FONTAINE'S PERIOD RINGS

SANYAM GUPTA

Abstract. This is a report on the TER done under the supervision of Prof. Benoit Stroh at Sorbonne University. The aim of this project is to understand the absolute Galois group of $\mathbb{Q}_p$, and its continuous representations. This is a subject of central importance in arithmetic and algebraic geometry, especially within the Langlands curriculum.

Contents

1. Preliminaries

1.1. **A brief summary of Witt Vectors.** Let R be a ring of characteristic p, then we say that it is *perfect* if the Frobenius morphism $\phi : R \to R$ given by $a \mapsto a^p$ is an isomorphism. Some examples of perfect rings are: finite fields of characteristic p; algebraically closed field of characteristic p, or the ring of integers of an algebraically closed field of characteristic p. The theory of Witt vectors allows us to construct a ring A, in which p in not nilpotent, and such that A is separated and complete for the topology defined by the ideals $p^n A$, i.e., the p-adic topology.

Definition 1 (Strict p-ring)**.** Let p be an integral prime. A ring R is called *strict p-ring* provided that R is complete and Hausdorff with respect to the p-adic topology , p is not a zero-divisor in R, and the residue ring $K = R/p$ is perfect ring (i.e., the map $x \to x^p$ is bijective on K).

Example 1.1. Let $R = \mathbb{Z}_p$, then R is complete and Hausdorff with respect to the p-adic topology, also p is not a zero-divisor in R. The residue field $K = \mathbb{F}_p$, which is a finite field, so it is perfect. Thus, $\mathbb{Z}_p$ is a strict p-ring.

The following is the main result from the theory of Witt vectors.

Theorem 1. *Let R be a perfect ring of characteristic p.*

(1) *There is a strict p-ring $W(R)$ with residue ring R, which is unique up to canonical isomorphism.*

(2) *There exists a unique multiplicative section of* $\pi : W(R) \to R$, *denoted by* $\tau : R \to W(R)$ *(i.e.,* $\pi \circ \tau = \mathrm{id}_{W(R)}$*), called the Teichmüller map.*

(3) *Every element* x *of* $W(R)$ *can be written uniquely in the form* $x = \sum_{n=0}^{\infty} \tau(x_n)p^n$ *for* $x_n \in R$.

(4) *The formation of* $W(R)$ *and* τ *is functorial in* R, *in that if* $f : R \to R'$ *is a homomorphism of perfect rings of characteristic* p, *and* $W(R')$ *is the strict* p*-ring with residue ring* R' *and section* τ', *then there is a unique homomorphism* $F : W(R) \to W(R')$ *making the following two squares commute:*

$$\begin{array}{ccc} W(R) & \xrightarrow{F} & W(R') \\ \downarrow & & \downarrow \\ R & \xrightarrow{f} & R' \end{array}$$

$$\begin{array}{ccc} W(R) & \xrightarrow{F} & W(R') \\ {\scriptstyle\tau}\uparrow & & \uparrow{\scriptstyle\tau'} \\ R & \xrightarrow{f} & R' \end{array}$$

The map F *is given by*

$$F\left(\sum_{n=0}^{\infty} \tau(x_n)p^n\right) = \sum_{n=0}^{\infty} \tau'(f(x_n))p^n.$$

Proof. cf. [6], Chpater 2. ∎

Example 1.2. If $R = \mathbb{F}_P$, then $W(R) = \mathbb{Z}_p$ and more generally if R is a finite field of characteristic p, then $W(R)$ is the ring of integers of the unique unramified extension of $\mathbb{Q}_p$ whose residue field is R. If $R = \overline{\mathbb{F}}_p$, then $W(R) = \mathcal{O}_{\widehat{\mathbb{Q}_p^{ur}}}$.

Example 1.3. Let A be an unramified extension of $\mathbb{Z}_p$ (i.e. pA is the unique prime in A) and $K = A/pA \simeq \mathbb{F}_q$. Then A is a strict p-ring, and is hence the unique strict p-ring with residue field $\mathbb{F}_q$. We can construct the Teichmuller representatives as follows: we know that $\mathbb{F}_q$ is the the

splitting field of $X^q - X \in \mathbb{F}_p[X]$, so the non-zero elements of $\mathbb{F}_q$ are the roots of the polynomial $X^{q-1} - 1$. By Hensel's lemma, each element $\alpha \in \mathbb{F}_q^*$ has a unique lift $\tau(\alpha) \in A$ also satisfying $\tau(\alpha)^{q-1} - 1 = 0$. Setting $\tau(0) = 0$ completes the definition of the map τ.

1.1.1. *Teichmüller map.* Suppose that R is a perfect ring of characteristic p. If $x \in x_0 \in R$, then for every $n \geq 0$, choose an element $\tilde{x_n}$ in $W(R)$ whose image in R under the map $\pi : W(R) \to R$ is $x^{p^{-n}}$. The sequence $\tilde{x_n}^{p^n}$ then coverges in $W(R)$ to an element $[x]$ which depends only on x. The map $\tau : R \to W(R)$, $x \mapsto [x]$ is the Teichmüller map, which is a section of the projection map $\pi : W(R) \to R$. The Teichmüller elements (the elements in the image of the Teichmüller map) are a distinguished set of representatives of the elements of R. Given two elements $x, y \in W(R)$, one can write

$$x + y = \sum_{n=0}^{+\infty} [S_n(\underline{X}, \underline{Y})]p^n, \quad xy = \sum_{n=0}^{+\infty} [P_n(\underline{X}, \underline{Y})]p^n,$$

where $S_n, P_N \in \mathbb{Z}[X_i^{p^{-n}}, Y_i^{p^{-n}}]_{i=0,\ldots,n}$ are universal homogeneous polynomials of degree 1 (if we consider the degree of X_i and Y_i to be 1). Some initial examples of these polynomials: $S_0(X_0, Y_0) = X_0 + Y_0$ and $S_1(X_0, X_1, Y_0, Y_1) = X_1 + Y_1 + p^{-1}((X_O^{1/p} + Y_0^{1/p})^p) - X_0 - Y_0)$. The easiest way to construct $W(R)$ is then by setting $W(R) = \prod_{n=0}^{+\infty} R$ and by making it into a ring using the addition and multiplication defined by the P_n and S_n, which are given simple functional equations.

1.2. **Ramification.** Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. We have $\iota : \mathbb{Q} \hookrightarrow \mathbb{Q}_p \to \overline{\mathbb{Q}}_p$, where the first embedding is the canonical embedding of $\mathbb{Q}$ in $\mathbb{Q}_p$, and we canonically extend the p-adic absolute on $\mathbb{Q}$ to $\mathbb{Q}_p$, the second map is the unique embedding of $\mathbb{Q}_p$ into its algebraic closure, and we uniquely extend the p-adic absolute value on $\mathbb{Q}_p$ to $\overline{\mathbb{Q}}_p$ (because $\mathbb{Q}_p$ is complete with respect to the p-adic absolute value). Let $\tau : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ be an emmbedding (non-unique) over $\iota : \mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}_p$. For $\alpha \in \overline{\mathbb{Q}}$ define

$$|\alpha|_\tau = \big|\tau(\alpha)\big|_p,$$

then $|*|_\tau$ is an absolute value on $\overline{Q}$. Then the decomposition group D_p at p is defined as

$$D_p := \{\sigma \in G_{\mathbb{Q}} : \left|\sigma(\alpha)\right|_\tau = |\alpha|_\tau \, \forall \, \alpha \in \overline{\mathbb{Q}}\}.$$

Note that the definition of D_p depends on the choice of $\tau : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$.

Example 1.4. The l-adic cyclotomic character $\chi_l : G_{\mathbb{Q}} \to \mathbb{Q}_l^*$ is unramified at all primes $p \neq l$.

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(n, K)$ be an n-dimensional Galois representation over a field K, and let p be an integral prime.

We recall some basic facts about the extensions of valuations.

Proposition 2. (1) *The residue field of $\overline{\mathbb{Q}}_p$ is $\overline{\mathbb{F}}_p$.*

(2) *Let $\sigma \in G_{\mathbb{Q}_p}$, then σ preserves the valuation ring $\mathcal{O}_{\overline{\mathbb{Q}}_p}$ and the maximal ideal $\mathfrak{P}$ of $\overline{\mathbb{Q}}_p$.*

(3) *We have a natural map $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$, given by $\sigma \mapsto \overline{\sigma}$, where $\overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)}$.*

(4) *The above natural map is a continuous homomorphism.*

Proof. (1) Let l be the residue field of $\overline{\mathbb{Q}}_p$. Let $\overline{\mathbb{F}}_p$ be the algebraic closure of $\mathbb{F}_p$ containing l. Let $\alpha \in \overline{F}_p$, and suppose $f(x) \in \mathbb{F}_p[x]$ be its minimal polynomial. Let $F(x) \in \mathbb{Z}_p[x]$ be a lift of $f(x)$. Then $\overline{\mathbb{Q}}_p$ contains all the roots of $F(x)$, so its residue class field l must contain all the roots of $f(x)$. Thus $\alpha \in l$. So, $l = \overline{\mathbb{F}}_p$.

