gives a continuous action of $G_{\mathbb{Q}_p}$ on $\widetilde{E}$.

Theorem 3.11. *The field $\widetilde{E}$ is algebraically closed.*

Proof. It is enough to prove that every monic polynomial $P(T) \in \widetilde{E}^+[T]$ has a root in $\widetilde{(E)}$ and we do this by induction on the degree of $P(T)$. Let $P_n(T)$ denote $\theta_n(P) \in (O_{\mathbb{C}_p}/I)[T]$ (which means that we take each coefficients nth coordinate whicg will give us a polynomial with coefficients lying in $O_{\mathbb{C}_p}/I$) and for each n, choose some monic lift $\widetilde{P}_n(T) \in O_{\mathbb{C}_p}[T]$ of P_n. Since $\mathbb{C}_p$ is algebraically closed the polynomial $\widetilde{P}_n(T)$ has a root $\widetilde{\alpha}_{n,n} \in O_{\mathbb{C}_p}$. Let $\alpha_n \in \widetilde{E}$ be an element such that $\alpha_{n,n} \in O_{\mathbb{C}_p}/I$ is the image of $\widetilde{\alpha}_{n,n} \in O_{\mathbb{C}_p}$. We then have $P(\alpha_n) \to 0$ as $n \to \infty$. If $P'(\alpha_n)$ does not converge to 0, then Hensel's lemma tells us that for $n \gg 0$ $P(T)$ has a root close to some α_n and we are done. If $P'(\alpha_n) \to 0$ then by induction $P'(T)$ has $\deg P - 1$ roots in $\widetilde{E}$ and $\{\alpha_n\}_{n \geq 0}$ then converges to one of them, which is then also a root of $P(T)$. □

Let L be a finite extension of $\mathbb{Q}_p$. Let us define $L_n = L(\zeta_{p^n})$ and $L_\infty = \cup_{n \geq 0} L_n$. $H_L = \mathrm{Gal}(\overline{\mathbb{Q}_p}|L_\infty)$. This is obviously a normal subgroup of the absolute Galois group. Let $\widetilde{E}_L^+$ be the set of $x \in \widetilde{E}^+$ such that $x_i \in O_{L_\infty}/I$ for all $i \geq 0$ and let $\widetilde{E}_L = \widetilde{E}_L^+[1/\pi]$ so that $\widetilde{E}_L$ is a perfect field. The Frobenius map $x \mapsto x^p, O_{L_\infty}/I \to O_{L_\infty}/I$ is surjective, so $\theta_n : \widetilde{E}_L^+ \to O_{L_\infty}/I$ is surjective for all $n \geq 0$.

Lemma 3.12. *We have $\widetilde{E}_L = \widetilde{E}^{H_L}$*

Proof. $\widetilde{E}_L \subset \widetilde{E}^{H_L}$ is trivial. The reverse implication is an easy consequence of the Ax-Sen-Tate-theorem which states that following:if we have a complete p-adic field F and a field K contained in its algebraic closure then $\hat{\overline{F}}^{G_K} = \hat{K}$. □

Proposition 3.13.

1. $\overline{\widetilde{E}_K} = \cup_{L|K} \widetilde{E}_L$
2. $\overline{\widetilde{E}_K}$ *is dense in* $\widetilde{E}$
3. $\mathrm{Gal}(\overline{\widetilde{E}_K}|\widetilde{E}_K) = H_K$

Proof. If $L|K$ is finite then the previous lemma implies that $\widetilde{E}_K = \widetilde{E}_L^{\mathrm{Gal}(L_\infty|K_\infty)}$ so that $\widetilde{E}_L|\widetilde{E}_K$ is a finite Galois extension by Artin's lemma [Berger]. Conversely, if $F \subset \widetilde{E}$ is some finite extension of $\widetilde{E}_K$ then it is generated by finitely many elements having finitely many conjugates. The group H_K acts on those elements and some open subgroup of finite index fixes all of them, so that there exists $L|K$ finite such that $F \subset \widetilde{E}_L$. This and the fact that $\widetilde{E}$ is algebraically closed prove the first claim.

The fact that the map $x \mapsto x^p : O_{L_\infty}/I \to O_{L_\infty}/I$ is surjective implies that $\theta_n \widetilde{E}_L^+ = O_{L_\infty}$ and then the first claim implies that $\theta_n(\overline{\widetilde{E}_K}^+) = \cup_{L|K} O_{L_\infty}/I = O_{\mathbb{C}_p}/I$ for all $n \geq 0$ so that by lemma 3.10. $\overline{\widetilde{E}_K}$ is dense in $\widetilde{E}$.

