ÉCOLE POLYTECHNIQUE

INSTITUT POLYTECHNIQUE DE PARIS

CENTRE DE MATHÉMATIQUES LAURENT SCHWARTZ

Journées mathématiques X-UPS

Année 2009

Les représentations linéaires et le grand théorème de Fermat

Corinne BLONDEL

Le groupe $\mathrm{GL}(2)$ **sur le corps des nombres** p**-adiques**

Journées mathématiques X-UPS (2009), p. 89-100.
https://doi.org/10.5802/xups.2009-03

Les Éditions de l'École polytechnique
Route de Saclay
F-91128 PALAISEAU CEDEX
https://www.editions.polytechnique.fr

Centre de mathématiques Laurent Schwartz
CMLS, École polytechnique, CNRS,
Institut polytechnique de Paris
F-91128 PALAISEAU CEDEX
https://portail.polytechnique.edu/cmls/

CENTRE MERSENNE

Publication membre du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org

Journées mathématiques X-UPS
2009, p. 89–100 doi: 10.5802/xups.2009-03

LE GROUPE GL(2) SUR LE CORPS DES NOMBRES p-ADIQUES

par

Corinne Blondel

Table des matières

1. Le corps $\mathbb{Q}_p$ des nombres p-adiques

1.a. Valeur absolue p-adique. Outre la valeur absolue usuelle, archimédienne, que l'on notera ici $|\ |_\infty$, on peut définir sur $\mathbb{Q}$ des valeurs absolues dites ultramétriques, comme suit. Soit p un nombre premier. La *valuation p-adique* $v_p(x)$ d'un entier non nul x est le plus

Publication originelle dans Journées X-UPS 2009. Les représentations linéaires et le grand théorème de Fermat. Éditions de l'École polytechnique, 2009.

grand entier i tel que p^i divise x. Elle s'étend en un homomorphisme de $\mathbb{Q}^\times$ dans $\mathbb{Z}$ en posant pour a et b entiers non nuls : $v_p(a/b) = v_p(a) - v_p(b)$.

Exemples. $v_2(12/5) = 2$, $v_3(12/5) = 1$, $v_5(12/5) = -1$.

Écrivons $x = p^{v_p(x)} \cdot a/b$ et $y = p^{v_p(y)} \cdot c/d$ avec a, b, c, d premiers à p et supposons pour fixer les idées que $v_p(x) \leqslant v_p(y)$. De l'expression

$$x + y = p^{v_p(x)} \, \frac{ad + p^{v_p(y)-v_p(x)}bc}{bd}$$

découle la propriété essentielle de la valeur absolue p-adique :

$$v_p(x+y) \geqslant \min\{v_p(x), v_p(y)\}, \text{ avec égalité si } v_p(x) \neq v_p(y).$$

On obtient la *valeur absolue p-adique* de $\mathbb{Q}$ en posant

$$|x|_p = p^{-v_p(x)} \text{ pour } x \in \mathbb{Q}^\times \quad \text{et } |0|_p = 0.$$

Elle est multiplicative : $|xy|_p = |x|_p|y|_p$, et nulle seulement en 0. C'est une valeur absolue *ultramétrique* : elle vérifie l'inégalité ultramétrique, plus forte que l'inégalité triangulaire $|x+y|_p \leqslant |x|_p + |y|_p$:

$$|x+y|_p \leqslant \max\{|x|_p, |y|_p\}, \text{ avec égalité si } |x|_p \neq |y|_p.$$

Les valeurs absolues p-adiques et la valeur absolue archimédienne sont reliées par l'égalité suivante, valide pour tout nombre rationnel x non nul :

$$|x|_\infty \times \prod_{p \text{ premier}} |x|_p = 1.$$

Par exemple, si $x = 60$, $|60|_\infty \times 2^{-2} \times 3^{-1} \times 5^{-1} = 1$.

1.b. Le corps $\mathbb{Q}_p$ des nombres p-adiques. Qui dit valeur absolue sur un corps dit distance sur ce corps. Le corps $\mathbb{Q}$ est donc muni d'une métrique (ultramétrique) par la valeur absolue p-adique. De même que $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour la valeur absolue $|\ |_\infty$, *le corps $\mathbb{Q}_p$ des nombres p-adiques est le complété de $\mathbb{Q}$ pour la valeur absolue $|\ |_p$.*