(2) We know that for any $\alpha \in \overline{\mathbb{Q}}_p$ and $\sigma \in G_{\mathbb{Q}_p}$, we have $\left|\sigma(\alpha)\right| = |\alpha|$.

(3) We nned to verify that if $\overline{\sigma}(\overline{\alpha}) = 0$ in $\overline{\mathbb{F}}_p$, then $\overline{\alpha}$. But $\overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)} = 0$, so $\sigma(\alpha) \in \mathfrak{P}$, since $|\alpha| = \left|\sigma(\alpha)\right| < 1$, so $\alpha \in \mathfrak{P}$, i.e., $\overline{\alpha}$.

(4) The map is a homomorphism is easy to check. To show the continuity, let $\mathbb{F}_p \subset k \subset \overline{\mathbb{F}}_p$ be a finite extension

■

1.2.1. *Wild Ramification.* Let K be an Henselian field with respect to a valuation v. Let L/K be an algebraic extension, denote by T/K the maximal unramified subxtension of L/K (which is the composite of all unramified subextensions).

Proposition 3. *The residue class field of T is the separable closure λ_s of κ in the residue class field extension λ/κ of L/K, whereas the value group of T equals that of K.*

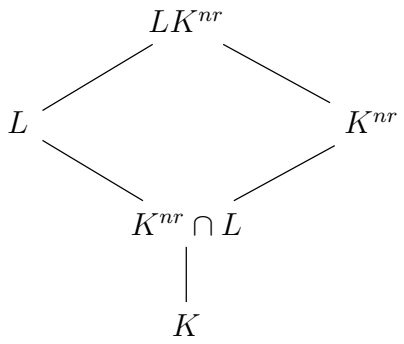
Proof. Let λ_0 be the residue clas field of T and assume that $\overline{\alpha} \in \lambda$ is separable over. We need to show that $\overline{\alpha} \in \lambda_0$. Let $\overline{f}(x) \in \kappa[x]$ be the minimal polynomial of $\overline{\alpha}$ over κ, and $f(x) \in \wr[x]$ be a monic lift of $\overline{f}(x)$. Then $f(x)$ is irreducble and by Hnesel's lemma has a root $\alpha \in L$ such that $\overline{\alpha} = \alpha \pmod{\mathfrak{P}}$, i.e., $[K(\alpha) : K] = [\kappa(\overline{\alpha}) : \kappa]$, so $K(\alpha)/K$ is unramified, $K(\alpha) \subseteq T$, and thus $\overline{\alpha} \in \lambda_0$.

We know that $e(T/K) = [w(T^*) : v(K^*)]$, since T/K is unramified, so $w(T^*) = v(K^*)$. ■

If $p > 0$ is the characteristic of κ, then one has the following weker notion accompanying that of an unramified extension.

Definition 2. An algebraic extension L/K is called *tamely ramified* if the extension λ/κ of the residue class fiels id separable and one has $p \nmid [L : T]$. In the infinite case this latter condition is taken to mean that the degree of each finite subextension of L/T is prime to p.

Recall that, if L/K is finite, then $e(L/K) = e(L/T)e(T/K) = e(L/T)$, since T/K is unramified. Suppose that the valuation v on K is discrete, and L/K is separable, then $e(L/K)f(L/K) = [L : K]$. Furthermore, if λ/κ is separable, then L/K is unramified (resp. tamely ramified) if and only if $e(L/K) = 1$ (resp. $p \nmid e(L/K)$). An extension L/K is wildly unramified if it is not tamely ramified.



The above diagram implies that L/K is tamely ramified iff LK^{nr}/K^{nr} is tamely ramified. Thus it suffices to assume that $K = K^{nr}$, i.e., L/K is totally ramified.

Lemma 4. *Let K be a p-adic field and L/K be a finite extension, let π_L be a uniformizer of L, then L/K is totally ramified if and only if $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ and the minimal polynomial of π_L is Eisenstein.*

Proof. See [7]. ∎

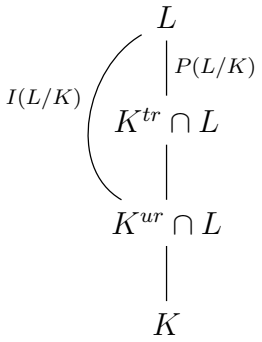
Theorem 5. *Let K be a p-adic number field and let L/K be a finite extension such that $p \nmid n = [L : K]$. Then L/K is totally tamely ramified if and only if $L = K(\pi_K^{\frac{1}{n}})$.*

Proof. Since L/K is totally ramified, we have $\kappa_L \cong \kappa_K$. Let $\mathfrak{P}$ and $\mathfrak{p}$ be the prime ideals of L and K with uniformizers π_L and π_K resp. Then, total ramification implies that $\pi_L^n = \pi_K u$ for some $u \in \mathcal{O}_L^*$. Since, $\kappa_L \cong \kappa_K$, there exists $u_0 \in \mathcal{O}_K^*$ such that $u \pmod{\mathfrak{P}} = u_0 \pmod{\mathfrak{p}}$. We can replace, π_K with $\pi_K u_0^{-1}$, so that we can assume that $u \equiv 1 \pmod{\mathfrak{P}}$. Now by Hensel's lemma $x^n - u$ has a root α in $\mathcal{O}_L$. Let $\pi = \frac{\pi_L}{\alpha}$, then $\pi^n = \pi_K$, so the minimal polynomial of $\pi \in \mathcal{O}_L$ is $x^n - \pi_K$ (this is Eisenstein at π_K). Thus from the above lemma $\mathcal{O}_L = \mathcal{O}_K[\pi]$, so $L = K(\pi) = K(\pi_K^{\frac{1}{n}})$. ∎

If L/K^{nr} is a finite extension, then it is totally ramified, equivalently $e(L/K^{nr}) = [L : K^{nr}]$. Suppose $p \nmid [L : K^{nr}]$, then L/K^{nr} is totally tamely ramified if and only if $L = K^{nr}(\pi_K^{\frac{1}{n}})$.

Corollary 5.1. *Tamely ramified extensions of K form a distinguished class.*

Let K^{tr} be the maximal tamely ramified extension of K. Then for any Galois extension L/K we define the *wild ramification group* $P(L/K) \subseteq \mathrm{Gal}(L/K)$ to be $\mathrm{Gal}(L/L \cap K^{tr})$. We have the following tower:



giving rise to the filtration

$$\{\mathrm{id}\} \subseteq P(L/K) \subseteq I(L/K) \subseteq \mathrm{Gal}(L/K).$$

Now, L/K is tamely ramified if and only if $K^{tr} \cap L = L$, i.e., $P(L/K)$ is trivial. As per usual, we shorten $P(\overline{K}/K)$ to P_K.

Theorem 6. *Let L/K be a Galois extension of p-adic number fields. Then, $P(L/K) = I_1(L/K)$ where*

$$I_1(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{m}_L^2}\}.$$

1.3. **Setting.** Let K be a finite extension of $\mathbb{Q}_p$. Let $v_p : K \to K \to \mathbb{Q} \sqcup \{+\infty\}$ be the valuation on K normaliwed by $v_p(p) = 1$. The image of $K^\times$ under v_p is a discrete subgroup of $\mathbb{Q}$ containing $\mathbb{Z}$, so it is equal to $\frac{1}{e}$ for some positive integer e., where e is the *absolute ramification index* of K. A uniformizer of K is an element of minimal posiitve valuation, that is of valuation $\frac{1}{e}$. We fix a uniformizer π of K.

Let $\mathcal{O}_K = \{x \in K : v_p(x) \geq 0\}$ be the ring of integers of K. We recall that $\mathcal{O}_K$ is a local ring whose maximal ideal is $\mathfrak{m}_K = \{x \in K : v_p(x) > 0\}$. The quotient $\mathcal{O}_K/\mathfrak{m}_K$ is called the residue field, denote it by k, then k is a finite field of characteristic p.

Let $W(k)$ denote the ring of Witt vectors with coefficients in k. Set $K_0 = \mathrm{Frac}(W(k))$, by the theory of Witt vectors K_0 is the unique unramified extension of $\mathbb{Q}_p$ with residue field k. We also have a canonical embedding $K_0 \to K$, and thorugh this embedding, K/K_0 is totally ramified of degree e. Therefore, K_0 is the maximal subextension of K which is unramified over $\mathbb{Q}_p$.

1.4. **The absolute Galois group of K.** Let us fix an algebraic closure $\overline{K}$ of K, then the valuation v_p extends uniquely to $\overline{K}$ (see [5], Chapter 2, Theorem 4.8). Let $\mathcal{O}_{\overline{K}} = \{x \in \overline{K} : v_p(x) \geq 0\}$ be the ring of integers of $\overline{K}$, this is a local ring whose maximal ideal is denoted by $\mathfrak{m}_{\overline{K}}$.

Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K.

