Représentations p-adiques de $\mathrm{GL}_2(\mathbb{Z}_p)$ sur $\overline{\mathbb{F}}_p$

Brieuc Lair, Julien Marquet-Wagner
Sous la direction de Yitong Wang

Juin 2023

Introduction

Nous établissons la classification des représentations de $\mathrm{GL}_2(\mathbb{Z}_p)$ sur des $\overline{\mathbb{F}}_p$. Cette étude s'insère dans le cadre plus général de la classification des représentations p-adiques de $\mathrm{GL}_2(\mathbb{Q}_p)$, qui, de façon plus générale encore, est le point de départ du programme de Langlands p-adique. Une telle classification est déjà connue pour $\mathrm{GL}_2(\mathbb{Q}_p)$ sur des espaces vectoriels en caractéristique $l \neq p$. En nous limitant au cas simple de $\mathrm{GL}_2(\mathbb{Z}_p)$, nous sommes déjà en mesure d'illustrer comment la contrainte $l = p$ rend la tâche complexe. En effet, dans ce cas, les théorèmes classiques de la théorie des représentations cessent d'être valides. En particulier, on ne peut plus simplement se limiter à l'étude des caractères pour étudier les représentations.

Afin d'obtenir une théorie satisfaisante, nous prenons le point de vue général des représentations d'algèbres, et nous adoptons une approche catégorique. De cette façon, nous pouvons considérer la catégorie des représentations comme une sorte d'espace vectoriel catégorifié. Ceci nous permet de démontrer efficacement le théorème de Brauer-Nesbitt, qui porte sur le dénombrement des classes d'isomorphismes de représentations de groupes finis dans le cas $l = p$.

Le théorème central de ce mémoire est la clasification des représentations de $\mathrm{GL}_2(\mathbb{F}_p)$ en $\overline{\mathbb{F}}_p$-espaces vectoriels. Ce théorème s'accompagne de l'outillage pour déduire la classification des représentations de $\mathrm{GL}_2(\mathbb{Z}_p)$ sur $\overline{\mathbb{F}}_p$.

Table des matières

1 Préliminaires **2**

2 Représentations d'algèbres **7**
2.1 Lemme de Schur 8
2.2 Des représentations de groupes vers les représentations d'algèbres 8

3 Produit tensoriel et espaces d'applications **9**

4 La catégorie des modules à gauche vue comme un 2-espace vectoriel **10**
4.1 Catégories $\Bbbk$-linéaires 10
4.2 Décomposition d'un module dans la base des modules irréductibles 12
4.3 Théorème de structure de Weddeburn 13

5 Théorème de Brauer-Nesbitt **13**

6 Classification des représentations lisses irréductibles de $\mathbf{GL}_2(\mathbb{Z}_p)$ **16**

1 Préliminaires

Commençons par définir les objets mathématiques qui vont intervenir dans l'ensemble de ce mémoire.

Nous allons tout d'abord détailler la structure du corps valué des *nombres p-adiques*. On s'intéressera brièvement au corps $\mathbb{F}_p$ et sa clôture algébrique $\overline{\mathbb{F}}_p$. Finalement, on définira la notion de représentation *lisse irréductible*, et on s'intéressera à ses invariants à travers un lemme.

Nombres p-adiques

Tout nombre rationnel $r \in \mathbb{Q}^*$ peut se décomposer de manière unique comme $r = \frac{a}{b} \cdot p^n$ avec a, b des entiers non-nuls premiers entre eux tels que $ab \nmid p$, et n un entier. On appelle n la valuation p-adique de r, que l'on note $n = v_p(r)$.
On peut définir à partir de la valuation p-adique une norme sur $\mathbb{Q}$ appelée norme p-adique $|\cdot|_p$, définie pour $r \in \mathbb{Q}^*$ par $|r|_p \overset{\text{def}}{=} p^{-v_p(r)}$, et $|0|_p = 0$.
On vérifie sans difficultés que $|\cdot|_p$ est une valeur absolue sur le corps $\mathbb{Q}$.

On va maintenant construire le corps complété de $(\mathbb{Q}, |\cdot|_p)$, en utilisant des suites de Cauchy, comme on le ferait pour construire $\mathbb{R}$ comme complété de $(\mathbb{Q}, |\cdot|_\infty)$.

Considérons l'anneau commutatif $\mathcal{C}$ des suites de Cauchy dans $(\mathbb{Q}, |\cdot|_p)$. L'ensemble des suites de $\mathcal{C}$ convergentes vers 0 en est un idéal, noté $\mathcal{I}$. Ainsi, le quotient $\mathbb{Q}_p = \mathcal{C}/\mathcal{I}$ est un anneau commutatif. On peut injecter $\mathbb{Q}$ dans $\mathbb{Q}_p$ faisant correspondre un rationnel r à la suite constante égale à r.

Proposition 1.1. *$\mathbb{Q}_p$ est un corps.*

Démonstration. Montrons que tout élément non-nul de $(\mathbb{Q}_p, |\cdot|_p)$ est inversible. Soit $(a_n)_{n\in\mathbb{N}}$ une suite de Cauchy ne convergeant pas vers 0. Alors il existe une suite $(\varphi(n))_{n\in\mathbb{N}}$ et $\varepsilon > 0$ tel que $|a_{\varphi(n)}|_p \geq \varepsilon$ pour tout $n \in \mathbb{N}$. Donc en appliquant le critère de Cauchy pour $\frac{\epsilon}{2}$, il vient qu'il existe un rang $N \in \mathbb{N}$ tel que pour tout $n \geq N$ on a $|a_n| \geq \frac{\varepsilon}{2} > 0$.

Finalement, on peut définir la suite $(\frac{1}{a_n})$ pour tout $n \geq N$, donc quitte à ajouter 0 aux N premiers termes, on a bien trouvé un inverse à la suite (a_n).

Donc $\mathbb{Q}_p$ est un anneau commutatif où tout élément non nul est inversible, i.e un corps. □

On peut munir naturellement $\mathbb{Q}_p$ de la norme $|\cdot|_p$. En effet, on a par inégalité triangulaire $||a_n|_p - |a_m|_p| \leq |a_n - a_m|_p$. Pour $(a_n) \in \mathbb{Q}_p$, il vient que la suite des normes $(|a_n|_p)$ est de Cauchy dans $\mathbb{R}$, donc converge pour la valeur absolue classique.

On définit donc sur $\mathbb{Q}_p$ la norme $|\cdot|_p$ par $|(a_n)|_p = \lim_{n\to\infty} |a_n|_p$. On vérifie que cette valeur ne dépend pas du choix du représentant de la classe d'équivalence de (a_n), et que la norme d'un rationnel est égale dans $\mathbb{Q}$ et $\mathbb{Q}_p$. Il ne nous manque plus qu'à montrer que $\mathbb{Q}_p$ est complet pour pouvoir conclure.

Proposition 1.2. *$\mathbb{Q}_p$ est complet.*

Démonstration. On commence par montrer que toute suite de Cauchy de rationnels converge dans $\mathbb{Q}_p$ vers sa classe. En effet, en notant A_n la suite constante égale à a_n, il faut montrer que $\lim_{n\to\infty} |A_n - (a_m)_{m\in\mathbb{N}}|_p = 0$, soit par définition $\lim_{n,m\to\infty} |a_n - a_m|_p = 0$, ce qui est vrai car (a_n) est de Cauchy.

Considérons maintenant $(S_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $\mathbb{Q}_p$. D'après le premier point, pour tout $n \in \mathbb{N}$, il existe un rationnel a_n tel que $|S_n - a_n|_p \leq \frac{1}{n}$. On a alors $\lim_{n\to\infty} |S_n - A_n|_p = 0$, i.e la suite (S_n) converge vers $(a_n)_{n\in\mathbb{N}}$. On en conclus que $(\mathbb{Q}_p, |\cdot|_p)$ est complet. □

Définition 1.3 (nombres p-adique)**.** *Le complété $\mathbb{Q}_p$ de $\mathbb{Q}$ pour la norme $(|\cdot|_p)$, construit ci-dessus, est appelé corps des nombres p-adiques.*

Il existe une description de $\mathbb{Q}_p$ explicite. En effet, on pourra vérifier que,

$$\mathbb{Q}_p = \left\{ \sum_{i=k}^{+\infty} a_i \cdot p^i | k \in \mathbb{Z}, 0 \leq a_i < p \right\} \quad .$$

Définition 1.4 (entiers p-adique)**.** *On définit l'anneau des entiers p-adiques $\mathbb{Z}_p$ comme l'ensemble des nombres p-adiques de norme inférieure à 1, i.e*

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p : |x|_p \leq 1 \right\}.$$

De la même manière que $\mathbb{Q}_p$, on a $\mathbb{Z}_p = \{\sum_0^{+\infty} a_i \cdot p^i \mid 0 \leq a_i < p\}$.