Or dans un espace ultramétrique (X, d), une suite (x_n) est de Cauchy si et seulement si $d(x_n, x_{n+1})$ tend vers 0 quand n tend vers $+\infty$. Dans $(\mathbb{Q}, |\ |_p)$ cela signifie que la valuation p-adique de $x_{n+1} - x_n$ tend vers $+\infty$. On obtient ainsi la description de $\mathbb{Q}_p$: tout élément x de $\mathbb{Q}_p$ s'écrit de façon unique sous la forme $x = \sum_{i \in \mathbb{Z}} a_i p^i$

avec $a_i \in \{0, \dots, p-1\}$ et $a_i = 0$ pour i assez petit, disons $i \leqslant i_0$ (dépendant de x). En effet la suite des sommes partielles $\sum_{i_0 \leqslant i \leqslant n} a_i p^i$ est de Cauchy et l'ensemble de ces éléments forme un corps complet auquel la valuation et la valeur absolue p-adiques se prolongent. La valuation et la valeur absolue de x ci-dessus sont

$$v_p(x) = \inf\{i \in \mathbb{Z} \mid a_i \neq 0\}, \qquad |x|_p = p^{-v_p(x)}.$$

On a implicitement prolongé la valuation p-adique à $\mathbb{Q}$ et $\mathbb{Q}_p$ en posant $v_p(0) = +\infty$.

Par construction, $\mathbb{Q}_p$ est complet et $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$ (pour la métrique p-adique).

1.c. Topologie de $\mathbb{Q}_p$. Remarquons pour commencer que l'image de $\mathbb{Q}_p^\times$ par la valeur absolue p-adique est $p^{\mathbb{Z}}$ qui est un sous-groupe discret de $\mathbb{R}^{+\times}$. En conséquence toute boule fermée de rayon strictement positif est ouverte et toute boule ouverte de rayon strictement positif est fermée : l'espace topologique $\mathbb{Q}_p$ est *totalement discontinu* (c'est la définition même, tout point possède une base de voisinages à la fois ouverts et fermés).

À cause de l'inégalité ultramétrique : $|x+y|_p \leqslant \max\{|x|_p, |y|_p\}$, les boules de $\mathbb{Q}_p$ centrées en 0 sont des sous-groupes additifs. La multiplicativité $|xy|_p = |x|_p|y|_p$ nous dit que toute boule de rayon inférieur ou égal à 1 centrée en 0 est stable par multiplication.

Examinons en particulier la boule unité fermée de $\mathbb{Q}_p$:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant 1\}.$$

C'est *l'anneau des entiers p-adiques*, formé des sommes $\sum_{i \geqslant 0} a_i p^i$, $a_i \in \{0, \dots, p-1\}$; en particulier $\mathbb{Z}_p$ est l'adhérence de $\mathbb{Z}$ dans $\mathbb{Q}_p$. La boule unité ouverte est l'idéal maximal $p\,\mathbb{Z}_p$ de $\mathbb{Z}_p$, soit l'ensemble des sommes $\sum_{i \geqslant 1} a_i p^i$, $a_i \in \{0, \dots, p-1\}$. Enfin les boules fermées $p^i\,\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geqslant i\}$, $i \in \mathbb{Z}$, forment un système fondamental de voisinages de 0.

Nous allons montrer que la boule unité $\mathbb{Z}_p$ est compacte. Il en résultera que l'espace topologique $\mathbb{Q}_p$ est *localement compact*.

Montrons donc que toute suite $(b_n)_{n \in \mathbb{N}}$ d'éléments de $\mathbb{Z}_p$ possède un point d'accumulation. La boule unité $\mathbb{Z}_p$ est réunion disjointe de p

classes modulo $p\,\mathbb{Z}_p$. L'une de ces classes, disons $b_{i_1} + p\,\mathbb{Z}_p$, contient une infinité de termes de la suite. Continuons : on peut construire une sous-suite $(b_{i_n})_{n\in\mathbb{N}}$ en choisissant à chaque étape b_{i_j}, $j \geqslant 2$, tel que :

- $b_{i_j} \in b_{i_{j-1}} + p^{j-1}\,\mathbb{Z}_p$;
- $i_j > i_{j-1}$;
- $b_{i_j} + p^j\,\mathbb{Z}_p$ contient une infinité de termes de la suite.

La sous-suite $(b_{i_n})_{n\in\mathbb{N}}$ est une suite de Cauchy : $|b_{i_j} - b_{i_{j-1}}|_p \leqslant p^{-(j-1)}$. Elle converge donc vers un point d'accumulation de la suite initiale.

Compacité locale et totale discontinuité sont des propriétés fondamentales dans l'étude des groupes p-adiques. En particulier, on y rencontre souvent des quotients de groupes compacts par des sous-groupes ouverts ; un tel quotient est discret car quotient par un sous-groupe ouvert, mais compact car quotient d'un groupe compact, or discret et compact entraîne fini.