Lemma 7. *For $\alpha \in \overline{K}$ and $\sigma \in G_K$ we have $\big|\sigma(\alpha)\big| = |\alpha|$.*

Proof. Let $f(x)$ be the minimal polynomial of α, then the minimal polynomial of $\sigma(\alpha)$ is also $f(x)$ (since $\sigma(f(\alpha)) = f(\sigma(\alpha))$), so $N_{K(\alpha)/K}(\alpha) = f(0) = N_{K(\sigma(\alpha))/K}(\sigma(\alpha))$. It follows that

$$\big|\sigma(\alpha)\big| = \big|N_{K(\sigma(\alpha))/K(\sigma(\alpha))}\big|^{1/n} = \big|N_{K(\alpha)/K}(\alpha)\big|^{1/n} = |\alpha|,$$

where n is the degree of f. ∎

Lemma 7 implies that the G_K acts on $\overline{K}$ by isometry and therefore stabilizes $\mathcal{O}_{\overline{K}}$ and $\mathfrak{m}_{\overline{K}}$. This induces anatural action of G_K on the residue field $\overline{k}$. This defines a group homomorphism $G_K \to \mathrm{Gal}(\overline{k}/k)$, which is surjective. The kernel of this morphism is the inertia subgroup; which we denote by I_K is what follows. The fixed field of I_K is the maximal unramified extension of K; we will denote it by K^{ur}. In other

words we have following exact sequence

$$1 \to I_K \to G_K \to \mathrm{Gal}(\overline{k}/k) \to 1.$$

We already know the structure of $\mathrm{Gal}(\overline{k}/k)$: if the cardinality of k is $q = p^r$, then $\mathrm{Gal}(\overline{k}/k) \simeq \hat{\mathbb{Z}}$ is the profinite group generated by the Frobenius map $\mathrm{Frob}_q : x \to x^q$.

We shorten $P(\overline{K}/K)$ to P_K, as we did with the inertia subgroup. By Theorem 5 we can explicitly describe K^{tr}. Namely, it's $K^{ur}(\{\sqrt[n]{\pi_K} : (n,p) = 1\})$ or, combinig this with our description of K^{ur}, it is $K(\{\sqrt[n]{\pi_K}, \zeta_n : (n,p) = 1\})$. This also implies that the most of the complicated nature of G_K, where K is a p-adic nulber field, is concentrated in P_K. Thus, statements of the form "Property/claim $---$ for G_K is difficult" is really a statement about P_K. In other words, we want to show that G_K/P_K is a relatively simple group. We already know that $G_K/I_K \simeq \mathrm{Gal}(\overline{k}/k) \simeq \hat{\mathbb{Z}}$ and it follows easily from theorem 5 that $I_K/P_K \simeq= \varprojlim_{n, p\nmid n} \mathbb{Z}/n\mathbb{Z} \simeq \prod_{l\neq p} \mathbb{Z}_l$. In fact, Theorem 5 actually shows more. Namely, it shows that P_K is normal in G_K and that

$$G_K/P_K = \mathrm{Gal}(K^{tr}/K) \simeq \prod_{l\neq p} \mathbb{Z}_l \rtimes \hat{\mathbb{Z}}.$$

1.5. **The cyclotomic extension.** Let K be a finite extension of $\mathbb{Q}_p$, and let $\mu_n \subset \overline{K}$ be the group of n-th roots of unity. Then the extension $K(\mu_n)/K$ is Galois and its Galois group canonically embeds into $(\mathbb{Z}/n\mathbb{Z})^\times$: if $\sigma \in \mathrm{Gal}(K(\mu_n)/K)$ and $\zeta_n \in \mu_n$ is a primitive n-th root of unity, then $\sigma(\zeta_n)$ is also a primitive n-th root of unity, so $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$, for some $a_\sigma \in \mathbb{Z}$, uniquely determined modulo n by σ, and $(a_\sigma, n) = 1$. We obtain the following injection

$$\chi_{n,K} : \mathrm{Gal}(K(\mu_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto (a_\sigma \pmod n).$$

Remark. The map $\chi_{n,K}$ is in general not surjective although it is for all n when $K = \mathbb{Q}_p$.

If n is coprime to p, then $K(\mu_n)/K$ is unramified, because $X^n - 1$ is separable over k_K. In this case, $K(\mu_n)$ appears as a subextension of K^{ur}, and if $n = p^r$ is a power of p, then the extension $K(\mu_{p^r})/K$ is totally ramified. Let $\mu_{p^\infty} := \cup_{r\geq 1}\mu_{p^r}$, then

$$K_{p-cycl} = K(\mu_{p^\infty}) := \bigcup_{r\geq 0} K(\mu_{p^r})$$

is an infinite Galois extension of K. Recall that $K(\mu_{p^r})/K$ is Galois and its Galois group $\mathrm{Gal}(K(\mu_{p^r})/K)$ canonically embeds in $(\mathbb{Z}/p^r\mathbb{Z})^\times$, this gives rise to the following injetcive group homomorphism:

$$\chi_{p^\infty} : \mathrm{Gal}(K(\mu_{p^\infty})/K) = \varprojlim_r \mathrm{Gal}(K(\mu_{p^r})/K) \hookrightarrow \varprojlim_r (\mathbb{Z}/p^r\mathbb{Z})^\times.$$

We claim that $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$, where $\mathbb{Z}_p^\times$ are the p-adic units. Indeed, $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times$ is a subset consisting of elements (a_n), where $a_1 \not\equiv 0 \pmod p$, so (a_n) corresponds to a unit in $\mathbb{Z}_p$. Conversely, if $\sum_{n\geq 1} x_n l^n \in \mathbb{Z}_p^\times$, then $x_0 \in (\mathbb{Z}/pZ)^*$, thus $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$. Let

$$\chi_{cycl} : G_K \to \mathbb{Z}_p^\times$$

be the homomorphism obtained by precomposing χ_{p^∞} with the canonical surjection $G_K \twoheadrightarrow \mathrm{Gal}(K(\mu_{p^\infty})/K)$.

Now, $\mathbb{Z}_p^\times \subset \mathbb{Q}_p^\times = \mathbb{Q}_p \setminus \{0\}$, so we actually have the following group homomorphism

$$\chi_{cycl} : G_K \to \mathbb{Z}_p^\times \hookrightarrow \mathbb{Q}_p^\times = \mathrm{GL}(1, \mathbb{Q}_p).$$

It is easy to see that:

$$\mathrm{Ker}(\chi_{cycl}) = \{\sigma \in G_K : \sigma|_{K(\mu_{p^r})} = \mathrm{id}\ \forall\, r \geq 1.\}$$

So the subextension of $\overline{K}/K$ corresponding to $\mathrm{Ker}(\chi_{cycl})$ is $K(\mu_{p^\infty})/\mathbb{Q}$. More generally, for all positive integers $n \geq 1$, the subextension associated to $\mathrm{Ker}(\chi_{cycl} \pmod{p^r})$ is $K(\mu_{p^r})/K$.

2. Galois Representations

The main program of algebraic number theory and arithmetic geometry is to understand the structure of the Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{Q}/Q)$. One can try to do so by understanding the representations of $G_{\mathbb{Q}}$. However, this in itself is not an easy task, as the group $G_{\mathbb{Q}}$ is extremely big. We know that the absolute Galois group $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{Q_p}/Q_p)$ of $\mathbb{Q}_p$ for a prime p is naturally embeded into $G_{\mathbb{Q}}$ and the image of $G_{\mathbb{Q}_p}$ in $G_{\mathbb{Q}}$ is called the *decomposition group* at p, denoted by D_p. It is very difficult to directly study the representations of $G_{\mathbb{Q}}$, and the theory that is obtained is not very rich. Instead, by studying the restriction of representation of $G_{\mathbb{Q}}$ to $G_{\mathbb{Q}_p}$ we get a richer theory. In general, one can study the representations of the Galois group of any finite extension K of $\mathbb{Q}_p$.

2.1. **Complex Galois Representations.** In this section, we analyse the complex representations of $G_{\mathbb{Q}}$. Let $\rho : G_{\mathbb{Q}}$ be a complex n-dimensional Galois representation. The topologies of $G_{\mathbb{Q}}$ and $\mathbb{C}$ are very qualitatively different, and this puts strong restrictions on the possible ρ. One such difference is that $G_{\mathbb{Q}}$ has arbitrary small subgroups, in the sense that any neighborhood of the identity contains some subgroup (because the open subgroups $\mathrm{Gal}(\overline{Q}/K)$ for $K/\mathbb{Q}$ finite Galois form a neighborhood basis of identity). While, as we know that, $\mathrm{GL}(n, \mathbb{C})$ has no small subgroups: there exists a neighborhood V of identity, such that the only subgroup contained in V is trivial.

