Introduction to representation theory

Maxence Michot

August 25, 2024

This report was written during my internship at the university of Duisburg-Essen, that I did with Dr. Vytautas Paskunas, whom I thank for supervising me. The goal of the internship was to get familiar with tools of number theory and representation theory, more specifically to understand the following paper by [BP] R. Beuzart-Plessis, in the case where the group G is $GL_n(F)$, where F is a p-adic field. The first chapter is heavily inspired by the pdf of the course 'Algebraic number theory', which I took during my internship.

I will try to make this document accessible to anyone who has never seen p-adic fields before, but that is not a guarantee. Missing proofs can most often times be found in [Sp]

Contents

1 p-adic fields and their rings of integers

Definition 1.1. Let K be a field. An **absolute value** on K is a function $|.| : K \to \mathbb{R}_+$ such that the following two conditions hold for all $x, y \in K$:

1. $|x + y| \leq |x| + |y|$
2. $|xy| = |x||y|$
3. $|x| = 0 \implies x = 0$

Definition 1.2. A **valued field** is a field equipped with an absolute value.

Example 1.3. $(\mathbb{R}, |.|)$ and $(\mathbb{Q}, |.|)$ are valued fields

Definition 1.4. Let p be a prime number. We define the p-adic absolute value on $\mathbb{Q}$ as follows : If $n = p^\alpha m \in \mathbb{Z}$ where $p \nmid m$, then $|n|_p = p^{-\alpha}$. In other words, $|n|_p = p^{-\nu_p(n)}$. If $x = \frac{a}{b} \in \mathbb{Q}$, then $|x|_p = |a|_p - |b|_p$

Remark 1.5. This is well defined and an absolute value. I will only show the well-definedness. Indeed, if $\frac{a}{b} = \frac{c}{d}$, then $|ad|_p = |bc|_p$, which implies that

$$p^{-(\nu_p(a)+\nu_p(d))} = p^{-(\nu_p(b)+\nu_p(c))}$$

Taking logs yields the desired result.

Proposition 1.6. *The p-adic absolute value is ultrametric, which means that it verifies the following identity :*

$$\forall x, y \in \mathbb{Q}, |x+y|_p \leq \max(|x|, |y|)$$

Proof. Let $x = p^\alpha m, y = p^\beta l \in \mathbb{Z}$. We have $p^{\min(\alpha,\beta)}|x+y$, hence $\nu_p(x+y) \geq \min(\alpha, \beta)$. Thus, $-\nu_p(x+y) \leq \max(-\alpha, -\beta)$, hence

$$|x+y|_p \leq p^{\max(-\alpha,-\beta)} = \max(p^{-\alpha}, p^{-\beta}) = \max(|x|_p, |y|_p)$$

Now take $x = \frac{a}{b}, y = \frac{c}{d}$. We have

$$|x+y|_p = \frac{|ad+bc|_p}{|bd|_p} \leq \frac{\max(|ad|_p, |bc|_p)}{|bd|_p} = \max(|x|_p, |y|_p)$$

□

Remark 1.7. This absolute value means that the more a number is divisible by p, the "smaller" it is. The notion of closeness is not the one of $\mathbb{Q}$ equipped with the usual absolute value. With this new absolute value, n and $n+1$ can vastly differ in their absolute values.

Definition 1.8. We say that an absolute value $|.|$ is **discrete** if the values taken by $log(|.|)$ is a discrete subset of $\mathbb{R}$.

Example 1.9. $|.|_p$ is discrete.

Remark 1.10. One can show that such an absolute value is ultrametric.

Definition 1.11. A **discrete valuation ring** (DVR) is a principal ideal domain with exactly one non-zero maximal ideal.

Definition 1.12. Let A be a DVR and $\mathfrak{m}$ be its maximal ideal. Then $\kappa := A/m$ is called the **residue field**

Proposition 1.13. *Let* $(k, |.|)$ *be a complete discretely valued field. Then,*

$$A = \{x \in k | |x| \leq 1\}$$

is a discrete valuation ring, with maximal ideal

$$\mathfrak{m} = \{x \in k | |x| < 1\}$$

and group of units

$$A^\times = \{x \in k | |x| = 1\}$$

Proof. A is clearly a ring, as follows from the axioms of an absolute value. Recall that a ring has a unique maximal ideal if and only if $A \setminus A^\times$ is an ideal. The group of units is clearly $\{x \in k | |x| = 1\}$, and as $\mathfrak{m} = \{x \in k | |x| < 1\}$ is an ideal, this shows that $\mathfrak{m}$ is the only maximal ideal. As the valuation is discrete, one can choose an element x of $\mathfrak{m}$ of maximal valuation. Such an element will generate all of $\mathfrak{m}$. I will not give a proof for this, but it can be found in [Sp] □