1.d. L'anneau $\mathbb{Z}_p$ et les caractères de $\mathbb{Q}_p$. Les boules fermées

$$p^i\,\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geqslant i\}$$

pour $i \in \mathbb{N}$ sont évidemment des idéaux de $\mathbb{Z}_p$. Ce sont les seuls. Soit en effet A un idéal non nul de $\mathbb{Z}_p$ et posons $a = \inf\{v_p(x) \mid x \in A\}$; c'est un entier positif ou nul et $A \subseteq p^a\mathbb{Z}_p$. Si $z \in A$ a pour valuation a, alors $v_p(zp^{-a}) = 0$ donc $p^a \in z\,\mathbb{Z}_p$ et $A = p^a\,\mathbb{Z}_p$.

Ainsi $\mathbb{Z}_p$ est principal et possède un unique idéal maximal $p\,\mathbb{Z}_p$. Le quotient $\mathbb{Z}_p/p\mathbb{Z}_p$ est un corps, appelé *corps résiduel* de $\mathbb{Q}_p$ et isomorphe à $\mathbb{Z}/p\mathbb{Z}$: l'homomorphisme

$$\sum_{i\geqslant 0} a_i p^i \longmapsto a_0 \qquad (a_i \in \{0,\dots,p-1\})$$

passe au quotient en un isomorphisme de $\mathbb{Z}_p/p\mathbb{Z}_p$ sur $\mathbb{Z}/p\mathbb{Z}$.

Soit χ un homomorphisme *continu* du groupe additif $\mathbb{Q}_p$ dans $\mathbb{C}^\times$. Son image est réunion des images des sous-groupes additifs $p^i\,\mathbb{Z}_p$ pour $i \in \mathbb{Z}$. Ces sous-groupes sont compacts : leurs images par χ sont des sous-groupes compacts de $\mathbb{C}^\times$, donc contenus dans $\mathbb{U}$, sous-groupe des nombres complexes de module 1.

D'autre part soit $\mathcal{U}$ un voisinage ouvert de 1 dans $\mathbb{C}^\times$ ne contenant pas de sous-groupe non trivial. Son image inverse $\chi^{-1}(\mathcal{U})$ est un ouvert de $\mathbb{Q}_p$: elle contient le sous-groupe $p^i\,\mathbb{Z}_p$ pour i assez grand. Le noyau de χ contient donc un sous-groupe de la forme $p^j\,\mathbb{Z}_p$.

Enfin, les groupes quotients $p^i\,\mathbb{Z}_p/p^j\mathbb{Z}_p$, pour $i \leqslant j$, sont des p-groupes, isomorphes à $\mathbb{Z}/p^{j-i}\,\mathbb{Z}$. Il en résulte que l'image de χ dans $\mathbb{U}$ est contenue dans le sous-groupe des racines de l'unité d'ordre une puissance de p.

On appelle *caractères* de $\mathbb{Q}_p$ les homomorphismes continus du groupe additif $\mathbb{Q}_p$ dans $\mathbb{C}^\times$.

1.e. Le groupe multiplicatif $\mathbb{Q}_p^\times$. Un système fondamental de voisinages de l'unité dans $\mathbb{Q}_p^\times$ est formé des sous-groupes (multiplicatifs) $U_i = 1 + p^i\,\mathbb{Z}_p$, $i \geqslant 1$, qui sont ouverts et compacts. Pour $j \geqslant i \geqslant 1$, les groupes quotients U_i/U_j sont des p-groupes finis.

De plus $\mathbb{Q}_p^\times$ possède un unique sous-groupe ouvert compact maximal, le groupe $U_0 = \mathbb{Z}_p^\times$ des *unités p-adiques*, formé des éléments de valeur absolue 1. (Le seul sous-groupe compact de $\mathbb{R}^{+\times}$ est $\{1\}$!) C'est bien sûr le groupe des éléments de $\mathbb{Z}_p$ qui sont inversibles *dans* $\mathbb{Z}_p$.

Le groupe $U_0/U_1 = \mathbb{Z}_p^\times/(1+p\,\mathbb{Z}_p)$ est cyclique d'ordre $p-1$: il est isomorphe au groupe multiplicatif $(\mathbb{Z}/p\,\mathbb{Z})^\times$. Ses éléments peuvent se relever en $p-1$ racines de l'unité d'ordre $p-1$ dans U_0, par une technique d'approximations successives assez caractéristique.