Proposition 8. *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(n, \mathbb{C})$ be a complex Galois representation. Then ρ factors as $G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}(n, \mathbb{C})$ for some finite Galois $K/\mathbb{Q}$.*

Proof. Let $V \subseteq \mathrm{GL}(n, \mathbb{C})$ be an open neighborhood of identity such that it does not contain any non-trivial subgroups of $\mathrm{GL}(n, \mathbb{C})$. Since ρ is continuous, $\rho^{-1}(V)$ is a open neighborhood of identity in $G_{\mathbb{Q}}$, so there is a finite subset $S \subset \overline{\mathbb{Q}}$, such that $G(S) \subset \rho^{-1}(V)$, but $G(S) =$

$\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, where $K = \mathbb{Q}(S)$. So, $G(S) \subset \mathrm{Ker}(\rho)$ and the result follows. ■

Thus, the theory of complex Galois representations is identical to the representation theory of finite groups [6].

2.2. **l-adic Galois Representations.** Let $K/\mathbb{Q}_p$ be a finite extension, then a Galois representation $\rho : G_K \to \mathrm{GL}(n, F)$ of G_K is called a l-adic Galois representation of dimension n of G_K if F is a finite extension of $\mathbb{Q}_l$ (where l is some prime may or may not be equal to p). Among all representations of G_K, the simplest ones are of course one dimensional representation (also called characters of G_K). We have already seen an example of such character: the cyclotomic character χ_{cycl}. We give two more examples of such characters:

Example 2.1.

$$\omega_{cycl} : G_K \xrightarrow{\chi_{cycl}} \mathbb{Z}_p^\times \xrightarrow{(\mathrm{mod}\ p)} \mathbb{F}_p^\times \xrightarrow{[\cdot]} \mathbb{Z}_p^\times$$

where the last map takes an element to its Teichmuller representative. This is a finite order character, whise order divides $p-1$. When $K = \mathbb{Q}_p$, the order of ω_{cycl} is exactly $p-1$.

Example 2.2. The other family of characters is that of unramified characters, i.e., those which acts on the inertia subgroup trivially. Since $G_K/I_K \simeq \mathrm{Gal}(\overline{k}/k)$ is procyclic, continuous unramified characters are easy to describe: they are all of the form:

$$\mu : G_K \to G_K/I_K \simeq \mathrm{Gal}(\overline{k}/k) \xrightarrow{\mathrm{Frob}_q \to \lambda} \mathbb{Z}_p^\times$$

for λ varying in $\mathbb{Z}_p^\times$.

We can describe all the characters of G_K explicitly using local class field theory.

At this point, we want to emphasize that p is a fixed prime from the beginning and l is any prime. When $l \neq p$, then the incompatibility

of the topologies of G_K (p-adic in nature) and $\mathrm{GL}(n, F)$ (F is an extension of $\mathbb{Q}_l$, so l-adic in nature), gives rise to the famous theorem of Grothendieck:

Theorem 9 (Grothendieck's l-adic monodromy theorem)**.** *Let $K/\mathbb{Q}_p$ be a finite extension. Then all l-adic representations of G_K are potentially semistable.*

Proof. See [4]. ■

In what follows our main focus will be the p-adic Galois representations, that is, when $l = p$.

3. Semi-linear representations

Denote by $\mathbb{C}_p$ the p-adic completetion of $\overline{\mathbb{Q}}_p$, it is well known that $\mathbb{C}_p$ is algebraically closed.

Let K be a finite extension of $\mathbb{Q}_p$, let V be a given representation of G_K. Let $W = \mathbb{C}_p \otimes_{\mathbb{Q}_p} V$, then W is a $\mathbb{C}_p$-representation of G_K, because there is a natural action of G_K on $\mathbb{C}_p$.

In what follows, we let G be a topological group and B be a topological ring equipped with a continuous action of G, compatible with the ring structure of B: $g \cdot (a + b) = g \cdot a + g \cdot b$, and $g \cdot (ab) = (g \cdot a)(g \cdot b)$ for all $g \in G$ and $a, b \in B$.

Definition 3. A B-semi-linear representation (or B-representation) is a B-module V equipped with a continuous action of G such that :

$$g \cdot (x + y) = g \cdot x + g \cdot y \quad \text{and} \quad g \cdot (ax) = g(a)g(x),$$

for all $g \in G$, $a \in B$, and $x, y \in V$.

Remark. The following are easy observations:

(1) Clearly, if the action of G on B is trivial, then the notion of B-semi-linear representations coincides with the notion of B-linear representations. If $B = \mathbb{Q}_p$ with the p-adic topology then we say that it is a p-adic representation.

(2) By definition, B itself is a B-semi-linear representation, and we can make B^n into a B-semi-linear reprsentation by defininig component wise G-action.

Let V_1 and V_2 be two B-semi-linear reprsentations of G over B, a homomorphism $\phi : V_1 \to V_2$ is a B-linear mapping which commutes with the G action. Thus, the B-semi-linear representations form a category, we denote it by $\mathrm{Rep}_B(G)$.

3.0.1. *Scalar extension.* Let C be a closed subring of B, which is stable under the G-action: $g \cdot c \in C \, \forall c \in C$ and $g \in G$. So we have the category $\mathrm{Rep}_C(G)$ of C-semi-linear representations of G, and there is a canaonical functor $\mathrm{Rep}_C(G) \to \mathrm{Rep}_B(G)$ taking W to $B \otimes_C W$.

This construction allows us to obtain semi-linear representations from the classical linear representations. Let E be a field endowed with trivial G-action, and let B be an E-algebra with a continuous G-action. Then the category $\mathrm{Rep}_E(G)$ is the category of classical (linear) representations of G over E. We can obtain B-semi-linear representations from E-linear reprsentations by extension of scalars: $V \mapsto V \otimes_E B$.

Example 3.1. Let $\chi : G \to E^* = \mathrm{GL}(1, E)$ be a multiplicative character. Let $E = \langle e_\chi \rangle$, where $\{e_\chi\}$ is a basis of E over E, and $g \cdot e_\chi = \chi(g) e_\chi$. We know that the basis of $B \otimes_E E$ is $\{1_B \otimes_E e_\chi\}$, and $g \cdot (b(1_B \otimes_E e_\chi)) = g \cdot (b \otimes_E e_\chi) = g \cdot b \otimes_E g \cdot e_\chi = (g \cdot b)(g \cdot (1_B \otimes_E e_\chi))$. We denote the B-semi-linear representation obtained in this manner by $B(\chi)$.

Definition 4. We say that a B-representation W is *free* if W as a B-module is free. Furthermore, a free B-representation W of G is said to be *trivial* if one of the following equivalent conditions hold:

(1) There exists a G-invariant B-basis of W.

(2) W is isomorphic to B^d in $\mathrm{Rep}_B(G)$ for some $d \in \mathbb{Z}_{>0}$.

Let $V \in \mathrm{Rep}_B(G)$ be a B-semi-lienar representation, then we denote by V^G the subset of V which consists of the fixed points of V under the action of G: $V^G := \{v \in V : g \cdot v = v \forall g \in G\}$. Naturally, V^G is endowed with a B^G module structure. We have the following natural functors:

$$\begin{aligned} \mathrm{Rep}_B(G) &\to \mathrm{Rep}_{B^G}(G) \\ V &\mapsto V^G \\ \mathrm{Rep}_{B^G}(G) &\to \mathrm{Rep}_B(G) \\ W &\mapsto B \otimes_{B^G} W. \end{aligned}$$

Since $V^G \subset V$, the universal property of the extension of scalars implies that there exists a unique morpshim $\alpha_V : B \otimes_{B^G} V^G \to V$, such that the following diagram commutes:

$$\begin{array}{ccc} B \otimes_{B^G} V^G & \xrightarrow{\alpha_V} & V \\ {\scriptstyle v \mapsto 1 \otimes v}\uparrow & \nearrow & \\ V^G & & \end{array}$$

Remark. If V is a trivial representation in $\mathrm{Rep}_B(G)$, then the morphism $\alpha_V : B \otimes_{B^G} V^G \to V$ is an isomorphism, because $(B^d)^G = (B^G)^d$. Suppose that V and V^G are free of finite rank over B and B^G respectively, then the coverse also holds true.

3.1. **Hilbert's theorem 90.** We now device a machinery to recognize trivial representations. In this subsection, we assume that L is an abstract topological field with a continuous action of a finite group G, endowed with the discrete topology. Under these assumptions, $K = L^G$ is a subfield of L, called the fixed field of G and L/K is a finite Galois extension with Galois group G.