La clôture $\overline{\mathbb{F}}_p$

Tout le contenu de ce paragraphe est détaillé dans le cours d'Algèbre 2 de l'ENS.

Pour p un nombre premier, rappelons que $\mathbb{F}_p$ désigne l'unique corps à p éléments, à isomorphisme près. On admettra la proposition suivante :

Proposition 1.5. *Pour tout $k \geq 1$, il existe un corps à p^k éléments, noté $\mathbb{F}_{p^k}$, et unique à isomorphisme près. Les seuls corps fini de cardinal multiple de p sont les $\mathbb{F}_{p^k}$.*

Remarque. Pour l'existence, on remarque que le polynôme $X^{p^k} - X$ dans $\mathbb{F}_p[X]$ possède p^k racines distinctes (sa dérivée est -1 donc les racines sont simples), et on peut montrer que l'ensemble de ces racines forme un corps : il s'agit d'un groupe additif, et les racines non-nulles sont les racines $p^k - 1$ ièmes de l'unité, donc forment un groupe multiplicatif commutatifs. Pour l'unicité, on peut utiliser que deux corps de cardinal p^k sont exactement les corps de décomposition de $X^{p^k} - X$, donc isomorphes.

Si $\mathbb{K}$ est un corps, un polynôme $P \in \mathbb{K}[X]$ est dit *scindé* si il peut être décomposé comme produit de polynômes de degré 1.

Définition 1.6 (extension algébrique)**.** *Une extension algébrique d'un corps $\mathbb{K}$ est une extension de corps de $\mathbb{K}$ dans laquelle tous les éléments sont algébriques sur $\mathbb{K}$, i.e racines d'un polynôme non-nul à coefficient dans $\mathbb{K}$.*

Définition 1.7 (clôture algébrique)**.** *Une clôture algébrique de $\mathbb{K}$ est une extension algébrique de $\mathbb{K}$ dans laquelle tous les polynômes sont scindés.*

Le théorème général suivant n'est pas démontré dans ce papier, on pourra retrouver les preuves chez Lang [Lan02] chapitre V, paragraphe 2, corollaires 2.6 et 2.9.

Théorème 1.8. *Tout corps $\mathbb{K}$ admet une clôture algébrique, unique a isomorphisme près.*

On notera $\overline{\mathbb{K}}$ cette clôture.
On va plutôt s'intéresser à l'unique clôture utile pour ce mémoire, $\overline{\mathbb{F}}_p$, en lui donnant une forme explicite.

Lemme 1.9. *Une union croissante (pour l'inclusion) de corps est un corps.*

Démonstration. En effet, notons par exemple $\mathbb{K} = \bigcup_{n\in\mathbb{N}} \mathbb{K}_n$, avec $\mathbb{K}_i \subset \mathbb{K}_j$ pour $i \leq j$. Alors pour $x, y \in \mathbb{K}$, il existe un rang $N \in \mathbb{N}$ tel que $x, y \in \mathbb{K}_N$. On conclus de la structure de corps de $\mathbb{K}_N$ que $\mathbb{K}$ est un corps. □

Proposition 1.10. *Pour p un nombre premier, $\overline{\mathbb{F}}_p = \bigcup_{n\in\mathbb{N}^*} \mathbb{F}_{p^n}$.*

Démonstration. Premièrement, on a l'inclusion $\bigcup_{n\in\mathbb{N}^*} \mathbb{F}_{p^n} \subset \overline{\mathbb{F}}_p$ d'après la remarque de la proposition 1.5. Il nous reste à démontrer que l'union est algébriquement close.

Soit $P \in \bigcup_{n\in\mathbb{N}^*} \mathbb{F}_{p^n}[X]$. Alors il existe $N \in \mathbb{N}$ tel que $P \in F_{p^N}[X]$. Si P est scindé dans $F_{p^N}[X]$, alors on a fini. Supposons donc qu'il est produit de polynômes irréductibles, dont au moins un de degré plus grand que 2. Notons $(P_i)_{i\in\{1,\dots,n\}}$ ces facteurs.

On peut alors considérer le corps de rupture $(\mathbb{F}_{p^N}[X])/(P_1)$. Il s'agit d'un corps fini de degré multiple de p (par exemple car il s'agit d'un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel), donc un $\mathbb{F}_{p_0^k}$. Par construction du corps de rupture, $P_1 = (X - \alpha)\tilde{P}_1$ dans $\mathbb{F}_{p_0^k}$ avec α une racine de P_1. Finalement, on peut itérer l'opération un nombre fini de fois pour avoir P_1 scindé, puis on le refait pour les autres P_i, et on en conclut qu'il existe $l \in \mathbb{N}$ tel que P soit scindé dans $\mathbb{F}_{p^l}$. □

Représentations

Ce court paragraphe est destiné à introduire les représentations de groupes topologiques. On pourra retrouver de nombreuses preuves et compléments dans la littérature, par exemple dans le cours d'Algèbre 1 à l'ENS par Gaëtan Chenevier.

Dans toute la suite, on note $\mathbb{E}$ un corps, π un $\mathbb{E}$-espace vectoriel, et G un groupe topologique, mais on gardera comme exemple principal $G = \mathrm{GL}_2(\mathbb{Q}_p)$ ou $\mathrm{GL}_2(\mathbb{Z}_p)$, et $\mathbb{E} = \overline{\mathbb{F}}_p$. On muni $\mathrm{GL}_2(\mathbb{Q}_p)$ et $\mathrm{GL}_2(\mathbb{Z}_p)$ de la topologie induite par l'inclusion $\mathrm{GL}_2(\mathbb{Q}_p) \subset \mathrm{M}_2(\mathbb{Q}_p) \cong \mathbb{Q}_p^4$, et π sera toujours muni de la topologie discrète, sauf exception explicite.

On rappelle que dans un groupe topologique, les translations à gauche et à droite sont des homéomorphismes.

Définition 1.11 (représentation)**.** *On appelle représentation du groupe G, ou G-représentation, un couple (ρ, π) avec π un espace vectoriel et ρ un morphisme $\rho : G \to GL(\pi)$.*

Il est équivalent de se donner une G-représentation (ρ, π) et une action linéaire $\tilde{\rho} : G \times \pi \to \pi$, i.e telle que $\tilde{\rho}(\alpha x + \beta y) = \alpha\tilde{\rho}(x) + \beta\tilde{\rho}(y)$.

Dans la suite de ce mémoire, on notera une G-représentation π sans préciser de morphisme explicite.

Comme on travaille avec des groupes topologiques, il est raisonnable d'exiger des représentations qu'elles préservent un minimum la structure topologique. On aboutit ainsi à la définition de *représentation lisse* :

Définition 1.12 (représentation lisse)**.** *Une G-représentation est dite* lisse *si pour π muni de la topologie discrète, l'application $G \times \pi \to \pi$ est continue.*

Un moyen de caractériser une représentation lisse est à l'aide de ses invariants. Pour U un sous-groupe de G, on note :

$$\pi^U = \{x \in \pi | u \cdot x = x, \forall u \in U\}$$

On a ainsi la caractérisation suivante.

Proposition 1.13. *Les propriétés suivantes sont équivalentes :*
(i) π est une G-représentation lisse ;
(ii) pour tout $x \in \pi$, il existe un sous-groupe ouvert U de G tel que $x \in \pi^U$;
(iii) pour tout $x \in \pi$, Stab(x) est ouvert ;

Démonstration. (i) $\implies$ (ii) et (iii) : soit $\tilde{\rho} : G \times \pi \to \pi$ l'action linéaire associés. Alors pour tout $x \in \pi$, l'ensemble $\pi^{-1}(x)$ est un ouvert (car π est muni de la topologie discrète).

On peut donc écrire $\pi^{-1}(x) = \bigsqcup_{y \in \pi} U_y \times \{y\}$, avec U_x non-vide car $1 \in U_x$. Ainsi, chacun des termes $U_y \times \{y\}$ est ouvert, et en considérant la première projection, il vient que $U_x = \mathrm{Stab}(x)$ est un ouvert non vide, tel que $x \in \pi^{U_x}$.

(ii) ou (iii) $\implies$ (i) : soit $x \in \pi$. On écrit encore $\pi^{-1}(x) = \bigsqcup_{y\in\pi} U_y \times \{y\}$. Comme π est muni de la topologie discrète, si on montre que $\pi^{-1}(x)$ est ouvert, on aura montré que la représentation est lisse. Pour cela, il suffit de montrer que tous les U_y sont ouvert. Soit donc $g \in U_y$ quelconque. Alors on a $g \cdot y = x$, et par (ii) il existe un ouvert $U \subset G$ tel que $y \in \pi^U$ (même chose par (iii) avec $U = \mathrm{Stab}(y)$) d'où pour tout $u \in U$, on a $(gu)\cdot y = g\cdot(u\cdot y) = x$, donc $gU \subset U_x$. L'image de U par la translation à gauche par g est un ouvert qui contient g. On a ainsi trouvé un voisinage ouvert de g, donc pour tout $y \in \pi, U_y$ est ouvert.