Proposition 1.14. *Let $(k, |.|)$ be a complete discretely valued field. Let A be its valuation ring, $\mathfrak{m} = (\varpi)$ its maximal ideal and let $R \subset \mathcal{O}_F$ be a system of representatives for $A/\mathfrak{m}$. Then, every $x \in k \setminus \{0\}$ can be written as*

$$x = \varpi^m \sum_{i=0}^{\infty} a_i \varpi^i$$

with $m = \nu(x)$ and $a_i \in R$

Proof. A proof of this can be found in [Sp] □

Recall the following definition : The completion of a vector space is defined to be the set of all Cauchy sequences of that space, modulo zero-sequences. One can show that this construction makes this space complete, and in the case where the vector space is a field, it also endows the completion with a field structure. For more information, see [As]

Definition 1.15. We define $\mathbb{Q}_p$ to be the completion of $(\mathbb{Q}, |.|_p)$ and $\mathbb{Z}_p$ to be its ring of integers.

Definition 1.16. A ***p*-adic field** F is a finite extension of $\mathbb{Q}_p$

With the following two theorems, one can show that a p-adic field F is a complete discretely valued field. Hence, every element in F can be represented as in 1.14. The first one is useful for the proof of the second and will be useful later, which is why I put it here.

Lemma 1.17 (Hensel's lemma)**.** *Let A be a discretely valued ring and k its fraction field. If $f \in A[X]$ is primitive and decomposes in*

$$\bar{f} = \bar{g}\bar{h} \in \kappa[X]$$

with $\bar{g}$ and $\bar{h}$ coprime, then, there exists $g, h \in A[X]$ such that

- $g = \bar{g}$ *mod* $\mathfrak{m}$, $h = \bar{h}$ *mod* $\mathfrak{m}$
- *deg*(g) = *deg*$(\bar{g})$
- $f = gh$

Theorem 1.18 (Extension of absolute values)**.** *Let $(k, |.|)$ be a complete discretely valued field, and let L/K be a finite field extension of degree n. Then, $|.|$ extends uniquely to L, which makes L a complete discritely valued field such that for $x \in L$,*

$$|x|_L = N_{L/K}(x)^{1/n}$$

Example 1.19. In $\mathbb{Q}_p$, the set of all elements of norm ≤ 1 is $\mathbb{Z}_p$. As $\mathbb{Q}$ injects into $\mathbb{Q}_p$ and $\mathbb{Z}$ into $\mathbb{Z}_p$, I will treat elements of $\mathbb{Q}$ as elements of $\mathbb{Q}_p$. p is an element of norm < 1, and also an element which has the biggest norm which is stricly smaller than 1. Hence it generates a maximal ideal of $\mathbb{Z}_p$. Thus, every element of $x \in \mathbb{Q}_p$ can be written as

$$x = p^{\nu_p(x)} \sum_{k=0}^{\infty} a_k p^k$$

Example 1.20. In $\mathbb{Q}_p$,

$$\frac{1}{1-p} = \sum_{k=0}^{\infty} p^k$$

A reason why this series makes sense is that this is absolutely convergent series in $\mathbb{Q}_p$ and since $\mathbb{Q}_p$ is complete, the series converges.

Now let's talk a bit about the topology of $\mathbb{Q}_p$. This topology is a little bit special, as every point has a neighbourhood of compact-open subsets around it.

Proposition 1.21. *For $x \in \mathbb{Q}_p$, $(x + p^n\mathbb{Z}_p)_{n\in\mathbb{N}}$ forms a basis of compact open subsets around x.*

Proof. As $(\mathbb{Q}_p, +)$ is a topological group, it only suffices to show that $(p^n\mathbb{Z}_p)_{n\in\mathbb{N}}$ forms a basis of compact open subsets around 0. Let U be an open subset around 0. Let $B(0, \epsilon) \subset U$ be a ball of radius $\epsilon > 0$. There exists an N such that for $p^N\mathbb{Z}_p \subset B(0, \epsilon)$. Moreover

$$p^N\mathbb{Z}_p = \{x \in \mathbb{Q}_p||x|_p \leq \frac{1}{p^N}\} = \{x \in \mathbb{Q}_p||x|_p < \frac{1}{p^{N-1}}\}$$

The first expression gives us the compactness, the second gives the openness. □

Remark 1.22. This is still true for all p-adic fields, with ϖ instead of p

Now for a theorem that links the analytic view of $\mathbb{Z}_p$, with an algebraic one :

Theorem 1.23. $\mathbb{Z}_p \cong \lim_{n\in\mathbb{N}^*} \mathbb{Z}/p^n\mathbb{Z}$ *in the category of topological rings*

Proof. According to 1.14 we can write an element x of $\mathbb{Z}_p$ as

$$x = \sum_{k=0}^{\infty} a_k p^k$$

with $a_k \in [\![0, p-1]\!]$ Let us define

$$\phi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$$

which maps an element $x = \sum_{k=0}^{\infty} a_k p^k$ to

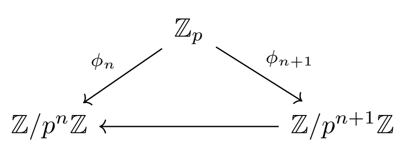
$$\phi_n(x) = \sum_{k=0}^{n-1} a_k p^k$$

This is well defined and a ring homomorphism. Let $x \in \mathbb{Z}/p^n\mathbb{Z}$.