Theorem 10. *Keeping the above notations and the assumptions. Let $V \in \mathrm{Rep}_L(G)$, the following holds:*

(1) *the morphism $\alpha_V : L \otimes_K V^G \to V$ is surjective,*

(2) *if V is finite dimensional over L, then α_V is an isomorphism, that is W is trivial.*

Proof. (1) Let $G = \{g_1, \ldots, g_n\}$ ($g_1 = \mathrm{id}$) and $\lambda_1, \ldots, \lambda_n$ be a basis of L over K. Then by Artin's linear independence theorem the matrix $(g_i(\lambda_j))_{ij}$ is invertible, so there exists a non-trivial solution to the following linear system:

$$\begin{pmatrix} g_1(\lambda_1) & g_1(\lambda_2) & \cdots & g_1(\lambda_n) \\ g_2(\lambda_1) & g_2(\lambda_2) & \cdots & g_2(\lambda_n) \\ \vdots & \vdots & \ddots & \vdots \\ g_n(\lambda_1) & g_n(\lambda_2) & \cdots & g_n(\lambda_n) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Denote such a solution by $(\mu_1, \mu_2, \ldots, \mu_n)^t$, then we have the following

$$\sum_{i=1}^{n} \mu_i g(\lambda_i) = \begin{cases} 1 & \text{if } g = \mathrm{id} \\ 0 & \text{otherwise.} \end{cases}$$

Define the trace function $\mathrm{Tr} : V \to V$ as $v \mapsto \sum_{g \in G} g \cdot v$. Then, $h \cdot \mathrm{Tr}(v) = h \cdot \sum_{g \in G} g \cdot v = \sum_{g \in G} (hg) \cdot v = \sum_{g \in G} g \cdot v = \mathrm{Tr}(v)$. Therefore, $\mathrm{Tr}(V) \subset V^G$. Furthermore, we have

$$\begin{aligned} \sum_{i=1}^{n} \mu_i \,\mathrm{Tr}(\lambda_i v) &= \sum_{i=1}^{n} \mu_i \Big(\sum_{g \in G} g \cdot (\lambda_i v)\Big) \\ &= \sum_{g} \sum_{i=1}^{n} \mu_i g \cdot (\lambda_i v) \\ &= \sum_{g} \left(\sum_{i=1}^{n} \mu_i g \cdot \lambda_i\right) g \cdot v \\ &= v \end{aligned}$$

which implies the surjectivity because:

$$\alpha_V(\sum_{i=1}^{n} \mu_i \otimes \mathrm{Tr}(\lambda_i v)) = \sum_{i=1}^{n} \mu_i \,\mathrm{Tr}\big(\lambda_i(v)\big) = v.$$

(2) Suppose V is a finite dimensional L-vector space. Then injectivity is equivalent to the claim that α_V carries a K-basis of V^G to a L-linearly independent set in V, so it is sufficient to show that every finite family of linearly independent vectors in V^G over $L^G = K$ remains linearly independent over L. Let $(v_1, \ldots, v_m)$ be a linearly independent family in V^G over K. We suppose that m is minimal such that there exist $0 \neq a_i \in L$ for $i \in \{1, \ldots, m\}$. By rescaling and shuffling we assume without loss of any generality that $a_1 = 1$. Let $g \in G$, then

$$(g - \mathrm{id})(a_1 v_1 + \cdots + a_m v_m) = 0,$$

since $a_1 = 1$ and $g \cdot v_1 = v_1$, we have $(g(a_2) - a_2)v_2 + \cdots + (g(a_m) - a_m)v_m = 0$, which contradicts the minimality of m, so $g(a_i) = a_i$ for $i \geq 2$ and for all $g \in G$ so $a_i \in K$ for $i \geq 2$, which is a contradiction because $(v_1, \ldots, v_m)$ is linearly independent over K, hence $a_i = 0$ for $i \geq 2$.

■

Remark. Theorem 10 does not hold in general when $G = \mathrm{Gal}(L/K)$, where L/K is an infinite extension and G is equipped with the natural profinite topology. Otherwise, consider $G = G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with its natural action on $L = \overline{\mathbb{Q}}_p$, then $K = L^G = \mathbb{Q}_p$ Consider the $\mathbb{Q}_p$-semi-linear representation $\mathbb{Q}_p(\chi_{cycl})$ obtained by the cylotomic character χ_{cycl}. Then $\mathbb{Q}_p(\chi_{cycl})$ is not isomorphic to $\mathbb{Q}_p$ in the category $\mathrm{Rep}_{\overline{\mathbb{Q}}_p}(G_{\mathbb{Q}_p})$.

4. Notion of B-admissible representations

In this section we describe Fontaine's general philosophy for isolating the most interesting representations of the Galois group of a p-adic field. In this section let G be a topological group, and E be a fixed topological field such that the action of G on E is trvial. Let B be atopological E-algebra with a G-action. The category $\mathrm{Rep}_E(G)$ is the category of E-linear representations of G and the category $\mathrm{Rep}_B(G)$ is the category of B-semi-linear reprsentations of G.

Definition 5 (B-admissible)**.** Let $V \in \mathrm{Rep}_E(G)$ be finite dimensional over E. We say that V is B-admissible if the B-semilinear representation $B \otimes_E V$ is trivial.

We denote by $\mathrm{Rep}_E^{B-adm}(G)$ the full sub-category of $\mathrm{Rep}_E(G)$ consisting of finite dimensional representations of E which are B-admissible.

Proposition 11. *The category* $\mathrm{Rep}_E^{B-adm}(G)$ *is stable under direct sums, tensor products, and duals: let* $V, V' \in \mathrm{Rep}_E(G)$ *be* B*-admissibe representations, then* V^**,* $V \oplus V'$ *and* $V \otimes V'$ *are also* B*-admissible.*

Proof. ■

Definition 6. The E-algebra B is said to (E, G)-regular if the following conditions hold:

(1) B is a domain,

(2) $(\mathrm{Frac}B)^G = B^G$,

(3) if $b \in B$, $b \neq 0$ and the E-line Eb is stable under G, then $b \in B^*$.

Remark. If B is (E, G)-regular, then B^G is a field: let $b \in B^G$, $b \neq 0$, then clearly the line Eb is stable under G. Thus, b is a unit in B, so B^G is a field. The second condition implies that $b^{-1} \in B^G$.

Example 4.1. B_{HT} is $(\mathbb{Q}_p, G_K)$-regular.

Suppose that B is (E,G)-regular, and let $V \in \mathrm{Rep}_E(G)$ be any finite dimensional E-representation of G, then $B \otimes_E V$, equipped with the G-action $g(\lambda \otimes v) = g(\lambda) \otimes g(v)$, is a free B-representation of G. Let $D_B(V) = (B \otimes_E V)^G$. Then D_B could be seen as a fucntor from $\mathrm{Rep}_E(G)$ to the category of B_G-vector spaces. Recall from § 3.0.1 that we have the following map:

$$\begin{aligned} \alpha_{B\otimes_E V} : B \otimes_{B^G} D_B(V) &\to B \otimes_E V \\ \lambda \otimes v &\mapsto \lambda v \end{aligned}$$

$\alpha_{B\otimes_E V}$ is B-linear and commutes with the action of G, where G acts on $B \otimes_{B^G} D_B(V)$ via $g(\lambda \otimes x) = g(\lambda) \otimes x$.

Theorem 12. *Assume B is (E,G)-regular. Then,*

(1) *For any finite dimensional E-representation $V \in \mathrm{Rep}_E(G)$, the map $\alpha_{B\otimes_E V} : B \otimes_{B^G} D_B(V) \to B \otimes_E V$ is injective and $\dim_{B^G}(D_B(V)) \leq \dim_E V$. Furthermore, the following are equivalent:*

   (a) *$B \otimes_E V$ is trivial (equivalently V is B-admissible),*

   (b) *the morphism $\alpha_{B\otimes_E V}$ is an isomorphism,*

   (c) $\dim_{B^G} D_B(V) = \dim_E V$.

(2) *The restriction of D_B to $\mathrm{Rep}_E^{B-adm}(G)$ is an exact and faithful functor. In $\mathrm{Rep}_E^{B-adm}(G)$ we have the following:*

   (a) *$\mathrm{Rep}_E^{B-adm}(G)$ is stable under subrepresentations, quotients, direct sums, tensor products, and duals.*

   (b) *For $V, V' \in \mathrm{Rep}_E^{B-adm}(G)$, there is a natural isomorphism $D_B(V) \otimes_{B^G} D_B(V') \simeq D_B(V \otimes_E V')$.*

Proof. (1) We first show the injectivity. Let $L := \mathrm{Frac}(B)$, since B is (E,G)-regular, we have $L^G = B^G = K$, and we have the

following commutative diagram:

$$\begin{array}{ccc} B \otimes_K (B \otimes_E V)^G & \xrightarrow{\alpha_{B\otimes_E V}} & B \otimes_E V \\ \downarrow & & \\ B \otimes_K (L \otimes_E V)^G & & \downarrow \\ \downarrow & & \\ L \otimes_K (L \otimes_E V)^G & \xrightarrow{\alpha_{L\otimes_E V}} & L \otimes_E V \end{array}$$

where the vertical arrows are injective by construction. So, to prove the injectivity of the top arrow it suffices to prove the injectivity of the bottom arrow, but the injectivity of the bottom arrow follows by copying the argument of Theorem 10 (2). To prove the equivalence of (a) and (b) in (1), we note that the condition V is B-admissible means that there exists a B-basis $\{x_1, \ldots, x_r\}$ of $B \otimes_E V$ such that each x_i is G-invariant. Since $\alpha_W(1 \otimes x_i) = x_i$, and α_W is always injetcive, the condition is equivalent to α_W being an isomorphism.