En particulier, π est une G-représentation lisse. □

Une sous-représentation de (ρ, π) est une représentation (ρ_τ, τ) telle que τ est un sous-espace vectoriel de π et on a $g \cdot x \in \tau$ pour tout $g \in G$ et $x \in \tau$. Autrement dit, τ est stable par chaque endomorphisme $\pi(g)$. Pour conclure ce paragraphe, on définit les représentations *irréductibles* :

Définition 1.14 (représentation irréductible)**.** *Une G-représentation π est dite irréductible si ses seules sous-représentations sont 0 et π.*

Notations

Nous ferons l'abus, peu habituel en mathématiques mais courant en informatique, d'utiliser la même notation pour plusieurs objets différents [1]. Nous ferons en particulier cet abus pour utiliser la même notation pour des morphismes et des espaces d'applications.

Un exemple important qui montre l'utilité de cette convention est l'adjonction de Curry, dont nous empruntons encore une fois le nom à l'informatique. On note habituellement

$$\mathrm{Hom}_{\mathbb{K}}(U \otimes V; W) \cong Hom_{\mathbb{K}}(U; [V; W])$$

mais nous n'hésiterons pas à écrire

$$U \otimes V \to W \quad \cong \quad U \to V \to W$$

où «$\to$» sera toujours associatif à droite.

Toujours grâce à Curry, on préfère voir une fonction à plusieurs variables comme une fonction donnant une fonction. Par exemple, la où on note habituellement le produit tensoriel

$$\begin{array}{ccc} U \times V & \longrightarrow & U \otimes V \\ (u; v) & \longmapsto & u \otimes v \end{array}$$

nous noterons plutôt

$$\begin{array}{ccccc} U & \longrightarrow & V & \longrightarrow & U \otimes V \\ u & \longmapsto & v & \longmapsto & u \otimes v \end{array}$$

1. En fait, ce type d'abus reste parfaitement formel dans le contexte de l'informatique grâce à la notions de *typeclass* qui permet d'obtenir des fonctions polymorphes ad-hoc.

2 Représentations d'algèbres

On a une théorie plus générale des représentations d'*algèbres* que l'on va utiliser pour déduire les propriétés du cas particulier des groupes.

Définition 2.1 (Algèbre)**.** *Une $\Bbbk$-algèbre pour un corps $\Bbbk$ est un anneau qui admet aussi une structure de $\Bbbk$-espace vectoriel compatible qui rend le produit bilinéaire.*

Plus formellement, une $\Bbbk$-algèbre est la donnée d'un anneau A et d'un morphisme $\iota : \Bbbk \to Z(A)$ de $\Bbbk$ dans le centre de A.

Définition 2.2 (Bimodule)**.** *Un bimodule est la donnée d'un $\Bbbk$-e.v. sur lequel agissent deux $\Bbbk$-algèbres A et B, l'une à gauche et l'autre à droite.*

On est dans la situation suivante où les deux produits scalaires sont notés «$\cdot$» :

$$\begin{array}{ccc} A \otimes M \\ \big\downarrow{\scriptstyle \cdot} \\ M \end{array} \qquad\qquad \begin{array}{ccc} M \otimes B \\ \big\downarrow{\scriptstyle \cdot} \\ M \end{array}$$

Et on exprime la compatibilité avec le produit scalaire :

$$\begin{array}{ccc} A \otimes A \otimes M & \xrightarrow{*\otimes 1} & A \otimes M \\ \big\downarrow{\scriptstyle \cdot\otimes 1} & & \big\downarrow{\scriptstyle \cdot} \\ A \otimes M & \xrightarrow{\quad\cdot\quad} & A \end{array} \qquad\qquad \begin{array}{ccc} M \otimes B \otimes B & \xrightarrow{1\otimes *} & M \otimes B \\ \big\downarrow{\scriptstyle 1\otimes \cdot} & & \big\downarrow{\scriptstyle \cdot} \\ M \otimes B & \xrightarrow{\quad\cdot\quad} & M \end{array}$$

Définition 2.3 (Représentation d'algèbres)**.** *Une représentation d'algèbre sur un espace vectoriel V est maintenant une fonction « $\cdot$ » : $A \otimes V \longmapsto V$ telle que le diagramme suivant commute*

$$\begin{array}{ccc} A \otimes A \otimes V & \xrightarrow{*\otimes 1} & A \otimes V \\ \big\downarrow{\scriptstyle 1\otimes \cdot} & & \big\downarrow{\scriptstyle \cdot} \\ A \otimes V & \xrightarrow{\quad\cdot\quad} & V \end{array}$$

On remarque qu'une représentation d'algèbres est en fait simplement un *module à gauche* (que l'on peut aussi voir comme un $(A; \Bbbk[X])$-bimodule).

Donc la théorie des représentations d'algèbres se ramène à la théorie des bimodules !

2.1 Lemme de Schur

Théorème 2.4 (Lemme de Schur)**.** *Soit $(S_i)_i$ un système de représentants des classes d'isomorphisme de représentations irréductibles de A. On a :*

$$S_i \to S_j \neq 0 \quad \longleftrightarrow \quad i = j$$

Démonstration. Si $f : S_i \to S_j \neq 0$, alors $\mathrm{Im}(f) \neq \{0\}$, donc $\mathrm{Im}(f) = S_j$ car $\mathrm{Im}(f)$ est une sous-représentation non nulle de S_i, et $\mathrm{Ker}(f) = \{0\}$ car $\mathrm{Ker}(f) \neq S_j$ et $\mathrm{Ker}(f)$ est une sous-représentation de S_i.

Donc f est un isomorphisme, donc $S_i = S_j$ et $i = j$. □

Si S est une représentation irréductible d'une algèbre A, on note $D(S)$ l'algèbre des endomorphismes de S.

Théorème 2.5. *Si $\Bbbk$ est algébriquement clos, et si S est une représentation irréductible en dimension finie de la $\Bbbk$-algèbre A, alors $D(S) \cong \Bbbk$.*

Démonstration. Soit $\varphi \in D(S)$. Le polynôme minimal π_φ de φ est irréductible car S est irréductible, donc de degré 1 car $\Bbbk$ est algébriquement clos. □

2.2 Des représentations de groupes vers les représentations d'algèbres

Si on se donne un groupe topologique G, une représentation de G est un morphisme de groupes $G \longrightarrow (V \longrightarrow V)$ pour un certain espace vectoriel V. Mais les endomorphismes de V admettent une structure d'algèbre que l'on souhaiterait exploiter.

On cherche donc une construction universelle $G \mapsto \Bbbk G$, l'*algèbre du groupe* G, qui à tout G associe une algèbre de façon à avoir une bijection

$$\begin{array}{ccc} G \longrightarrow (V \longrightarrow V) & \cong & \Bbbk G \longrightarrow (V \longrightarrow V) \\ f & \longmapsto & \Bbbk f \\ g \mapsto f(1g) & \longleftarrow & f \end{array}$$

En des termes plus formels, on cherche un *adjoint à l'oubli* des algèbres (topologiques) vers les groupes (topologiques).

On admet qu'il existe une telle adjonction. On peut rapidement suggérer une construction qui a du sens *dans le cas où $\Bbbk$ est muni de la topologie discrète* : on considère les listes $[(\lambda_i, \bar{g_i})] : \mathtt{List}(\Bbbk \times \mathrm{CC}(G))$ de couples d'un scalaire et d'une composante connexe de G, que l'on munit de la structure d'espace vectoriel évidente, et que l'on considère comme monoïde (noté additivement) pour la concaténation, et que l'on munit du produit qui à deux listes associe la liste de tous les produits possibles de leurs éléments. On munit cet espace de la topologie finale pour la surjection $G \twoheadrightarrow \mathrm{CC}(G)$. On passe ensuite au quotient par la relation suivante :

$$\begin{aligned} [(\lambda_i, \bar{g_i})] \widetilde{[}(\mu_i, \bar{h_i})] \Longleftrightarrow & \forall A \text{ algèbre}, \forall f : \mathrm{CC}(G) \to A, \\ & \sum_i \lambda_i f(\bar{g_i}) = \sum_i \mu_i f(\bar{h_i}) \end{aligned}$$

On définit comment associer à un morphisme de groupes $G \to A$ un morphisme d'anneaux $\Bbbk G \to A$. À f, on associe la fonction $[(\lambda_i, \bar{g_i})] \mapsto \sum_i \lambda_i f(\bar{g_i})$. Par construction, cette fonction est un morphisme d'anneaux topologiques. On a la fonction évidente $G \to \Bbbk G$, qui est par construction continue.

On peut maintenant librement passer des représentations continues de groupes aux représentations d'algèbres.