Finally, the fact that $\widetilde{E}_K = \widetilde{E}_L^{\mathrm{Gal}(L_\infty|K_\infty)}$ implies that $\mathrm{Gal}(\widetilde{E}_L|\widetilde{E}_K) = \mathrm{Gal}(L_\infty|K_\infty)$ by Artin's lemma and the third claim now follows from the first. □

Now let $E_{\mathbb{Q}_p} = \mathbb{F}_p((\pi))$ which is a subfield of $\widetilde{E_{\mathbb{Q}_p}}$ since $H_{\mathbb{Q}_p}$ fixes π. Let E be the separable closure of $E_{\mathbb{Q}_p}$ inside $\widetilde{E}$. The group $H_{\mathbb{Q}_p}$ acts on E and therefore we have a map $H_{\mathbb{Q}_p} \to \mathrm{Gal}(E|E_{\mathbb{Q}_p})$.

$E_{\mathbb{Q}_p}^{rad}$ is the smallest field extension of $E_{\mathbb{Q}_p}$ where every element has pth root.

Lemma 3.14. *$E_{\mathbb{Q}_p}^{rad}$ is dense in $\widetilde{E_{\mathbb{Q}_p}}$*

For a proof see [Berger].

$E_{\mathbb{Q}_p}$ and E are quite natural objects to consider. So to study $\mathrm{Gal}(E|E_{\mathbb{Q}_p})$ is also quite natural as it is quite similar to an absolute Galois group. Now we are ready to prove a very important theorem:

Theorem 3.15. *The map $H_{\mathbb{Q}_p} \to \mathrm{Gal}(E|E_{\mathbb{Q}_p})$ is an isomorphism.*

Proof. Lemma 3.14. implies that the algebraic closure of $E_{\mathbb{Q}_p}$ is dense in the algebraic closure of $\widetilde{E_{\mathbb{Q}_p}}$. E is dense in the algebraic closure of $E_{\mathbb{Q}_p}$ but we will not prove this here (see Berger 3.3.2.). If we put these together with Proposition 3.13. then we get that E is dense in $.\widetilde{E}$.

The map $H_{\mathbb{Q}_p} \to \mathrm{Gal}(E|E_{\mathbb{Q}_p})$ is therefore injective, since if $h \in H_{\mathbb{Q}_p}$ acts trivially on E then it acts trivially on $\widetilde{E}$ by continuity and Proposition 3.13. implies that $h = 1$. Finally, if $h \in \mathrm{Gal}(E|E_{\mathbb{Q}_p})$ then h extends by continuity to a map on $\widetilde{E}$ trivial on $E_{\mathbb{Q}_p}^{rad}$ and so on $\widetilde{E_{\mathbb{Q}_p}}$ which therefore comes from an element of $H_{\mathbb{Q}_p}$ again by Proposition 3.13. □

The main idea of the proof was the density argument. E is a field which is very natural to consider but it is difficult to work with. Fortunately it is dense in the field $\widetilde{E}$ which is a perfect field and therefore has the nice properties we have proved in Proposition 3.13.

If we put together Hilbert's theorem 90 (abelian and non-abelian cohomology version) with the previous theorem then we get the following:

Theorem 3.16. *If K is a finite extension of $\mathbb{Q}_p$ then $H^1(H_K, E) = \{0\}$ and if $d \geq 1$ then $H^1(H_K, \mathrm{GL}_d(E)) = \{1\}$(here the cocycles are continuous for the discrete topology).*

Theorem 3.15. means that $E_{\mathbb{Q}_p} = E^{H_{\mathbb{Q}_p}}$. Motivated by that we define $E_K = E^{H_K}$ where K is a finite extension of $\mathbb{Q}_p$ on which $\Gamma_K = G_K/H_K$ acts. The notation E_K is a bit misleading as it only depends on K_∞.