Now we prove the equivalence of (b) and (c) in (1). It is clear that (b) implies (c). So assume (c) and denote by d the common dimension of V over E and $D_B(V)$ over B^G. Let $\{e_j\}$ be a K-basis of $D_B(V)$ and let $\{v_i\}$ be a E-basis of V, so relative to these bases we can express $\alpha_{B\otimes_E V}$ using a $d \times d$ matrix (b_{ij}) over B. In other words, $e_j = \sum b_{ij} \otimes v_i$. The determinant $\det \alpha_{B\otimes_E V} := \det\big(b_{ij}\big) \in B$ is nonzero due to the isomorphism property over $L = \mathrm{Frac}(B)$ (as scalar extension of $\alpha_{B\otimes_E V}$ to a L-linear injection between C-vector spaces with the same finite dimension d must be an isomorphism). We want that $\det\big(\alpha_{B\otimes_E V}\big) \in B^\times$, so then $\alpha_{B\otimes_E V}$ is an isomorphism over B. Since B is an (E, G)-regular ring, to show that nonzero $\det\big(\alpha_{B\otimes_E V}\big) \in B$ is a unit it suffices to show that it spans a G-stable E-line in B. The vector $e_j = \sum b_{ij} \otimes v_i \in D_B(V) \subset B \otimes_E V$ are G-invariant, so passing to the d-th exterior powers

on $\alpha_{B\otimes_E V}$ gives that

$$\wedge^d(\alpha_{B\otimes_E V})(e_1\wedge\cdots\wedge e_d) = \det\big(b_{ij}\big)v_1\wedge\cdots\wedge v_d$$

is a G-invariant vector in $B\otimes_E\wedge^d V$. But G acts on $v_1\wedge\cdots\wedge$ by some character $\eta : G\to E^*$, so G muct act on $\det\big(b_{ij}\big)\in B\setminus\{0\}$ through the E^*-valued η^{-1}. Hence, $\det\big(b_{ij}\big)$ is invertible in B and therefore $\alpha_{B\otimes_E V}$ is an isomorphism.

■

5. $\mathbb{C}_p$-ADMISSIBILITY

5.1. **Ax-Sen-Tate Theorem.** For any $\alpha\in\overline{K}$, set

$$\Delta_K(\alpha) = \min\{v(\alpha'-\alpha)\},$$

where α' are conjugates of α over K. Then $\Delta_K(\alpha)=+\infty$ if and only if $\alpha\in K$.

We now state and prove the Ax-Sen's lemma, which says that if all the conjugates α' are close to α, then α is close to an element of K. We follow [1]. We begin with a lemma.

Lemma 13. *Let $R\in K[X]$ be a monic polynomial of degree $d\geq 2$ such that $v(\lambda)\geq r$ for any root λ of R in $\overline{K}$. Let $m\in\mathbb{N}$ with $0<m<d$, then there exists $\mu\in\overline{K}$, such that μ is a root of $R^{(m)}(X)$, the m-th derivative of $R(X)$, and*

$$v(\mu)\geq r-\frac{1}{d-m}v_p\left(\binom{d}{m}\right).$$

Proof. We can write

$$R(X)=\prod_{i=1}^{d}(X-\lambda_i)=\sum_{i=0}^{m}(-1)^i S_{d-i}(\lambda_1,\ldots,\lambda_d)X^i,$$

where S_n $(n>0)$ is the n-th symmeteric polynomial in d variables, and $S_0=1$. Let $b_i=(-1)^iS_{d-i}(\lambda_1,\ldots,\lambda_d)$, so $R(X)=\sum_{i=0}^{d}b_iX^i$. It

follows that $v_p(b_i) \geq (d-m)r$. Write

$$\frac{1}{m!}R^{(m)}(X) = \sum_{i=m}^{d} \binom{i}{m} b_i X^{i-m} = \binom{d}{m} \prod_{i=1}^{d-m} (X - \mu_i),$$

then $b_m = \binom{d}{m}(-1)^{d-m}\mu_1\mu_2\cdots\mu_{d-m}$. Therefore, we have

$$\begin{aligned}\frac{1}{(d-m)}\sum_{i=1}^{d-m} v_p(\mu_i) &= \frac{1}{(d-m)}v_p(b_m) - \frac{1}{(d-m)}v_p\left(\binom{d}{m}\right) \\ &\geq r - \frac{1}{(d-m)}v_p\left(\binom{d}{m}\right).\end{aligned}$$

So exists i, such that

$$v_p(\mu_i) \geq r - \frac{1}{(d-m)}v_p\left(\binom{d}{m}\right).$$

Which completes the proof of the lemma.

■

Proposition 14 (Ax-Sen's Lemma)**.** *Let $K/\mathbb{Q}_p$ be a finite extension, and $\alpha \in \overline{K}$, then there exists $a \in K$ such that $v_p(\alpha - a) > \Delta_K(\alpha) - \frac{p}{(p-1)^2}$.*

Proof. For any $n \in \mathbb{Z}_{\geq 1}$, let $l(n)$ be the largest integer l such that $p^l \leq n$. Let $\varepsilon(n) = \sum_{i=1}^{l(n)} \frac{1}{p^i - p^{i-1}}$. Then

$$n < p \Leftrightarrow l(n) = 0 \Leftrightarrow \varepsilon(d) = 0.$$

Claim. If $[K(\alpha) : K] = d$, then there exists $a \in K$ such that $v_p(\alpha - a) > \Delta_K(\alpha) - \varepsilon(d)$.

We note that the above claim implies the proposition, since $\varepsilon(d) \leq \varepsilon(d+1)$ and $\lim_{d\to+\infty} \varepsilon(d) = \frac{p}{(p-1)^2}$.

To prove the claim we proceed by induction. If $d = 1$, then $l(d) = 0 = \varepsilon(d)$, and $\Delta_K(\alpha) = 0$, take $a = \alpha - p$, so that $v_p(\alpha - a) = 1$.

Now we assume that $d \geq 2$. Let $P \in K[X]$ be the minimal polynomial of α over K. Let

$$R(X) = P(X + \alpha),\ R^{(m)}(X) = P^{(m)}(X + \alpha).$$

We have two cases: if d is not a power of p, then $d = p^s n,\ s \in \mathbb{Z}_{\geq 0}$, where $n \geq 2$ is coprime to p, otherwise, write $d = p^s p,\ s \in \mathbb{Z}_{\geq 1}$. Let $m = p^s$, so that $m < d$.

Let $r = \Delta_K(\alpha)$, by lemma 13, there exists $\mu \in \overline{K}$, such that μ is a root of $R^{(m)}(X)$, and

$$v_p(\mu) \geq r - \frac{1}{d-m} v_p(\binom{d}{m}).$$

Set $\beta = \mu + \alpha$. Then $P^{(m)}(\beta) = 0$, and $P^{(m)}(X) \in K[X]$ with degree $d - m$, so β is algebraic over K of degree $\leq d - m$. If $\beta \in K$, then we choose $a = \beta$. Otherwise $\beta \notin K$, then by induction hypothesis there exists $a \in K$ such that $v_p(\beta - a) \geq \Delta_K(\beta) - \varepsilon(d - m)$.

Now we want to verify that $v_p(\alpha - a) > r - \varepsilon(d)$.

Case 1: Suppose $d = p^s n$ $(n \geq 2)$, n is coprime to p and $m = p^s$. Recall, the Legendre's formula:

$$v_p(k!) = \sum_{i=1}^{\infty} \left\lfloor \frac{k}{p^i} \right\rfloor.$$

We have the following:

$$\begin{aligned} v_p(d!) &= p^{s-1} n + \cdots + n + v_p(n!) \\ v_p(m!) &= p^{s-1} + \cdots + p + 1 \\ v_p((d-m)!) &= p^{s-1}(n-1) + \cdots + (n-1) + v_p((n-1)!). \end{aligned}$$

Since, $(n, p) = 1$, we have $v_p(n!) = v_p((n-1)!)$. Therefore, $v_p(\binom{d}{m}) = 0$, so $v_p(\mu) = v_p(\beta - \alpha) \geq r$. If β' is a conjuagte of β, $\beta' = \alpha' + \mu'$ then

$$v_p(\beta' - \beta) = v_p(\alpha' - \alpha + \mu' - \mu) \geq r,$$

which implies $\Delta_K(\beta) \geq r$. Hence $v_p(\beta - a) \geq r - \varepsilon(d - p^s)$, and $v(\alpha - a) \geq \min\{v_p(\alpha - \beta), v_p(\beta - a)\} \geq r - \varepsilon(d)$.

Case 2: Suppose $d = p^s p$, and $m = p^s$. Then $v_p(\binom{d}{m}) = 1$, and $v_p(\mu) \geq r - \frac{1}{p^{s+1}-p^s}$. Let β' be any conjugate of β, $\beta' = \mu' + \alpha'$, then

$$v_p(\beta' - \beta) = v(\mu' - \mu + \alpha' - \alpha) \geq r - \frac{1}{p^{s+1} - p^s},$$

which implies $\Delta_K(\beta) \geq r - \frac{1}{p^{s+1}-p^s}$. Then

$$v_p(\beta - a) \geq r - \frac{1}{p^{s+1} - p^s} - \varepsilon(p^{s+1} - p^s) = r - \varepsilon(p^{s+1}).$$

Hence $v_p(\alpha - a) = v(\alpha - \beta + \beta - a) \geq r - \varepsilon(d)$. ■

We give an application of Ax-Sen's Lemma (proposition 14).