3 Produit tensoriel et espaces d'applications

Les bimodules admettent une structure qui "se comporte bien" catégoriquement : on peut considérer les produits tensoriels et les espaces de morphismes.

Définition 3.1 (Produit tensoriel de bimodules)**.** *Si $M : {}_A Mod_B$ et $N : {}_B Mod_C$, alors on peut considérer*[2] *$M \otimes_B N : {}_A Mod_C$.*

Définition 3.2 (Espaces de morphismes)**.** *Étant donnés $M : {}_A Mod_B$ et $N : {}_A Mod_C$, on peut considérer les fonctions* linéaires à gauche *comme un module $M \xrightarrow{A\bullet} N : {}_B Mod_C$.*

De même, avec $M : {}_A Mod_B$ et $N : {}_C Mod_B$, on peut considérer les fonctions linéaires à droite *comme un module $M \xrightarrow{\bullet B} N : {}_C Mod_A$.*

Si $M, N : {}_A Mod_B$, alors l'espace des fonctions bilinéaires $M \xrightarrow{A\bullet B} N$ n'a pas de structure de bimodule naturelle.

Définition 3.3 (Restriction)**.** *Si on a quatre algèbres A, A', B, B' et deux fonctions $f : A \to A'$ et $g : B \to B'$, alors on peut donner un foncteur $(f; g)^* : {}_{A'} Mod_{B'} \implies {}_A Mod_B$ qui transporte la structure de bimodule par f et g.*

Dans le cas où f et g sont des inclusions, ceci définit la restriction *de structure.*

Dans la suite, on va souvent parler de retrictions de représentations, c'est à dire de restrictions de modules à gauche, que l'on pourra simplement noter $(\subseteq; 1)^* : {}_{A'} Mod_B \implies {}_A Mod_B$ dans les cas où $A \subseteq A'$.

Le «bon comportement catégorique» des bimodules se trouve dans la généralisation de l'adjonction $\otimes - \mathrm{Hom}$, ou adjonction de Curry. Avec $M : {}_A\mathrm{Mod}_B$; $N : {}_B\mathrm{Mod}_C$; $V : {}_A\mathrm{Mod}_C$

$$M \otimes_B N \xrightarrow{A\bullet B} V \quad \cong \quad N \xrightarrow{B\bullet} M \xrightarrow{A\bullet} V$$

(On a la même adjonction pour les applications linéaires à droite.)

On en déduit plus de structure sur les représentations.

2. Cette construction généralise le produit tensoriel, au sens où $M \otimes_B N$ représente les fonctions bilinéaires sur $M \times N$. La notion de fonction bilinéaire est cependant un peu plus subtile ici que dans le cas des espaces vectoriels puisqu'on perd le bon comportement des multiplications scalaires.

Définition 3.4 (Induction, Coinduction, Restriction)**.** *Étant donnés $A \subseteq B$ deux algèbres et V une représentation de A, on définit*

1. $Ind_A^B V \triangleq (\subseteq, 1)^* B \otimes V : {}_B Mod$
2. $Coind_A^B V \triangleq (\subseteq, 1)^* B \xrightarrow{A\bullet} V : {}_B Mod$

Et à partir d'une représentation W de B, on construit
$Res_A^B W \triangleq (\subseteq; 1)^* W : {}_A Mod$

4 La catégorie des modules à gauche vue comme un 2-espace vectoriel

On peut voir la catéogrie des A-modules comme un "2-espace vectoriel" (cf. Kapranov et Voevodsky [KV94] pour la définition utilisée ici, cf. Baez [Bae96] pour la notion de *2-Hilbert*, cf. nLab [nLa23b] [nLa23a] pour un panorama général), c'est à dire une structure qui mime un espace vectoriel mais qui, au lieu de se construire sur un ensemble, se construit sur une catégorie.

	Espace Vectoriel			2-Espace Vectoriel		
	E			${}_A\mathrm{Mod}$		
	$\mathbb{K}$			$\Bbbk - \mathrm{Vect}$		
	$E \times E$	$\longrightarrow$	E	${}_A\mathrm{Mod} \times {}_A\mathrm{Mod}$	$\longrightarrow$	${}_A\mathrm{Mod}$
$+ :$	$(x; y)$	$\longmapsto$	$x + y$	$(M; N)$	$\longmapsto$	$M \oplus N$
	$\mathbb{K} \times E$	$\longrightarrow$	E	${}_A\mathrm{Mod} \times \Bbbk - \mathrm{Vect}$	$\longrightarrow$	${}_A\mathrm{Mod}$
$\cdot :$	$(\lambda; v)$	$\longmapsto$	λv	$(M; V)$	$\longmapsto$	$M \otimes V$

Nous allons développer cette analogie pour obtenir des théorèmes sur la structure des A-modules.

4.1 Catégories $\Bbbk$-linéaires

On considère les categories *enrichies en k-espaces vectoriels*, c'est à dire des structures données par :

— De objets `obj`

— Des flèches $\begin{array}{ccccc} \texttt{obj} & \to & \texttt{obj} & \mapsto & \Bbbk - \mathrm{Vect} \\ x & \mapsto & y & \mapsto & x \to y \end{array}$

— Des identités $(x : \texttt{obj}) \to \Bbbk \to (x \to x)$

— Des lois de composition $(x; y; z : \texttt{obj}) \to (y \to z) \otimes (x \to y) \to (x \to z)$

— Où ces deux dernières familles de flèches sont naturelles en leurs variables.

Dans les catégories $\Bbbk$-linéaires, $\Bbbk - \mathrm{Vect}$ joue le même rôle que les ensembles pour les catégories usuelles. (En fait, on peut considérer la notion générale de catégorie enrichie [nLa23c] [Bé65] et voir que les catégories usuelles sont des catégories enrichies dans Set, à quelques problèmes d'univers près.) On peut réécrire les grandes lignes de la théorie des catégories usuelles dans le langage des catégories $\Bbbk$-linéaires. En particulier [3] :

3. En oubliant les problèmes d'univers que l'on rencontre en chemin

— $\Bbbk - \mathrm{Vect}$ est une catégorie $\Bbbk$-linéarie (de la même manière que Set) ;
— Si $C; D$ sont $\Bbbk$-linéaires, alors $C \Rightarrow D$ (les foncteurs) est $\Bbbk$-linéaire ;
— On réobtient le lemme de Yoneda !

Yoneda Avec C une catégorie $\Bbbk$-linéaire, on peut considérer $\mathrm{Hom} : C^{op} \times C \Rightarrow \Bbbk - \mathrm{Vect}$. Par curryfication, on obtient
— $\mathbb{y} : C \Rightarrow (C^{op} \Rightarrow \Bbbk - \mathrm{Vect})$ immersion de Yoneda dans les préfaisceaux
— $\mathbb{y} : C^{op} \Rightarrow (C \Rightarrow \Bbbk - \mathrm{Vect})$ immersion de Yoneda dans les foncteurs [4]

Le lemme de Yoneda (qui se démontre comme dans le cas usuel, nous omettons la démonstration) est encore valide : les foncteurs $\mathbb{y}$ sont pleinement fidèles. Pour les applications qui viennent, on retiendra :

$$M \cong N \iff \mathbb{y}M \dot{\cong} \mathbb{y}N$$
$$i.e.\ \forall C, M \xrightarrow{A\bullet} C \cong N \xrightarrow{A\bullet} C$$

On va se servir de ce résultat pour étudier la structure des A-modules et rendre utile l'analogie avec les espaces vectoriels.

Compatibilité de Yoneda avec la structure de 2-e.v. On a une structure de 2-e.v. sur ${}_A\mathrm{Mod} \Rightarrow \Bbbk - \mathrm{Vect}$:

$$F \oplus G : \begin{array}{ccc} M & \longmapsto & FM \oplus GM \\ f\downarrow & \longmapsto & \downarrow Ff \oplus Gf \\ N & \longmapsto & FN \oplus GN \end{array} \qquad F \cdot V : \begin{array}{ccc} M & \longmapsto & FM \otimes V \\ f\downarrow & \longmapsto & \downarrow Ff \otimes 1 \\ N & \longmapsto & FN \otimes V \end{array}$$

(Cette structure est un peu parachutée, mais on aurait pu l'obtenir plus systématiquement en poussant l'analogie avec les espaces vectoriels. Moralement, on a catégorifié l'argument par lequel on munit les fonctions linéaires entre deux e.v. d'une structure vectorielle.)