Nous allons montrer d'abord que tout élément de U_i, pour $i \geqslant 1$, est puissance $(p-1)$-ième d'un élément de U_i. Soit donc $1+x \in 1+p^i\,\mathbb{Z}_p$ et posons $y_0 = x/(p-1)$. Alors

$$(1+y_0)^{p-1} = 1 + (p-1)y_0 + y_0^2\phi$$

est congru à $1+x$ modulo $p^{2i}\,\mathbb{Z}_p$ donc $(1+x)(1+y_0)^{-(p-1)} \in 1+p^{2i}\,\mathbb{Z}_p$. On itère le procédé pour obtenir une suite $1+y_0, \ldots, 1+y_n, \cdots$ vérifiant

- $y_n \in p^{2^n i}\,\mathbb{Z}_p$;
- $(1+x)(1+y_0)^{-(p-1)} \cdots (1+y_n)^{-(p-1)} \in 1 + p^{2^{n+1}i}\,\mathbb{Z}_p$.

La suite $((1+y_0)\cdots(1+y_n))_{n\in\mathbb{N}}$ est de Cauchy et converge vers un élément $1+z$ de U_i tel que $1+x = (1+z)^{p-1}$.

(Remarque : cette démonstration reste valide en remplaçant $p-1$ par un entier premier à p.)

Soit maintenant $\xi \in U_0/U_1$ et $u \in U_0$ d'image ξ dans le quotient. Alors u^{p-1} appartient à U_1 et peut s'écrire $(1+u_1)^{p-1}$, de sorte que $u(1+u_1)^{-1}$ est une racine $(p-1)$-ième de l'unité dans $\mathbb{Q}_p$, qui a pour image ξ dans U_0/U_1.

Notons μ_{p-1} le groupe des racines $(p-1)$-ièmes de l'unité dans $\mathbb{Q}_p$: il est d'ordre $p-1$ et isomorphe à U_0/U_1. On peut aussi écrire de façon unique les éléments de $\mathbb{Q}_p$ sous la forme :

$$x = \sum_{i\in\mathbb{Z}} a_i p^i \text{ avec } a_i \in \mu_{p-1} \cup \{0\} \text{ et } a_i = 0 \text{ pour } i \text{ assez petit.}$$

1.f. Les quasi-caractères de $\mathbb{Q}_p^\times$. Dans l'écriture précédente, remarquons que si x est non nul alors $xp^{-v_p(x)}$ appartient à $\mathbb{Z}_p^\times$: tout élément de $\mathbb{Q}_p^\times$ s'écrit de façon unique sous la forme $x = p^{\,v_p(x)}\,u$ où u est une unité p-adique. Un homomorphisme χ du groupe multiplicatif $\mathbb{Q}_p^\times$ dans $\mathbb{C}^\times$ est donc uniquement déterminé par

- sa restriction à $p^{\mathbb{Z}}$, donnée par $\chi(p^i) = \chi(p)^i$, $i \in \mathbb{Z}$, pour $\chi(p) \in \mathbb{C}^\times$ arbitraire ;
- sa restriction à $\mathbb{Z}_p^\times$.

Nous ne considérerons que des homomorphismes *continus* de $\mathbb{Q}_p^\times$ dans $\mathbb{C}^\times$, que l'on appelle des *quasi-caractères* de $\mathbb{Q}_p^\times$. Or $\mathbb{Z}_p^\times$ est un groupe compact totalement discontinu. Il en résulte d'une part, que l'image de $\mathbb{Z}_p^\times$ par un quasi-caractère est un sous-groupe compact de $\mathbb{C}^\times$, donc contenu dans $\mathbb{U}$, et d'autre part que le noyau d'un quasi-caractère est un sous-groupe *ouvert* de $\mathbb{Q}_p^\times$: c'est le même raisonnement que plus haut, pour les caractères de $\mathbb{Q}_p$.

Dans le prochain exposé, on travaillera en particulier avec des quasi-caractères *non ramifiés* : triviaux sur $\mathbb{Z}_p^\times$ entier ; la donnée d'un tel quasi-caractère équivaut à la donnée d'un nombre complexe non nul. Grâce à la suite exacte

$$1 \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{Q}_p^\times \xrightarrow{|\ |_p} p^{\mathbb{Z}} \longrightarrow 1$$

on peut écrire tout quasi-caractère non ramifié χ sous la forme

$$\chi(x) = |x|_p^\alpha \qquad (x \in \mathbb{Q}_p^\times)$$

pour un $\alpha \in \mathbb{C}$, ce qui revient à écrire $\chi(p) = p^{-\alpha}$.

2. Le groupe $\mathbf{GL(2, \mathbb{Q}_p)}$

2.a. Définition et topologie. L'algèbre $M(2, \mathbb{Q}_p)$ des matrices 2×2 inversibles à coefficients dans $\mathbb{Q}_p$ possède, en tant qu'espace vectoriel de dimension finie sur $\mathbb{Q}_p$, une structure d'espace vectoriel normé (toutes les normes sur $M(2, \mathbb{Q}_p)$ sont équivalentes ; on utilisera dans la suite la norme sup) : c'est un espace métrique localement compact et complet. Le groupe multiplicatif

$$\mathrm{GL}(2, \mathbb{Q}_p) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{Q}_p,\ ad - bc \neq 0 \}$$

des éléments inversibles de $M(2, \mathbb{Q}_p)$ est un ouvert dense de $M(2, \mathbb{Q}_p)$. La topologie induite fait de $\mathrm{GL}(2, \mathbb{Q}_p)$ un groupe topologique localement compact et totalement discontinu.