Proposition 15. *We have* $\mathbb{C}_p^{G_K} = K$.

Proof. Let $\alpha \in \mathbb{C}_p^{G_K}$. Since $\mathbb{C}_p$ is a completion of $\overline{\mathbb{Q}_p}$, we can find element $\alpha_n \in \overline{\mathbb{Q}_p}$, such that $v_p(\alpha - \alpha_n) \geq n$, it follows that

$$v_p(\sigma(\alpha_n) - \alpha_n) \geq \min\{v_p(\sigma(\alpha_n - \alpha)), v_p(\alpha_n - \alpha)\} \geq n,$$

for any $\sigma \in G_K$. Thus $\Delta_K(\alpha_n) \geq n$, the above theorem implies that there exists $a_n \in K$ such that $v_p(\alpha_n - a_n) \geq n - \varepsilon$, where $\varepsilon = \frac{p}{(p-1)^2}$. This implies $v_p(\alpha - a_n) \geq n - \varepsilon$. The sequence $(a_n)_{n\geq 1}$, then converges to α. Since $a_n \in K$ for all n, we obtain $\alpha \in K$. ■

5.2. **Hilbert's Theorem 90 for infinite extensions.** As we have seen already that Theorem 10 does not hold for infinite extension, we now present an analog for infinite extensions. Let K^{ur} be the maximal unramified extension of K inside $\overline{K}$, denote by $\hat{K}^{ur}$ the p-adic completion of K^{ur}, then we have a natural embedding of $\hat{K}^{ur}$ into $\mathbb{C}_p$ and we equip $\hat{K}^{ur}$ with the canonical action of $\mathrm{Gal}(K^{ur}/K)$.

Lemma 16. *Every finite unramified extension L/K is Galois. Furthermore, there exists a unique element* $\mathrm{Frob}_{L/K} \in \mathrm{Gal}(L/K)$, *called the arithmetic Frobenius such that for every $\alpha \in \mathcal{O}_L$,* $\mathrm{Frob}_{L/K}(\alpha) \equiv \alpha^q \pmod{\pi_L}$, *where q is a p-power such that $k_K = \mathbb{F}_q$, and π_L is a uniformizer of L.*

Proof. Since L/K is unramified, $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_L$, such that $\overline{f_{\alpha,L/K}} \in k_K[x]$ is separable, where $f_{\alpha,L/K}$ is the minimal polynomial of α, whixh is also separable. Therefore, L/K is Galois. We have the natural surjection $\pi : \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k_K)$, since L/K is unramified, this surjection is also injective, so $\pi : \mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(k_L/k_K)$. Now, let $k_L = \mathbb{F}_{q^n}$ then k_L/k_K is a Galois extension with cyclic Galois group generated by the Frobenius element: $\sigma : a \mapsto a^q$. Take $\mathrm{Frob}_{L/K} = \pi^{-1}(\sigma)$ be the corresponding element in $\mathrm{Gal}(L/K)$. ■

Remark. The inverse $\mathrm{Frob}_{L/K}^{-1}$ of $\mathrm{Frob}_{L/K}$ in $\mathrm{Gal}(L/K)$ is called the *geometric Frobenius.*

Recall that $\overline{\mathbb{F}}_q = \cup_{n\geq 1}\mathbb{F}_{q^n}$, and that $K^{ur} = \cup_{(m,p)=1}K(\mu_m)$ (union of all unramified extensions L/K inside $\overline{\mathbb{Q}}_p$). This is Galois and we have

$$\mathrm{Gal}(K^{ur}/K) \simeq \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \varprojlim_{n\geq 1} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \varprojlim_{n\geq 1} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

The group automorphism $\phi_q : x \mapsto x^q$ is a topological generator of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, let Frob_K be the element in $\mathrm{Gal}(K^{ur}/K)$ corresponding to ϕ_q. Therefore, $\mathrm{Gal}(K^{ur}/K)$ is a *procyclic group.*

Proposition 17. *Any finite dimensional $\hat{K}^{ur}$-semi-linear representation of $\mathrm{Gal}(K^{ur}/K)$ is trivial.*

Proof. Let $\mathcal{O}$ be the ring of integers of K^{ur}, and $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$. Let k be the residue field of K, then the residue field $\mathcal{O}/\mathfrak{m}$ of K^{ur} is isomorphic to the separable closure (here it is equal to the algebraic closure) $\overline{k}$ of k.

Now, suppose that W is a finite dimensional $\hat{K}^{ur}$-semi-linear representation. We want to show that there exist a $\mathrm{Gal}(K^{ur}/K)$-invariant $\hat{K}^{ur}$-basis of W. Fix $B = (v_{1,0}, \ldots, v_{d,0})$ as a $\hat{K}^{ur}$-basis of W. We claim that there exist a sequence $B_n = (v_{1,n}, \ldots, v_{d,n})$ of $\hat{K}^{ur}$-basis of W such that $B_0 = B$ and $v_{i,n+1} \equiv v_{i,n} \pmod{\mathfrak{m}^n}$ and $\mathrm{Frob}(v_{i,n}) \equiv v_{i,n} \pmod{\mathfrak{m}^n}$ for all $i \in \{1, \ldots\}$ By induction. Firstly for $n = 1$, we have

to show that $v_{i,2} \equiv v_{i,1} \pmod{\mathfrak{m}}$ and $\mathrm{Frob}(v_{i,1}) \equiv v_{i,1} \pmod{\mathfrak{m}}$ for all i.

Suppose that B_n has been constructed. To construct B_{n+1} from B_n, since $v_{i,n+1} \equiv v_{i,n} \pmod{\mathfrak{m}^n}$, we look for vectors $(w_1, \ldots, w_n)$ in $\mathcal{O}_W$ such that $\mathrm{Frob}(v_{i,n} + \pi^n w_i) \equiv v_{i,n} + \pi^n w_i \pmod{\mathfrak{m}^{n+1}}$ for all i. Let $\overline{w}_i$ be the image of w_i in $\mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$, so in other words we need to solve the following system of equations:

$$\mathrm{Frob}(\overline{w}_i) - \overline{w}_i = \overline{c}_i (1 \leq i \leq d)$$

where $\overline{c}_i$ is defined as the image of $\frac{\mathrm{Frob}(v_{i,n} - v_{i,n})}{\pi^n}$ in $\mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$. So it is sufficient to show that $\mathrm{Frob} - \mathrm{id}$ is surjective on $\mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$. This follows from the triviality of $\mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$ and the fact the $\mathrm{Frob} - \mathrm{id}$ is surjective on $\overline{k}$.

■

We are now ready to prove the main theorem of this section:

Theorem 18. *Let V be a $\mathbb{Q}_p$-linear finite diemnsional representation of G_K. Then V is $\mathbb{C}_p$ admissible if and only if the inertia subgroup of G_K acts on V through finite quotient.*

Proof. First we assume that the inertia subgroup acts on V through finite quotient, that is there exists a finite extension L of K^{ur} such that $\mathrm{Gal}(\overline{K}/L)$ acts trivially on V. By Hilbert's theorem for finite extensions (Theorem 10), the L-semi-linear representation $L \otimes_{\mathbb{Q}_p} V$ admits an L-basis $v_1, \ldots, v_d$ on which the action of $\mathrm{Gal}(L/K^{ur})$ is trivial. Consequently, $\mathrm{Gal}(K^{ur}/K)$ operates on the $\cap K^{ur}$-span of $v_1, \ldots, v_d$. By Proposition 17, this semi-linear representation is trivial. Therefore V is $(L \cdot \cap K^{ur})$-admissible. It is then also $\mathbb{C}_p$-admissible.

The hard part of the proof is the converse. For that we refer to [2]. ■

6. Hodge-Tate representations

Since we proved that a $\mathbb{Q}_p-$linear finite dimensional representation of G_K is $\mathbb{C}_p-$admissible if and only if the inertia subgroup of G_K acts on V by finite quotient, we showed that $\mathbb{C}_p-$admissibility detects those representations which are potentially unramified and so it's too strong and doesn't capture all interesting representations as shows the following example

Example 6.1. The p-adic cyclotomic character

$$\chi_{cycl} : Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathbb{Z}_p^\times \subset \mathbb{Q}_p^\times$$

is not $\mathbb{C}_p-$admissible

The main idea of what will follows in this chapter, the Sen's theory, is that we can still extract a lot of arithmetic informations from the data of $\mathbb{C}_p \otimes_{\mathbb{Q}_p} V$.