We have

$$\phi_n^{-1}(x) = \{\sum_{k=0}^{n-1} a_k p^k + \sum_{i=n}^{\infty} b_i p^i | b_i \in [\![0, p-1]\!]\} = x + p^n\mathbb{Z}_p$$

. As $\mathbb{Z}/p^n\mathbb{Z}$ is equipped with the discrete topology, and as $\phi_n^{-1}(x)$ is open according to 1.21, ϕ_n is a continuous ring homomorphism, and it makes the following diagram commute :



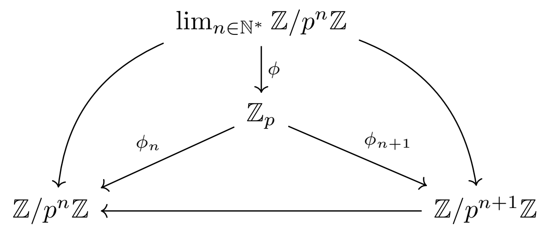
Now let $(x_n)_{n\in\mathbb{N}^*} \in \lim_{n\in\mathbb{N}^*} \mathbb{Z}/p^n\mathbb{Z}$. This means that x_{n+1} is equal to x_n modulo p^n. Thus, in a certain cense, x_{n+1} can only have p different values, which makes sense because we want to write (x_n) as a series in which each term can take p different value. Let us then define

$$\phi : \lim_{n\in\mathbb{N}^*} \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p$$

which maps (x_n) to

$$x_1 + \sum_{n=1}^{\infty} \frac{x_{n+1} - x_n}{p^n} p^n$$

We then check that ϕ is a continous ring homomorphism, which makes the following diagram commute :



and hence the desired result

□

I will end with a lemma which I will use later.

Lemma 1.24 (Krasner's lemma)**.** *Let F be a p-adic field. Let $\alpha, \beta \in F$. Denote $\alpha = \alpha_1, \cdots, \alpha_n$ the galois conjugates of α. If for all $i \in [\![2, n]\!]$,*

$$|\beta - \alpha| < |\beta - \alpha_i|$$

then, $F(\alpha) \subset F(\beta)$

Proof. Suppose $\alpha \notin F(\beta)$. Then, let us consider the extension $L/F(\beta)$ generated by the galois conjugates of α over $F(\beta)$. By construction $L/F(\beta)$ is Galois. Hence there exists some $\sigma \in$Gal$(L/F(\beta))$ such that $\sigma(\alpha) \neq \alpha$. Hence, $\sigma(\alpha) = \alpha_i$ for some $i \in [\![2, n]\!]$. Moreover, $|.| \circ \sigma$ is still an absolute value on L. By uniqueness in 1.18, we have that $|.| = |.| \circ \sigma$. Thus,

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

which is absurd □

Let's now talk a bit about ramification, as I will need it in the future. I will use notions which were in the number theory course given by F.Ivorra in the semester 2 of my M1 without redemonstrating them.

First of all, let us recall that rings of integers are Dedekind rings, and as such, there exists a unique prime decomposition of ideals :

Theorem 1.25. *Let A be a dedeking ring and let I be an ideal of A. Then, there exists a unique decomposition of I into prime ideals :*

$$I = \prod_{J prime} J^{e_J}$$

with $e_J \in \mathbb{N}$

Let us now fix a finite extension of Dedeking Rings B/A (as in B is a ring and a A-module of finite type). Let us write $L := Frac(B)$, and $K := Frac(A)$

Definition 1.26. Let $\mathfrak{p}$ be a prime ideal of A. Let us consider the decomposition of $\mathfrak{p}$ in B :

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

with $e_i \in \mathbb{N}$ Then e_i is called the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$ and if we let $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ and $\kappa(\mathfrak{P}_i) = B/\mathfrak{P}_i$, then the degree of the residue field extension $f_i := [\kappa(\mathfrak{p}) : \kappa(\mathfrak{P})]$ is called the **inertia degree**

Remark 1.27. The inertia degree is well defined. Indeed, if $e_1, \cdots, e_n$ generates B as an A-module, then for $x \in B$,

$$x = \sum_{i=1}^{n} a_i e_i$$

and if we denote by $\pi_i : B \to \kappa_{\mathfrak{P}_i}$ then

$$\pi_i(x) = \sum_{i=1}^{n} \pi_i(a_i)\pi_i(e_i)$$

which means that the degree of the residue field extension is less or equal to that of the field extension

Theorem 1.28.

$$\sum_{i=1}^{r} e_i f_i = [L : K]$$

Proof. Can be found in [Sp] □

Returing to the context of p-adic fields, we have the fact that the rings of integers of such fields are DVR. Hence, they have a unique maximal ideal. As they are also Dedekind rings, they have a unique prime ideal. Hence the following corollary.