Lemma 3.17. *If π_K is a uniformizer of E_K then $E_K = k_{K_\infty}((\pi_K))$.*

Proof. Since E_K is a finite extension of $E_{\mathbb{Q}_p} = \mathbb{F}_p((\pi))$ the lemma follows from the structure theorem of local fields (stated at the end of the first chapter) and the fact that the residue field of E_K is $\overline{\mathbb{F}}_p^{H_K} = k_{K_\infty}$. □

Let $\widetilde{A} = W(\widetilde{E})$ the ring of Witt vectors over $\widetilde{E}$ and let $\widetilde{B} = \widetilde{A}[1/p]$. $\widetilde{B}$ will be a field (see Berger chapter 5). This field is equipped with the Frobenius $\phi = W(x \mapsto x^p)$ and an action of $G_{\mathbb{Q}_p}$ lifting the action of $G_{\mathbb{Q}_p}$ in $\widetilde{E}$. We also denote by π the element $[\epsilon] - 1 \in \widetilde{A}$ so that the image of π in $\widetilde{E}$ is $\pi = \epsilon - 1$. We cannot construct Witt vectors over E because it is not perfect, so we use a different method to construct a field $B = A[1/p]$ which is stable under ϕ and $G_{\mathbb{Q}_p}$ and such that $A/pA = E$.

Let $A_{\mathbb{Q}_p}$ be the p-adic completion of $\mathbb{Z}_p[[\pi]][1/\pi]$ inside $\widetilde{A}$ and let $B_{\mathbb{Q}_p}[1/p]$ so that $B_{\mathbb{Q}_p}$ is a local field whose residue field is $E_{\mathbb{Q}_p}$.

Lemma 3.18. *If $K|\mathbb{Q}_p$ is a finite extension, then there exist a unique finite unramified extension $B_K|B_{\mathbb{Q}_p}$ contained in $\widetilde{B}$ and whose residue field is E_K.*

Proof. One can take $B_K = B_{\mathbb{Q}_p}[y]$ where y is a root of a polynomial whose reduction modulo p is the minimal polynomial of a primitive element of $E_K|E_{\mathbb{Q}_p}$. □

Let B be the p-adic completion of the maximal unramified extension of $B_{\mathbb{Q}_p}$ inside $\widetilde{B}$. If we set $A = \widetilde{A} \cap B$ then $A/pA = E$ and furthermore, B is stable under ϕ and the action of $G_{\mathbb{Q}_p}$ because of its definition. Finally, we have $\mathrm{Aut}(B|B_{\mathbb{Q}_p}) = \mathrm{Gal}(E|E_{\mathbb{Q}_p}) = H_{\mathbb{Q}_p}$ and for each finite extension $K|\mathbb{Q}_p$ we have $B_K = B^{H_K}$ since $(B_{\mathbb{Q}_p}^{unr})^{H_K} = (\hat{B}_{\mathbb{Q}_p}^{unr})^{H_K}$ by Ax-Sen-Tate theorem. again by Hilbert's theorem 90 we have:

Theorem 3.19. *If K is a finite extension of $\mathbb{Q}_p$ then $H^1(H_K, A) = \{0\}$ and if $d \geq 1$ then $H^1(H_K, \mathrm{GL}_d(A)) = \{1\}$ (here the cocycles are continuous for the p-adic topology).*

An important question is the topology to be considered on $\widetilde{(A)}$. As it is a ring of Witt vectors we can consider the p-adic topology and the weak topology. From now on we will consider the weak topology as the action of G_K on $\widetilde{A}$ will not be continuous for the p-adic topology (just the weak topology).

Let K be a finite extension of $\mathbb{Q}_p$ and let R be one of the rings E_K, A_K, B_K so that R is equipped with a Frobenius ϕ and an action of $\Gamma_K = G_K/H_K$. Now we are ready to define our most important notion:

Definition 3.20. *A (ϕ, Γ)-module over R is a free $R-$module D of finite rank d which is equipped with a semilinear Frobenius ϕ such that $\mathrm{Mat}(\phi) \in \mathrm{GL}_d(R)$ and a commuting and continuous semilinear action of Γ_K.*

If D is a (ϕ, Γ)-module over B_K then we say that D is étale if there is a basis of D in which $\mathrm{Mat}(\phi) \in \mathrm{GL}_(A_K)$.

Our main goal will be to porve that the category of $\mathbb{Q}_p$-linear representations of G_K is equivalent the category of (ϕ, Γ)-modules over B_K. First we will define a functor from $\mathbb{F}_p$-linear representations to (ϕ, Γ)-modules over E_K.