Alors l'immersion de Yoneda $\mathbb{y}$ transporte bien la structure de 2-e.v. :
— $\mathbb{y}M \oplus yN \cong y(M \oplus N)$ par

$$\begin{array}{ccccc} C \longmapsto & (M \to C) \oplus (N \to C) & \longrightarrow & M \oplus N \to C \\ & (f; g) & \longmapsto & (x, y) \mapsto fx + gy \end{array}$$

— $\mathbb{y}M \otimes V^* \cong \mathbb{y}(M \otimes V)$ par

$$\begin{array}{ccccccc} C \longmapsto & (M \to C) \otimes V^* & \longrightarrow & V \to (M \to C) & \longrightarrow & M \otimes V \to C \\ & (f; \varphi) & \longmapsto & v \mapsto x \mapsto f(x)\varphi(v) & \longmapsto & (x; \varphi) \mapsto f(x)\varphi(v) \end{array}$$

4. Nous avons été surpris de découvrir que, dans ce contexte, les théoriciens des catégories préfèrent parler de "copréfaisceaux" pour unifier les nomenclatures, où un "copréfaisceau" est un faisceau contravariant, *i.e.* … un foncteur.

4.2 Décomposition d'un module dans la base des modules irréductibles

Essayons de "deviner" le résultat.

On sait que, dans un espace de Hilbert E muni d'une base orthogonale $(\vec{e}_i)_i$, tout vecteur $\vec{u}$ s'écrit sous la forme suivante :

$$\vec{u} = \sum_i \frac{\langle \vec{u} \mid \overrightarrow{e_i} \rangle}{\langle \overrightarrow{e_i} \mid \overrightarrow{e_i} \rangle} \overrightarrow{e_i}$$

On "devine" la formule suivante (qui ne sera valide que lorsque A sera *semi-simple*) :

$$M \cong \bigoplus_i S_i \otimes \left(M \xrightarrow{A\bullet} S_i \diagup D(S_i) \right)^* \tag{4.1}$$

La formule usuelle sur les espaces vectoriels est claire en dualisant : on considère les duaux $\vec{u}^* \triangleq \vec{v} \mapsto \langle \vec{u} \mid \vec{v} \rangle$, et le résultat apparaît. On "devine" que la démonstration du résultat sur les 2-Hilberts passera par le même procédé. On a alors une bonne surprise : le "dual" d'un A-module correspond exactement à son image par $\mathbb{y}$! On applique donc Yoneda :

$$\begin{aligned}
\mathbb{y}\left(\bigoplus_i S_i \otimes \left(M \xrightarrow{A\bullet} S_i \diagup D(S_i) \right)^* \right) &\cong \bigoplus_i \mathbb{y}\left(S_i \otimes \left(M \xrightarrow{A\bullet} S_i \diagup D(S_i) \right)^* \right) \\
&\cong \bigoplus_i \mathbb{y}S_i \otimes \left(M \xrightarrow{A\bullet} S_i \diagup D(S_i) \right)^{**} \\
&\cong \bigoplus_i \mathbb{y}S_i \otimes \left(M \xrightarrow{A\bullet} S_i \diagup D(S_i) \right) \\
&\cong \bigoplus_i \mathbb{y}S_i \otimes_{D(S_i)} M \xrightarrow{A\bullet} S_i
\end{aligned}$$

où $D(S_i)$ est l'algèbre des endomorphismes de S_i (par le lemme de Schur, c'est une algèbre à division).

On a alors, avec W un A-module fixé :

$$\begin{array}{ccc}
\bigoplus_i \left(S_i \xrightarrow{A\bullet} W \right) \otimes_{D(S_i)} \left(M \xrightarrow{A\bullet} S_i \right) & \longrightarrow & M \xrightarrow{A\bullet} W \\
\sum_i g_i \otimes f_i & \longmapsto & \sum_i g_i \circ f_i
\end{array}$$

— Cette flèche est *injective*

— *Lorsque A est semi-simple*, elle est aussi *surjective*.

Pour pousser encore plus loin la comparaison avec les espaces vectoriels :

— Par le lemme de Schur, $S_i \xrightarrow{A\bullet} S_j \neq 0 \Leftrightarrow i = j$, donc la "base" $(S_i)_i$ est "orthogonale".

— Lorsque $\Bbbk$ est algébriquement clos (ce qui est le cas dans nos applications à $\Bbbk = \overline{\mathbb{F}_p}$), comme $D(S_i) \cong \Bbbk$, cette "base" est même "orthogonale".

4.3 Théorème de structure de Weddeburn

Soit A une $\Bbbk$-algèbre. On note A_{reg} l'algèbre A *vue comme A-module*. On a

$$A \quad \cong \quad A_{\text{reg}} \to A_{\text{reg}}$$

Notons $F_i \triangleq \bigoplus_i S_i \otimes \left(A_{\text{reg}} \xrightarrow{A\bullet} S_i \diagup D(S_i) \right)^*$.

En décomposant A dans la base de ses représentation irréductibles avec 4.1, puis par «2-bilinéarité» de l'opérateur «$\to$», on obtient (de la même manière que l'on aurait développé un produit scalaire par bilinéarite) :

$$\begin{array}{rcl} A & \cong & A_{\text{reg}} \to A_{\text{reg}} \\ & \cong & \displaystyle\bigoplus_i S_i \otimes F_i \quad \longrightarrow \quad \bigoplus_j S_j \otimes F_j \\ & \cong & \oplus_{i,j} (S_i \to S_j) \otimes F_i \otimes F_j \\ & \cong & \oplus_i D(S_i) \otimes F_j \otimes F_j \end{array}$$

où pour passer à la dernière ligne on a sorti les termes qui sont annulés par le lemme de Schur.

Dans le cas où $\forall i, \dim(F_i) < +\infty$, en posant $m_i \triangleq \dim(F_i)$, on obtient alors

$$A \quad \cong \quad \oplus_i \text{Mat}_{m_i}(D(S_i)) \tag{4.2}$$

Cette formule est la formule classique du théorème de structure de Weddeburn.

5 Théorème de Brauer-Nesbitt

On souhaite dénombrer les représentations irréductibles d'un groupe donné. Le théorème de structure de Weddeburn 4.2 montre que toute algèbre est isomorphe à un produit d'algèbres de matrices sur des algèbres à division. L'idée est de compter le nombre de telles sous-algèbres. Pour cela, on a une astuce qui consiste à quotienter par les commutateurs. En effet, dans un algèbre de matrices sur une algèbre à division, les commutateurs sont le noyau de la trace, dont de codimension un. La dimension du quotient de A par $[A;A]$ coïncide donc avec le nombre de représentations irréductibles. On étudie donc :

$$A \diagup \text{Rad}A \diagup [A \diagup \text{Rad}A ; A \diagup \text{Rad}A]$$

On montre :

$$\begin{aligned}
{}^{A}\!/_{\mathrm{Rad}A}\!/_{[{}^{A}\!/_{\mathrm{Rad}A};\,{}^{A}\!/_{\mathrm{Rad}A}]} &= {}^{A}\!/_{\mathrm{Rad}A}\!/_{T\left({}^{A}\!/_{\mathrm{Rad}A}\right)} \\
&= {}^{A}\!/_{\mathrm{Rad}A}\!/_{T(A)}\!/_{\mathrm{Rad}A} \\
&\cong {}^{A}\!/_{T(A)}
\end{aligned}$$

où $T(A) \triangleq \{a \in A \mid \exists n \geq 0, a^{p^n} \in [A;A]\}$.

Lemme 5.1. *Si $a, b \in A$, alors $(a+b)^p \equiv a^p + b^p \ \ [[A;A]]$.*

Démonstration. On écrit $(a+b)^p = \sum_{f \in {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \to \{a;b\}} \prod_{i=0}^{p-1} f(i)$.

On fait agit ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ sur ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \to \{a;b\} : f \bullet k \triangleq t \mapsto f(i+k)$.

On remarque que $f \mapsto \prod_{i=0}^{p-1} f(i)$ passe au quotient sous cette action.

$$\begin{aligned}
\prod_{i=0}^{p-1} f(i+k) &= \prod_{i=0}^{p-k-1} f(i+k) * \prod_{i=p-k}^{p-1} f(i+k) \\
&= \prod_{i=k}^{p-1} f(i) * \prod_{i=0}^{k-1} f(i) \\
&\equiv \prod_{i=0}^{k-1} f(i) * \prod_{i=k}^{p-1} f(i) \quad [[A;A]]
\end{aligned}$$

En sommant sur les orbites :

$$(a+b)^p = \sum_{f : {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \backslash {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \to \{a;b\}} |\mathcal{O}_f| * \prod_{i=1}^{p} f(i)$$

Or ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ est un p-groupe, et on travaille en caractéristique p, donc les seules orbites qui contribuent à cette somme sont les orbites de taille 1, c'est à dire $\overline{i \mapsto a}$ et $\overline{i \mapsto b}$.

Dont $(a+b)^p \equiv a^p + b^p \ \ [[A;A]]$. □

On a en fait démontré que $a \mapsto a^p$ définit un endomorphisme. Cet endomorphisme est l'*endomorphisme de Frobénius*.

On en déduit que $T(A)$ est un $\Bbbk$-s.e.v. de A.