Corollary 1.29. *Let E/F be a finite extension of p-adic fields of dimension n. If e and $f \in \mathbb{Z}$ such that*

- $\varpi_E^e = \varpi_F$
- $[\kappa_E : \kappa_F] = f$

Then,

$$n = ef$$

2 Smooth representations

In this section, we take $G = Gl_n(F)$ where F is a p-adic field. The topology on this group is given by the topology on F and by the product topology. This makes G into a topological group which also has a basis of compact open subsets.

Definition 2.1. A **smooth representation** of G is a pair (V, π) such that V is a complex finite dimensional vector space, and $\pi : G \to GL(V)$ is a **smooth** group homomorphism, meaning that for every vector $v \in V$, there exists an open subgroup K of G such that for all $g \in K$, $\pi(g)(v) = v$.

Remark 2.2. We will often fix a representation π and forget about it, and we will write abusively $g.v$ for $\pi(g)(v)$.

Proposition 2.3. *Let ϖ be a normalized uniformizer for F, i.e. $val(\varpi) = 1$. Then, (V, π) is a smooth representation if and only if, for all $v \in V$ there exists some N such that $1+\varpi^N GL_n(\mathcal{O}_F)$ stabilizes v.*

Proof. Let $v \in V$. Suppose there exists an N such that $1 + \varpi^N GL_n(\mathcal{O}_F)$ stabilizes v. Then, according to 1.22, this set is open. It is also clearly a group. Reciprocally, if there exists an open subgroup K such that $K \subset Stab(v)$, then according to 1.22, because $1 \in K$, there exists some N such that $1 + \varpi^N GL_n(\mathcal{O}_F)$ stablizes v

□

Example 2.4. An example of such a representation when $F = \mathbb{Q}_p$ and $\dim(V) = 1$ is the following character

$$\chi : x \mapsto e^{2i\pi\{x\}_p}$$

where $\{x\}_p$ denotes the fracitonal part of x.

Remark 2.5. Composing this character with Tr_{F/Q_p} gives a character of any p-adic field.

Remark 2.6. More constructions of such smooth representations can be found in [Bu]

Definition 2.7. Denote $\mathcal{C}_c^\infty(G)$ the set of complex valued, compactly supported locally constant functions on G. Such functions will be called smooth functions.

Remark 2.8. The reason why locally constant functions are the ones being considered for "smoothness" is very much linked to the topology of p-adic fields. This topology has a basis of compact-open sets. If a function happened to not be locally constant, it then wouldn't be continuous. The following proposition precises this :

Proposition 2.9. *A function $f \in \mathcal{C}_c^\infty(G)$ is smooth (meaning it is (left) invariant under translation by some open subgroup) if and only if it is locally constant.*

Proof. Suppose f is smooth. Let $K \leqslant G$ be an open subgroup under which f is invariant. Let $x \in G$. Then $f(Kx) = f(x)$ As Kx is open, f is locally constant. Reciprocally, suppose f is locally constant, and let $x \in G$. Then there exists U open such that $f(U) = f(x)$. Thus, Ux^{-1} is an open set containing 1. Hence Ux^{-1} contains an open subgroup according to 1.22, which gives the desired result. □

3 Haar measures and integration on groups

The goal of this section is to create a theory of integration on all **locally compact groups**. We already know how to define the lesbegue measure on $\mathbb{R}^d$. This part will generalize this.

Definition 3.1. Let G be a locally compact group. A (left) **Haar measure** on G is a borelian regular measure λ such that, for all $g \in G$, and for all borelians B,

$$\lambda(g.B) = \lambda(B)$$

Example 3.2. On $(\mathbb{R}^d, +)$, the Lesbegue measure is a Haar measure.

Example 3.3. On $(\mathbb{R}_+^*, \times)$, $\frac{dx}{x}$ is a Haar measure. Indeed, if $[a, b]$ is a segment of $\mathbb{R}_+^*$ and $r > 0$, then, by a change of variables,

$$\int_{ra}^{rb} \frac{dx}{x} = \int_a^b \frac{dx}{x}$$

Because segments generate the entier σ-algebra, this concludes.

Example 3.4. Let $f : [0, 2\pi] \to \mathbb{C}$ such that $f(t) = e^{it}$. Then, the measure on S^1 given by $\lambda(B) = \frac{m(f^{-1}(B))}{2\pi}$ where m is the lesbegue measure is a Haar measure on the circle.