Pour étudier dans l'exposé suivant les représentations de ce groupe, on aura besoin de certains de ses sous-groupes remarquables, dont certains ont des définitions géométriques naturelles, et des rapports entre ces sous-groupes, en particulier certaines décompositions de $\mathrm{GL}(2, \mathbb{Q}_p)$ les reliant.

Commençons par décrire un système fondamental de voisinages de l'unité constitué de sous-groupes ouverts et compacts ; il s'agit des sous-groupes K_i définis pour i entier strictement positif par :

$$K_i = \{ \left(\begin{smallmatrix} 1+a & b \\ c & 1+d \end{smallmatrix}\right) \mid a, b, c, d \in p^i \, \mathbb{Z}_p \} = I + p^i M(2, \mathbb{Z}_p)$$

autrement dit, K_i est formé des matrices congrues à l'identité modulo $p^i \, \mathbb{Z}_p$. C'est aussi la boule fermée de centre I et rayon $1/p^i$. Tous ces sous-groupes sont contenus dans

$$K = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{Z}_p,\ ad - bc \in \mathbb{Z}_p^\times \} = \mathrm{GL}(2, \mathbb{Z}_p)$$

qui est un sous-groupe ouvert compact de $\mathrm{GL}(2, \mathbb{Q}_p)$ (on verra plus loin qu'il est maximal pour ces propriétés).

2.b. Éléments géométriques. Le fait que $G = \mathrm{GL}(2, \mathbb{Q}_p)$ opère sur l'espace vectoriel $V = \mathbb{Q}_p \times \mathbb{Q}_p$ permet de construire des sous-groupes remarquables comme fixateurs ou stabilisateurs de données relatives à l'espace vectoriel.

- Le centre Z de G, formé des matrices scalaires, est le sous-groupe qui stabilise toutes les droites de V.

• Le stabilisateur d'une droite D de V est un *sous-groupe de Borel* $B(D)$ de G.

• Le sous-groupe de $B(D)$ fixant D point par point et agissant trivialement sur le quotient V/D est le *radical unipotent* de $B(D)$, noté $N(D)$.

• Le stabilisateur de deux droites supplémentaires D et D' de V est un *sous-groupe de Levi* $T(D, D')$ de G.

On notera que $T(D, D')$ normalise $N(D)$ et que $B(D)$ est produit semi-direct de $N(D)$ par $T(D, D')$.

On travaille ici matriciellement, il nous suffira d'utiliser les droites $\left(\begin{smallmatrix}\mathbb{Q}_p\\0\end{smallmatrix}\right)$ et $\left(\begin{smallmatrix}0\\\mathbb{Q}_p\end{smallmatrix}\right)$. On pose donc :

$$\begin{aligned}
N &= \{\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right) \mid b \in \mathbb{Q}_p\} \simeq \mathbb{Q}_p,\\
T &= \{\left(\begin{smallmatrix}a&0\\0&d\end{smallmatrix}\right) \mid a, d \in \mathbb{Q}_p^\times\} \simeq \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times,\\
B &= \{\left(\begin{smallmatrix}a&b\\0&d\end{smallmatrix}\right) \mid a, d \in \mathbb{Q}_p^\times,\ b \in \mathbb{Q}_p\} \simeq T \ltimes N.
\end{aligned}$$

L'élément $w = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ de $\mathrm{GL}(2, \mathbb{Z}_p)$, qui permute les deux droites, joue aussi un rôle important. Remarquons que

$$w\begin{pmatrix}a&0\\0&d\end{pmatrix}w^{-1} = \begin{pmatrix}d&0\\0&a\end{pmatrix} \quad \text{et} \quad w\begin{pmatrix}1&b\\0&1\end{pmatrix}w^{-1} = \begin{pmatrix}1&0\\b&1\end{pmatrix},$$

en particulier wBw^{-1} est le stabilisateur de la droite $\left(\begin{smallmatrix}0\\\mathbb{Q}_p\end{smallmatrix}\right)$, image de $\left(\begin{smallmatrix}\mathbb{Q}_p\\0\end{smallmatrix}\right)$ par w.

Le groupe quotient du normalisateur de T dans G par T, appelé groupe de Weyl, est essentiel dans la théorie des représentations des groupes linéaires et classiques. Il s'identifie ici au groupe à deux éléments $W = \{I, w\}$ engendré par w.