On remarque aussi que $\mathrm{Rad}A \subseteq T(A)$.

Lemme 5.2. *On a :*

$$T(A)\!/_{RadA} = T\left({}^{A}\!/_{RadA}\right)$$

Démonstration. Notons ${}^{\cdot}\!/_{\mathrm{Rad}A} : A \twoheadrightarrow {}^{A}\!/_{\mathrm{Rad}A}$. Montrons qu'elle induit la bijection souhaitée.

— $T(A)/\mathrm{Rad}A \subseteq T(A/\mathrm{Rad}A)$:
Si on a $a \in A$ et $n \geq 0$ tq $a^{p^n} \in [A;A]$, alors $(a/\mathrm{Rad}A)^{p^n} = a^{p^n}/\mathrm{Rad}A \in [A;A]/\mathrm{Rad}A = [A/\mathrm{Rad}A, A/\mathrm{Rad}A]$.
— $T(A/\mathrm{Rad}A) \subseteq T(A)/\mathrm{Rad}A$: Si $(a/\mathrm{Rad}A)^{p^n} \in [A/\mathrm{Rad}A, A/\mathrm{Rad}A] = [A;A]/\mathrm{Rad}A$:
Alors $(a/\mathrm{Rad}A)^{p^n} \in [A;A]/\mathrm{Rad}A$. Donc il existe $c \in \mathrm{Rad}A$ tq $a^{p^n} + c \in [A;A]$.
Par nilpotence de c, il existe $m \geq 0$ tq $c^{p^n} = 0$.
Alors $(a^{p^n} + c)^{p^m} \equiv a^{p^{n+m}} + c^{p^m} = a^{p^{n+m}}$ $[[A;A]]$.
Donc $a^{p^{n+m}} \in [A;A]$. Donc $a \in T(A)$.

□

Maintenant que l'on a déterminé le cas général, on peut réduire au cas des algèbres de groupes.

On va avoir besoin de deux définitions :

Définition 5.3. *Soit p un nombre premier (sous-entendu ici, car on ne le fera pas varier). On note G^r le sous-groupe des éléménts p-réguliers, c'est à dire les éléments d'ordre premier à p. On note G^s le sous-groupe des éléments p-singuliers, c'est à dire les éléments d'ordre une puissance de p.*

Théorème 5.4 (Brauer-Nesbitt)**.** *Soit G un groupe fini. Le nombre de représentations irréductible de G sur $\Bbbk$ un corps algébriquement clos en caractéristique p est égal au nombre de classes de conjugaison de G^r dans G.*

Soit $(x_i)_i$ un système de représentants des classes de conjugaison de G^r dans G, que l'on fixe pour la suite. On commence par deux lemmes :

Lemme 5.5. *Tout élément de G s'écrit $g = st$ où $s \in G^r$ et $t \in G^s$, et $st = ts$.*

Démonstration. On écrit $\omega(g) = ab$ où $a \wedge p = 1$ et b est une puissance de p. Alors il existe $\lambda, \mu \in \mathbb{Z}$ tels que $a\lambda + b\mu = 1$. Alors $g = g^{a\lambda}g^{b\mu} = g^{b\mu}g^{a\lambda}$, et $s = g^{b\mu}$ et $t = g^{a\lambda}$ conviennent. □

Lemme 5.6. *Si $\sum_g \lambda_g g \in [\Bbbk G; \Bbbk G]$, alors la somme des coefficients λ_g s'annule sur chaque classe de conjugaison.*

Démonstration. Tout élément de $[\Bbbk G; \Bbbk G]$ est de la forme $ab - ba$. On a : $ab - ba = a(ba)a^{-1} - ba$. En écrivant $ba = \sum_g \lambda_g g$, et avec $a \in G$, on obtient $ab - ba = \sum_g \lambda_g (aga^{-A} - g)$. Alors comme aga^{-1} et g sont toujours dans la même classe de conjugaison, la somme des coefficients s'annule sur chaque classe de conjugaison. □

On démontre maintenant que $(x_i)_i$ donne bien une famille libre et génératrice.

Démonstration. Montrons que la famille est génératrice. Avec 5.5 $g \in G$, on peut écrire $g = st$ avec s régulier et t singulier, et $st = ts$. On a alors, pour un certain n,

$$\begin{aligned}(st - s)^{p^n} &\equiv s^{p^n} t^{p^n} s^{p^n} [[\Bbbk G, \Bbbk G]] \\ &= s^{p^n} - s^{p^n} = 0\end{aligned}$$

Donc $st \equiv s[T(\Bbbk G)]$. Donc g modulo $T(\Bbbk G)$ est image d'un élément de G^r. Et $\Bbbk G / T(\Bbbk G)$ est commutatif, donc l'image de G^r est bien l'image des x_i.

Montrons que la famille est libre. Il suffit de montrer que $\sum_i \lambda_i x_i \in T(\Bbbk G) \Longrightarrow \forall i, \lambda_i = 0$. Soit donc $\sum_i \lambda_i x_i \in T(\Bbbk G)$. D'après 5.6, la somme des coefficients s'annule sur chaque classe de conjugaison. Or chacun des x_i est seul dans sa classe de conjugaison. Donc $\forall i, \lambda_i = 0$. □

On obtient alors que $\dim \Bbbk G / T(\Bbbk G) = \#\mathrm{Conj}(G^r)$.

On a finalement prouvé le théorème de Brauer-Nesbitt 5.4.

6 Classification des représentations lisses irréductibles de $\mathbf{GL}_2(\mathbb{Z}_p)$

Dans cette partie, nous allons nous intéresser à certaines propriétés de $\mathbb{Q}_p$ et $\mathbb{Z}_p$. Nous allons notamment évoquer la structure de *pro-p-groupe*, et étudier certains quotients. Nous aboutirons finalement à la classifications des représentations lisses irréductibles de $\mathrm{GL}_2(\mathbb{Z}_p)$ sur $\mathbb{E}$ un corps algébriquement clos de caractéristique p.

On commence par donner la définition et quelques exemples de pro-p-groupes.

Définition 6.1 (pro-p-groupe)**.** *Un* groupe profini *est un groupe topologique compact admettant un système fondamental (une base) de voisinages de* 1 *composé de sous-groupes distingués.*

Un groupe profini est de plus appelé pro-p si l'indice de chacun de ces sous-groupes distingués est une puissance de p.

Remarque. On retrouve généralement dans la littérature (voir par exemple Wilson [[Wil98]] chapitre 2) une définition équivalente (on l'admettra) de groupe profini, en termes de limite inverse :

Soit I un ensemble partiellement ordonné, et tel que $\forall x_1, x_2 \in I$, il existe un élément $j \in I$ tel que $x_1 \leq j$ et $x_2 \leq j$.

Un système inverse $(X_i, \varphi_{i,j})$ de groupes topologiques indexé par I est une famille $(X_i)_{i \in I}$ de groupes topologiques et une famille $(\varphi_{i,j} : X_j \to X_i)_{i,j \in I}$ de morphismes continus tels que $\varphi_{i,i} = id_{X_i}$ et $\varphi_{i,j}\varphi_{j,k} = \varphi_{i,k}$ pour tout $i, j, k \in I$.

Une famille $(\psi_i)_{i \in I}$ de morphismes est dite compatible si on a $\varphi_{i,j}\psi_j = \psi_i$ dès que $i \leq j$.

Une limite inverse (X, φ_i) d'un système inverse $(X_i, \varphi_{i,j})$ de groupes topologiques est un groupe topologique X muni d'une famille compatible de morphismes continus $(\varphi_i : X \to X_i)_{i\in I}$ telle que la propriété universelle suivante est respectée :
si Y est un groupe topologique et $(\psi_i : Y \to X_i)$ est une famille compatible de morphismes continus, alors il existe un unique morphisme continu $\psi : Y \to X$ tel que $\varphi_i\psi = \psi_i$.

Le résultat principal, admis ici, est que tout système inverse $(X_i, \varphi_{i,j})$ admet une limite inverse (X, φ_i) unique à isomorphisme près. Elle est notée $\varprojlim(X_i, \varphi_{i,j})$, ou plus simplement $\varprojlim X_i$.
Un exemple classique est $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z}$.

On peut démontrer l'exemple précédent en utilisant notre définition initiale.

Proposition 6.2. *$\mathbb{Z}_p$ est un pro-p-groupe.*

Démonstration. En effet, $\mathbb{Z}_p$ est la boule unité de l'espace complet $\mathbb{Q}_p$. Le groupe topologique $\mathbb{Z}_p$ est donc complet, et de plus les $\{p^k\mathbb{Z}_p \mid k \geq 1\}$ forment une base de voisinage de 0 constitué de sous-groupes normaux.