Example 3.5. For $G = GL_n(\mathbb{R})$, a Haar measure is given by

$$\lambda(B) = \int_B \frac{dx}{|det(x)^n|}$$

Let B be a borelian and $g \in G$. Then, the jacobian of g is g itself, as a map from $\mathbb{R}^{n^2}$ to itself. In the basis of standard vectors, the matrix of g as a map from $\mathbb{R}^{n^2}$ to itself is just a block diagonal matrix, whose every block in the diagonal is g itself as an $n \times n$ matrix. Hence, the determinant of the jacobian is $\det(g)^n$. the rest follows from the change of variables formula.

Theorem 3.6 (Existence and uniqueness of Haar measure)**.** *Let G be a locally compact topological group. Then, there exists a unique, up to scalar multiplication, measure λ which is a Haar measure on G.*

Remark 3.7. The proof of this theorem resembles that of the construction of the lesbegue measure.

Remark 3.8. If we fix some compact borelian B, then, because a Haar measure is finite on compact sets, we can fix a value to B, for example $\lambda(B) = 1$. There will then exist a unique Haar measure which verifies this. In the future, we will fix a Haar measure on p-adic fields F such that $\lambda(\mathcal{O}_F) = 1$.

4 Parabolic subgroups and cusp forms

Definition 4.1. Let V be a complex finite dimensional vector space of dimension n. A **flag** on V is a finite sequence of increasing sub vector spaces (V_k) such that

$$\{0\} = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_k = V$$

Remark 4.2. If d_i is the dimension of the ith vector space, then

$$0 = d_0 < d_1 < \cdots < d_k = n$$

Example 4.3. If for all i, $d_i = i$, then the flag is called **complete**. It is the case where, for instance, V_i is the vector space generated by the first i standard basis vectors.

Definition 4.4. Let (V_k) be a flag. The **parabolic subgroup** associated with this flag is the group

$$P = \{g \in GL_n(F) | \forall i \in [\![1, k]\!] g.V_i = V_i\}$$

In the rest of this section, we will fix V a finite dimensional complex vector space, and for a flag (V_i), we will denote P the corresponding parabolic subgroup.

Definition 4.5. A basis $e_1, \cdots, e_n$ such that $e_1, \cdots, e_{d_1}$ is a basis of V_1, $e_1, \cdots, e_{d_2}$ is a basis of V_2, $\cdots$, $e_1, \cdots, e_n$ is a basis of V_k is called a **basis adapted to the flag**.

Let us now also fix a basis adapted to the flag.

Remark 4.6. In such a basis, the elements of P can be written as

$$\begin{pmatrix} A_1 & * & \cdots & * \\ 0 & A_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & A_k \end{pmatrix}$$

where A_i is an invertible matrix of size $\dim(V_i/V_{i-1})$

Definition 4.7. $M = \prod_{i=1}^{k} GL(V_i/V_{i-1})$ is called the **Levi component** of the parabolic subgroup

Remark 4.8. In the basis adapted to the flag, M can be embedded in P by

$$\begin{aligned} M &\to GL_n(\mathbb{C}) \\ (g_1, \cdots g_k) &\mapsto \begin{pmatrix} g_1 & 0 & \cdots & 0 \\ 0 & g_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & g_k \end{pmatrix} \end{aligned}$$

Definition 4.9. $N = \{g \in P | \forall i \in [\![1, n]\!] (g - I_n).V_i \subset V_{i-1}\}$ is called the **Unipotent subgroup** of P

Remark 4.10. N is normal in P.

Example 4.11. In a basis adapted to the flag, the elements of N are of the form

$$\begin{pmatrix} I_1 & * & \cdots & * \\ 0 & I_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & I_k \end{pmatrix}$$

where I_k is the identity matrix of size d_k.

Theorem 4.12 (Levi decomposition)**.** *P can be written as $P = MN$ where M is the Levi and N is the unipotent subgroup.*

Proof. Clearly, according to their matrix forms, $MN \subset P$. Let now $A \in P$ such that

$$A = \begin{pmatrix} A_1 & A_{1,2} & \cdots & A_{1,n} \\ 0 & A_2 & \cdots & A_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & A_k \end{pmatrix}$$

We can also see that

$$\begin{pmatrix} A_1^{-1} & 0 & \cdots & 0 \\ 0 & A_2^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & A_k^{-1} \end{pmatrix} \begin{pmatrix} A_1 & A_{1,2} & \cdots & A_{1,n} \\ 0 & A_2 & \cdots & A_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & A_k \end{pmatrix}$$

is an upper triangular matrix with identity blocks in its diagonal. Hence, it is an element of N. Thus, $A \in MN$ ☐

Now to the main important word of this report :

Definition 4.13. Let (V, π) be a smooth representation of G. (V, π) is said to be **supercuspidal** if for all proper parabolic subgroups P of G, and for all vectors $v \in V$ then

$$\int_N \pi(n)(v)dn = 0$$

where N denotes the Levi component of the parabolic subgroup

Remark 4.14. As G is locally compact, N also is. Moreover, this definition doesn't depend on the choice of the Haar measure.