Proposition 3.21. *If W is an $\mathbb{F}_p$-linear representation of G_K od dimension d and if we set $D(W) = (E \otimes_{\mathbb{F}_p} W)^{H_K}$ then $D(W)$ is a (ϕ, Γ)-module over E_K od dimension d and $E \otimes_{E_K} D(W) = E \otimes_{\mathbb{F}_p} W$ so that $W = (E \otimes_{E_K} D(W))^{\phi=1}$.*

Proof. If W is an $\mathbb{F}_p$-linear representation of G_K of dimension d then its restriction to H_K defines a class $[W] \in H^1(H_K, \mathrm{GL}_d(\mathbb{F}_p))$ and by extending scalars from $\mathbb{F}_p$ to E we get a class in $H^1(H_K, \mathrm{GL}_d(E))$. This last group is trivial according to Theorem 3.16. which means that $E \otimes_{\mathbb{F}_p} W$ is isomorphic to E^d as semilinear E-representations of H_K. In particular if we set $D(W) = (E \otimes_{\mathbb{F}_p} W)^{H_K}$ then $D(W)$ is an E_K vector space of dimension d which is stable under ϕ and the action of Γ_K. Finally the facts that $E \otimes_{\mathbb{F}_p} W \simeq E^d$ and $D(W) \simeq E_K^d$ (not as (ϕ, Γ)-modules!) imply that $E \otimes_{E_K} D(W) = E \otimes_{\mathbb{F}_p} W$. □

The exact same proof with A instead of E (and theorem 3.19. instead of 3.16.) gives us the corresponding result below.

Proposition 3.22. *If T is an $\mathbb{Z}_p$-linear representation of G_K od dimension d and if we set $D(T) = (A \otimes_{\mathbb{Z}_p} T)^{H_K}$ then $D(T)$ is a (ϕ, Γ)-module over A_K od dimension d and $A \otimes_{A_K} D(T) = A \otimes_{\mathbb{Z}_p} T$ so that $T = (A \otimes_{A_K} D(T))^{\phi=1}$.*

Finally we will have different proof for B_K because we don't have a cohomological statement theorem 3.16 or 3.19 for B_K. If we apply the same functor we will now get étale (ϕ, Γ)-modules.

Proposition 3.23. *If V is an $\mathbb{Q}_p$-linear representation of G_K od dimension d and if we set $D(V) = (B \otimes_{\mathbb{Q}_p} V)^{H_K}$ then $D(V)$ is an étale (ϕ, Γ)-module over B_K od dimension d and $B \otimes_{B_K} D(V) = B \otimes_{\mathbb{Q}_p} V$ so that $V = (B \otimes_{B_K} D(V))^{\phi=1}$.*

Proof. The representation V admits a G_K-stable lattice T (we will not prove this here, see Fontaine) and since $A \otimes_{\mathbb{Z}_p} T \simeq A^d$ as semilinear A-representations of H_K we have $B \otimes_{\mathbb{Z}_p} V \simeq B^d$ as semilinear B-representations of H_K which implies the result as in the proof of proposition 3.21. The (ϕ, Γ)-module is étale since $D(V) = B_K \otimes_{A_K} D(T)$. □

In order to prove that the functor D has an inverse we will need the following lemma:

Lemma 3.24. *If k is a separably closed field(in our case this will be E) of characteristic p, V is a finite dimensional k-vector space and if V is a (ϕ, Γ)-module over k then:*

1. *V admits a basis of elements fixed by ϕ*
2. *$1 - \phi : V \to V$ is surjective.*

Proof. Choose some element $e_0 \in V$. Let $e_i = \phi^i(e_0)$ and let d be dimension of $\mathrm{Span}(\{e_i\})$ (note that V was finite dimensional). So we can write $e_d = a_0 e_0 + a_1 e_1 + \ldots + a_{d-1} e_{d-1}$. First we are searching for an element that is fixed by ϕ. After we have found one we will consider the factor space V/kV and proceed with an induction argument. We are searching for the fixed element in the constructed subspace, so in other words in the form $v = b_0 e_0 + \ldots + b_{d-1} e_{d-1}$. The condition that ϕ fixes v is equivalent to the following system of equations:

$$b_0 = b_{d-1}^p a_0 \tag{69}$$

$$b_i = b_{i-1}^p + b_{d-1}^p a_i, \text{ for } 1 \leq i \leq d-1 \tag{70}$$

This means that choosing a b_{d-1} will then determine the other b_i-s. A $b_{d-1} = x$ is good if and only if it satisfies the following equation:

$$x = a_0^{p^{d-1}} x^{p^d} + a_1^{p^{d-2}} x^{p^{d-1}} + \ldots + a_{d-1} x^p \tag{71}$$