Comme $\mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z}$, on a $[\mathbb{Z}_p : p^k\mathbb{Z}_p] = p^k$ donc $\mathbb{Z}_p$ est un pro-p-groupe. □

Pour $r \in \mathbb{N}^*$, on note $K(r) = 1 + p^r\mathrm{M}_n(\mathbb{Z}_p)$. Il s'agit de sous-groupes compacts ($\mathbb{Z}_p$ est compact donc par le théorème de Théorème de Tychonov, $\mathrm{M}_n(\mathbb{Z}_p)$ l'est aussi) qui forment une base de voisinage de 1 dans $\mathrm{GL}_n(\mathbb{Z}_p)$. De plus, le noyau du morphisme surjectif $\mathrm{GL}_n(\mathbb{Z}_p) \twoheadrightarrow \mathrm{GL}_n\left(\mathbb{Z}_p/p^r\mathbb{Z}_p\right)$ est exactement $K(r)$, d'où

$$\mathrm{GL}_n(\mathbb{Z}_p)/K(r) \cong \mathrm{GL}_n\left(\mathbb{Z}_p/p^r\mathbb{Z}_p\right) \cong \mathrm{GL}_n\left(\mathbb{Z}/p^r\mathbb{Z}\right) \qquad .$$

Lemme 6.3. *Le groupe $K(1)$ est un pro-p-groupe.*

Démonstration. Par ce qui a été dit précédemment, il vient que $K(1)$ est compact, et possède une base de voisinage de 1. Comme les $K(r)$ sont normaux dans $\mathrm{GL}_n(\mathbb{Z}_p)$, ils le sont aussi dans $K(1) \subset \mathrm{GL}_n(\mathbb{Z}_p)$. Il reste donc à montrer que $[K(1) : K(r)]$ est une puissance de p pour tout $r \geq 2$.
Soit $s > t \geq 2$. Alors on a d'après le troisième théorème d'isomorphisme

$$\frac{\left(\dfrac{K(1)}{K(s)}\right)}{\left(\dfrac{K(t)}{K(s)}\right)} \cong \frac{K(1)}{K(t)} \qquad \text{d'où} \qquad [K(1) : K(s)] = [K(1) : K(t)] \cdot [K(t) : K(s)]$$

donc il suffit de montrer que $[K(r) : K(r+1)]$ est une puissance de p pour tout $r \geq 1$.
Etudions le morphisme

$$\begin{array}{rccc} \varphi & : & K(r)/K(r+1) & \to & \mathrm{M}_n(\mathbb{F}_p) \\ & & 1 + p^r \cdot A & \mapsto & A \quad [p] \end{array} \qquad .$$

Il est surjecif, en effet si on prend $B \in \mathrm{M}_n(\mathbb{F}_p)$ et $\tilde{B}$ la matrice où pour chaque élément de B on a choisit un représentant, alors $\varphi(1 + p^r \cdot \tilde{B}) = B$.
Montrons qu'il est injectif : soit $1+p^r \cdot A$ et $1+p^r \cdot B$ dans $K(r)/K(r+1)$ telles que $A \equiv B \quad [p]$. Il vient que $A - B \equiv 0 \quad [p]$, donc $1 + p^r \cdot (A - B) = 1 + p^{r+1} \cdot C = 0$ pour C dans $\mathrm{GL}_n(\mathbb{Z}_p)$, ce qui conclut.
Finalement, on a $[K(r) : K(r+1)] = |\mathrm{GL}_n(\mathbb{F}_p)| = p^{n^2}$, donc $K(1)$ est bien un pro-p-groupe. □

On va maintenant classifier les $\mathrm{GL}_2(\mathbb{Z}_p)$-représentations lisses et irréductibles sur un corps algébriquement clos de caractéristique p. On commence par démontrer le *lemme des pro-p-groupes*, puis on montrera qu'une $\mathrm{GL}_2(\mathbb{Z}_p)$-représentation lisse irréductible est une $\mathrm{GL}_2(\mathbb{F}_p)$-représentation lisse irréductible. On concluera en prouvant la classification.

Théorème 6.4 (Lemme des p-groupes)**.** *Soit H un pro-p-groupe et π une H-représentation non triviale, en caractéristique p.*
Alors $\pi^H \neq \{0\}$.

Démonstration. On commence par montrer que l'on peut se ramener au cas H fini. Rappelons que π est muni de la topologie discrète.
Pour tout $x \in \pi$, comme π est lisse et H profini, il existe un sous-groupe normal U non-vide, voisinage de 1 et d'indice une puissance de p tel que $x \in \pi^U$. Ainsi H/U est de cardinal une puissance de p, et π^U est une représentation non-triviale de H/U. Donc si on montre que la représentation admet un vecteur invariant $y \in (\pi^U)^{H/U}$, alors $y \in \pi^H$.

On montre maintenant le cas H fini. Remarquons que le $\mathbb{F}_p$ espace vectoriel engendré par $Hx = \{hx | h \in H\}$ est de dimension finie donc fini. On peut donc se restreindre au cas V fini, de cardinal une puissance de p. Comme V est fini on peut le décomposer en union d'orbites pour l'action de H. Par la formule orbite-stabilisateur, toutes les orbites ont pour cardinal une puissance de p. Finalement, en considérant l'égalité $|V| = \sum_{Hx \text{ orbite}} |Hx|$ modulo p, et comme il existe une orbite de taille 1 (l'orbite de $\{0\}$), il existe au moins p orbites de taille 1, i.e $V^H \neq 0$ □

En particulier, tout pro-p groupe admet une unique représentation irréductible, la représentation triviale.
De plus, pour π une $\mathrm{GL}_n(\mathbb{Q}_p)$-représentation lisse, en considérant la restriction à $K(1)$, il vient $\pi^{K(1)} \neq \{0\}$. On en déduit aussi la proposition suivante.

Proposition 6.5. *Il existe une bijection naturelle entre les $\mathrm{GL}_n(\mathbb{F}_p)$-représentations lisses irréductibles et les $\mathrm{GL}_n(\mathbb{Z}_p)$-représentations lisses irréductibles.*

Démonstration. Soit V une $\mathrm{GL}_n(\mathbb{Z}_p)$-représentation lisse et irréductible. Alors $V^{K(1)} \neq \{0\}$, montrons que $V^{K(1)}$ est K-stable. Soit $x \in V^{K(1)}$, $g \in \mathrm{GL}_n(\mathbb{Z}_p)$ et $k \in K(1)$. Alors comme $K(1)$ est normal dans $\mathrm{GL}_n(\mathbb{Z}_p)$, on a $k \cdot (g \cdot x) = (kg) \cdot x = g(g^{-1}kg) \cdot x = g \cdot x$. Donc $V^{K(1)}$ est une sous-représentation de V, et $V^{K(1)} = V$ car $V^{K(1)}$ est non triviale et V est irréductible, donc $K(1)$ agit

trivialement sur V.
On peut ainsi passer au quotient, et on obtient une $\mathrm{GL}_n(\mathbb{Z}_p)/K(1) \cong \mathrm{GL}_n(\mathbb{F}_p)$-représentation. □

Dans la suite, on utilisera le terme *poids* pour qualifier une $\mathrm{GL}_n(\mathbb{Z}_p)$-représentation lisse irréductible, ou de manière équivalente une $\mathrm{GL}_n(\mathbb{F}_p)$-représentation lisse irréductible.

Proposition 6.6. *Toute représentation lisse π de $\mathrm{GL}_n(\mathbb{Q}_p)$ contient un poids, i.e il existe une $\mathrm{GL}_n(\mathbb{F}_p)$-représentation V irréductible qui est une sous-représentation de $\pi\mid_{\mathrm{GL}_n(\mathbb{F}_p)}$.*

Démonstration. Soit $x \in \pi^{K(1)}, x \neq 0$. Alors $\mathrm{GL}_n(\mathbb{Z}_p)\cdot x = \{g\cdot x | g \in \mathrm{GL}_n(\mathbb{Z}_p)\}$ est fini (car $K(1)$ agit trivialement sur x et $\mathrm{GL}_n(\mathbb{Z}_p)/K(1)$ est fini). Donc le $\mathbb{E}$ espace vectoriel engendré par $\mathrm{GL}_n(\mathbb{Z}_p)\cdot x$ est une sous-représentation de $\pi\mid_{\mathrm{GL}_n(\mathbb{Z}_p)}$ de dimension finie, i.e elle admet une sous-représentation irréductible, comme voulu. □

On conclut cette partie par la classification tant attendue.