Definition 4.15. A representation is said to be **irreducible** if no non-trivial sub-representations exist.

Definition 4.16. Denote $\mathcal{C}^{\infty}_{c,cusp}(G) \subset \mathcal{C}^{\infty}_{c}(G)$ the subspace of cusp forms, i.e. of functions f such that for all proper parabolic subgroups $G = MN$, and for all $x \in G$

$$\int_N f(xn)dn = 0$$

Let us now define a Fourier transform on $M_n(F)$: We first fix a non trivial continuous additive character $\psi_F : F \to \mathbb{C}^{\times}$ One way to construct such a character would be by 2.5. Another is given in [Bu], which has the advantage of being trivial on $\mathfrak{p}_F$ and non trivial on $\mathcal{O}_F$. We will choose this one. Next, we choose a non degenerate bilinear form B on $M_n(F)$ that is G invariant. We can take, for example

$$\begin{aligned} M_n(F) \times M_n(F) &\to F \\ (A, B) &\longmapsto Tr(AB) \end{aligned}$$

Using elementary matrices, we see that this form is non-degenerate.

Definition 4.17. Let $\phi \in \mathcal{C}^{\infty}_{c}(M_n(F))$. We define the **Fourier transform** of ϕ to be

$$\hat{\phi}(Y) = \int_{M_n(F)} \phi(X)\psi_F(B(X, Y))dX$$

Remark 4.18. This is very similar to the Fourier tranform on the group $(\mathbb{R}^d, +)$ with the usual scalar product instead of B and the exponential being the character from $(\mathbb{R}, +)$ to $(\mathbb{R}^{\times}, \times)$. This is merely a generalization to locally compact abelian groups. For further references, see this

5 How to construct a supercuspidal representation for $G = GL_n(F)$

We will construct an example for the following theorem :

Theorem 5.1. *Let $G = GL_n(F)$. Then, there exists a supercuspidal irreducible representation of G.*

In order to prove the preceding theorem, we will prove this one :

Theorem 5.2. $\mathcal{C}^{\infty}_{c,cusp}(G) \neq \{0\}$

And, in order to prove this theorem, we will find a non zero function $\phi \in \mathcal{C}^{\infty}_{c,cusp}(M_n(F))$, and lift it via the exponential map. In order to understand how to lift this function, and how the second theorem implies the first, I refer to [BP]

In the following section, we fix E/F a finite extension of p-adic fields, with $n = [E : F]$, with n being the same as the one of $GL_n(F)$. Let us also fix α such that $E = F[\alpha]$, and let us fix an F-basis $\mathcal{B}$ of E. This is possible because as the characteristic is 0, this extension is separable. We will need a few propositions before we get to the bulk of it.

Proposition 5.3. *There is an injective group morphism* $E^{\times} \to G$

Proof. Every element of $E^{\times}$ can be seen as a linear transformation of F : we see $x \in E$ as $m_x : y \mapsto xy$. These functions are clearly invertible. Once a basis is fixed, we thus have an inclusion. □

Remark 5.4. We will often make no difference between x and m_x.

For context reasons, we will denote $\mathfrak{t}_{ell}(F)$ the image of $E^{\times}$ in G.

Definition 5.5. We will write $\mathfrak{t}_{ell,reg}(F)$ the subset of $\mathfrak{t}_{ell}(F)$ consisting of elements with a minimal polynomial with distinct roots in an algebraic closure of F

Definition 5.6. Define $\mathfrak{t}_{ell,reg}(F)^G$ to be the subset of G with elements that are G-conjugated to an element of $\mathfrak{t}_{ell,reg}(F)$. In other words,

$$\mathfrak{t}_{ell,reg}(F)^G = \{gXg^{-1} | g \in G,\ X \in \mathfrak{t}_{ell,reg}(F)\}$$

Remark 5.7. We know that in $\mathbb{R}$, the set of polynomials with distinct roots in $\mathbb{C}$ is open. Here, a similar proof can be applied. And the function ϕ that we would want to take is something resembling $\mathbb{1}_{\mathfrak{t}^G_{ell,reg}}$ The problem is that this is then non-constructive.

Proposition 5.8. *Let* $B \in M_n(F)$*. Then,* $B \in \mathfrak{t}_{ell,reg}(F)^G \iff E = F[\lambda]$ *for* λ *some eigenvalue of* μ_B *in* $\bar{F}$

Proof. Suppose $B \in \mathfrak{t}_{ell,reg}(F)^G$. Then $B = gXg^{-1}$ for some $g \in GL_n(F)$ and $X \in \mathfrak{t}_{ell,reg}(F)$. Thus, X is diagonalizable in $\bar{F}$. Thus, as its minimal polynomial in $\bar{F}$ is equal to its characteristic polynomial in $\bar{F}$. As $\chi_F \in F[X]$, then the minimal polynomial of X is of degree n, and hence if X is multiplication by β, $E = F[\beta]$ by equality of dimensions. Moreover, we have :

$$\chi_B = \chi_X = \chi_\beta = \mu_\beta = \mu_X = \mu_B$$

which implies that β is an eigenvalue of B, as $\chi_B(\beta) = 0$.