This equivalent to the following polynomial having a root in k:

$$a_0^{p^{d-1}} t^{p^d-1} + a_1^{p^{d-2}} t^{p^{d-1}-1} + \ldots + a_{d-1} t^{p-1} - 1 \tag{72}$$

This polynomial is separable so it has a root in k which gives us a $v \in V$ which is fixed by ϕ. By induction we have that V/kv has a basis whose element are fixed by ϕ. $(1-\phi)(xv) = (x-x^p)v$. To check that this is surjective we need to see that the equation $(x-x^p)v = av$ has a solution, or equivalently $(x - x^p - a)v = 0$ has a solution. As the polynomial $x - x^p - a$ is separable it will have a solution so $1 - \phi : kv \to kv$ is indeed surjective. V therefore admits a basis of elements fixed by ϕ which proves item (1). The fact that $1 - \phi : kv \to kv$ is surjective if $\phi(v) = v$ and item (1) then imply item (2). □

A corollary of this theorem is that a (ϕ, Γ)-module V over A also admits a basis with elements fixed by ϕ. We will apply these theorem to construct the inverse functor of D.

Theorem 3.25. *If D is a (ϕ, Γ)-module of dimension d over E_K then $W(D) = (E \otimes_{E_K} D)^{\phi=1}$ is an $\mathbb{F}_p$-vector space of dimension d and $E \otimes_{\mathbb{F}_p} W(D) = E \otimes_{E_K} D$*

Proof. Since $E \otimes_{E_K} D$ is a (ϕ, Γ)-module over E and E is seperably closed, the previous lemma tells us that $E \otimes_{E_K} D$ has a basis of elements fixed by ϕ which implies the proposition. □

Theorem 3.26. *If D is a (ϕ, Γ)-module of dimension d over A_K then $T(D) = (A \otimes_{A_K} D)^{\phi=1}$ is an $\mathbb{Z}_p$-module of dimension d and $A \otimes_{\mathbb{Z}_p} T(D) = A \otimes_{A_K} D$*

Proof. The same as above except that we here use the corollary of the lemma. □

Theorem 3.27. *If D is an étale (ϕ, Γ)-module of dimension d over B_K then $V(D) = (B \otimes_{B_K} D)^{\phi=1}$ is an $\mathbb{Q}_p$-vector space of dimension d and $B \otimes_{\mathbb{Q}_p} V(D) = B \otimes_{B_K} D$*

Proof. Since D is étale, it is of the form $B_K \otimes_{A_K} D_0$ where D_0 is a (ϕ, Γ)-module over A_K and the previous theorem tells us that $A \otimes_{A_K} D_0 = A \otimes_{\mathbb{Z}_p} T(D_0)$ where $T(D_0)$ is a free $\mathbb{Z}_p$-module of rank d so that $B \otimes_{B_K} D = B \otimes_{\mathbb{Q}_p} V(D)$ where $V(D) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T(D_0)$ is a $\mathbb{Q}_p$-vector space of dimension d. □

Now if we put these theorems together we get the following equivalences of categories:

Theorem 3.28. *The functor $V \mapsto D(V)$ defines an equivalence of categories:*

1. *$\{\mathbb{F}_p$-linear representations of $G_K\} \to \{(\phi, \Gamma)$-modules over $E_K\}$*
2. *$\{$free $\mathbb{Z}_p$-representations of $G_K\} \to \{(\phi, \Gamma)$-modules over $A_K\}$*
3. *$\{\mathbb{Q}_p$-linear representations of $G_K\} \to \{$étale (ϕ, Γ)-modules over $B_K\}$*

Proof. The functors defined in the previous theorems are all inverse to the D functors. □

4 The local Langlands programme

In the 1960's a Canadian professor Robert Langlands proposed a series of conjectures. The global version gives a correspondence between the representations of the absolute Galois group of a number field(i.e. a finite extension of $\mathbb{Q}$) and cuspidal representations of $\mathrm{GL}_n(\mathbb{A}_F)$ where $\mathbb{A}_F$ is the ring of adeles. In this chapter we will give a description of local Langlands conjecture. The local Langlands conjecture is a generalization of local class field theory which originates from the follwoing result:

Theorem 4.1 (local Kronecker-Weber)**.** *Every abelian extension of $\mathbb{Q}_p$(i.e where the Galois group is abelian) is contained in a cyclotomic extension.*