Théorème 6.7. *Les poids de $\mathrm{GL}_2(\mathbb{F}_p)$ sont les $F(a,b) = Sym^{a-b}\mathbb{E}^2 \otimes det^b$ où $0 \leq a-b \leq p-1$ et $0 \leq b < p-1$, $\mathbb{E}^2$ est la représentation standard $GL_2(\mathbb{F}_p) \hookrightarrow GL_2(\mathbb{E})$ et det est la représentation associée au déterminant.*

Remarque. Nous faisons deux remarques avant d'attaquer la preuve. Premièrement, on peut considérer $b \in \mathbb{N}$ tant qu'on prend $F(a+p-1, b+p-1) \cong F(a,b)$. Secondement, l'action sur $\mathrm{Sym}^d\mathbb{E}^2$ est donnée par $g(v_1 \dots v_d) = (gv_1)\dots(gv_d)$. Plus concrètement, $\mathrm{Sym}^d\mathbb{E}^2 \cong \mathbb{E}[X,Y]_{(d)}$ l'espace des polynômes homogènes de degré d en X et Y. L'isomorphisme envoie la base $\binom{1}{0}^i \binom{0}{1}^{d-i}$ sur la base X^iY^{d-i}, et l'action de la matrice $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ envoie un polynôme homogène de degré d $f(X,Y)$ sur $f(\alpha X + \gamma Y, \beta X + \delta Y)$. On peut maintenant prouver le théorème.

On note $T(\mathbb{F}_p)$ les matrices triangulaires supérieures, et $U(\mathbb{F}_p)$ les matrices unipotentes (*i.e.* telles que $M - \mathrm{Id}$ est nilpotente).

La preuve que nous donnons est, à traduction près, celle de [Her] (proposition 8).

Démonstration. On montre d'abord que les $F(a;b)$ sont irréductibles. Quitte à effectuer un produit tensoriel par une représentation de dimension 1, on suppose $b = 0$. On prouve d'abord que $(\mathrm{Sym}^a\overline{\mathbb{F}}_p)^{U(\mathbb{F}_p)} = \overline{\mathbb{F}}_p \cdot X^a$. Le sens $\supseteq$ est clair. Soit $f \in (\mathrm{Sym}^a\overline{\mathbb{F}}_p)^{U(\mathbb{F}_p)}$. On a, pour tout $u \in \mathbb{F}_p$:

$$\left(\begin{pmatrix}1 & u\\ & 1\end{pmatrix} f\right)(X;Y) = f(X, uX+Y) = f(X;Y)$$

Posons $g(Y) \triangleq f(X;Y) - f(X;0) \in \overline{\mathbb{F}}_p(X)[Y]$. Le degré (en Y) de g est $< p$. Nous avons donc

$$g(-uX) = f(X;-uX) - f(X;0) = 0$$

pour tout $u \in \mathbb{F}_p$, donc g a $p > \deg(g)$ racines distinctes, donc $g = 0$. Donc $f(X;Y) = f(X;0)$, donc f est un monôme en X, donc dans $\overline{\mathbb{F}}_p \cdot X^a$.

Montrons que X^a engendre $\mathrm{Sym}^a(\overline{\mathbb{F}}_p^2)$. Si $u \in \mathbb{F}_p$, alors

$$\begin{pmatrix} 1 & \\ u & 1 \end{pmatrix} X^a = (X+uY)^a = \sum_{i=0}^{a} \binom{a}{i} u^i X^{a-i} Y^i$$

$\mathrm{Sym}^a(\overline{\mathbb{F}}_p^2)$ a pour base $\binom{a}{i}$ où $0 \leq i \leq a$. Considérons les $\begin{pmatrix} 1 & \\ u & 1 \end{pmatrix} X^a$. D'après l'équation ci-dessus, le déterminant de la matrice de passage est un déterminant de Vandermonde, donc non nul, donc les $\begin{pmatrix} 1 & \\ u & 1 \end{pmatrix}$ forment une base de $\mathrm{Sym}^a(\overline{\mathbb{F}}_p^2)$.

Enfin, soit $V \neq 0$ une sous-représentation de $\mathrm{Sym}^a(\overline{\mathbb{F}}_p^2)$. Par le lemme des p-groupes, $V^{U(\mathbb{F}_p)} \neq 0$, donc doit être égal à $\overline{\mathbb{F}}_p \cdot X^a$. Comme ce sous-espace engendre tout $\mathrm{Sym}^a(\overline{\mathbb{F}}_p^2)$, on a $V = \mathrm{Sym}^a(\overline{\mathbb{F}}_p^2)$ et $\mathrm{Sym}^a(\overline{\mathbb{F}}_p^2)$ est irréductible.

Montrons maintenant que les $F(a;b)$ sont distinctes. $T(\mathbb{F}_p)$ est normal dans $U(\mathbb{F}_p)$ et agit donc sur $F(a;b)^{U(\mathbb{F}_p)} = \overline{\mathbb{F}}_p \cdot X^{a-b}$. Calculons cette action :

$$\begin{pmatrix} x & \\ & y \end{pmatrix} X^{a-b} = xX^{a-b}(xy)^b = x^a y^b X^{a-b}$$

c'est à dire que $T(\mathbb{F}_p)$ agit par le caractère $\chi_{a;b} : \mathrm{diag}(x;y) \mapsto x^a y^b$. Si $F(a;b) \cong F(a';b')$, alors on doit avoir $a-b = a'-b'$ d'après les dimensions. On doit aussi avoir $\chi_{a;b} = \chi_{a';b'}$ d'après ce que nous venons de voir, d'où $a \cong a', b \cong b'[p-1]$. D'après les encadrements de b, ceci impose $b = b'$ d'où aussi $a = a'$.

Montrons enfin que la famille des $F(a;b)$ est exhaustive. D'après le théorème de Brauer-Nesbitt, le nombre de représentations irréductibles est égal au nombre de classes de conjugaison d'éléments d'ordre permier à p. En utilisant la réduction de Jordan et le fait que deux matrices sont conjuguées dans $\mathbb{F}_p$ si et seulement si elles sont conjuguées dans $\overline{\mathbb{F}}_p$, on montre que l'on a quatre types de classes de conjugaison :

1. Les éléments du centre $\begin{pmatrix} x & \\ & x \end{pmatrix}$;
2. Les éléments diagonaux non centraux $\begin{pmatrix} x & \\ & y \end{pmatrix}$ où $x \neq y$;
3. Les éléments diagonalisables sur $\mathbb{F}_{p^2}$: $\begin{pmatrix} \alpha & \\ & \alpha \end{pmatrix}$;
4. Les éléments non diagonalisables $\begin{pmatrix} x & 1 \\ & x \end{pmatrix}$.

Les trois premiers sont bien d'ordre premier à p, mais pas le quatrième. Il y a $p-1$ classes de conjugaison dans (1) ; $(p-1)(p-2)/2$ dans (2) ; et $p(p-1)/2$ dans (3). En tout, on obtient $p(p-1)$ classes de conjugaison d'éléments d'ordre premier à p. Ce nombre est bien égal au nombre de paires $(a;b)$ de paramètres de $F(a;b)$. □

Références

[Bae96] John C. Baez. Higher-dimensional algebra ii : 2-hilbert spaces, 1996.

[BBMP12] Christophe Breuil, E Bois-Marie, and Vytautas Pašk¯. Towards a modulo p langlands correspondence for gl2. *Memoirs of the American Mathematical Society*, 1016, 01 2012.

[BL94] Laure Barthel and Ron Livne. Irreducible modular representations of GL_2 of a local field. *Duke Mathematical Journal*, 75:261–292, 1994.

[BL95] Laure Barthel and Ron Livne. Modular representations of gl2 of a local-field : The ordinary, unramified case. *Journal of Number Theory*, 55:1–27, 1995.

[Bre] Christophe Breuil. Representations of galois and of gl2 in characteristic p. `https://www.imo.universite-paris-saclay.fr/~christophe.breuil/PUBLICATIONS/New-York.pdf`.

[Bre03] Christophe Breuil. Sur quelques représentations modulaires et p-adiques de gl2(qp) : I : (on some modular representations and p-adics of. *Compositio Mathematica*, 138(2):165–188, 2003.

[Bé65] Jean Bénabou. Catégories relatives. In *Comptes rendus hebdomadaires de l'Académie des sciences*, volume 260, pages 3824–3827, 1965.

[Her] Florian Herzig. The mod p representation theory of p-adic groups.

[KV94] Mikhail M. Kapranov and Vladimir Voevodsky. 2-categories and zamolodchikov tetrahedra equations. 1994.

[Lan02] Serge Lang. *Algebra*. Springer, New York, NY, 2002.

[Lor18] M. Lorenz. *A Tour of Representation Theory*. Graduate studies in mathematics. American Mathematical Society, 2018.

[nLa23a] nLab authors. 2-Hilbert space. `https://ncatlab.org/nlab/show/2-Hilbert+space`, June 2023. Revision 4.

[nLa23b] nLab authors. 2-vector space. `https://ncatlab.org/nlab/show/2-vector+space`, June 2023. Revision 58.

[nLa23c] nLab authors. enriched category. `https://ncatlab.org/nlab/show/enriched+category`, June 2023. Revision 124.

[Wil98] John S. Wilson. *Profinite groups*. Oxford University Press, 1998.