2.c. Décomposition de Bruhat. Utilisons tout de suite le groupe de Weyl W pour la *décomposition de Bruhat* de G. Elle peut s'obtenir par un raisonnement simple d'algèbre linéaire et est valable sur n'importe quel corps.

Soit D la droite $\left(\begin{smallmatrix}\mathbb{Q}_p\\0\end{smallmatrix}\right)$ et $g \in G$. Si g ne stabilise pas D, alors $g(D) = D'$ est une droite supplémentaire de D dans V. Or N opère transitivement sur l'ensemble des droites supplémentaires de D dans V. Il existe donc un élément n de N tel que $n(\left(\begin{smallmatrix}0\\\mathbb{Q}_p\end{smallmatrix}\right)) = g(D)$.

Mais $\left(\begin{smallmatrix}0\\ \mathbb{Q}_p\end{smallmatrix}\right)$ est l'image de D par w. On obtient $nw(D) = g(D)$, ce qui signifie que $w^{-1}n^{-1}g$ appartient à B, soit $g \in NwB$.

Ainsi, *G est réunion disjointe de B et NwB.* Cette propriété est souvent exprimée sous la forme moins précise : $G = BWB$. On peut remarquer que l'écriture d'un élément x de NwB sous la forme nwb avec $n \in N$, $b \in B$, est unique : en effet

$$nwb = n'wb' \Longrightarrow n'^{-1}n = wb'b^{-1}w^{-1} \in N \cap wBw^{-1} = \{1\}.$$

Exemple, avec $b \in \mathbb{Q}_p$, $b \neq 0$:

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1 & b^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & -b^{-1} \end{pmatrix} \begin{pmatrix} 1 & b^{-1} \\ 0 & 1 \end{pmatrix}.$$

C'est une des formules les plus utiles, elle est valide bien entendu sur n'importe quel corps.

2.d. Décomposition d'Iwasawa. C'est une décomposition très utile en théorie des représentations car elle permet d'obtenir des modèles assez simples pour une famille importante de représentations de G, comme nous le verrons dans l'exposé suivant. Pour l'établir, il suffit de montrer que le sous-groupe compact maximal $K = \mathrm{GL}(2, \mathbb{Z}_p)$ opère transitivement sur l'ensemble des droites de V. Montrons qu'en effet toute droite D de V est dans l'orbite de la droite $\left(\begin{smallmatrix}\mathbb{Q}_p\\ 0\end{smallmatrix}\right)$ sous K. Soit $\left(\begin{smallmatrix}a\\ b\end{smallmatrix}\right)$ une base de D.

- Si $v_p(a) > v_p(b)$ l'élément $\left(\begin{smallmatrix}ab^{-1} & 1\\ 1 & 0\end{smallmatrix}\right)$ de K envoie $\left(\begin{smallmatrix}1\\ 0\end{smallmatrix}\right)$ sur $\left(\begin{smallmatrix}ab^{-1}\\ 1\end{smallmatrix}\right)$, autre base de D.
- Si $v_p(a) \leqslant v_p(b)$ l'élément $\left(\begin{smallmatrix}1 & 0\\ ba^{-1} & 1\end{smallmatrix}\right)$ de K envoie $\left(\begin{smallmatrix}1\\ 0\end{smallmatrix}\right)$ sur $\left(\begin{smallmatrix}1\\ ba^{-1}\end{smallmatrix}\right)$, autre base de D.

Ceci fait, on raisonne comme ci-dessus : soit $g \in G$, il existe $k \in K$ tel que $k[g(\left(\begin{smallmatrix}\mathbb{Q}_p\\ 0\end{smallmatrix}\right))] = \left(\begin{smallmatrix}\mathbb{Q}_p\\ 0\end{smallmatrix}\right)$, donc kg appartient à B. C'est la *décomposition d'Iwasawa* : $G = KB$. Il n'y a pas d'unicité dans cette décomposition puisque

$$K \cap B = \{\left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right) \mid a, d \in \mathbb{Z}_p^{\times}, b \in \mathbb{Z}_p\}.$$

Exemple : $\begin{pmatrix} 0 & p \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & p \end{pmatrix}$.

2.e. Décomposition de Cartan. Soit A l'ensemble des matrices de la forme $\left(\begin{smallmatrix} p^a & 0 \\ 0 & p^b \end{smallmatrix}\right)$ avec $a, b \in \mathbb{Z}$ et $a \leqslant b$; c'est un semi-groupe contenu dans T. Alors A *constitue un système de représentants des doubles classes de G modulo K.* C'est la *décomposition de Cartan* : $G = KAK$, qui généralise la décomposition de $\mathbb{Q}_p^\times$ en $p^{\mathbb{Z}}\,\mathbb{Z}_p^\times$. La version condensée $G = KAK$ est moins précise que le premier énoncé car elle ne spécifie pas que les doubles classes d'éléments distincts de A sont distinctes, c'est-à-dire disjointes.