Local class field theories goal is to provide a description of a maximal abelian extension of any local field K. Let K be a finite extension of $\mathbb{Q}_p$, k its residue field. G_K and G_k will be absolute Galois groups respectively. We saw earlier that there is homomorphism $G_K \to G_k$. G_k is topologically generated by the Frobenius element. Let W_K denote the elements of G_K whose image is an integral power of the Frobenius element. This is a subgroup of G_K and is called the **Weil-group** of K. One of the main results of Local class field theory is the followong isomorphism:

$$W_K^{ab} \simeq K^* \tag{73}$$

Using this isomorphism we can identify the set of 1-dimensional continuous representations of $K^* = \mathrm{GL}_1(K)$ with the set of 1-dimensional continuous representations of W_K. Our goal will be to generalize this result to n-dimensional representations however we will need a few more notions as the generalizations does not go directly. First we consider finite dimensional representations of $\mathrm{GL}_n(K)$.

Definition 4.2. *A representation is called **smooth** if each vectors stabilizer is an open subgroup. A representation is called **admissible** if for any subgroup $H \subset \mathrm{GL}_n(K)$ V^H is finite dimensional.*

Note that if a representation is smooth and irreducible it is automatically admissible. Let $A_n(K)$ denote the set of equivalence classes of admissible and irreducible representations of $\mathrm{GL}_n(K)$ (over $\mathbb{C}$). Note that these representations can be infinite dimensional. Let $A_n^0(K)$ denote the equivalence classes of **cuspidal**,admissible and irreducible representations of $\mathrm{GL}_n(K)$. For a definition of this notion, see [Ca, 2]. This side is the automorphic side of the correspondence.

We will now turn to the Galois side. Let $G_n^0(K)$ denote the equivalence classes of n-dimensional irreducible l-adic representations of the Weil-group. The following theorem is due to Harris and Taylor(Henniart gave a simpler proof later):

Theorem 4.3. *There is a on-tone- correspondence between $A_n^0(K)$ and $G_n^0(K)$ which preserves L-functions and ϵ-factors.*

So when $l \neq p$ the local Langlands conjecture is now a theorem. The most important open question now in this field is Fontaine-Mazur conjecture stated at the end of section 2.

The case where $l = p$ is now very important research area. The exact formulation of the Langlands conjecture is not even known in this case however recent developments have indicated that a similar connection must exist in the p-adic case as well. Such a correspondence has been proven for the case of $\mathrm{GL}_2(\mathbb{Q}_p)$ by Pierre Colmez in 2010([Co1, 3]):

Theorem 4.4. *Let L be a finite extension of $\mathbb{Q}_p$. There is a one-to-one correspondence between the 2-dimensional, irreducible L-representations of $G_{\mathbb{Q}_p}$ and the unitary, admissible and irreducible L-representations of* $\mathrm{GL}_2(\mathbb{Q}_p)$.

The main tool of the proof are the (ϕ, Γ)-modules described in the previous section. However not much is known in the case of $\mathrm{GL}_n(\mathbb{Q}_p)$ where $n > 2$.

References

[1] L. Berger, Galois representations and (Φ, Γ)-modules: `http://perso.ens-lyon.fr/laurent.berger/ihp2010.php`

[2] H. Carayol, Preuve de la conjecture de Langlands locale pour GLn: travaux de Harris-Taylor et Henniart, *Séminaire Bourbaki*, (1999)

[3] P. Colmez, Représentations de $\mathrm{GL}_2(\mathbb{Q}_p)$ et (φ, Γ)-modules, *Astérisque* **330** (2010), 281–509.

[4] J.-M. Fontaine,Yi Ouyang, Theory of p-adic Galois-representations: `staff.ustc.edu.cn/~yiouyang/galoisrep.pdf`

[5] A. Grothendieck, Sur quelque point d'algèbre homologique, Tohoku Math. J. (2) Volume 9, Number 2 (1957), 119-221.

[6] A. Kret, Galois representations, Master's Thesis, 2009.

[7] J.S. Milne, Algebraic Numkber Theory: `www.jmilne.org/math`, (2012)

[8] J.S. Milne, Class Field Theory: `www.jmilne.org/math`, (2011)

[9] J.S. Milne, Lectures on Étale Cohomology: `www.jmilne.org/math`, (2012)

[10] J.Neukirch, Algebraic Number Theory, Grundlehren der mathematischen Wissenschaften, 322, Berlin, Springer-Verlag, (1999).

[11] J.H. Silverman, The Arithmetic of Elliptic Curves, Garduate Texts in Mathematics, Spinger-Verlag, (2008)