Conversely, if $E = F[\lambda]$ for λ an eigenvalue of B, then

$$\chi_B = \mu_\lambda = \chi_\lambda$$

As two cyclic endomorphisms with the same characteristic polynomials are conjugated, it suffices to show that multiplication by λ has a characteristic polynomial with distinct roots. As its characteristic polynomial is equal to its minimal polynomial, this is trivially the case, and hence the desired result.

□

I will first show a non-constructive proof of the opennes of $\mathfrak{t}_{ell,reg}(F)^G$ in $M_n(F)$

Lemma 5.9. *Let $\alpha \in \bar{F}$ such that μ_α is of degree n. Then, there exists $\epsilon > 0$ such that for all $q \in F[X]$ monic of degree n such that*

$$|\mu_\alpha - q|_p < \epsilon$$

there exists $\beta \in \bar{F}$ such that $q(\beta) = 0$ and $F[\alpha] = F[\beta]$.

Remark 5.10. The abolute value on polynomials is the one given by the maximum of all the absolute values of the coefficients in F

Proof. Let α such that μ_α is of degree n and denote A the associated matrix. Let $0 < \epsilon < 1$ that we will fix alter. Let q be a monic polynomial of degree n such that $|\mu_\alpha - q| < \epsilon$. Because $M \mapsto \chi_M$ is surjective from $M_n(F)$ to monic polynomials in F of degree n (take for instance companion matrices), there exists a B such that $q = \chi_B$. As the set of all polynomials separated in F is opên, we can choose ϵ small enough such that χ_B has distinct roots, i.e B has distinct eigenvalues.

Let now $\delta > 0$ such that if β is a root of χ_B then $|\beta - \alpha| < \delta$ (possible because the function which maps a polynomial to its roots is continuous), and let $\epsilon_2 = min(\epsilon, \delta)$. There exists a $C > 0$ which only depends on ϵ_2 such that $|chi_A(\beta) - q(\beta)| < C\epsilon$. Indeed, this C is given by :

$$\begin{aligned}
|\chi_A(\beta) - q(\beta)| &\leq \sum_{i=0}^{n} |\chi_{A_i} - q_i||\beta|^i \\
&\leq \epsilon \sum_{i=0}^{n} |\beta|^i \\
&\leq \epsilon \sum_{i=0}^{n} (|\alpha| + \epsilon_2)^i \\
&< C\epsilon
\end{aligned}$$

as $\epsilon < 1$. It also doesn't depend on B or β. So, we can suppose ϵ small enough such that

$$|\chi_A(\beta)| < \epsilon$$

In $\bar{F}$, $\chi_A(\beta) = \prod_{i=1}^{n}(\beta - \alpha_i)$ where the α_i are the Galois conjugates of α, with $\alpha_1 = \alpha$. We now take ϵ_3 =min(ϵ_2,$\min_{i \neq j}(|\alpha_i - \alpha_j|/2)$), then for all $j \neq 1$,

$$|\beta - \alpha| < |\beta - \alpha_j|$$

Then, for $i \neq j$,

$$\begin{aligned}
|\beta - \alpha_j| &= |\beta - \alpha - (\alpha_j - \alpha)| \\
&\leq max(|\beta - \alpha|, |\alpha - \alpha_j|) \\
&\leq |\alpha - \alpha_j|
\end{aligned}$$

Then, by , this shows that $F[\alpha] \subset F[\beta]$. But, as $[F[\beta] : F] \leq n$ and $[F[\alpha] : F] = n$, we have

$$F[\alpha] = F[\beta]$$

□

Theorem 5.11. $\mathfrak{t}_{ell,reg}(F)^G$ *is an open subset of* $M_n(F)$

Proof. Let $\alpha \in \mathfrak{t}_{ell,reg}(F)^G$. Then, according to 5.9 there exists an $\epsilon > 0$ such that for all $q \in F[X]$ monic of degree n such that $|\mu_\alpha - q| < \epsilon$ then $q = \mu_\beta = \chi_\beta$ such that $F[\alpha] = F[\beta]$. According to 5.8 this means that $\beta \in \mathfrak{t}_{ell,reg}(F)^G$. this means that

$$\{\chi_x | x \in \mathfrak{t}_{ell,reg}(F)^G\}$$

is open in $\{P \in F_n[X], P \text{ monic }\}$. By continuity of $x \mapsto \chi_x$, this concludes the proof. ☐

Definition 5.12. Let

$$\mathcal{P} = \{A \in End_F(E) | \forall n \in \mathbb{Z}\ , A\mathfrak{p}_E^n \subset \mathfrak{p}_E^{n+1}\}$$