Pour faire encore une démonstration géométrique, il nous faut introduire la notion de $\mathbb{Z}_p$*-réseau.* Un $\mathbb{Z}_p$-réseau de V est un sous-$\mathbb{Z}_p$-module L de V de la forme $L = \mathbb{Z}_p\, u + \mathbb{Z}_p\, v$ où (u, v) est une base de V. Par exemple

$$L_{0,0} = \mathbb{Z}_p \times \mathbb{Z}_p = \mathbb{Z}_p \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbb{Z}_p \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

est un $\mathbb{Z}_p$-réseau de V. Les $\mathbb{Z}_p$-réseaux sont ouverts et compacts dans V. Tout $\mathbb{Z}_p$-réseau est un voisinage de 0 dans V et si L est un $\mathbb{Z}_p$-réseau, l'ensemble des $p^i L$ pour $i \in \mathbb{Z}$ est un système fondamental de voisinages de 0.

Le groupe G opère transitivement sur les bases, donc sur les $\mathbb{Z}_p$-réseaux. Le fixateur du $\mathbb{Z}_p$-réseau $L_{0,0}$ est $K = \mathrm{GL}(2, \mathbb{Z}_p)$ car :

- $\forall u, v \in \mathbb{Z}_p$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) \in \left(\begin{smallmatrix} \mathbb{Z}_p \\ \mathbb{Z}_p \end{smallmatrix}\right)$ entraîne $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M(2, \mathbb{Z}_p)$;
- $\left(\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right), \left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right)\right)$ base de $\left(\begin{smallmatrix} \mathbb{Z}_p \\ \mathbb{Z}_p \end{smallmatrix}\right)$ entraîne $ad - bc \in \mathbb{Z}_p^\times$.

Le quotient G/K s'identifie donc à l'ensemble des $\mathbb{Z}_p$-réseaux de V.

Montrons maintenant que *chaque orbite de K dans l'ensemble des $\mathbb{Z}_p$-réseaux de V contient un et un seul $\mathbb{Z}_p$-réseau de la forme*

$$L_{a,b} = \begin{pmatrix} p^a\,\mathbb{Z}_p \\ p^b\,\mathbb{Z}_p \end{pmatrix} = \begin{pmatrix} p^a & 0 \\ 0 & p^b \end{pmatrix} \begin{pmatrix} \mathbb{Z}_p \\ \mathbb{Z}_p \end{pmatrix} \quad \text{avec } a, b \in \mathbb{Z} \text{ et } a \leqslant b.$$

Soit en effet L un $\mathbb{Z}_p$-réseau de base $\left(\left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} y_1 \\ y_2 \end{smallmatrix}\right)\right)$. On peut supposer, quitte à permuter ces vecteurs, que l'élément de plus petite valuation de $\{x_1, x_2, y_1, y_2\}$ est x_1 ou x_2. En utilisant l'action de $w \in K$ qui échange les deux coordonnées, on se ramène au cas où x_1 est de valuation minimale, puis en faisant agir $\left(\begin{smallmatrix} 1 & 0 \\ -x_2 x_1^{-1} & 1 \end{smallmatrix}\right) \in K$ on obtient un $\mathbb{Z}_p$-réseau de base $\left(\left(\begin{smallmatrix} x_1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} y_1 \\ y_2 \end{smallmatrix}\right)\right)$. Ici y_2 est forcément non nul et

l'hypothèse sur les valuations montre que $(\left(\begin{smallmatrix} x_1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ y_2 \end{smallmatrix}\right))$ est une autre base de ce $\mathbb{Z}_p$-réseau. Enfin, puisque $\mathbb{Q}_p^\times = p^{\mathbb{Z}}\mathbb{Z}_p^\times$, $(\left(\begin{smallmatrix} p^{v_p(x_1)} \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ p^{v_p(y_2)} \end{smallmatrix}\right))$ en est aussi une base.

L'unicité s'obtient en remarquant d'abord que l'application de l'ensemble des $\mathbb{Z}_p$-réseaux dans $\mathbb{Z}$ définie par

$$L \longmapsto a(L) = \inf\{i \in Z \mid p^{-i}L \subset L_{0,0}\}$$

est constante sur les orbites de K. Elle envoie $L_{a,b}$ sur a qui est donc déterminé par l'orbite. Le quotient $L_{0,0}/p^{-a(L)}L$ est fini et l'application à valeurs dans $\mathbb{N}$:

$$L \longmapsto c(L) = \operatorname{card}\left(L_{0,0}/p^{-a(L)}L\right)$$

est elle aussi constante sur les orbites de K, de valeur p^{b-a} en $L_{a,b}$. Ainsi a et b sont entièrement déterminés par l'orbite considérée.