Definition 7. A $\mathbb{Q}_p-$linear representation of G_K is said Hodge-Tate if $\mathbb{C}_p \otimes_{\mathbb{Q}_p} V$ decomposes as

$$\mathbb{C}_p \otimes_{\mathbb{Q}_p} V = \mathbb{C}_p(\chi_{cycl}^{n_1}) \oplus \mathbb{C}_p(\chi_{cycl}^{n_2}) \oplus \cdots \oplus \mathbb{C}_p(\chi_{cycl}^{n_d})$$

for some integers $n_1, \ldots, n_d$

Proposition 19. *The integers n_i's of the decomposition of $\mathbb{C}_p \otimes_{\mathbb{Q}_p} V$ are uniquely determined up to permutations, they are called Hodge-Tate weights of the representation V.*

Proof. Let

$$\begin{aligned}\mathbb{C}_p \otimes_{\mathbb{Q}_p} V &= \mathbb{C}_p(\chi_{cycl}^{n_1}) \oplus \mathbb{C}_p(\chi_{cycl}^{n_2}) \oplus \cdots \oplus \mathbb{C}_p(\chi_{cycl}^{n_d}) \\ &= \mathbb{C}_p(\chi_{cycl}^{m_1}) \oplus \mathbb{C}_p(\chi_{cycl}^{n_2}) \oplus \cdots \oplus \mathbb{C}_p(\chi_{cycl}^{m_r})\end{aligned}$$

Let $W = Hom_{\mathbb{C}_p}(\mathbb{C}_p(\chi_{cycl}^{n}), \mathbb{C}_p(\chi_{cycl}^{m})) \simeq \mathbb{C}_p(\chi_{cycl}^{n-m})$ equpped with its Galois action, it follows that

$$Hom_{Rep_{\mathbb{C}_p}(G_K)}(\mathbb{C}_p(\chi_{cycl}^{n}), \mathbb{C}_p(\chi_{cycl}^{m})) \simeq \mathbb{C}_p(\chi_{cycl}^{n-m}) = W^{G_K}$$

so if $n = m$, $\mathbb{C}_p^{G_K} = K$ by the Ax-Sen-Tate theorem while if $n \neq m$ as we have shown previously $V = \mathbb{Q}_p(\chi_{cycl}^{n-m})$ is not admissible i.e. W is not trivial, hence we showed that $Hom_{Rep_{\mathbb{C}_p}(G_K)}(\mathbb{C}_p(\chi_{cycl}^n), \mathbb{C}_p(\chi_{cycl}^m))$ is a one dimensional $K-$vector space if $n = m$ and is zero otherwise, from which $d = r$ and $n_i = m_i \ \forall i = 1, \dots, n$. ■

Remark. In the previous proof we have shown that $\mathbb{C}_p(\chi_{cycl}^n)$ has no non-zero invariant vector when $n \neq 0$.

Definition 8. Let $\mathbb{C}_p(n)$ the vector space $\mathbb{C}_p$ with the following action of $G_{\mathbb{Q}_p} = Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$:

$$g \cdot v = \chi_{cycl}(g)^n g(v) \quad \forall g \in G_{\mathbb{Q}_p}$$

and $\overline{\mathbb{Q}}_p(n)$ as the vector space $\overline{\mathbb{Q}}_p$ with the action induced by the previous one.

Definition 9. We call Hodge-Tate ring the following ring:

$$\begin{aligned} B_{HT} &= \bigoplus_{n \in \mathbb{Z}} \mathbb{C}_p(n) \\ &\simeq \bigoplus_{n \in \mathbb{Z}} \mathbb{C}_p(\chi_{cycl}^n) \\ &\simeq \mathbb{C}_p[t, t^{-1}] \end{aligned}$$

and we denote

$$B'_{HT} = \mathbb{C}_p((t))$$

Proposition 20. *We have the following properties:*

(1) $B_{HT} \subset Frac(B_{HT}) \subset B'_{HT}$.

(2) $(B_{HT})^{G_{\mathbb{Q}_p}} = (B'_{HT})^{G_{\mathbb{Q}_p}} = \mathbb{Q}_p$

Proof. The first property is clear while the second follows directly from the Ax-Sen-Tate theorem because

$$(B_{HT})^{G_{\mathbb{Q}_p}} = \bigoplus (\mathbb{C}_p(n))^{G_{\mathbb{Q}_p}} = \mathbb{Q}_p \oplus 0 \oplus \cdots \oplus 0 \oplus \cdots = \mathbb{Q}_p$$

while, since the graded ring of B'_{HT},

$$Gr_* B'_{HT} = \bigoplus_{m\in\mathbb{Z}} t^m \mathbb{C}_p[[t]]/t^{m-1} B'_{HT}$$

, is (canonically) isomorphic to B_{HT} we have a $G_{\mathbb{Q}_p}-$equivariant inclusion $B_{HT} \hookrightarrow B'_{HT}$, it follows that $(B'_{HT})^{G_{\mathbb{Q}_p}} = \mathbb{Q}_p$. ■

Remark. We had shown previously that B_{HT} and B'_{HT} are $(\mathbb{Q}_p, G_K)-$regular.

We recall breifly the definition of admissibility in the actual setting and we will prove later that is equivalent to being Hodge-Tate

Definition 10 (B_{HT}-admissible (resp. B'_{HT}-admissible)**.** Let $V \in \mathrm{Rep}_E(G)$ be finite dimensional over E. We say that V is B_{HT}-admissible (resp- $B'_{HT}-$admissible) if the B_{HT}-semilinear representation $B_{HT}\otimes_E V$ is trivial (resp. if the B'_{HT}-semilinear representation $B'_{HT} \otimes_E V$ is trivial)

Theorem 21. *Let V be a finite dimensional $\mathbb{Q}_p-$representation, then*

V is Hodge-Tate $\Leftrightarrow$ it is $B_{HT}-$admissible $\Leftrightarrow$ it is $B'_{HT}-$admissible

Proof. Since $B_{HT} = \oplus_{m\in\mathbb{Z}} \mathbb{C}_p(\chi^m_{cycl})$ as a $\mathbb{C}_p-$semilinear representation it follows that

$$(V \otimes_{\mathbb{Q}_p} B_{HT})^{G_K} \simeq \bigoplus_{m\in\mathbb{Z}} (V \otimes \mathbb{C}_p(\chi^m_{cycl}))^{G_K}$$

If V is Hodge-Tate with $m_1, \ldots, m_s$ as Hodge-Tate weights and $e_1, \ldots, e_s$ as corresponding multiplicities. Therefore the space $(V \otimes \mathbb{C}_p(\chi^{-m_i}_{cycl}))^{G_K}$ has then dimension e_i and so, summing up, all these contrinutions, we find that $(V \otimes_{\mathbb{Q}_p} B^{G_K}_{HT}$ has the same $\mathbb{Q}_p-$dimension of V.
Conversely ■

Example 6.2 (Hodge-Tate classification of characters of $G_{\mathbb{Q}_p}$). Whenever $p > 2$, a character of $G_{\mathbb{Q}_p}$ with values in $\mathbb{Q}_p^\times$ is Hodge-Tate if and only if it's of the form

$$\mu_\lambda \cdot \chi^a_{cycl} \cdot \omega^b_{cycl}$$

where $a \in \mathbb{Z},\ b \in \mathbb{Z}/(p-1)\mathbb{Z}$

Proof. We already know that all the characters of $G_{\mathbb{Q}_p}$ with values in $\mathbb{Q}_p^\times$ are of the form

$$\mu_\lambda \cdot \chi_{cycl}^a \cdot \omega_{cycl}^b$$

where $a \in \mathbb{Z}_p,\ b \in \mathbb{Z}/(p-1)\mathbb{Z}$ and since the representations $\mathbb{C}_p(\mu_\lambda)$ and $\mathbb{C}_p(\omega_{cycl}^b)$ are $\mathbb{C}_p-$admissible we obtain

$$\mathbb{C}_p(\mu_\lambda \cdot \chi_{cycl}^a \cdot \omega_{cycl}^b) \simeq \mathbb{C}_p(\chi_{cycl}^a)$$

hence the Hodge-Tate weight is a and so it should be an integer. ■

References

1. James Ax, *Zeros of polynomials over local fields—the galois action*, Journal of Algebra **15** (1970), no. 3, 417–428.
2. Xavier Caruso, *An introduction to p-adic rings*, (2019).
3. Richard (1831–1916) Dedekind, Robert (1861–1930). Red. Fricke, Emmy (1882–1935). Red. Noether, and Oystein (1899–1968). Red. Ore, *Über den zusammenhang zwischen der theorie der ideale und der theorie der höheren kongruenzen*, online, 1930.
4. Jean-Marc Fontaine and Yi Ouyang, *Theory of p-adic Galois Representations*, `https://www.imo.universite-paris-saclay.fr/~fontaine/galoisrep.pdf`, [Online; accessed 22-June-2023].
5. Jürgen Neukirch, *Algebraic number theory*, Springer Berlin Heidelberg, 1999.
6. Jean-Pierre Serre, *Local fields*, Springer New York, 1979.
7. Andrew Sutherland, *Totally ramified extensions and Krasner's lemma*, `https://math.mit.edu/classes/18.785/2016fa/LectureNotes11.pdf`, 2016, [Online; accessed 22-June-2023].