Proposition 5.13. *In a good basis,*

$$\mathcal{P} = \begin{pmatrix} \mathfrak{p}_F & \mathcal{O}_F & \cdots & \mathcal{O}_F \\ \mathfrak{p}_F & \mathfrak{p}_F & \cdots & \mathcal{O}_F \\ \vdots & \vdots & \ddots & \vdots \\ \mathfrak{p}_F & \cdots & \mathfrak{p}_F & \mathfrak{p}_F \end{pmatrix}$$

Proof. Let e be the ramification index of $[E : F]$. This means that $\varpi_E^e = \varpi_F$. Let $\pi(e_1) \cdots \pi(e_f)$ be a basis of the residue field extension κ_E/κ_F. We will show that $(\varpi_E^k e_i)_{1 \leq k \leq e, 1 \leq i \leq f}$ is a basis in which all elements of $\mathcal{P}$ look like what is above. First of, let's show that this is indeed a basis. Suppose there exists $\lambda_{k,i}$ such that

$$\sum \lambda_{k,i} \varpi_E^k e_i = 0$$

. We can, without loss of generality, suppose that these lambda have positive valuation. Then, applying π, we get

$$\sum_i \sum_k \pi(\lambda_{k,i}) \pi(\varpi_E^k) \pi(e_i) = 0$$

and as $(\pi(e_i))$ is a basis, we get that, for all i,

$$\sum_{k=0}^{e-1} \lambda_{k,i} \varpi_E^k \in \mathfrak{p}_F$$

but, if this is non zero, it is in contradiction with the fact that $\varpi_E^k = \varpi_F$ (contradiction with the absolute value of these elements). Hence, $\sum_{k=0}^{e-1} \lambda_{k,i} \varpi_E^k = 0$. As the λ's have valuation 0, this implies that they are 0. So, $(\varpi_E^k e_i)$ is a free family. According to 1.29, it is a basis. Let now $A \in \mathcal{P}$. A sends $\varpi_E^k e_i$ to an element of valuation $k+1$. Hence $A\varpi_E^k e_i$can be written as

$$\sum_{i=0}^{k} a_i \varpi_E^i + \sum_{i=k+1}^{e-1} b_i \varpi_E^i$$

with $a_i \in \mathfrak{p}_F$ and $b_i \in \mathcal{O}_F$. Hence the desired result.

☐

Just have to verify the thing with the lambda having val 0.

Definition 5.14. For $k \in \mathbb{Z}$, define $\mathcal{P}^k$ to be $\{A \in End_F(E) | \forall n \in \mathbb{Z}\ , A\mathfrak{p}_E^n \subset \mathfrak{p}_E^{n+k}\}$

The goal is now to show that if $m = val(\alpha)$ then $\alpha + \mathcal{P}^{1-m}$ is an open subset of $\mathfrak{t}_{ell,reg}(F)^G$. I haven't had the time to show this if you're reading it.

Suppose that it is true.

Let us now define

$$\phi = \mathbb{1}_{\mathfrak{t}_{ell,reg}(F)^G}$$

The above statement tells us that $\phi \in \mathcal{C}_c^\infty(G)$

In [BP], the author proves that $\hat{\phi}$ is a cusp form. Here,

$$\begin{aligned}
\phi(\hat{X}) &= \int_{M_n(F)} \mathbb{1}_{\alpha+\mathcal{P}^{1-m}} \psi_F(Tr(XY))dY \\
&= \int_{\alpha+\mathcal{P}^{1-m}} \psi_F(Tr(XY))dY \\
&= \int_{\mathcal{P}^{1-m}} \psi_F(Tr(X(\alpha+Y)))dY \\
&= \psi_F(Tr(X\alpha)) \int_{P^{1-m}} \psi_F(Tr(XY))dY
\end{aligned}$$

Now, for all $Y \in \mathcal{P}^{1-m}$, $\psi_F(Tr(XY)) = 1$ if and only if $Tr(XY) \in \mathfrak{p}_F$ if and only if $X \in \mathcal{P}^m$. This can be seen with elementary matrices. Choosing the Haar measure in order to normalize the final result, we have :

$$\hat{\phi}(X) = \psi_F(Tr(X\alpha))\mathbb{1}_{\mathcal{P}^m}(X)$$

References

[As] I.Assem *Introduction au language catégorique*, Calvage Mounet, 2022

[BP] R. Beuzzart-Plessis *A short proof of the existence of supercuspidal representations for all reductive p-adic groups*, ArXiv

[Sp] J. Sprang *Algebraic number theory I and II*, lecture notes.

[Bu] C. J. Bushnell *The Admissible dual of GL_n via compact open subgroups*, Princeton Univeristy Press, 1993.

[Re] D.Renard *Représentations des groupes réductifs p-adiques* Cours spécialisés [Specialized Courses] 17, Société mathématique de France, Paris, 2010, vi+332 pp