La décomposition de Cartan s'en déduit immédiatement. Soit $g \in G$. Le $\mathbb{Z}_p$-réseau $g(L_{0,0})$ est dans une unique orbite de K, il existe donc une unique paire d'entiers $a, b \in \mathbb{Z}$ avec $a \leqslant b$, et $k \in K$, tels que $g(L_{0,0}) = kLa, b$. Alors $g^{-1}k\left(\begin{smallmatrix} p^a & 0 \\ 0 & p^b \end{smallmatrix}\right)$ fixe $L_{0,0}$ donc appartient à K, c.q.f.d.

2.f. Quelques conséquences. La décomposition d'Iwasawa implique que *l'espace quotient G/B est compact*. C'est en effet l'image du compact K par l'application continue de G dans son quotient G/B, qui est séparé car B est fermé dans G.

On peut déduire soit de la décomposition d'Iwasawa, soit de celle de Cartan, que $\mathrm{GL}(2, \mathbb{Z}_p)$ est un sous-groupe ouvert compact *maximal* de G : il suffit de vérifier qu'aucun élément de B n'appartenant pas à $B \cap K$, ou qu'aucun élément de A distinct de 1, ne peut engendrer un sous-groupe compact. On a même une propriété plus forte : *tout sous-groupe ouvert compact maximal de G est un conjugué de* $\mathrm{GL}(2, \mathbb{Z}_p)$ *par un élément de G.*

Pour le voir, partons d'un sous-groupe ouvert compact maximal H de G et du réseau $L_{0,0}$. Ce réseau est fixé par l'action de $H \cap K$ qui est un sous-groupe ouvert de H. Le quotient $H/H \cap K$ est fini puisqu'il est compact, en tant que quotient d'un espace compact par un sous-espace fermé, et discret, car quotient par un sous-espace ouvert. L'ensemble S des images du réseau $L_{0,0}$ par les éléments de H est

donc un ensemble fini de réseaux et la somme $\Lambda = \sum_{L \in S} L$ de ces réseaux est encore un réseau : c'est un $\mathbb{Z}_p$-module de type fini et il est facile de montrer qu'une partie génératrice minimale de Λ sur $\mathbb{Z}_p$ est nécessairement libre sur $\mathbb{Q}_p$.

Ainsi Λ est un réseau de V, fixé par H par construction. La démonstration du paragraphe précédent montre qu'il existe $g \in G$ tel que $\Lambda = g(L_{0,0})$. Alors le fixateur de Λ est égal à $g\,\mathrm{GL}(2, \mathbb{Z}_p)g^{-1}$ d'où l'assertion.

Pour terminer, repartons de la décomposition de Cartan $G = KAK$. Elle implique que l'ensemble $K\backslash G/K$ des doubles classes de G modulo K est dénombrable. Soit $g \in G$. L'application $k \mapsto kg$ de K dans la double classe KgK passe au quotient en une bijection de $K/K \cap gKg^{-1}$ sur KgK/K. Or $K/K \cap gKg^{-1}$ est un ensemble fini par le raisonnement du paragraphe précédent (K est compact et $K \cap gKg^{-1}$ est à la fois ouvert et fermé). Ainsi chaque double classe KgK est réunion d'un nombre fini de classes modulo K. Finalement, le quotient G/K est dénombrable.

Soit maintenant H un sous-groupe ouvert compact quelconque de G. Les quotients $K/H \cap K$ et $H/H \cap K$ sont finis (toujours le même argument) donc la dénombrabilité de G/K entraîne celle de $G/H \cap K$ puis de G/H. Nous pouvons conclure :

pour tout sous-groupe ouvert compact H de G,
l'espace quotient G/H est dénombrable.

Cette propriété permet en particulier d'obtenir, pour les représentations lisses irréductibles de G, la validité du lemme de Schur, point essentiel, comme nous le verrons dans le prochain exposé.

Références

[Ami75] Y. Amice – *Les nombres p-adiques*, Presses Universitaires de France, Paris, 1975.
[BH06] C. J. Bushnell & G. Henniart – *The local Langlands conjecture for* GL(2), Grundlehren Math. Wissen., vol. 335, Springer-Verlag, Berlin, 2006.
[Ser77] J.-P. Serre – *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1977.

Corinne Blondel, Institut de mathématiques de Jussieu (UMR CNRS 7586), Université Paris-Diderot, 75205 Paris Cedex 13
E-mail : corinne.blondel@imj-prg.fr